Airlock Change Log v5.2.7

Released 17th October 2024

Overview

This is a critical maintenance release fixing a known security issue for customers using SAML authentication (CVE-2024-45409) and delivers important performance improvements including:

Dashboard Performance: The Dashboard has been optimised and has been observed in testing to load between 6 to 25 times faster depending on the dataset being viewed;

Dashboard Loading Indicators: The Dashboard now displays loading status indicators for improved usability;

Allowlists & Blocklists Search: Search functionality has been put in place on the allowlists and blocklists tabs.

Detailed Changes:

1. Server (5.2.7.2415-Green)

Improvements / Fixes

- Dashboard performance has been substantially improved (HAS-6603);
- Add Allowlists & Blocklists UI search functionality (HAS-6619);
- Policy and Blocklist path rules are now sorted in inheritance and ascending order (HAS-6620);
- Fixed an upstream SAML security vulnerability CVE-2024-45409 (HAS-6678);
- Reduced the server recycle schedule from nightly to every three days to avoid dropping cached memory for database queries (HAS-6453);
- Added additional file validation when importing Allowlists / Application Captures (HAS-6568);
- Reduced the verbosity of server side Rails logging (HAS-6579);
- Fixed a temporary high CPU usage issue if execsummary is unable to take an exclusive lock of certain file resources (HAS-6585);
- Fixed an issue where resetting the local user via SSH returned an error message even though the operation was successful (HAS-6586);
- Improved the readability of the Airlock Menu via SSH (HAS-6589);
- Improved the resiliency of file enques for processing, preventing files being written to disk without processing in the event an error occurs during the enqueue process (HAS-6622);
- Fixed Crowdstrike Falcon LogScale form fields appearing missing on v5.2.6 (HAS-6631);
- Fixed an issue where backup tabs and server controls could appear under certain cloud deployment scenarios (HAS-6669).

2. Enforcement Agent Linux (v5.2.7.6427)

Improvements / Fixes

- The CPU core count is now printed to the log file at Linux Agent Startup (HAS-6584);
- Limited the error size written out to log files in standard logging (HAS-6640).

3. Enforcement Agent macOS (v5.2.7.8427)

Improvements / Fixes

- Improved the reliability of the agent during times of heavy system load and slow responsiveness, that previously resulted in an 'Agent Core has stopped' message. This also introduces the requirement for Software Signing core publisher to be trusted in order to exit Safe Mode. (HAS-6621);
- Limited the error size written out to log files in standard logging (HAS-6640);
- Extended handling of .dylib type files to improve handling consistency (HAS-6692).

4. Enforcement Agent Windows (v5.2.7.0)

Improvements / Fixes

- Improved the reliability of self upgrading agents through refactoring agent uninstallation logic, upgrade detection logic and modification of agent unload mechanisms (HAS-6626: HAS-6429, HAS-6615, HAS-6616, HAS-6617, HAS-6624, HAS-6625, HAS-6636, HAS-6672);
- Improved Assembly Reflection Prevention to detect additional file load techniques (HAS-6283);
- Added support for dll files being read as resources rather than directly loaded (HAS-6573);
- Fixed an issue where the agent would fail to control Constrained Language Mode correctly for (x86) interpreters in certain launch scenarios (HAS-6484);
- Additional agent hardening against tampering (HAS-6462);
- Fixed a rare occurrence where catalog digital signatures could fail validation for catalogs that use memberTags (HAS-6595);
- Added operating system detection logic for Windows Server 2025 (HAS-6614);
- Limited the maximum number of events that could be uploaded in a single BulkActivities to prevent backlogged execution queues in poor network connectivity scenarios (HAS-6633);
- Fixed an issue where moving an agent between policy groups with paths and then without paths could cause some trusted path executions to be reported (HAS-6634);
- Fixed a rare fltmc hang during driver unload (HAS-6681);
- Fixed a rare agent crash upon activation of Self Service OTP, while under heavy processing load. This was observed during internal stress testing. (HAS-6676).

Airlock Change Log v5.2.6

Released 15th August 2024

Overview

This is a maintenance release fixing known issues.

Detailed Changes:

1. Server (5.2.6.2324-Green)

Improvements / Fixes

- Limits have been put in place on Search to prevent users from proceeding with searches that return too many results, this ensures system stability when using the search feature (HAS-6454);
- Quotes are now supported in Blocklist command line metarule criteria (HAS-6527);
- Fixed a restriction that prevented allowlists uploaded via an XML or the API to share the same name, even though the version was different (HAS-6516);
- Upgrade underlying application environment (HAS-6434);
- Increased the application container shutdown timeout to improve graceful application restarts (HAS-6532);
- Fixed an issue where the Local User Management table would populate slowly or in some cases fail to populate at all (HAS-6569);
- Fixed an issue where zero width spaces would appear in various places within the product, particularly on the Bulk Add screen (HAS-6518);
- Fixed an authenticated XSS issue (HAS-6517);
- Updated application dependencies (HAS-6493);
- Fixed screen layout issues on the repository page File Packages tab when specific event counts are populated (HAS-6497);
- Fixed a search issue relating to the Grand Parent Process field (HAS-6577);
- Fixed an issue where a colon is still added to Crowdstrike Falcon LogScale URL when no port is provided (HAS-6576);
- Fixed an issue where firewalld was unintentionally set as a service dependency when it is not required (HAS-6512);
- ‘Unmanaged’ clients now have their own audit mode value in the products internal database. This provides more accurate REST API results relating to number of clients in effective audit mode (HAS-6010).

2. Enforcement Agent Linux (v5.2.6.6417)

Improvements / Fixes

- Fixed an issue where if the agent was moved to a policy group with no hashes it would fail to apply Safe Mode, if the previous mode was Enforcement (HAS-6535);

3. Enforcement Agent macOS (v5.2.6.8417)

Improvements / Fixes

- The runtime generalisation command line process ‘airlockcmd discover’ is now permitted when the agent does not have any policy applied yet (HAS-6442);

- Fixed an issue where if the agent was moved to a policy group with no hashes it would fail to apply Safe Mode, if the previous mode was Enforcement (HAS-6535);

4. Enforcement Agent Windows (v5.2.6)

Improvements / Fixes

- Fixed an issue when handling certain special characters for file upload that could cause event uploads to fail (HAS-5628);
- Fixed an issue where if a client re-registers on the server, while an OTP is currently active the revoke OTP button would be stuck greyed out (HAS-6436);
- Fixed an unexpected usermode service termination (HAS-6553);
- Added additional debug logging messages to assist troubleshooting (HAS-6571);

5. Application Capture Agent (v5.2.6)

Improvements / Fixes

- Fixed an issue when handling certain special characters for file upload that could cause the application capture uploads to fail (HAS-5628);

6. Baseline Builder (v5.3.2)

Improvements / Fixes

- Fixed an issue when handling certain special characters for file upload that could cause online baseline uploads to fail (HAS-5628);
- Fixed an issue where the baseline builder could fail to correctly retrieve publisher values (HAS-6565);

7. Relay Agent (v5.2.6)

Improvements / Fixes

- Fixed an exception on startup if the LocalSettings.xml is not valid. If an invalid LocalSettings.xml file is detected, the agent will now recreate it from a stored copy if available (HAS-6558).

Airlock Change Log v5.2.5

Released 30th June 2024

Overview

This is a maintenance release fixing known issues.

NOTE: From v5.2.5 onwards, the Windows Enforcement Agent will no longer be fully tested on Windows Vista / Server 2008 and listed as a supported operating system. This decision has been made to focus our development and quality assurance resources. Currently Airlock Digital is not aware of any installations across our customer base on these platforms. If any customers continue to have a need for Windows Vista / Server 2008 deployments, please contact Airlock Digital support and this decision will be re-evaluated. Please note that Server 2008 R2 remains supported as it is based on the Windows 7 architecture.

Additionally, this release removes support for new installations of Airlock on CentOS based systems as stable branches of the project have now reached End of Life (see https://www.redhat.com/en/topics/linux/centos-linux-eol). Existing installations will continue to function; however, customers are recommended to migrate to a supported Linux distribution. More information can be found in the Airlock v5.2.5 user manual, under section 2.1 Airlock Server.

Detailed Changes:

1. Server (5.2.5.2290-Green)

Improvements / Fixes

- Fixed an issue where exporting the process rules to XML format would not define the type of rule (parent / grandparent) (HAS-6079);
- The server installer now functions on Ubuntu operating systems (please note that server installation is not yet officially supported on this distribution) (HAS-6093);
- Fixed a number of links for CrowdStrike integrated customers (HAS-6295);
- Fixed unable to select publishers containing / characters on the Bulk Add screen (HAS-6307);
- Fixed small event count discrepancies when displaying information on the Dashboard , Bulk Add and Activity Viewer screens when certain filtering options are used (HAS-6344, HAS-6379, HAS-6365);
- Fixed reputation counts when Bulk Add is used from a Search (HAS-6353);
- Reduced the height of the invalid publisher's window to better fit on narrow displays (HAS-6367);
- Added the database index count to the Server Health page (HAS-6376);
- Fixed an error when changing the Show Unique selection to no on the activity viewer screen (HAS-6384);
- Fixed a service failure if the REST API is unable to connect to the external logging source when using TCP Syslog (HAS-6385);
- Upgraded internal application dependencies (HAS-6397, HAS-6406);
- Fixed an issue when file filtering on the Bulk Add screen, which could see the file events return even though filter events is set to on (HAS-6401);
- Fixed an error that could occur when perform database maintenance tasks (HAS-6410);
- Updated an installer check to ensure future server upgrade paths are followed (HAS-6411);

- Bulk Event Sending for Splunk & Crowdstrike Falcon External logging types. The server now sends multiple events in a single HTTP connection reducing the overall volume of request traffic (HAS-6332);
- Fixed an OTP Activate / Deactivate loop in the event the Agents ClientID is not found on the server (HAS-6435);
- Fixed an issue where Bulk Add returned to the top upon performing a bulk add (HAS-6438);
- Fixed an issue where the bulk add screen may not load events when scrolling to the bottom of the page (HAS-6439);
- Server installation scripts have been updated to reflect that CentOS 7.x & 8.x are no longer supported (HAS-6467);
- Fixed an issue where API key generation restrictions could be circumvented by authenticated users (HAS-6475);
- Fixed an issue where the Microsoft recommended block rules 10.1.0.2 would contain empty values for product versions (HAS-6478);
- Fixed an autenticated user impersonation bug which could allow users with the edit_users role (and permission to modify other users) to generate logs which appeared to be from other authenticated users in certain circumstances, please note that this issue was cosmetic and did not allow the inheriting of other user's security permissions. This issue impacted v5.2.2 -> v5.2.4 (HAS-6481).

2. Enforcement Agent Linux (v5.2.5.6413)

Improvements / Fixes

- Added support for full path parent and grandparent process trust (HAS-6326).

3. Enforcement Agent macOS (v5.2.5.8413)

Improvements / Fixes

- Added support for full path parent and grandparent process trust (HAS-6326).

4. Enforcement Agent Windows (v5.2.5.0)

Improvements / Fixes

- Fixed an issue where self-upgrade & downgrade does not function on Windows XP x86 (HAS-6340);
- Clients using Airlock -register will register as a new ClientID, however self-upgrade will cause the old original ClientID to be used, resulting in unpredictable policy assignments, now the client does not use the old clientID (HAS-6352);
- Fixed an issue where OTP's starting with leading zeroes are seen as invalid (HAS-6355);
- Implemented an unclean shutdown detection to assist troubleshooting (HAS-6364);
- Removed official support for Windows Vista & Server 2008. These operating systems still function however are not fully quality assured (HAS-6443).

Airlock Change Log v5.2.4

Released 15th April 2024

Overview

This is a small maintenance release improving scalability and stability.

Known Issue:

- The v5.2.3 Windows Agent has a known issue where the 'Self Upgrading Agents' feature will not successfully upgrade or downgrade the agent. Customers running v5.2.3 (and this specific version only) must upgrade to v5.2.4 or newer versions using the MSI installation method. This is fixed in v5.2.4 under (HAS-6339).

Detailed Changes:

1. Server (5.2.4.2151-Green)

Improvements / Fixes

- Fixed an issue where the Server Health tab on the dashboard could load slowly on large database sizes (HAS-5915);
- Reduced load times on the Activity Viewer through database query optimisation (HAS-6311/6268);
- Updated application dependencies (HAS-6292);
- Fixed an issue where the 15-minute filter would not correctly apply on the Activity Viewer / Bulk Add flow (HAS-6317);
- Added an improved health check support capability to assist in issue diagnosis (HAS-6327);
- Fixed a filtering issue on the bulk add screen where the visual filter checkboxes may not reflect the current view state (HAS-6341).

2. Enforcement Agent Linux (v5.2.4.6404)

- No changes in this build from the previous version.

3. Enforcement Agent macOS (v5.2.4.8404)

- No changes in this build from the previous version.

4. Enforcement Agent Windows (v5.2.4.0)

Improvements / Fixes

- Fixed a deadlock that could only occur in the event that LSASS unexpectedly crashes on Windows (HAS-6312);
- Added additional blocklist safety improvements for blocklist hashes and paths to help prevent impact from misconfigurations (HAS-6330);
- Fixed a cosmetic logging issue regarding errors during relay agent connections (HAS-6335);
- Fixed an issue that prevents self-upgrading impacting the v5.2.3 agent (HAS-6339).

Airlock Change Log v5.2.3

Released 20th March 2024

Overview

This is a maintenance release containing a number of stability and usability fixes.

Detailed Changes:

1. Server (5.2.3.2108-Green)

Improvements / Fixes

- Fixed an issue where process exclusions were not displaying correctly that contained a hyphen character (HAS-6228);
- Fixed the policy tester failing during the return of certain results (HAS-6258);
- Added macOS Sonoma as a reference baseline (HAS-6162);
- Fixed a filter issue on the publisher list which would result in a blank list (HAS-6207);
- Updated licence key removal behaviour in the event of a validation failure (HAS-6208);
- Fixed an issue where the observed IP would be assigned to relay agents in a communication list, rather than it's "local" ip address. This results in agents unable to communicate via the relay agent if DNS was incorrect / unavailable. (HAS-6227);
- Update the Microsoft Recommended Driver Blocklist (HAS-5390);
- Fixed an error when trying to delete some blocklist metarules (HAS-6281).

2. Enforcement Agent Linux (v5.2.3.6403)

Improvements / Fixes

- Fixed parameters passed into 'createbaseline' not being respected (HAS-6164);
- Fixed a certificate error seen when connecting to Airlock Cloud (HAS-6267).

3. Enforcement Agent macOS (v5.2.3.8403)

Improvements / Fixes

- Fixed an issue where parameters passed into the 'createbaseline' feature on airlockcmd would not be respected (HAS-6164).

4. Enforcement Agent Windows (v5.2.3.0)

Improvements / Fixes

- Fixed an issue where the agent was unable to retrieve PowerShell file metadata (including publisher) when the file was run from UNC shares (HAS-5770, HAS-6270);
- Fixed a deadlock during local IP address retrieval, this was seen during boot time at a single customer and impacts v5.2.x agent branch (HAS-6229);
- Fixed a deadlock that was found in testing on Windows XP when the agent was retrieving embedded file signatures during a Windows Update run (HAS-6189);
- Fixed an issue where self-upgrade failing to complete on 32-bit systems (HAS-6185);
- Fixed a BSOD found during proactive stress testing on insider builds of Windows. This has not been seen at a customer site and is unlikely to be seen in the wild (HAS-6147).

Airlock Change Log v5.2.2

Released 6th February 2024

Overview

This is a maintenance release containing a number of stability and usability fixes.

Detailed Changes:

1. Server (5.2.2.2072-Green)

Improvements / Fixes

- Fixed an issue where the scheduled backup time could drift from the configured backup time (HAS-5493);
- Fixed an issue where the policy tester may not change group colors on the repository page (HAS-5665 & HAS-6068);
- Fixed an issue where importing previously exported path, publishers and process rules that contains a comment would fail (HAS-5771);
- Added a UI option to unstick application capture containers (for support use) (HAS-5851);
- Added a "loading" notification when opening policies with large client lists (e.g. greater than 15,000). This is to prevent users clicking on clients still shown on the page from the previously selected policy group (HAS-5951);
- Fixed an error upon renaming administrative users (HAS-5972);
- Added additional information collection into the support scripts to assist with troubleshooting when logs are requested (HAS-5990);
- Fixed an issue where opening a repository page for a file returned via Quick Search could result in a timestamp error (HAS-6029);
- Fixed an issue where PDF report saved searches to be sent via email could fail (HAS-6031);
- Fixed an issue where restoring a backup did not function on RHEL / CentOS 9.x (HAS-6040);
- Fixed an issue on the bulk add screen where ‘select all’ did not respect the reputation filters (HAS-6043);
- Modified some error messages to be more descriptive and assist with troubleshooting (HAS-6052);
- Updated the included Quick Start Guide (HAS-6063);
- Added the ability to add a parent and grandparent process exclusion with the same value (HAS-6064);
- Updated software dependencies (HAS-6077).

2. Enforcement Agent Linux (v5.2.2.6396)

Improvements / Fixes

- Fixed an issue where systems could experience degraded performance when using FANotify Legacy under high event volume (HAS-6067).

3. Enforcement Agent macOS (v5.2.2.8396)

Improvements / Fixes

- No changes in this build from the previous version.

4. Application Capture Agent (v5.2.2.0)

Improvements / Fixes

- Fixed an issue where the application capture agent would fail to install when the /q MSI parameter is used (HAS-6039).

5. Enforcement Agent Windows (v5.2.2.0)

Improvements / Fixes

- Fixed an issue where the agent was unable to retrieve MSI file metadata (including publisher) when the MSI was run from mapped network shares (HAS-5770);
- Fixed a blocklist domain group memory leak which could result in very slow increases in memory usage (HAS-5999);
- Added debug logging to show the user that executed a file (and associated SID matches) and metarule name to assist blocklist metarule troubleshooting (HAS-6033);
- Fixed an issue where files could be seen as ‘Not Signed’ when read or access errors occur. This is rare, however has been seen by some customers during Adobe Acrobat automatic updates (HAS-6048);
- Fixed a rare and intermittent issue where domain group blocklist metarules could fail to match (HAS-6049);
- Fixed an issue in Notifier where constrained executions could incorrectly say "Blocklist - Constrained" in certain handling conditions. This did not impact the handling of the constrained mode and the files are correctly processed. (HAS-6078);
- Improved Constrained Language Mode to handle responses for non-standard PowerShell installations (HAS-6107);
- Added additional blocklist safety improvements to better handle scenarios where empty metarule criteria values have been provided (HAS-6122);
- Metarule ID’s and names are now included in debug logging (HAS-6115).

6. Baseline Builder (v5.2.2.0)

Improvements / Fixes

- Improved file publisher handling (HAS-6135).

Airlock Change Log v5.2.1

Released 14th November 2023

Overview

This is a maintenance release containing policy generation improvements and bugfixes.

Detailed Changes:

1. Server (5.2.1.1981-Green)

Improvements / Fixes

- Improved the Client Auto Upgrade feature to include additional logging and alerting when moving clients between policy groups (HAS-5618, HAS-5855);
- Improved server database generation and handling of client connections, helping to reduce the number of agent integrity check failures (HAS-5788, HAS-5842, HAS-5848, HAS-5854, HAS-5859, HAS-5888);
- Fixed an issue where the theme selection (dark mode / colourblind mode) would not persist through SAML login sessions (HAS-5670);
- Fixed an issue where SAML logins would occasionally fail (HAS-5797);
- DiscoveryID’s are now shown in the Group Settings panel (HAS-5685);
- The Operating System filter in the Add Publisher window is now linked with the search functionality (HAS-5673);
- Improved database re-indexing performance and efficiency (HAS-5759, HAS-5766)
- Updated application dependencies (HAS-5676, HAS-5697);
- If an application capture is approved on policy via its top-level category, the subcategory containing the app capture, and also the individual capture, is able to be deleted via app captures page without a prompt that it is in use (HAS-5710);
- Fixed an issue where the Bulk Add ‘Select All’ option only selects files to where the user has scrolled, this update now selects unrendered files (HAS-5686);
- Fixed an issue where exporting clients to CSV/XML would only include the first page of results, even when the ‘all clients’ checkbox was selected (HAS-5681);
- Fixed an issue where the activity viewer screen was sorted out of order (HAS-5698);
- Fixed an issue where adding publishers to multiple policy groups could fail if the publisher(s) already exist in the first policy group (HAS-5700);
- The internal web server version is now hidden in application responses (HAS-5704);
- Fixed an issue when moving a child application capture from an approved category to a non-approved category in policy caused an integrity check fail on the next agent policy update (HAS-5707);
- Added a source IP address to the SAML Login Server Activity History event (HAS-5712);
- Fixed an error that could be shown in the policy tester on the repository page when evaluating policy (HAS-5731);
- Adding a publisher via bulk-add to policy, does not actually "remove" the publisher from the list in Filter mode (HAS-5751);
- Fixed an issue where policy was unable to be modified unless the user had the view_agentstopcode security permission (which should not be required) (HAS-5753);
- Fixed an issue where the user is able to "partially" delete a metarule, if between pressing confirmation to delete, and check metarule exists, server connection is lost (HAS-5756);
- Fixed an issue where if the dashboard has a very high volume of events (multiple millions), aggregation could fail due to memory limitations resulting in a zero-event count being displayed (HAS-5772);

- Fixed a search issue where if First Seen is selected as an output column the search would fail to return results (HAS-5789);
- Improved blocklist metadata handling to prevent blocks in scenarios where the criteria value may be empty (HAS-5798);
- Fixed an issue where if the Bulk Add screen file selection includes hashes that do not exist in a repository entry, the process would fail (HAS-5837);
- Fixed an issue where the 'Hash' column on the activity viewer was unable to be expanded (HAS-5841);
- Fixed an issue where the Add Criteria blocklist button would be disabled if the first rule added contained 5 blocklist criteria (HAS-5845);
- Fixed an issue when adding multiple hashes via the REST API /hash/add endpoint would fail if one of the hashes already exists in the server (HAS-5890);
- Pressing the back button on Bulk Add from search results redirected to the OTP function incorrectly (HAS-5944);
- Fixed an issue where moving a disabled Application Capture package to a category that is enabled on policy did not generate a policy database update (HAS-5895).

2. Enforcement Agent Linux (v5.2.1.6352)

Improvements / Fixes

- Fixed an issue where Blocklist Path rules containing wildcard values at the end of the path, may not match if a file is executed from the immediate folder that the wildcard covers (HAS-5532);
- Fixed an issue where updating the Linux Agent from v5.1.x series to v5.2 would fail with the error 'unable to add to activity db' in the logs (HAS-5839);
- Implemented automatic UUID generation upon agent discovery when using the -discover command if no optional UUID is specified (HAS-5705).

3. Enforcement Agent MacOS (v5.2.1.8352)

Improvements / Fixes

- Fixed an issue where Blocklist Path rules containing wildcard values at the end of the path, may not match if a file is executed from the immediate folder that the wildcard covers (HAS-5532);
- Fixed an issue where the filename column display within notifier overlaps with file path on macOS Sonoma (HAS-5682);
- Implemented automatic UUID generation upon agent discovery when using the -discover command if no optional UUID is specified (HAS-5705);
- Fixed an issue where if a communication list is set, not in balanced mode, and there are >0 relay agents in the list it could result in an unhandled exception (HAS-5760);
- Added a check when creating the filelog table for the first time to prevent a crash (HAS-5865);
- Fixed a log entry where blocked executions would be labelled as an untrusted executions in certain log lines, this issue was cosmetic only (HAS-5867).

4. Application Capture Agent (v5.2.0.0)

Improvements / Fixes

- Fixed an issue where the Application Capture Agent would skip capturing a particular file if the files certificate table had an invalid length (HAS-5585).

5. Enforcement Agent Windows (v5.2.1.0)

Improvements / Fixes

- Fixed an issue where communication threads could hang when installed alongside an F5 Endpoint Inspector agent (HAS-5671);
- Fixed an issue where MSI & Powershell files may not have their publisher retrieved in edge case timing scenarios when Blocklist Metadata rules were active within policy (HAS-5678);
- Fixed an agent crash when parsing a specifically crafted and corrupted file. Special thanks to Gauthier Vidal and Jérémy Arab from Wavestone for the report (HAS-5917);
- Implemented automatic UUID generation upon agent discovery when using the -discover command if no optional UUID is specified (HAS-5705);
- Fixed a typo in the Windows Agent log message to correctly reference ‘discover’ instead of ‘register’ when the client is in sys-prep mode (HAS-5706);
- Fixed an agent crash when the no-check registry entry is specified and discover is called via a powershell command (HAS-5720);
- Pressing the "Cancel" button on notifier OTP activation, followed by subsequent attempt to use OTP Mode button, results in disabled OTP Mode button until agent restart (HAS-5730);
- Fixed an issue where Powershell could terminate unexpectedly when Constrained Language Mode is enabled in policy and there is a Microsoft AppLocker policy also applied to the system (HAS-5745);
- If an agent is installed in no-check (sys-prep) mode, the client will loop ‘discovery’ of the server if there is no network connectivity. This contributed to log bloat but also didn’t show that the agent was in a sys-prep state (HAS-5750);
- Fixed an issue where the agent is unable to be installed alongside the CrowdStrike Falcon sensor (HAS-5754);
- Fixed a BSOD that could occur on Windows XP & Windows Server 2003 when installed alongside Paolo Alto Endpoint products (HAS-5780);
- Fixed a rare interoperability deadlock that could occur when user credential stores are handled by LSASS during agent startup (HAS-5783);
- Fixed an issue where if UUID mode was enabled and SysPrep ‘no-check’ was also implemented, the agent would incorrectly ignore ‘no-check’ (HAS-5796);
- Improved blocklist metadata handling to prevent blocks in scenarios where the criteria value may be empty (HAS-5798);
- Fixed an issue where the Enforcement Agent was unable to be installed on Windows XP, Windows Server 2003 & Windows Server 2008 (HAS-5838).

6. Relay Agent (v5.2.1.0)

Improvements / Fixes

- Fixed an OTP loop that could occur on an Enforcement Agent communicating via a relay agent (HAS-5733);
- Improved relay database processing and handling of client connections, helping to reduce the number of client integrity check failures (HAS-5788);
- Improved the relay agent’s database integrity checking to prevent repeated policy updates (HAS-5832 HAS-5842, HAS-5848, HAS-5854, HAS-5859, HAS-5888).

Airlock Change Log v5.2

Released 31st August 2023

Overview

Airlock Digital v5.2 introduces a number of highly requested features, improves usability and provides customers with greater management flexibility.

- **Client Self Upgrade:** Agents now have the ability to be upgraded/downgraded from the Airlock console to newer versions. This initial feature supports a 'target' agent version on a per policy basis. Automatic 'current' and 'N-1' update methods will be added in forthcoming minor releases. Please note you must be running a v5.2 agent or greater first, before agents will be able to self-upgrade;
- **Grandparent process trust:** Customers can now allow file executions by their Grandparent process. This is particularly useful for development scenarios where applications such as development IDE's can be trusted and allowed to more freely load untrusted files;
- **Pre-Computed Dashboard Loading:** Data displayed on the dashboard is now data warehoused and pre-computed resulting in significantly faster dashboard load times for large event volumes;
- **Dark Mode & Colourblind Mode:** The server now supports additional display modes to improve accessibility;
- **Per-Script PowerShell Constrained Language Mode (CLM):** CLM enables PowerShell to operate with reduced functionality, preventing malicious activity. Airlock now has the capability to change PowerShell's Language Mode on a per-script basis. Untrusted scripts can run in CLM while trusted scripts run in Full Language Mode. This allows any user to utilise basic functionality of PowerShell in a risk managed way, without requiring scripts to be trusted by Airlock;
- **To Be Signed (TBS) Hash Blocklisting:** The Windows Agent now supports blocklisting TBS hashes. These hash values allow users to identify and block specific code signing certificates regardless of the file they are attached to. This is particularly useful for preventing the execution of files that have been signed by stolen / leaked certificates.
- **Agent runtime generalisation & Improved SysPrep:** Agents now support a mode where they can be 'reset' or 'generalised' at runtime and return to a fresh installation. This is useful for cloud environments where machines may be automatically cloned. SysPrep mode is now supported on Linux & macOS and optionally allows for clients to be held in a dormant state until the generalisation command is called.

Upgrade Notes:

- Client compatibility is unchanged from the previous release.
- Upgrading to v5.2 of the Airlock Server is only supported from v5.1.x. If the Airlock Server being upgraded is on an earlier release, you must first upgrade to v5.1.x before upgrading the server to v5.2.

Known Issues:

- Uploading 'additional agents' for the self-updating feature using the Safari Browser does not currently function, a workaround is to upload the agent using Chromium or Firefox browsers.

Detailed Changes:

1. Server (5.2.0.1855-Green)

New Features

- Dark Mode (HAS-1321);
- Client Self Upgrade support (HAS-5054, HAS-5368);
- TBS Hash Blocklisting (HAS-4998);
- SHA-256 Hashes & Hostname is now available as a blocklist metadata criteria (HAS-5006, HAS-5017);
- Grandparent Process Support (HAS-5014);
- Baseline, Applications & Blocklists now have a Summary ribbon showing where groups have been applied (HAS-5027);
- Per-Script Constrained Language Mode Support (HAS-5331);
- Logging support for CrowdStrike Falcon LogScale (HAS-5643).

Improvements / Fixes

- Dependency and Platform Upgrades (HAS-4945, HAS-4946, HAS-5233, HAS-5234, HAS-5524);
- Improve Bulk Add screen loading performance and reduce browser memory usage (HAS-4980);
- The status column is now filterable on the OTP screen (HAS-5007);
- The columns are now sortable on the OTP, User Management & Activity Viewer Screens (HAS-5008, HAS-5009, HAS-5015);
- Fixed an issue where revoking or deleting an OTP code returned to page one (HAS-5010);
- Fixed an issue where deleting an application capture category that contains captures did not correctly remove capture files from the server, causing a failed job and potential invalid database differentials (HAS-5658);
- Added ‘otpid’ in the /v1/otp/usage REST API endpoint (HAS-5011);
- Prevented the ‘enter 2-step verification code’ from being pre filled by password managers (HAS-5012);
- Added SAML copy/paste functionality to the SAML configuration page (HAS-5016);
- The user listing now shows the users 2-step enrolment status (HAS-5020);
- API Authentications are now logged in the Server Activity History for improved security auditing of API Key usage (HAS-5021);
- Nineteen new Server Activity History logs have been added to log modifications of settings in the product (HAS-5022, HAS-5601);
- The Publisher Listing can now be filtered by Operating System (HAS-5024);
- Fixed an issue where the Group Name & IP Addresses would be left out of the CSV / XML export on the policies page (HAS-5025);
- Added a User Based DN to the LDAP Configuration to resolve lookup performance issues in large environments (HAS-5026);
- User listing on the Settings tab can now be exported to CSV & XML (HAS-5005);
- The Bulk Add screen now allows files to be added to multiple application captures & publishers to be added to multiple policy groups in a single addition (HAS-5028);
- Local IP & External IP addresses of clients are now added to a file’s execution history, which can help determine what network location a client was in when a block event occurred (HAS-5029);
- Added the ability to set the number of workers outside of the application, that persists through upgrades (HAS-5525);

- Improved the performance of database maintenance and reindexing, particularly when there are duplicate events in the database (HAS-5030);
- Substantially improved Dashboard loading times through pre-computed Dashboard loading (HAS-5121);
- General UI visual improvements (HAS-5346);
- Pie Chart Link (text) is now clickable on the dashboard (HAS-5449);
- UI Icons are now consistent across Baseline, Application & Blocklist screens (HAS-5452);
- Fixed an issue where reindexing would exit with a rake error when called manually (HAS-5468);
- Fixed an issue where LDAPS would fail to connect to private SSL secured LDAP (HAS-5490);
- Improved the support collection scripts to gather additional contextual information when customers supply support bundles (HAS-5537);
- Fixed an issue where the Blocklist page could load slowly when a large number of domain security groups have been imported. This was fixed by adding two additional database indexes (HAS-5542);
- Updated the EULA (HAS-5565);
- For cloud customers added an upgrade preference, which can be specified to inform Airlock engineers as to the customers desired version / upgrade target (HAS-5574);
- Increased the size of the Move Clients modal & Bulk Add modals for improved usability (HAS-5589);
- Added the Database Execution History Count to the Server Health page (HAS-5603);
- Fixed an issue where RHEL baselines would import with the name CentOS instead of RHEL (HAS-5606);
- Fixed an issue where usernames could be intentionally renamed to strings that were unable to be used on the login page, resulting in an account lockout (HAS-5648);
- Prevent blank stop codes from being entered (HAS-5358);
- Improved the support tasks page (HAS-5560);
- Backup configurations are now hidden from cloud hosted instances (HAS-5573);
- Added RHEL 8.8 & 9.2 Baselines (HAS-5624);
- Updated the reputation threat definitions to reflect the updated VirusTotal integration (HAS-5297);
- Fixed an issue where multi select on the bulk add screen was not functional (HAS-5291).

2. Enforcement Agent Linux & macOS (v5.2.0.6338/8338)

New Features

- macOS agents now support blocking dynamic libraries (dylib) (HAS-4015);
- Support Self Upgrade Capability (HAS-5314);
- SHA-256 Hashes & Hostname is now supported as a blocklist metadata criteria (HAS-5006, HAS-5017);
- Agent runtime generalisation and improved SysPrep support (HAS-5437, HAS-5473);
- Grandparent Process Support (HAS-5014);

Improvements / Fixes

- Removed kernel drivers for CentOS / RHEL 7.x & 8.x systems. This was done as driverless performance is now comparable to driver mode. This change simplifies agent operation and can be rolled back on a case-by-case basis if desired through the v5.2 branch. CentOS / RHEL 6.x will continue to have driver support (HAS-5669);

- Fixed an issue where the proxy server display on airlockcmd status did not reflect the policies disabled status which could cause user confusion (HAS-4520);
- Added a customisable log location so agent logs can be written to a user-controlled location (HAS-5577);
- Added a timeout for the stop code prompt after 100 seconds to prevent stuck non interactive installs (HAS-5538);
- Fixed an issue where agents could take up to 15 minutes to re-establish connectivity via a relay agent after a client restart, when no direct connectivity to the main server was available (HAS-5636).

3. Enforcement Agent Windows (v5.2.0.0)

New Features

- TBS Hash Blocklisting (HAS-4998);
- Support Self Upgrade Capability (HAS-5054);
- Constrained Language Mode support (HAS-5331);
- SHA-256 Hashes & Hostname is now supported as a blocklist metadata criteria (HAS-5006, HAS-5017);
- Agent runtime generalisation and improved SysPrep support (HAS-5473);
- Grandparent Process Support (HAS-5014);

Improvements / Fixes

- Fixed an issue where Metadata rules with multiple Domain Groups (OR) were not adhered to (HAS-5659);
- DiscoveryID is now supported as a MSI parameter (HAS-5019);
- Reduced noise from client block notifications, by supressing popups when multiple blocks occur in a short period of time by implementing a ‘cooldown’ period (HAS-5038);
- Added the ability for Windows to register using UUID’s. This allows for multiple Windows machines with the same hostname to be registered on the same Airlock server, without causing duplicate registrations (HAS-5460);
- Blocklist match messages are now buffered to only log on full blocklist matches, this reduces log file size and improves readability (HAS-5222);
- Fixed an issue where usernames may not always be accurate on Multi-User systems when activating an OTP. In certain cases, OTP’s could previously be attributed to ‘other’ users also logged into the same system (HAS-5264);
- The agent ‘User Agent String’ has been updated to reflect a more modern browser to prevent issues with some corporate Proxy’s (HAS-5396);
- Safe Mode improvements have been made to handle edge case blank database conditions (HAS-5036);
- TLS Ciphers have been further restricted to only negotiate with TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 for further security (HAS-4620).

4. Relay Agent (5.2.0.0)

New Features

- Self-updating agents support (HAS-5368);
- Local IP & External IP client address support (HAS-5029)

Airlock Change Log v5.1.6

Released 4th July 2023

Overview

This is a maintenance release. The Windows Agent now includes blocklist metadata script support and macOS CPU utilisation has been significantly improved. Additionally, bugfixes are included across all agents, with a minor server fix.

Detailed Changes:

1. Server (5.1.6.1621-Leonard)

Improvements / Fixes

- Fixed an issue where the Trusted Execution Activity Uploading restriction could apply in groups that have less than 50 clients (HAS-5510).

2. Enforcement Agent Linux (v5.1.6.6295)

Improvements / Fixes

- Implemented database size reduction to prevent large filelog.db files on disk after significant (tens of millions) event volume (HAS-5516);
- Added RPC failure messages on standard logging to assist troubleshooting (HAS-5515);
- Fixed an issue where the agent would fail to start if an IPv6 bind is attempted and the system doesn't support IPv6. The agent will now fall back to IPv4 binding (HAS-5523).

3. Enforcement Agent macOS (v5.1.6.8295)

Improvements / Fixes

- Significantly reduced CPU utilisation of the macOS agent by 75% in typical usage scenarios through improved event handling (HAS-5506, HAS-5509);
- Added handling for an issue in the Apple ESFramework where platform binaries could be seen as Not Signed when applying macOS updates and security patches (HAS-5506);
- Implemented database size reduction to prevent large filelog.db files on disk after significant (tens of millions) event volume (HAS-5516);
- Added RPC failure messages on standard logging to assist troubleshooting (HAS-5515);
- Removed 'eventch nil' logging when the agent is sleeping on mac (HAS-5521);
- Fixed an issue where the agent would fail to start if an IPv6 bind is attempted and the system doesn't support IPv6. The agent will now fall back to IPv4 binding (HAS-5523).

4. Enforcement Agent Windows (v5.1.7)

Improvements / Fixes

- Blocklist metadata rule matching now supports script file types (HAS-5428);
- Fixed a BSOD that could occur on the v5.1.6 agent on Windows 11 when a file request is made from kernel mode without a file object (HAS-5500).

Airlock Change Log v5.1.5

Released 27th June 2023

Overview

This is a maintenance release containing agent and server bugfixes.

Detailed Changes:

1. Server (5.1.5.1596-Leonard)

Improvements / Fixes

- Added Windows Integrity Level Rules to Blocklisting Domain Security Groups (HAS-5429);
- Fixed an issue where 'Export Clients List' to CSV did not include Group Names & IP Addresses (HAS-5400);
- Removed a restriction for server upgrade in Unattended mode using the unattended installation file (HAS-4899);
- Fixed an issue when leaving a comment on a file repository page while logged in via an LDAP user would cause an HTTP 500 error (HAS-5427);
- Updated repository to reflect VirusTotal reputation provider change (HAS-5297).

2. Enforcement Agent Linux (v5.1.5.6274)

Improvements / Fixes

- Fixed an issue where file descriptors were not aggressively cleaned up during heavy load, which could result in more file descriptors open than required (HAS-5409);
- Increased the open file descriptor limit to help prevent a 'too many open files' error (HAS-5431);
- Substantially reduced CPU utilisation when processing trusted files (by hash value) under heavy load. *NOTE: v5.1.5.6271 has been replaced as an issue was identified where FILE CHECK's could be seen/logged under non-debug conditions* (HAS-5475).

3. Enforcement Agent macOS (v5.1.5.8274)

Improvements / Fixes

- Fixed an issue where the MacOS Agent preferences tab did not always update the System Preferences status (HAS-5392);
- Fixed an issue where parent process trust could be missed due to rule capitalisation, the process trust match is now case insensitive (HAS-5474);
- Substantially reduced CPU utilisation when processing trusted files (by hash value) under heavy load. *NOTE: v5.1.5.6271 has been replaced as an issue was identified where FILE CHECK's could be seen/logged under non-debug conditions* (HAS-5475).

4. Enforcement Agent Windows (v5.1.6)

Improvements / Fixes

- Added BypassIO support in Windows 11 to improve performance for more information about BypassIO, please see https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/bypassio (HAS-5415);
- Fixed a rare interoperability deadlock that could occur when user credential stores are handled by LSASS (HAS-5414);
- Fixed an issue where notifier -revokeotp cmdline does not function on Windows 7 (HAS-5382);
- Fixed rare issue where subsequent executions of the same file may not be uploaded under high load (HAS-5445, HAS-5448);
- Fixed an issue where using right click 'Uninstall' on the Windows MSI would require a reboot to remove the driver (HAS-5387);
- Added interoperability detection for Carbon Black Enterprise EDR (HAS-5451).

5. Relay Agent (v5.1.4)

Improvements / Fixes

- The Relay Agent now uses a x64 architecture (HAS-5413);
- Optimised the memory utilisation of the Relay Agent when under heavy load (greater than 20,000 clients online) (HAS-5413);
- Removed legacy functions to cleanup logging (HAS-5371).

Airlock Change Log v5.1.4

Released 26th May 2023

Overview

This is a maintenance release containing agent and server bugfixes.

NOTE: There is a known issue in Microsoft Windows 11 22H2 where applications may display duplicate popup notifications. This is not a bug in the Airlock Enforcement Agent, for further information please see the following KB article: https://support.airlockdigital.com/support/solutions/articles/9000227812-duplicate-popup-notifications-windows-11

Detailed Changes:

1. Server (5.1.4.1546-Leonard)

Improvements / Fixes

- Updated the label on the new files table to received time which is correct (HAS-5196);
- Fixed an issue where if a new policy group was created by a user with in one user group, users in other user groups were not always able to see the new policy group, unless user group permissions were re-rolled (HAS-5300);
- Fixed an issue where in some policy inheritance scenarios where bulk_add could fail causing a stuck application capture (HAS-5301);
- Added a UI warning when saving a user group that contains no permissions (HAS-5305);
- Prevented the clicking of ‘next’ and ‘last’ buttons if you are already on the last page in the activity viewer (HAS-5306);
- Fixed some UI alignments and other small UI tweaks (HAS-5321, HAS-5324);
- Added missing checkboxes on the reputation filters when using the OTP Bulk Add workflow (HAS-5348).

2. Enforcement Agent Linux (v5.1.4.6246)

Improvements / Fixes

- Fixed a deadlock that could occur during the handling of Dracut subsystem executions. This deadlock is most commonly encountered during a kernel upgrade (HAS-5344);
- Fixed a reporting issue where if the agent was in Audit mode and a blocklist rule was matched, it would report the execution as untrusted, even though the blocklist was processed (HAS-5307).

3. Enforcement Agent macOS (v5.1.4.8246)

Improvements / Fixes

- Fixed performance degradation when installed alongside the CrowdStrike sensor. This issue was most notable when large amounts of file executions are occurring (HAS-5320);
- Fixed a reporting issue where if the agent was in Audit mode and a blocklist rule was matched, it would report the execution as untrusted, even though the blocklist was processed (HAS-5307);

- Fixed an issue where after a system restart the airlock application icon could appear in the dock (HAS-5350);
- Fixed an issue where the macOS agent was unable to be sideloaded with a new configuration from the terminal or UI (HAS-5351).

4. Enforcement Agent Windows (v5.1.5)

Improvements / Fixes

- Fixed an interoperability deadlock with other third-party file system minifilters, where Airlock cache clean-up messages were (in rare circumstances) unable to reach the user mode component preventing file processing (HAS-5336);
- Added handling to prevent duplicate popup notifications in Windows (HAS-5269);
- Fixed an issue where Notifier would appear blank upon waking from sleep / hibernate or when significant event volume was seen on Windows 11. This issue is cosmetic only and does not impact file handling or server reporting (HAS-5339);
- Fixed a debug level 2 log message which did not separate new lines correctly (HAS-5345).
- Fixed an unexpected service termination when parsing a specifically corrupt file. This was found proactively in testing and has not been observed in customer environments (HAS-5367).

5. Relay Agent (v5.1.3)

Improvements / Fixes

- Fixed a database check integrity loop that could occur when policy groups are deleted. This loop is resolved when the relay agent is restarted. This does not impact downstream policy delivery, but could result in elevated network traffic between the relay agent and airlock server (HAS-5139).

Airlock Change Log v5.1.3

Released 27th April 2023

Overview

This is a maintenance release containing agent and server bugfixes.

Detailed Changes:

1. Server (5.1.3.1526-Leonard)

Improvements / Fixes

- Fixed an issue where clicking on the checkbox instead of the square on the bulk add reputation filters results in the filter not applying (HAS-5177);
- Fixed an issue where email alerts would not be sent from the Airlock Server if the remote email server had a self-signed TLS certificate and TLS was enabled for email sending (HAS-5202);
- Fixed an issue where apostrophe characters on path and process rules were not correctly processed (HAS-5209);
- Fixed an issue where malicious / suspicious events were not always flagged on the Server Activity History (HAS-5208);
- Updated a number of underlying system dependencies (HAS-5226).

2. Enforcement Agent Linux (v5.1.2.6239)

Improvements / Fixes

- Sudo or root access is now required to invoke an uninstallation (HAS-5164);
- Fixed an issue where updates to path, publisher and processes did not print out at update time in debug logs (HAS-5237);
- Fixed an issue where script file types (disabled by default) were incorrectly reported as blocked, when they should be reported as blocked [audit]. This was a reporting issue only and the action taken on files was correct (HAS-5260);

3. Enforcement Agent macOS (v5.1.2.8239)

Improvements / Fixes

- Sudo or root access is now required to invoke an uninstallation (HAS-5164);
- Fixed an issue where updates to path, publisher and processes did not print out at update time in debug logs (HAS-5237);
- Fixed an issue where script file types (disabled by default) were incorrectly reported as blocked, when they should be reported as blocked [audit]. This was a reporting issue only and the action taken on files was correct (HAS-5260);

4. Enforcement Agent Windows (v5.1.4)

Improvements / Fixes

- Fixed an issue where ‘Invalid new policy database’ is displayed in the client logs on every policy update. Please note that there is no issue updating policy databases and this was simply a visual error (HAS-5191);

- Improved script handling (HAS-5201);
- Reduced the size of local log files by moving the Blocklist criteria match messages to debug level logging only (HAS-5221);
- Added interoperability with the Qualys Cloud Agent to improve stability (HAS-5265);
- Fixed an issue where the operating system build was always reported as 2009 for recent Windows 10 & Windows 11 versions (HAS-5268).

Airlock Change Log v5.1.2

Released 10th March 2023

Updated 17th March 2023 (5.1.2.1485 -> 5.1.2.1496)

Overview

This is a maintenance release containing agent and server bugfixes.

Detailed Changes:

1. Server (5.1.2.1496-Leonard)

Improvements / Fixes

- Improved dashboard loading performance by 60% (HAS-5129);
- Fixed an issue where the main dashboard / activity viewer counts did not match those through to the Bulk Add screen when multiple group selections or ‘Not Includes’ filters are involved (HAS-5060 & HAS-5092);
- Fixed an issue where the dashboard unreviewed count displayed zero, even when unreviewed items were present (HAS-5103);
- Further improved the integrity of policy generation through a refactor (HAS-5097, HAS-4897 & HAS-5115);
- Fixed an issue where files opened in a new tab from the Bulk Add screen would show an error page (HAS-5093);
- Fixed an issue where applied client policy versions may not be correctly reflected on the clients table on the Airlock server (HAS-5109);
- Fixed an issue where OTP Restrictions were blank upon upgrade from an earlier server version, which prevented policy changes from being made until the OTP Restrictions were manually set per policy (HAS-5114);
- Fixed authenticated XSS on the blocklist screen (HAS-5122);
- Fixed an issue where the publisher would be filtered from view on the Bulk Add screen even when the filter is deselected (HAS-5123);
- Fixed a panic on policy generation reported in goerrors.log;
- Fixed a rails error on policy generation (HAS-5153).

2. Enforcement Agent Linux (v5.1.2.6228)

Improvements / Fixes

- Fixed a system deadlock that could occur when files take a long time to be processed, resulting in blocked kernel file reading. File processing is now performed on separate queues ensuring file events can be dequeued correctly (HAS-5079);
- Fixed an issue where airlockcmd would not correctly return or function when a system proxy is configured (HAS-5073);
- Fixed a crash when rapid executions were performed (HAS-5056);
- Improved file processing by ensuring process file channels are appropriately returned (HAS-5080);
- Improved performance through file cache modifications, lowering disk I/O (HAS-5084);
- Fixed an issue where proxy details contained within policy were not respected on first installation of the Agent (HAS-5048);
- An interoperability system has been implemented to assist with future compatibility with other endpoint protection tools if required (HAS-5081);

- Fixed an issue where the installer would not correctly use sudo during installation (HAS-4869);
- Fixed an issue where policy versions may not reflect correctly on the server, unless manual policy updates are invoked (HAS-5104);
- Fixed an issue where during the creation of a baseline using ‘createbaseline’ file processing may get stuck on symlinked files (HAS-5107);
- Fixed an issue where a file could be blocked in an extremely short time window, if the client processes and fails to apply a policy database (HAS-5110);
- Fixed an issue where an OTP code could be activated twice if multiple OTP issuances were performed. Note that the time window in which this can occur is small as usage must be concurrent and valid OTP codes are still required (HAS-5112);
- Fixed a rare deadlock which could occur when the username is retrieved for a given execution, the agent now performs local caching of UUID translations to avoid username retrieval at file runtime (HAS-5140);
- Fixed an issue where if an agent is upgraded to 5.1.0 or 5.1.1 from an older agent, the installer will show an ‘unsupported command in Linux’ error (HAS-5099).

3. Enforcement Agent macOS (v5.1.2.8227)

Improvements / Fixes

- Fixed an issue where proxy details contained within policy were not respected on first installation of the Agent (HAS-5048);
- Fixed an issue where airlockcmd would not correctly return or function when a system proxy is configured (HAS-5073);
- An interoperability system has been implemented to assist with future compatibility with other endpoint protection tools if required (HAS-5081);
- Fixed an issue where policy update notifications were seen for every policy update, rather than those the user manually invoked (HAS-5098);
- Fixed an issue where policy versions may not reflect correctly on the server, unless manual policy updates are invoked (HAS-5104);
- Fixed an issue where a file could be blocked in an extremely short time window, if the client processes and fails to apply a policy database (HAS-5110);
- Fixed an issue where an OTP code could be activated twice if multiple OTP issuances were performed. Note that the time window in which this can occur is small as usage must be concurrent and valid OTP codes are still required (HAS-5112);
- The settings checkbox in the macOS Notifier is now updated when command line debug on / off changes state (HAS-5139).

4. Enforcement Agent Windows (v5.1.3)

Improvements / Fixes

- Fixed an issue where on uninstall or upgrade v5.1.0 and v5.1.1 the Airlock Driver could not be removed without a reboot or a manual unload (HAS-5085);
- Fixed an issue on v5.1.0 and v5.1.1 where signing catalogs may not be correctly enumerated at runtime, which could rarely result in the observation of unsigned files, between Windows patch application & reboot (HAS-5101);
- Fixed a crash when the Crowdstrike proxy is used and a proxy is specified using a MSI parameter during install / upgrade (HAS-5106);
- Fixed a crash which can occur when the system has no network connection and a CrowdStrike proxy is used. This was resolved for edge cases in v5.1.3 (HAS-5106).

5. Relay Agent (v5.1.2)

Improvements / Fixes

- Fixed a crash when the relay agent is unable to connect to an upstream server during an event send (HAS-5045);
- Added support for UUID client registration used in recent macOS & Linux clients (HAS-5082);
- Prevented the processing of duplicate database downloads, reducing invalid policy checks by downstream Enforcement Agents (HAS-5083);
- Improved database integrity checking when downloading policy databases from the Airlock server (HAS-5087);
- Fixed an issue where the relay agent could provide a blank hashdb version number to clients, resulting in no hashdb version being displayed in notifier and triggering a database re-download (HAS-5089);
- The relay agent will no longer listen for client connections during initial synchronisation. After policies have completed synchronisation from the main Airlock server, client connections will be serviced (HAS-5090).

Airlock Change Log v5.1.1

Released 28th January 2023

Overview

This is a minor maintenance release containing agent, server and minor bugfixes.

Detailed Changes:

1. Server (5.1.1.1337-Leonard)

Improvements / Fixes

- Added a new privacy tab, which enables the disabling of command line collection globally within the product. Please note that only the agent versions listed in this release and newer will respect this setting (HAS-4947);
- Fixed an issue where parent process event fields were not appropriately sanitised, causing invalid JSON messages to be sent via the external logging function (extlogger). This will only be encountered by a customer when they have v5.1 Windows agents deployed in production (HAS-4953);
- Fixed a crash in extlogger upon startup when Splunk is configured as an external logging source (HAS-4952);
- Fixed an issue where the policy group filters on the Activity Viewer were not applying correctly when a child policy group was selected (HAS-4977);
- Fixed an issue where OTP codes were unable to be retrieved from the All-Clients policy view (HAS-4982);
- Re-added the visual 'view' toggle for Agent Stop Codes on the policies tab;
- Fixed a possible race condition in policy generation which could result in policy databases being invalid (HAS-5039);
- Fixed an issue where /v1/hash/query returned a "not found" response for hash values that are present on the server (HAS-5043).

2. Enforcement Agent Linux (v5.1.1.6167)

Improvements / Fixes

- Set filelog.db retention to 1 day on Linux to minimise the disk space used by the file, if desired this can now be disabled entirely by adding Filelogs = false to the clients config.toml (HAS-4951).
- Added the ability to disable command line collection (HAS-4947);
- Fixed an issue where file executions of a certain nature would only result in the first execution being reported (HAS-5000);
- Fixed a slow kernel memory leak when running in driver mode (HAS-5018).

3. Enforcement Agent macOS (v5.1.1.8166)

Improvements / Fixes

- Added the ability to disable command line collection (HAS-4947).

4. Enforcement Agent Windows (v5.1.1)

Improvements / Fixes

- Fixed an issue where OTP configurations were not correctly written out to the policy database locally on a client. This would result in OTP codes failing in the event the Airlock process was restarted (since the last server connection) and the client did not have network connectivity to an Airlock server (HAS-4942);
- Added the ability to disable command line collection (HAS-4947).

Airlock Change Log v5.1

Released 4th January 2023

Overview

Airlock Digital v5.1 introduces stability enhancements an updated core platform and blocklist metadata support for macOS & Linux.

- **Windows Performance & Interoperability Enhancements:** The Windows Enforcement Agent driver architecture has been re-written to further improve performance and interoperability when installed alongside other Endpoint Protection products. This is achieved through the migration of more file handling functions to the kernel, to prevent inspection of Airlock operations by other Endpoint Protection products on the system;
- **Command Line Blocklisting:** Introduced the ability to block (or allow) process executions via their command line. This makes the Blocklisting framework even more flexible to control application behaviour;
- **Full Path Parent Process Trust:** The parent process feature now supports specifying full paths to images (rather than just the image name itself);
- **Bulk Add Improvements:** The Bulk Add screen now has a filter that will automatically remove trusted files / publisher data. Making it easier to process large data sets;
- **Ability to disable OTP durations:** OTP durations can now be enabled / disabled within policy, enabling administrators to prevent the use of times such as 7 days for OTP mode;
- **File Repository Comments:** Comments can now be added on the File Repository page, enabling teams to discuss and leave notes against file entries;
- **Ability to Blocklist by Certificate Thumbprint:** File signing certificates can now be blocked by their certificate thumbprint. This can provide a mitigation when vendors code signing certificates are stolen.

Upgrade Notes:

- Client compatibility is unchanged from the previous release.
- Upgrading to v5.1 of the Airlock Server is only supported from v4.8.x or v5.0.x. If the Airlock Server being upgraded is on an earlier release, you must first upgrade to v4.8.x or v5.0.x before upgrading the server to v5.1.

Known Issues:

- Command Line Blocklisting on CentOS / RHEL based Linux (and their derivatives) may not function for all process launches. This is due to a limitation in retrieving the command line before the process is spawned. This is being investigated and is anticipated to be resolved in a future release.

Detailed Changes:

1. Enforcement Agent Windows (5.1.0.0)

New Features

- Command Line Blocklisting (HAS-3755);
- Support for Full Path Parent Process Trust (HAS-3800);
- Added the ability to disable certain OTP times within policy (HAS-4236);
- Added the ability to blocklist by certificate thumbprint (HAS-4237).

Improvements / Fixes

- Added Registry Key Protection for Agent Registry keys. This prevents tampering or modification of the agent service entries or registry configurations, further improving security of the agent (HAS-3654);
- Redesigned the kernel to user mode driver architecture to improve performance, this was achieved by reducing the amount of data transferred between these modes. Additionally, numerous operations have been moved to kernel mode to improve interoperability when installed alongside other Endpoint Protection products (HAS-3649);
- Added support for Full Path Parent Process Trust (HAS-3800);
- Fixed an issue where the agent would not install on Server 2008 and Windows Vista, due to the inability to detect Windows Patch Prerequisites. Note: This does not impact Server 2008 R2 or Windows 7 (HAS-3858);
- Improved performance of the agent during the installation of certain Operating System updates, by migrating publisher catalog removals to bulk database operations, reducing disk I/O;
- Fixed an issue where stopping an enforcement agent during an OTP code will result in ‘input OTP code’ being temporarily greyed out upon restart (HAS-1545);
- Fixed an interoperability deadlock that occurred when SysInternals SysMon was installed with Image Loads enabled in the SysMon policy (HAS-2697);
- Fixed an issue where PowerShell module files were seen as unsigned, even though they are catalog signed (HAS-3908);
- Fixed an issue where activities may not be uploaded to the server if the agent process was closed between activity collections (HAS-3947);
- Fixed a BSOD that occurred on the v5.0 release where certain registry access caused an access violation (HAS-3979);
- Fixed a BSOD that occurred on the v5.0 release where driver unload pending operations may not be fully cancelled (HAS-4011);
- Fixed a IRP Violation BSOD that occurred on the v5.0 release when running with Driver Verifier (HAS-4073);
- Fixed an issue where Client Notification Messages that include an apostrophe would not be processed (HAS-4159);
- Changed the precedence of communication using a Crowdstrike Proxy to match the communication flow shown in the user manual (HAS-4460);
- Implemented stateful agent communication logic to significantly reduce network chatter from the agent when it is attempting to reach the Airlock Server (HAS-4461);
- Fixed an issue where NTLM authentication via a proxy server would not be attempted upon install when a PROXYURL parameter was specified with credentials (HAS-4665);
- The agent will now cleanup registry entries that store proxy details when PROXYURL parameters are specified upon deployment (HAS-4666);
- Fixed a crash upon entering an OTP code when the local OTP database is not available, this could happen upon the client being offline after being recently installed or due to a recent policy move (HAS-4874);
- Fixed an issue where files over 2GB in size would report an invalid digital signature (HAS-4817);
- Fixed an issue where exported CSV's from Notifier don't always conform with RFC4180 when command lines containing quotes are seen. The export process now correctly double escapes quotes to ensure the resulting CSV is valid (HAS-4844);
- Added support for Windows 11 AppX application paths, previously some files run out of ProgramData could be seen as unsigned (HAS-4921).

2. Enforcement Agent macOS (v5.1.0.8150)

New Features

- Blocklist metadata support for macOS (HAS-3928);
- Added the ability to disable / enable Shell Script (.sh) support via policy (HAS-4002).

Improvements / Fixes

- Fixed an issue where Trusted Execution Activity Uploading (complete and summary) were not functional (HAS-4014);
- Fixed an issue where users receive an “Agentcore is Stopped” message in the event the ESFramework stops responding (HAS-4120);
- Fixed a rare crash during baselining of a system which would cause the Enforcement Agent to restart (HAS-4271);
- Fixed a crash when the local certificate database is nil (HAS-4912);
- Fixed an issue where the macOS agent was unable to complete the discovery / registration process when a relay agent was in use within policy (HAS-4911);
- The agent can now use an AgentClientConfig.xml configuration file to sideload upon installation, when the file is placed in the same directory as the installer (HAS-4911);
- Fixed an issue where the client version number would not be populated within the macOS installer filename upon download;
- Fixed a crash if the server returns an unexpected blank response to certain API calls (HAS-4925);
- Fixed an issue where parent process trust was not being respected by the agent (HAS-4932).

3. Enforcement Agent Linux (v5.1.0.6150)

New Features

- Blocklist metadata support for Linux (HAS-3928);
- Added the ability to disable / enable Shell Script (.sh) support via policy (HAS-4002);

Improvements / Fixes

- Fixed an issue where Trusted Execution Activity Uploading (complete and summary) were not functional (HAS-4014);
- Changed removing marks to mountpoint log message to debug logging (HAS-4037);
- Added a function to the Linux Agent installer to remove previous versions upon upgrade (HAS-4085);
- Drivers are now prevented from loading on new RHEL / CentOS 7 kernels if they continue to be developed, future versions will be driverless (HAS-4265);
- Improved error handling in the event the Airlock Database files are locked due to concurrent access (HAS-4472);
- Fixed an issue where capturing a baseline using airlockcmd createbaseline could miss some files;
- Fixed an issue where capturing a baseline using airlockcmd createbaseline would not capture publisher information on Ubuntu 14.x / 16.x (HAS-4067);
- The Linux Enforcement Agents have now been combined again, there is no longer a dedicated CentOS 6.x legacy package. The single agent now operates across all platforms (HAS-4462);
- Fixed a client crash when the client is communicating via a relay agent (HAS-4887);

- Fixed an issue where XML sideloading and airlockcmd loadconfig was not functional (HAS-4255);
- The Linux enforcement agent now checks for root privileges during install, if root privileges are found then sudo is no longer invoked. This fixes issues where sudo from root has been disabled (HAS-4869);
- Fixed a crash if the server returns an unexpected blank response to certain API calls (HAS-4925);
- Fixed an issue where parent process trust was not being respected by the agent (HAS-4932).

4. Server (5.1.0.1335-Leonard)

New Features

- Added Blocklist metadata support for Linux & macOS (HAS-3928);
- Added the ability to disable / enable Shell Script (.sh) support via policy (HAS-4002);
- Added the ability to filter & delete OTP entries on the OTP page (HAS-4098, HAS-4114);
- Added filtering of events on the Bulk Add screen to improve workflow, this can be enabled and disabled using a radio toggle (HAS-4229);
- Added 'NOT' filtering on the Server Activity page enabling events to be excluded from results (HAS-4230);
- OTP durations can now be enabled / disabled within policy, allowing administrators to prevent the use of times such as 7 days for OTP mode (HAS-4236);
- Added a new OTP Session API endpoint that allows the returning of events for a given OTP session. See the updated REST API documentation for additional information (HAS-4234);
- Added the ability to blocklist by certificate thumbprint (HAS-4237);
- Comments can now be added on the File Repository page, allowing teams to discuss and leave notes against file entries (HAS-4241);
- Exporting and Importing Path / Publisher / Parent process rules to XML now include comments (HAS-4394).

Improvements / Fixes

- Added User Created & Last Login Time to Local User Management (HAS-4089);
- Trusted Logging All Rules (Complete) can no longer be enabled on policy groups containing more than 50 clients. This prevents significant event volumes (HAS-4135);
- Fixed an issue where exporting the client list to XML would only populate a single client (HAS-4143);
- Client export to CSV now includes all columns on the policies page (HAS-4144);
- Fixed an issue where sorting clients by Disk Free did not consider single digits appropriately (HAS-4145);
- Viewing the full Airlock licence key after entry is now masked (HAS-4148);
- Fixed an issue where copy and paste was not able to be performed on the Blocklist Metadata rule form (HAS-4165);
- Added a cancel button on the password reset prompt page to prevent the user becoming stuck (HAS-4175);
- Major upgrade of the underlying platform version and associated dependencies including an uplift of the web server framework and database (HAS-1298, HAS-3940, HAS-4334, HAS-4333, HAS-4088);
- Added a new Server Activity History Message when an OTP is generated (HAS-4100);

- Fixed an issue where Server Activity History messages may not be logged when certain actions are performed via the REST API interface (HAS-4100);
- Columns are now sortable on the search tab by clicking column headers (HAS-4097);
- When configuring Splunk as an external logging target, defaults are now populated on the page making it easier to configure (HAS-4121);
- Added Ubuntu Reference Baselines into the product (HAS-4112);
- Fixed an issue where the EULA phase of the server installation script would not accept keyboard inputs (HAS-3881);
- Fixed an issue where the total client count in the 'all clients view' on the policies page is inconsistent between the top bar and status window (HAS-3962);
- Fixed a rare issue where if the ClientAPI is placed under significant and sustained load it could panic due to concurrent access, guards were put in place on a critical section to prevent the panic (HAS-4026);
- Improved the security of the Linux Agent Package upload to the webUI (HAS-4030);
- Fixed an issue where the /v1/agent/find REST API endpoint does not return expected results for numerical request parameters (HAS-4066);
- Fixed an issue where the REST API roles for a user could be unintentionally dropped if a specific sequence of actions are performed (HAS-4076);
- Updated certain application and baseline user roles to reflect their correct purpose, please see the Roles section of the Airlock User Manual for the updated role descriptions (HAS-4218, HAS-4254 HAS-4259, HAS-4292, HAS-4294, HAS-4295);
- Fixed an issue where if you move an application capture between categories, the UI will reflect the update, however the resulting database generation will still behave as if the application capture is linked to the old category, resulting in the potential for untrusted captures in policy that are unintended (HAS-4219);
- The Deny option is now greyed out on a right click of application categories that are unable to be denied (HAS-4224);
- Updated the included reference baselines within the product (HAS-4232);
- Updated the Microsoft Recommended Driver Blocklist rules to utilise the new certificate thumbprint blocking capability (HAS-4238);
- Updated message prompts to be clearer when applying and updating policies (HAS-4281, HAS-4463);
- Fixed an issue where blocklist metadata rule criteria that contains a trailing \ character is unable to be edited or deleted (HAS-4289);
- Fixed an issue where certain macOS file paths were not rendering correctly in the Activity Viewer (HAS-4291);
- Fixed an issue where a misconfigured external SIEM logger could cause rapid growth of the extlogger.log file, as the full error response was logged back to file (HAS-4314);
- Fixed an issue where if you edit a path rule that contains an attached comment, editing the path rule would remove the comment (HAS-4343);
- Added a Server Activity History log when the Licence Key is changed (HAS-4392);
- Fixed an issue where if a VirusTotal key was set and the Airlock Server did not have internet connectivity, it would cause a rails error upon loading of a File Repository entry (HAS-4397);
- The VirusTotal Augment snap-in now respects the proxy settings entered on the Reputation tab of the Airlock Web Interface (HAS-4397);
- Fixed an issue where using the 'select all' filter on the Mobile OTP page, when combined with a text filter, selects codes that are not currently visible. This can result in unintentional revocation of Mobile OTP codes (HAS-4467);
- Disabled the cipher TLS_RSA_WITH_AES_256_GCM_SHA384 on the Client API & REST API to improve security (HAS-4486);

- Removed the download for the Linux Baseline Builder from the webUI as baseline functionality is now included in the Enforcement Agent itself (HAS-4816);
- Added a policy group filter to the /v1/logging/exechistories endpoint which allows for events to be retrieved from only the desired policy groups (HAS-4872);
- Fixed an issue where Linux & macOS file paths were unable to be searched for in Quick Search due to character sanitisation, this restriction is now removed (HAS-4843);
- Improved error handling has been added for the import of Baselines & Application Captures. Invalid imports that fail to process will now log a Server Activity History message and also display a red cross icon (HAS-4859).
- Added a disk space check when backups are performed to prevent disk exhaustion when backups are written to the same volume that Airlock is installed (HAS-4818);
- Updated the Microsoft Recommended Block Rules ruleset (HAS-4845);
- Fixed an issue where adding files into application captures in quick succession could cause two database generations with the same version in the generatedb queue. This could result in clients receiving invalid differential databases, resulting in the clients falling back to a full database download, this generates higher than required network traffic (HAS-4897);
- Fixed an issue where initial policy generations on newly created policy groups could be blank due to a race condition in generation. The workaround is to make an additional policy change (HAS-4933).

5. Baseline Builder & Application Capture agent (v5.1.1.0)

Improvements / Fixes

- Fixed corrupted characters on the right click menu inside the Baseline Builder and Application Capture Save As menu (HAS-4865).

6. Relay Agent (v5.1.0.0)

Improvements / Fixes

- The Relay Agent now sorts the policy changes by the policy ID to prevent re-downloading processed events in specific double generation scenarios (HAS-4897).

Airlock Change Log v5.0.7

Released 10th November 2022

Overview

This is a minor maintenance release containing agent bugfixes and a minor server fix.

Detailed Changes:

1. Server (5.0.7.0-Noah)

Improvements / Fixes

- Fixed a rare issue where if a repository entry does not have a timestamp populated the repository page entry would fail to load with an error (HAS-4646).

2. Enforcement Agent Linux (v5.1.0.276)

Improvements / Fixes

- Added the ability to enable / disable the new UUID registration method for Linux. This has been set to disabled by default due to some customers reporting duplicate machine-id keys in virtualised environments (HAS-4616);
- Fixed an issue where 'Timed out processing file' could be seen in debug logging when operating in driverless mode (HAS-4622).

3. Enforcement Agent Windows (v4.8.7)

Improvements / Fixes

- Fixed an issue where self-signed script files run from an authenticated UNC share could be shown as having a valid publisher if that publisher certificate has been trusted in the local user's certificate store and the publisher is trusted within policy. Thanks to James Spencer from the Cyber Risk and Resilience Team and Ryan Newington from the Enterprise Engineering Team at Monash University for the report (HAS-4593);
- Fixed an issue where if the Windows Operating System has a non-standard drive letter assignment (not C:\) script control may not process executions in certain scenarios (please note this does not impact PE files such as .dll / .exe) (HAS-4641).

Airlock Change Log v5.0.6

Released 28th October 2022

Overview

This is a minor maintenance release containing two minor bugfixes.

NOTE: If customers deploy the 5.1.0.274 Linux Enforcement Agent and upgrade to a newer version in the future, it will result in duplicate client registrations to the server. It is recommended to deploy 5.1.0.275 where possible to avoid this.

Detailed Changes:

1. Enforcement Agent macOS (v5.1.0.275)

Improvements / Fixes

- Fixed an issue where the Airlock Server Name would show as blank in the preferences UI (HAS-4516)

2. Enforcement Agent Linux (v5.1.0.275)

Improvements / Fixes

- One way hash the machine UUID for registration using SHA-256 (HAS-4506)

3. Server (5.0.6.0-Noah)

Improvements / Fixes

- Improved the unique ID registration logic introduced in 5.0.5 server. Duplicate client entries no longer occur when updating clients to the new Linux & macOS agents (HAS-4401);
- Fixed an issue where discovery databases for clients are not populated with proxy authentication credentials. This could cause clients to not get a policy after initial installation where an authenticated proxy is required to communicate with the Airlock server (HAS-4419).

Airlock Change Log v5.0.5

Released 19th October 2022

Overview

This is a minor maintenance release containing updated macOS, Linux & Windows Agents

Detailed Changes:

1. Enforcement Agent macOS (v5.1.0.274)

Improvements / Fixes

- Changed the log & UI event label to say 'blocklist' instead of 'blocked' for blocklisted events;
- Support logs now include crash and diagnostic events;
- Improved agent performance by only computing SHA-256 hashes upon initial file sighting. Other hashing is now deferred for untrusted files, resulting in lower CPU overhead (HAS-4423);
- Agents now register using a unique ID to identify the endpoint, rather than hostname (when supported by the Airlock server). This prevents stale registrations upon hostname changes (HAS-4401).

2. Enforcement Agent Linux (v5.1.0.274)

Improvements / Fixes

- Changed the log & UI event label to say 'blocklist' instead of 'blocked' for blocklisted events;
- Fixed an issue where Linux captured baselines were not populated with an Export Name resulting in an import failure (HAS-4270);
- Handle a fatal exception when Airlock database files are not able to be created correctly upon install;
- Fixed a deadlock when airlockcmd functions are called in rapid succession by the user (HAS-4297 & HAS-4296);
- Improved channel buffering increasing stability;
- Fixed an issue where the log rotate entry was incorrect, resulting in failed log rotation (HAS-4336);
- Fixed an issue when an in place agent upgrade fails on CentOS / RHEL 7.x / 8.x systems (HAS-4335);
- Fixed an issue where if Automatic Linux Kernel Module Reload is enabled, the driver would not be re-applied upon kernel update. The agent now always reloads a driver if a compatible one is found when Linux Kernel Module Reload is enabled (HAS-4328);
- Improved agent performance by only computing SHA-256 hashes upon initial file sighting. Other hashing is now deferred for untrusted files, resulting in lower CPU overhead (HAS-4423);
- Removed global read permissions on log files from 644 to 640 (HAS-4469);
- Agents now register using a unique ID to identify the endpoint, rather than hostname (when supported by the Airlock server). This prevents stale registrations upon hostname changes (HAS-4401).

3. Enforcement Agent Windows (v4.8.4)

Improvements / Fixes

- Fixed a rare BSOD during a ‘preCall’ function where the driver is being loaded and protected on driver load. This can only occur if the driver partially loads and fails, it has only been seen during internal Airlock testing (HAS-4227);
- Fixed an issue where if a file contains a substitute Unicode character the file event may not be seen on the server (HAS-3916).

4. Server (5.0.5.0-Noah)

Improvements / Fixes

- Support the registration of agents using a Unique ID to identify the endpoint rather than a hostname (HAS-4401).

Airlock Change Log v5.0.4

Released 3rd August 2022

Overview

This is a minor maintenance release containing an updated macOS agent

Detailed Changes:

1. Enforcement Agent macOS (v5.1.0.241)

Improvements / Fixes

- Fixed an issue where the macOS agent could report differing hostnames within the web UI creating duplicate entries (due to changing .local suffix entries which may change based on network connection type) (HAS-4242);
- Fixed an issue where file deletion performance is poor due to agent self-protection mechanisms monitoring ESFramework deletion events. The agent now protects itself using a different mechanism removing the need to monitor deletion events (HAS-4243);
- Fixed an issue where an OpenVPN client connection event could temporarily block system actions upon connection for 60 seconds. This was due to the Agent retrieving the 'new' computers hostname when the network changed state (HAS-4244);
- Fixed an issue where some trusted files were shown in the notifier in macOS. This could cause confusion to the end user when managing policies (HAS-4245);
- The agent now deletes additional application configurations upon uninstallation to avoid settings such as debug mode persisting between installations (HAS-4246);
- Disabled Shell Script (.sh) enforcement by default on this release. This can manually be re-enabled if desired on the endpoint. However, this feature will be centrally configurable upon the release of Airlock v5.1 server through policy which this agent supports (HAS-4252)

Airlock Change Log v5.0.3

Released 18th July 2022

Overview

This is a minor maintenance release including an updated Windows Enforcement Agent within the v4.8 release series.

Detailed Changes:

1. Enforcement Agent Windows (v4.8.2)

Improvements / Fixes

- Fixed a rare BSOD that could occur when Airlock is installed with McAfee Anti-Virus on Windows 10 / 11 and McAfee mcshield.exe issues raw I/O directly to the underlying disk/volume. The Airlock filter now avoids interception of this request, preventing a Null Memory Descriptor condition (HAS-4190);
- Fixed the interoperability detection of legacy McAfee Anti-Virus on Windows XP / Server 2003. Successful detection will assist in avoiding deadlock conditions and improve performance (HAS-3924);
- Fixed an issue where a Windows APPX application is seen as unsigned if it was installed within ProgramData (HAS-4105).

2. Enforcement Agent macOS (v5.1.0.236)

Improvements / Fixes

- Fixed an issue where the Trusted Execution Activity Uploading setting would not be respected within policy (HAS-4188)

3. Server (5.0.3.0-Noah)

Improvements / Fixes

- Fixed an issue where API permissions are not saved when creating a new permissions group, which could result in API roles being dropped (HAS-4103);
- Added a visible show/hide toggle for Agent Stop Codes to prevent observation during screen sharing or by sneaky shoulder surfers (HAS-4111);
- Fixed an issue where Event Summary graphs on the Activity Viewer did not take into account child group selections when rendering, this could result in inaccurate or empty results from being displayed (HAS-4136);
- Fixed an issue where Bulk Add from Saved Searches would allow you to select files to add to an application capture, however viewing the application capture after the process would show that the files had not been added (HAS-3926);
- Fixed a rare ClientAPI panic that was observed during testing, when the system was placed under sustained extremely high load (HAS-4074);
- Updated third-party dependencies to the latest available versions.

Airlock Change Log v5.0.2

Released 8th June 2022

Overview

This is a Linux and macOS focused release providing stability and memory enhancements for both agents, including minor web improvements.

Detailed Changes:

1. Enforcement Agent Linux (v5.1.0.233)

New Features

- The Linux Enforcement Agent now has a shell-based UI which can be viewed over SSH. It can be viewed by running the command ‘airlockcmd ui’;
- Baseline Builder for Linux. This functionality is now integrated within the Enforcement Agent itself.

Improvements / Fixes

- The Linux Agent has been entirely rebuilt and now has substantially improved memory management, preventing high airlock memory usage scenarios;
- Fixed stability issues for systems using driverless operation with FANotify Legacy. Systems could stop functioning when a large amount of file modifications were performed on the system. The agent no longer subscribes to file modification events via FANotify and has an entirely new file cache design to ensure performance (HAS-4077);
- Changed FANotify to use entire filesystem Mark’s when available FAN_MARK_FILESYSTEM (HAS-4038);
- Fixed an issue where the agent would correctly handle Safe Mode (without a restart) when a core system publisher was added or removed (HAS-4062);
- Implemented improved communication logic where the agent will attempt to prevent isolation if a proxy server or relay agent is removed from policy, but there is no route to the Airlock Server (HAS-4063);
- The Linux Enforcement Agent is now split into two separate installers to retain support for CentOS / RHEL 6.x, this is to ensure that the modern Linux Enforcement Agent can continue to use modern build tooling that is not supported on older Linux platforms. The feature set between the two agents is at parity (HAS-4087).

2. Enforcement Agent macOS (v5.1.0.233)

New Features

- The agent now supports the blocking of Shell Scripts (.sh) (HAS-3923)

Improvements / Fixes

- Fixed an issue where the agent would correctly handle Safe Mode (without a restart) when a core system publisher was added or removed (HAS-4062);
- Implemented improved communication logic where the agent will attempt to prevent isolation if a proxy server or relay agent is removed from policy, but there is no route to the Airlock Server (HAS-4063);
- Added Multi User Session Support for the Airlock Notifier UI (HAS-4016).

3. Server (5.0.2.0-Noah)

Improvements / Fixes

- Fixed an issue on the Bulk Add screen where the reputation filter selections would not apply if a Publisher was clicked, leading to the filters being ‘disconnected’ from each other (HAS-4004);
- Fixed authenticated XSS on the Blocklists page when importing a predefined blocklist XML.

Airlock Change Log v5.0.1

Released 21st April 2022

Overview

This is a macOS focused release which includes a Windows Agent version downgrade due to identified issues impacting a subset of customers. Additional improvements and updates will be included in the upcoming v5.1 release.

NOTE: This release downgrades the version of the included Windows Agent to v4.8.1. This is due to reported stability issues in the v5.0.0 Windows Enforcement Agent in three (at the time of writing) customer environments, this downgrade is being performed out of an abundance of caution.

These issues are actively being investigated and only apply to the v5.0.0 Windows Enforcement Agent release. At this time, it is recommended that customers preference the use of the Windows Enforcement agent v4.8.1 until an updated v5.0.1 agent is released.

Detailed Changes:

1. Enforcement Agent macOS (v5.0.1.23)

New Features

- Baseline Builder for macOS. This functionality is now integrated within the Enforcement Agent itself (HAS-731)

Improvements / Fixes

- Fixed a parsing issue where the Apple ESFramework may provide an incorrect path, leading to incorrect file handling and an Executed (Enforced) file result, which is not valid (HAS-3976);
- Self Service OTP is now hidden from users if it is not enabled in policy (HAS-3977);
- Fixed an issue where OTP sessions would only upload a single execution event in the session. Internal event handling has been updated to ensure all events are logged (HAS-3980);
- Fixed an issue where OTP codes that start with a number 0 were unable to be entered into the UI (HAS-3917);
- Fixed an issue where valid OTP codes may not be respected if the client / server OTP counter became out of sync due to multiple OTP issuance. This was due to the internal OTP counter looking ahead incorrectly (HAS-3919);
- Fixed an issue where files that were previously blocked under enforcement mode may not be allowed during an OTP session. The Apple ESFramework cache is now appropriately cleared when moving to OTP mode (HAS-3963);
- Fixed an issue where the filename installation method would not function if the Airlock Server DNS name had a hyphen character in it. The file parsing for installation settings is now improved (HAS-3964);
- Linked the population of the verbose AEACoreDebug.log to only be filled when Debug Mode is enabled (HAS-3965).

2. Server (5.0.1.0-Noah)

Improvements / Fixes

- Added macOS Reference Baselines to the platform;
- Fixed incorrectly named RHEL baselines (they were referenced as CentOS after import);
- Downgraded the bundled Windows Enforcement Agent to v4.8.1;
- Fixed an issue where if the default server webUI port was changed, the SAML port was still hardcoded to 3128. The port changes are now linked to the SAML controller (HAS-3979);
- Changed the title of the settings ribbon on the Policies page to reflect that the settings are not inherited.

Airlock Change Log v5.0

Released 8th March 2022

Overview

Airlock Digital v5.0 introduces expanded operating system support and stability enhancements.

- **macOS Support:** Airlock v5.0 introduces macOS support, delivering the ability to enforce application control on macOS 10.15 and greater operating systems, without requiring a kernel driver;
- **Debian (Ubuntu) Linux Support:** The Linux Enforcement Agent now supports Debian based operating systems with no kernel driver required. This agent is tested on Ubuntu 14.04 and greater operating systems;
- **Windows Performance & Interoperability Enhancements:** The Windows Enforcement Agent driver architecture has been re-written to further improve performance and interoperability when installed alongside other Endpoint Protection products. This is achieved through the migration of more file handling functions to the kernel, to prevent inspection of Airlock operations by other Endpoint Protection products on the system;
- **Suspicious / Malicious File Alerting:** When a suspicious or malicious file is detected by the Airlock Cloud reputation service a Server Activity History message is now created in real-time. This message can be used to send an email or SIEM alert based off this detection;

Upgrade Notes:

- Client compatibility is unchanged from the previous release.
- Upgrading to v5.0 of the Airlock Server is only supported from v4.8. If the Airlock Server being upgraded is on an earlier release, you must first upgrade to v4.8 before upgrading the server to v5.0.

Detailed Changes:

1. Enforcement Agent Linux (5.0.0.0)

New Features

- Debian (Ubuntu) Support (HAS-3644);

Improvements / Fixes

- Added the -verify command line switch to the Linux agent to improve troubleshooting (HAS-3811);
- Fixed an issue where moving Linux Clients between groups while also changing the enforcement mode can result in misreporting of the operating mode. For example, the agent may report Enforcement Mode when it is actually in Safe Mode (HAS-3851);
- Fixed an issue where Trusted Execution Logging was not functional on the Linux Agent, the upload routines have been fixed to correctly report trusted logging events (HAS-3861);
- Fixed an issue where a bash shell may temporarily become unresponsive if -selfservice was called and the system had a network connection, but no connectivity to the central Airlock server. The connection function is now moved to a different thread to avoid the temporary hang (HAS-3862);
- Fixed an issue where blocklist path rules were not respected on the v4.8 Linux Agent (HAS-3878);

- Fixed an issue where ‘automatic kernel reload’ would not function on v4.8.x agents for systems that do not support ‘driverless’ operation (typically RHEL 6.x / CentOS 6.x systems).

2. Enforcement Agent macOS (5.0.0.334)

New Features

- Initial release.

3. Application Capture Agent (5.0.0.0)

Improvements / Fixes

- Fixed an issue where parsing a file containing certain control characters could cause a partial application capture import (HAS-3864).

4. Baseline Builder Windows (5.0.0.0)

Improvements / Fixes

- Fixed an issue where parsing a file containing certain control characters could cause a partial baseline capture import (HAS-3864).

5. Server (5.0.0.0-Noah)

New Features

- macOS Agent Support (HAS-3798);
- Debian (Ubuntu) Linux Agent Support (HAS-3644);
- Support Command Line Blocklisting as a secondary criterion (HAS-3755);
- Initial rule comment feature, comments can now be added to path / publisher / parent process and other rules in policy (HAS-3756);
- Suspicious / Malicious File Alerting (HAS-3805);

Improvements / Fixes

- Uplifted supporting web libraries to the latest version (HAS-3684);
- Fixed an issue where client search on the policies page was not correctly matching partial client hostnames (HAS-3747);
- Doubled the time of the GenerateDB timeout to prevent the premature termination of policy generations on extremely large policies;
- Added a Server Activity History message if the GenerateDB timeout protection is encountered (HAS-3831);
- Prevent the automatic restart of the application container if a database re-index is in progress (HAS-3836);
- Fixed an issue where if File – Modification Date / MD5 / Product Name is added as a search column, CSV / XML Search Exports will not contain any data (HAS-3854);
- Fixed an issue where if File – File Size is added as a column the search may encounter an error (HAS-3854);
- Fixed an error where if the user pressed ‘enter’ at the new group creation screen without completing the form it would cause a rails error (HAS-3855);

- Fixed an issue where duplicating a user group does not display or migrate REST API roles (HAS-3856);
- Fixed an issue where installing Airlock on RHEL 8.5 would encounter an error ‘initializing source docker://k8s.gcr.io/pause’, this was resolved by bundling the latest pause container in the image to support installation on 8.5 (HAS-3857);
- Added a check to ensure that every user group is named uniquely to prevent duplicate group names (HAS-3859);
- Fixed an issue where if a user generates an API key but doesn’t have the edit_user permission, the user will have permissions revoked (HAS-3865);
- Fixed an issue where command line parameters may not be correctly escaped when sending messages to a SIEM, resulting in an invalid JSON message (HAS-3872);
- Fixed multiple stored authenticated XSS vulnerabilities (HAS-3863) (HAS-3896);
- Updated the REST API /v1/agent/download endpoint to accept the new Linux Deb / macOS platforms (HAS-3873);
- Updated the application certificate bundles to ensure new certificate authorities are correctly recognised when logging to TLS secured SIEM endpoints (HAS-3874);
- Fixed an issue where single Linux files added to an Application Capture would have their paths incorrectly parsed in the capture, showing as network drives;
- Fixed an issue where if Podman is used as the image type the /var/tmp directory would have docker-tar files left behind after upgrading which could consume disk space. This release now cleans up these files post install / upgrade;
- Fixed an issue where the One Time Pad & Remove Selected buttons would become partially clickable on the policies page when pagination is active for clients (HAS-3894).

Airlock Change Log v4.8.1

Released 3rd January 2022

Overview

This incremental release Airlock v4.8.1 is a bugfix release with a new Windows client version. Customers not impacted by the below issues do not need to upgrade to this release.

NOTE: Upgrading to v4.8.1 will force a database re-index which may take between five minutes and several hours depending on the size of the database. The web interface and client connectivity will be unavailable until this process is complete. Upon completion, services will be restored automatically.

Detailed Changes:

1. Enforcement Agent Windows (v4.8.1.0)

Improvements / Fixes

- Fixed a regression where OTP codes would not remain active through a reboot (this only impacted the v4.8.0 Enforcement Agent) (HAS-3733);
- Updated in-built communication libraries and 'rapid' mode certificate behaviour to support the upcoming Airlock cloud platform refresh (HAS-3776); and
- The agent no longer attempts to check for an Authenticode Certificate on Java file types to improve performance and compatibility (HAS-3746);

2. Server (4.8.1.0-Garnett)

Improvements / Fixes

- Fixed an issue where client filtering on the policies page would may not return results unless the complete name of a client was entered (HAS-3747);
- Policy Names are now limited to 100 characters in length (HAS-3777); ○ Fixed an issue where adding Linux publishers to policy using the Bulk Add screen would result in them being added as Windows publishers and Linux clients would not apply them in policy (HAS-3740);
- Fixed an issue where Disk Free and Policy Version columns did not sort correctly on the policies page.

Airlock Change Log v4.8

Released 22nd November 2021

Overview

Airlock Digital v4.8 introduces major Linux improvements, platform performance enhancements and usability enhancements.

NOTE: Upgrading to v4.8 will force a database re-index which may take between five minutes and several hours depending on the size of the database. The web interface and client connectivity will be unavailable until this process is complete. Upon completion, services will be restored automatically.

NOTE: Upgrading to v4.8 introduces a breaking change to REST API keys. Due to the new permission management feature, API keys must be granted the appropriate permissions to continue to operate post upgrade. This is performed via the User Group Management screen in the Airlock Web UI.

- **Linux Publisher Trust:** Files can now be trusted on Linux through publishers, significantly improving the manageability of allowlisting within the Linux ecosystem. Publishers enable patching of systems to occur without requiring policy updates;
- **Linux Driverless Operation:** The Linux Enforcement Agent can now operate in a driverless mode (where supported by the Linux kernel). This enables Airlock Enforcement Agents to continue operation through kernel updates, with no driver updates required. Additionally, the agent can now operate with Linux Secure Boot enabled without requiring manual registration of signing keys on every endpoint;
- **REST API Permission Management:** Airlock now supports the assignment of permissions to API keys within the platform. Enabling API keys to be issued that only support certain functions. This enables API keys to be embedded in third party platforms or scripts while reducing security risk, as the keys can be restricted to their desired level of access;
- **VirusTotal Augment:** Airlock now supports the native viewing of VirusTotal file information from within the file repository page. Simply enter a VirusTotal API key (free or paid) on the Airlock Settings page and click on the VirusTotal File Check button. File information will be displayed natively without leaving the product;
- **Server Activity History (SAH) Export:** From the dashboard SAH information can now be searched and exported in the desired format. Enabling administrators to export audit log information from the product easily;
- **Trusted Execution Summary Logging:** This feature enables customers to log all files executed within their environments, while managing the high level of load typically associated with the activity. This enables administrators to build a repository of every file type supported by Airlock, without handling millions of file executions per day. This feature works by intelligently supressing the repeated execution of trusted files on endpoints over a thirty-day period. This feature was developed to meet new compliance requirements mandated by the Australian Government in the Essential Eight Maturity Model (October 2021);
- **Rebuilt Search:** Search functionality within the platform has been re-written from the ground up, reducing memory utilisation and providing a tenfold increase in search and report export performance;
- **Improved Bulk Add:** Bulk add screen functionality has been improved, including multi-select capability for publishers and a more responsive UI.

Upgrade Instructions:

- Client compatibility is unchanged from the previous release, however to use new features such as Linux Publisher Trust or Linux Driverless Operation agents must be upgraded to v4.8 or newer.

Detailed Changes:

1. Enforcement Agent Windows (4.8.0.0)

New Features

- Trusted Execution Summary Logging;
- Support for the validation of legacy MD5 digital signatures (HAS-3544);
- Support dual signed signatures on files, the agent will now skip the embedded signature if it is found to be invalid and validate the appended signature if present. Previously only embedded signatures of files were used for checking (HAS-3590);
- Achieved 'Certified for Windows' through the Microsoft Hardware Compatibility Program. This is part of Airlock's commitment to quality assurance. Airlock Digital's hardware certification reports can be viewed on the Windows Compatible Products List: https://partner.microsoft.com/en-us/dashboard/hardware/search/cpl
- Windows 11 & Server 2022 operating system support. Previous versions are found to be compatible, however this release adds specific OS version reporting (HAS-3639).

Improvements / Fixes

- Increased the amount of text that can be seen in a Windows 10 / 11 Toast UI Notification (HAS-3427);
- Memory usage of the agent has been reduced when uploading activities to the server (HAS-3401);
- Debug logging now shows memory utilisation and file handle usage to improve troubleshooting (HAS-3449);
- Memory utilisation of the agent has been reduced through improved file parsing (HAS-3610);
- Upon an OTP expiration or revocation, events are now immediately pushed to the server, rather than waiting for the next client check-in improving responsiveness (HAS-3643);
- Fixed an issue where untrusted or blocked files could occur when applying Windows Updates. This issue is rare and could occur if newly patched files are loaded by the system immediately after patch application while the Airlock Enforcement Agent is still processing security catalogs. In this situation a small window may result in the newly patched files being seen as unsigned. The catalog watcher process has been improved to eliminate this occurrence (HAS-3543);
- Implemented code review recommendations and feedback from Airlocks annual independent code audit (HAS-3558);
- Windows Enforcement Agent tray icons have been updated for high resolution displays (HAS-3484);
- Fixed an issue where it is possible to activate an OTP twice if the Airlock Server counter is more than one ahead, caused by multiple code generations server side (HAS-3417);
- Fixed an unexpected service termination when files were parsed that are either corrupt or do not have valid resource sections;
- Fixed an issue where trusted logging events would not be uploaded for cached executions (HAS-3424);

- Fixed an issue where users were unable to copy the last row of data from the notifier to the clipboard in v4.7 agents (HAS-3414);
- Improved certificate chain validation of self-signed files (HAS-3609);
- Fixed a rare race condition where during database updates files could be seen as untrusted (HAS-3395);
- Added a two-minute timeout for the Agent Stop Code entry box. This prevents MSI uninstallations from hanging if the Stop Code is not specified by the administrator and one is applied (HAS-3361);
- Added the ability to enable / disable Root Certificate Updates during Publisher validation for troubleshooting (HAS-3641);
- Fixed an issue where if a file was flagged for deletion upon load, the agent would attempt to calculate the hash values in user mode for a file that no longer exists, resulting in mismatched hashes, the hash values for such calculations are no longer reported and only the SHA-256 kernel mode hash is reported in the file repository (HAS-3314);
- Fixed an issue where Airlock -verify did not recognise the publisher of script files (HAS-3199);
- Fixed a path parsing issue which caused some Windows AppX packages to not be seen as signed, this was observed primarily with Skype on the Windows Store (HAS-3593);
- Resolved a deadlock with Symantec Endpoint Protection & Airlock when PowerShell script control is enabled in Airlock. Investigation showed this was a hierarchy inversion bug in the kernel between the two products. The resolution was to change the driver altitude of the Airlock Enforcement Agent to avoid Symantec double locking files (HAS-3608).

2. Enforcement Agent Linux (4.8.0.0)

New Features

- Publisher Trust;
- Driverless operation (on supported Linux kernels);
- CentOS / RHEL 9.x support (including Stream);
- RHEL 8.5 support;
- Oracle Linux (including v5 Unbreakable Kernel) support;
- Rocky Linux Support.

Improvements / Fixes

- Added the ability to sideload the Linux Enforcement Agent with the AirlockClientAgentConfig.xml files (HAS-3326);
- Fixed an issue where if a file was executed under a parent process file and then the same file was executed under a different parent, it may still be trusted due to file caching (HAS-3497);
- Linux Safe Mode is now updated to operate with the new Publisher Trust feature (HAS-3402).

3. Server (4.8.0.0-Garnett)

New Features

- REST API Permission Management;
- Server Activity History Export;
- VirusTotal Augment integration on repository page.

Improvements / Fixes

- Significant platform uplift to more recent versions of the underlying web server, worker and database components (HAS-3456) (HAS-3578);
- Clients now report the LocalIP of the client to the policy table, renamed old IP Address to Observed IP (HAS-3389);
- Updated Baselines within the product including Windows 11 and new CentOS / RHEL platforms;
- Assembly Reflection Prevention is now enabled by default within policy (HAS-3640);
- Airlock backup error handling is now improved with associated server activity messages (HAS-3405);
- Publisher sorting is now case insensitive (HAS-3416);
- Additional Server Activity Logging has been introduced for greater auditability of editing user groups, downloading clients and modifying policies (HAS-3390);
- Computer listings on the Policy page are now paginated which prevents slow loading when large numbers of clients are installed (HAS-3366);
- All baselines used to display Windows icons even if they were Linux ones, now the correct icons are assigned (HAS-2747);
- Fixed an issue where the Stale Client Status was not implemented in the All Clients View on the policies page (HAS-3042);
- Changed the way policy writes occur when updating policies in the web UI to be more efficient and reduce errors if users browse away from the page during the update process (HAS-3194);
- Compiled HTML (.chm) files are now selected by default when creating a policy, previously it was deselected (HAS-3642);
- Fixed an issue where Stale Clients would not be correctly tagged due to the stale client check job running at the same time as other jobs (HAS-3211);
- Fixed an issue where the Realtime Activity Viewer Screen filters were disconnected, so if you used the text filter, the type filter was no longer functional (HAS-2779);
- The Policy ‘Hostname’ column is now expanded to reduce text wrapping (HAS-3029);
- Added prevention for selection of the incorrect installation directory during server upgrade (HAS-3342);
- Made server file permissions more restrictive (HAS-3298);
- Correctly escaped invalid characters upon XML Export from the File Repository Page (HAS-3369);
- Fixed an issue where Quick Search results may not be displayed within Bulk Add when certain files are searched for (HAS-3370);
- Set the default database execution history retention to 6 months to ensure performant Airlock servers are maintained (HAS-3388);
- Added a warning upon disabling client to server proxy configuration to prevent isolated clients (HAS-3426);
- Fixed an issue where extlogger would use high CPU on a newly installed instance when the execution history database was blank (HAS-3398);
- Fixed an issue where the dot character was treated non literally on the database / path exclusions tester, being used as a wildcard (HAS-3515);
- Searching for OTP – ID “Self Service” in the search functionality causes an error (HAS-3545);
- Using a single wildcard on Linux paths on the path exclusion tester matched the rest of the string incorrectly, being treated as a double wildcard (HAS-3546);
- Fixed an issue where path characters in rules were not treated literally in the UI, which may cause issues upon editing or deletion of path rules (this did not impact the path rules processed by agents (HAS-3607);

- Added the ability to send a ‘Test Email’ to validate email configuration of the server (HAS-3598);
- Fixed an issue where upon re-vising the publisher ‘group tree’ window on the bulk add screen the group would show selected, however clicking add would prompt the user to select a group;
- Fixed an issue where users with the view_otp permission could generate OTP codes if they also had the view_policies permission, this was fixed to ensure the create_otp role is required to generate OTP codes;
- Fixed an issue where if a new file was seen for the first time, while an OTP code was active, it would not be shown in the ‘New Files Seen’ window in the dashboard;
- Fixed an issue where if the client check in timer is modified, there could be a mismatch of the client online status between a policy group and the ‘all clients’ view on the policies page;
- Usability improvements to the Bulk Add screen (HAS-3612-15, HAS-3619-3623);
- Fixed an issue where the parent process column would not be populated for scheduled searches;
- Added the Microsoft Recommended driver block rules as a blocklisting package;
- Updated the Microsoft Recommended Block Rules to the latest version, including an updated changes block rule package. These updated packages must be imported manually into policy and will not change any existing policies automatically.

4. Baseline Builder Linux (4.8.0.0)

Improvements / Fixes

- Added support for the capture of Shared Object (.so) files during baseline capture;
- Added publisher support.

5. Relay Agent (4.8.0.0)

Improvements / Fixes

- Added the forwarding of Local IP Address information from v4.8 Enforcement Agents.

6. Application Capture Agent (4.8.0.0)

Improvements / Fixes

- Added a new feature that enables Application Captures to include only file loads, file writes or both within a capture. This enables the capture of Applications that are more ‘specific’ to the Application itself (HAS-3380);
- Improved filtering of file writes where the file has not been fully written to disk at the time of capture, resulting in some files being captured twice, once with incorrect hash value and once with the correct value (HAS-3447).

7. Baseline Builder (4.8.0.0)

Improvements / Fixes

- Added support for the capture of .psm1 & .chm files to provide file parity with the Airlock Enforcement Agent;
- Implemented code review recommendations and feedback from Airlocks annual independent code audit (HAS-3558).

Airlock Change Log v4.7.5

Released 11th October 2021

Overview

This is a Windows Enforcement Agent only release fixing an issue impacting a subset of customers. Other improvements and updates will be included in the upcoming v4.8 release.

NOTE: Due to certificate signing changes mandated by Microsoft and the CABForum, Airlock Digital can no longer sign drivers and executables with SHA-1 code. The v4.7.5 agent will no longer install on certain editions of legacy windows without the appropriate security patches applied, please see: https://support.airlockdigital.com/support/solutions/articles/9000204448-unable-to-install-airlock-enforcement-agent-due-to-missing-sha-2-code-signing-updates

Detailed Changes:

1. Enforcement Agent Windows (v4.7.5.0)

Improvements / Fixes

- Fixed a BSOD that can occur due to memory corruption when reading the kernel using noncached I/O. This issue only impacts Windows v4.7.x agents in specific circumstances, such as viewing machine properties within Hyper-V. (HAS-3343);
- Fixed an issue where process protection would not be correctly applied on Windows 7 x86 agents (HAS-3567).

Airlock Change Log v4.7.4

Released 12th August 2021

Overview

This incremental release Airlock v4.7.4 is a bugfix release with one new Window client version. Customers not impacted by the below issues do not need to upgrade to this release.

NOTE: Due to certificate signing changes mandated by Microsoft and the CABForum, Airlock Digital can no longer sign drivers and executables with SHA-1 code. This may impact the ability for Airlock to run on legacy platforms that do not have the appropriate patches installed, please see the following article for further information: https://support.airlockdigital.com/support/solutions/articles/9000204448-unable-to-install-airlock-enforcement-agent-due-to-missing-sha-2-code-signing-updates

Detailed Changes:

1. Server (4.7.4.0-Gasol)

New Features

- Added a new REST API endpoint called /v1/agent/config which enables the download of Enforcement Agent XML configurations (HAS-3036).

Improvements / Fixes

- Fixed an issue where if you use the ‘text’ filter on the Realtime Activity Viewer screen the ‘type’ filter is no longer functional (HAS-2779);
- Fixed an environment error where SAML logins would periodically stop functioning and require an Airlock service restart to restore login functionality (HAS-2657);
- Fixed an issue where the group details for a file execution could be shown incorrectly on the Activity Viewer page (HAS-3362);
- Fixed an issue where offline installations on CentOS / RHEL 8.2+ would fail with an image pull error. The installer now caches the local pod images required for offline installation (HAS-3358);
- Expanded the policy table ‘hostname’ column to reduce text wrapping of computer rows (HAS-3029);
- Fixed an issue where specifying a static date range on search could result in a search exception (HAS-3098).

2. Enforcement Agent Windows (v4.7.4.0)

Improvements / Fixes

- Fixed an issue where file exceptions may occur even when the publisher of a file is trusted and trusted process rules are in use within policy. This only impacts the Airlock Enforcement Agent v4.7.3. Please see the following KB article for more information regarding this issue and workarounds (if required): https://support.airlockdigital.com/support/solutions/articles/9000205292-file-exceptions-occur-even-when-the-publisher-of-a-file-is-trusted-and-trusted-process-rules-are-in-use (HAS-3376);
- Added interoperability with Forcepoint DLP / Forcepoint One & LanDesk Software Monitor.

Airlock Change Log v4.7.3

Released 20th July 2021

Overview

This incremental release Airlock v4.7.3 is a bugfix release focusing on system stability and performance optimisation.

NOTE: Due to certificate signing changes mandated by Microsoft and the CABForum, Airlock Digital can no longer sign drivers and executables with SHA-1 code. This may impact the ability for Airlock to run on legacy platforms that do not have the appropriate patches installed, please see the following article for further information: https://support.airlockdigital.com/support/solutions/articles/9000204448-unable-to-install-airlock-enforcement-agent-due-to-missing-sha-2-code-signing-updates

NOTE: CentOS / RHEL 8.0, 8.1 & 8.2 support has been deprecated. Before updating to this release, please ensure updates are performed on the Airlock Digital Server.

Detailed Changes:

1. Server (4.7.3.0-Chandler)

Improvements / Fixes

- Fixed an issue where users could see all enforcement agents in the ‘all clients’ view, including the clients in groups they did not have permissions to visibly see in the policy tree (HAS-3291);
- Fixed a rare issue where path rules could end up double escaped in client policy when clients communicate via a relay agent. This resulted in clients not applying path rules correctly. This was seen to occur in around 1 in 5000 policy generations and is fixed by generating a new policy (HAS-3293);
- Change the way policy rules were written in the UI to improve reliability on policy update to use bulk database jobs instead of single writes per rule (HAS-3194);
- Fixed an extlogger crash upon first run when configuring Splunk as an external logger for the first time (HAS-3189);
- Modified the time of a scheduled ‘mark stale clients’ job to avoid conflicts with other jobs in the system (HAS-3292);
- Fixed an issue where upon updating the server to CentOS / RHEL 8.4 with the latest security updates, the application would become unreachable upon reboot of the system;
- Changed the Publisher Popout Window on the Bulk-Add screen to be open by default (HAS-3026).

2. Enforcement Agent Windows (v4.7.3.0)

Improvements / Fixes

- Improved the interoperability of the agent when installed alongside other Anti-Virus solutions, by implementing native retrieval of file version information, rather than relying on a Windows API to retrieve the information (HAS-3268);
- Fixed an issue when calling the -verify switch where null information is returned for script file types (HAS-3199), thank you to Kien Tran for the report;
- Added interoperability for the FireEye Endpoint Agent (HAS-3284);
- Added interoperability for Elastic Endgame (HAS-3188);

- Disable retrieval of certificate information for temporary PowerShell script files, cmd, bat and .NET Native Image cache files to improve performance (HAS-3266) (HAS-3265) (HAS-3260);
- Improved performance and interoperability of the agent by removing the need for catalog signed file publisher validation at runtime (HAS-3294);
- Fixed a regression where the support commands -clear-publishers and -rebuild-catalogs would not be respected (HAS-3296);
- Fixed a Blocklist Metadata file check issue where rules which contain multiple parent processes may only have the first parent process evaluated in the rule, if the same file was launched from multiple parent processes within the agent cache validity window. (HAS-3295).

3. Enforcement Agent Linux (v4.7.3.0)

Improvements / Fixes

- Added the checking of Shared Libraries (.so) files on Linux as they were previously not seen by the agent. NOTE: This may result in customers seeing additional untrusted executions after upgrading to this release (HAS-3241);
- Disabled the logging of trusted (debug level) logging by default, airlock.log file sizes are now significantly smaller (HAS-3144);
- Fixed an incompatibility with CentOS 8.4, CentOS Stream and RHEL 8.4 with kernel 4.18.0-305 causing a system hang (HAS-3245);
- Prevent file executions greater than 100GB in size to avoid a kernel timeout on file checking (HAS-3181).

Airlock Change Log v4.7.2

Released 28th May 2021

Overview

This incremental release Airlock v4.7.2 is a bugfix release focusing on system stability. It is recommended for customers that are impacted by one or more of the issues listed in this version. Customers that are not experiencing any of the following issues do not need to update to this release.

Detailed Changes:

1. Server (4.7.2.0-Howard)

Improvements / Fixes

- Disabled the automatic dashboard and activity viewer refresh based on user feedback (HAS-3024);
- Set the 'Include Child Groups' dashboard filter to default yes, rather than no (HAS-3028);
- Rebuilt the External Logging feature to use less CPU and send events more reliably (HAS-3003);
- Fixed an issue where the External Logging feature in Airlock could send more events than is reported by the dashboard (HAS-3003);
- Added the option to send HTTPS events to Splunk with Certificate Validation Disabled, to fix an issue introduced in v4.7.0 where HTTPS event sending would stop functioning (HAS-2993);
- Added the target filename in the response header from /v1/agent/download to allow customers to appropriately name the file on disk which is returned from the REST API endpoint (HAS-3035);
- Fixed an issue where Linux files would not be displayed in the Application Capture file browser when imported from an Application Capture XML (HAS-3025).

2. Enforcement Agent Windows (4.7.2.0)

Improvements / Fixes

- Improved the interoperability of the agent when installed alongside other Anti-Virus solutions, by changing the method of file version retrieval on Windows Vista and newer versions of Windows. The version information is now retrieved using the 'FILE_VER_GET_PREFETECHED' flag to avoid kernel contention and overall reduces the chance of a deadlock (HAS-3060);
- Fixed a deadlock when installed with Cisco AMP Endpoint Protection (HAS-3059);
- Fixed an issue in the Notifier Launcher which could cause a deadlock on Windows Server based RDS systems with multiple user sessions upon login. This issue was caused by notifier loading too quickly upon login when the users shell was not yet available. This issue can be worked around by disabling the Notifier Launcher on older releases of the enforcement agent as stated in https://support.airlockdigital.com/a/solutions/articles/9000199086 (HAS-3010);
- Fixed a rare BSOD that may occur when the Airlock Enforcement Agent is installed with Sophos Anti-Virus when Sophos savonaccess.sys tries to read a file from kernel mode (HAS-2994);

- Fixed an issue where double wildcard regex would not apply. For example, the following rule '****/git/****' would not be respected by the client, due to a regex conversion error. Rules with a single instance of double wildcarding, for example C:\*\git** function correctly (HAS-3079);
- Fixed an issue where the Airlock Enforcement Agent could not be installed on systems without a C:\ drive (HAS-3014);
- Fixed an issue where the Airlock Enforcement Agent could hang on filter unload during uninstallation where removable drives are used in the system, requiring a reboot of the machine to complete uninstall (the agent will stop running upon the uninstallation commencement). Airlock Agents v4.7.0 & v4.7.1 are the versions affected by this issue (HAS-3031);
- Added a right click option in the notifier to copy the file hash to the clipboard only, rather than the full file details to improve usability.

3. Enforcement Agent Linux (4.7.2.0)

Improvements / Fixes

- Fixed an issue where historical events could be repeatedly uploaded by the client to the server due to a database lock after a bulk activity upload (HAS-3069);
- Fixed an issue where the agent may report thread exhaustion if over 10,000 file executions were performed within 10 minutes (HAS-3072);
- Added Online / Offline status awareness to the agent, rather than the agent attempting to upload activities and failing when network connectivity was not available (HAS-3080);
- Fixed an issue where double wildcard regex would not apply. For example, the following rule '****/git/****' would not be respected by the client, due to a regex conversion error. Rules with a single instance of double wildcarding, for example C:\*\git** function correctly (HAS-3079).

Airlock Change Log v4.7.1

Released 19th April 2021

Detailed Changes:

1. Enforcement Agent Windows (4.7.1.0)

Improvements / Fixes

- Fixed a regression in v4.7.0 where OTP codes would no longer persist through a system reboot (HAS-2932);
- Fixed an issue where if a file was audited or blocked as a result of a blocklist path rule, the agent would not correctly retrieve the files path or filename and they would show blank in the notifier. Please note that blocklist metadata rules are unaffected (HAS-2910);
- Added protection against blank blocklist criteria being handled by the enforcement agent for additional safety (HAS-2925).

2. Enforcement Agent Linux (4.7.1.0)

Improvements / Fixes

- Fixed an issue where if a proxy is configured in policy and the proxy is unavailable for connection, the client will fall back to direct communication using the stored IP address, rather than attempting direct connection via the server DNS name first (HAS-2927).

3. Relay Agent (4.7.1.0)

Improvements / Fixes

- Fixed an issue where if the Relay Agent could not contact the server upon the initial discovery, the agent would require a service restart before attempting to connect again (HAS-2924).

4. Server (4.7.1.0-Garnett)

Improvements / Fixes

- Fixed an issue where emailed Save Searches could be empty or miss results due to a race condition in report creation and sending (HAS-2887);
- Re-mapped the edit_clients permission to allow the deletion of computers from policy (previously the permission was tied to edit_policies which was incorrect) (HAS-2944);
- Prevent Empty Blocklist Path Rules from being created (HAS-2940).

Airlock Change Log v4.7

Released 1st March 2021

Overview

Airlock Digital v4.7 introduces user centric control and adds further extensibility to the platform.

- **Codeless Self Service:** Users can now activate OTP Mode from the enforcement agent, without the need to handle an OTP Code. This activation can be permitted for all users on an endpoint, or offered to select users dynamically, depending on what Domain Security Group they are a member of;
- **Blocklisting Enhancements:** Blocklists now support up to five criteria, enabling granular control over a file's execution to support advanced use cases. Additional Blocklist criteria have also been added to control a files execution based on Domain Security Group (controlling certain users' ability to execute a file) and the Operating System version a file is being executed on;
- **SIEM Logging via REST API:** Airlock Cloud customers can now 'pull' SIEM logs from the cloud via the REST API, removing the need to expose ports to the internet to receive logs or the use of other custom solutions;
- **Compiled HTML Script (.chm) support:** Airlock now supports the blocking of .chm files.

Upgrade Instructions:

- Client compatibility is unchanged from the previous release, however to use new features such as Codeless Self Service or the new Blocklisting Enhancements you must upgrade agents to v4.7 or newer;
- Note: Relay Agents, Baseline Builder & Application Capture Agents are unchanged for this release and do not need to be upgraded to be compatible.

Detailed Changes:

1. Enforcement Agent Windows (4.7.0.0)

New Features

- Codeless Self Service;
- Ability to blocklist files by a user's group membership;
- Ability to blocklist files by Operating System version;
- Compiled HTML Script Control (.chm) support;
- Ability to revoke an OTP from the command line.

Improvements / Fixes

- Added a more verbose level of debug logging to better troubleshoot issues when they arise;
- Fixed a system deadlock during user login when installed with Symantec Endpoint Protection and greater than five users are already logged into the system (HAS-1904);
- Removed TLS v1.3 from the supported communication protocols due to communication issues in some enterprise environments, TLS v1.2 is exclusively used (HAS-2756);
- Added communication support for Airlock's upcoming multi-tenant cloud platform (HAS-2351);
- Fixed an issue where the Enforcement Agent could not be stopped or uninstalled on Windows XP / Server 2003 if the agent was in 'discovery' without manually terminating the running Airlock process (HAS-2826).

2. Enforcement Agent Linux (4.7.0.0)

New Features

- Codeless Self Service.

Improvements / Fixes

- Fixed an issue where an Enforcement Agent database lock may cause missed event uploads to the Airlock server, additionally resulting in thread exhaustion if sustained heavy load occurs (HAS-2533 / HAS-2824);
- Fixed an issue where the Linux Enforcement Agent would not fall back to direct communication if a proxy server was configured and the proxy is unavailable (HAS-2535);
- Added the ability to disable debug mode by specifying airlock -debug on / off at a bash shell.
- Proactive security optimisations in the agent codebase.

3. Server (4.7.0.0-Garnett)

New Features

- Codeless Self Service;
- Blocklisting now supports up to five criteria including new Domain Security Group and Operating System version options;
- Automatic date internationalisation to switch between DD/MM/YYYY & MM/DD/YYYY formats;
- Added the ability to remove files from Baselines and Application Captures from the Repository page.

Improvements / Fixes

- Added a ‘group’ column to the All Clients view on the Policies tab;
- Fixed an issue where the child policies filter would not correctly show events on the Dashboard (HAS-2360);
- Renamed the existing ‘Self Service’ to ‘Mobile OTP’ to reflect its function more accurately (HAS-2512);
- Fixed an issue where relay agent security certificates were not updated if the Relay Agent was renamed, this resulted in downstream clients getting an invalid security certificate and failing to communicate (HAS-2508);
- Replaced the Airlock SSH menu with a more user friendly one, preventing accidental clicks which could result in the server shutting down or being rebooted (HAS-2358);
- Fixed an issue where if you sent the /v1/application/new REST endpoint two requests it would fail to respond (HAS-2518);
- Fixed an issue where the /v1/hash/application/remove REST endpoint only removes a single hash from the application, even if multiple hash values are specified (HAS-2525);
- Fixed an issue where the /v1/application/delete REST endpoint would throw an exception if a malformed request was received (HAS-2524);
- Fixed an issue where the /v1/hash/application/add REST endpoint would respond with two errors if the request was not correctly formed (HAS-2523);
- Fixed an issue where the /v1/baseline/reference REST endpoint responded with an ‘internal server error’ when called (HAS-2522);

- Fixed an issue where the /v1/license/set REST endpoint would blank the license details if an existing licence was already set within the product (HAS-2526);
- Fixed an issue where the /v1/agent/download REST endpoint would return no content if a Linux agent was requested (HAS-2534);
- Fixed an issue where the /v1/application/delete REST endpoint would return incomplete parameters even when a correctly formed request was sent (HAS-2562);
- Fixed an issue where the /v1/group/path/add and /v1/group/path/remove REST endpoint would sanitise Linux path forward slashes resulting in paths unable to be added or removed (HAS-2577);
- Fixed an issue where groups created via the REST API don't appear for users until the group is re-saved in the UI (HAS-2573);
- Fixed an issue where the group tree depth restriction was not enforced via the REST API. It was nice to see unlimited groups, however the restriction removal is not yet ready for production (HAS-2574);
- Disabled TLS v1.3 support for all endpoints to prevent rare communication issues in some enterprise networks caused by third party networking equipment;
- Disabled TLS 1.0 and TLS 1.1 on the REST API endpoint;
- Deprecated two CBC Cipher Suites to further improve security on the REST API / Client API;
- Fixed an issue where OTP Codes were unable to be issued for an endpoint after filter selection and deselection on the policy page, without a page refresh (HAS-2527);
- Fixed an issue where if webpage content was paged into the Blocklist Import Hashes window it would break rendering on the page (HAS-2529);
- Fixed an issue where the free disk space warning would not accurately display the amount of free disk remaining;
- Fixed a non-fatal ClientAPI panic which occurred when clients failed to report their version when checking into the 'Unmanaged' policy group (HAS-2543);
- Fixed an issue where importing path rules via an XML could result in double rules being populated in the UI (HAS-2538);
- Fixed an issue where importing path rules via an XML could only be performed once per page refresh (HAS-2563);
- Fixed an issue where if a computer failed to report its last check-in date it would prevent the policies group from being displayed (HAS-2532);
- Fixed an issue where if bracket ( ) characters were used in the Activity Viewer or Blocklist path rule testers, they would not be treated literally, leading to incorrect results (HAS-2549);
- Fixed an issue where on Chromium based browsers v87+ would make the login page render incorrectly with the box floating on the top of the screen (HAS-2554);
- Fixed rare GenerateDB errors that could prevent databases from successfully generating (HAS-2576);
- Fixed an issue where installing Airlock on CentOS / RHEL 8.2 on machines hosted in Microsoft Azure would render the machine inoperable on the next reboot. This was caused by a grub bootloader bug which was fixed in RHEL 8.3. Workarounds have been implemented to disable transparent huge paging at software start, rather than by editing the grub bootloader (HAS-2608);
- Fixed an issue where Airlock services could become available after a Podman container restart on CentOS / RHEL 8.x systems (HAS-2757);
- Fixed an issue where if an Enforcement Agent uploaded a 0 bytes filesize it could cause the repository page to not render correctly (HAS-2604);
- The policy group filter dropdown on the main dashboard is now sorted alphabetically (HAS-2621);

- Activity Viewer file links when clicked now open in a new browser tab, to prevent the current view from being lost (HAS-2623);
- Clarified the message displayed when a file is added to an application capture from the repository page, to make it clear that only the single file is being added by hash, rather than by filename (HAS-2624);
- Fixed a number of regular expression errors that could occur on the dashboard (HAS-2627);
- SAML Email assertion matching is now case insensitive, preventing failed logins due to mismatch capitalisation (HAS-2630);
- SAML failed login assertions are now displayed in the Server Activity History, improving the ability to troubleshoot login failures (HAS-2629);
- SAML logging is now piped to a log file on disk to assist SAML troubleshooting (HAS-2631);
- Updated terminology throughout the product, most notably all references to ‘Whitelisting’ or ‘Whitelist’ have been replaced with ‘Allowlisting’ or ‘Allowlist’ (HAS-2633);
- Fixed an issue where uploading a new version of the Linux Enforcement Agent via the web interface would fail;
- Fixed an issue where clients would suddenly be redirected to the Unmanaged group due to an invalid license, even if a valid license was applied. This was due to a parsing error of the endpoint count when the license was updated using certain methods (HAS-2669);
- Fixed an authenticated stored XSS vulnerability on the repositories screen (HAS-2678);
- Fixed an issue where if you put in certain XML invalid characters into the proxy username or password fields in policy, it would malform the Enforcement Agent XML configuration (HAS-2681);
- Fixed an issue where characters such as apostrophes were sanitised from user e-mail addresses, preventing logins for some users (HAS-2674);
- Display a warning if a blocklist is moved directly from disabled to enforced, without going through audit first (HAS-2676);
- The Quick Search ‘File – First Seen’ column is now replaced with ‘File – Status’ which is more useful for finding potentially malicious files (HAS-2638);
- Display a Linux logo for Linux Baselines, rather than displaying Windows logos on every Baseline (HAS-2747);
- Fixed an issue if a Mobile OTP Code was revoked on a client that no longer is registered in the Airlock Server an error would occur (HAS-2776);
- Fixed an issue where the Realtime Activity viewer would sort events by the Event Time rather than the Received Time which could result in events not being seen (HAS-2793);
- Fixed an issue where the clients Online / Offline count in the ‘All Clients’ view on the Policies tab display zero (HAS-2800).

4. Baseline Builder Linux (4.7.0.0)

Improvements / Fixes

- Fixed an issue where if the Baseline Builder was installed on the same machine as the Enforcement Agent and the Enforcement Agent was uninstalled, it will also remove Baseline Builder related files, preventing future online captures.

5. Relay Agent (4.7.0.0)

Improvements / Fixes

- Deprecated two CBC Cipher Suites to further improve communication security;
- Disabled TLS v1.3 support to prevent rare communication issues in some enterprise networks caused by third party networking equipment

Airlock Change Log v4.6

Released 2nd October 2020 (Updated 7th December 2020)

NOTE: There are breaking changes regarding the way Windows Agents are deployed. Before deploying v4.6 agents these changes must be understood or installations / upgrades will fail. Please read the 'Windows Enforcement Agent Installation Changes' document for information.

In the event deployments are performed incorrectly and installation issues occur, please contact Airlock Support at https://support.airlockdigital.com for assistance.

Overview

Airlock Digital v4.6 brings greater security, usability and adds additional enterprise features.

- **SAML Authentication Support:** Administrators can now use a SAML identity provider to authenticate against the Airlock server;
- **Global 2-Step Verification Enforcement:** Administrators can set a global policy to enforce 2-Step Verification for all users authenticating against the Airlock server for local and LDAP logins;
- **Multiple Relay Agent Support:** Four relay agents can now be assigned to a single Communication List in both a load balanced and priority communication modes. This enables greater scalability and fault tolerance;
- **User Based Blocklisting:** Blocklists now support username as a criteria, allowing files to be prevented or allowed to execute based on the logged in user;
- **Linux Automatic Kernel Reload:** Linux enforcement agents can now automatically survive kernel updates, with no intervention required;
- **Assembly Reflection Prevention:** The enforcement agent can now block reflected assemblies, increasing the level of security provided by the Airlock Enforcement agent.

Upgrade Instructions:

- All users will be prompted to reset their credentials (when local logins are used) post upgrade to v4.6;
- Client compatibility is unchanged from the previous releases, however to use new features such as Assembly Reflection Prevention or User Based Blocklisting you must upgrade agents to v4.6.1 or newer;
- Relay agents must be updated to v4.6.0.0 (if applicable) before upgrading clients to v4.6.1, otherwise policy download issues may occur;

Detailed Changes:

1. Enforcement Agent Windows (4.6.5.0)

New Features

- Assembly reflection prevention;
- Ability to Blocklist files by the username that executed them;
- CrowdStrike proxy detection and fallback;
- Ability to revoke an active OTP Code from the notifier;
- SHA-512 certificate validation support;
- Windows Script Component file support.

Improvements / Fixes

- Completely re-worked the way certificate validation of files is performed in the agent to use lower level Windows API's. This improves performance and also interoperability with other applications performing certificate checking at the same time (HAS-1653);
- File executions that occur when an OTP code is active now upload much faster, if an OTP code is revoked files will be queued for upload immediately;
- Fixed an issue where the client did not correctly upload the 'Original Filename' to the file repository (HAS-1984);
- The right to left Unicode character is now sanitised from all input, preventing attackers from confusing administrators (HAS-2072);
- Fixed OpenJDK not being detected as a Java process, resulting in .jar files not being enforced (HAS-1990);
- Fixed a deadlock when Entrust Entelligence Security Provider is installed on the same system as the Airlock Enforcement Agent (HAS-1653);
- Fixed an issue where some process exit events could be missed, resulting in some command lines for processes not being captured (HAS-1919);
- Fixed an issue where parent processes may not correctly be retrieved (non-existent) when files are launched from a parent in the SYSTEM security context (HAS-2185);
- Prevented notifier high memory usage by limiting the number of events displayed to 5000 at any time (HAS-2183);
- Added interoperability with a number of commercial anti-virus providers such as Kaspersky to prevent system instability;
- Removed reboot prompts from the agent installer as a reboot is not required (HAS-2290);
- Improved protection for Airlock application files to prevent tampering (HAS-2305);
- Fixed a rare system hang where during Safe Mode or certain OTP Database operations the Airlock database read could be null. Added additional handling to prevent this condition;
- Fixed an issue where file version comparisons would be incorrectly interpreted when enforcing Blocklist rules, resulting in possible incorrect file blocks (v4.6.3);
- Fixed a BSOD with exception SYSTEM_THREAD_EXCEPTION_NOT_HANDLED_M when installed with Symantec Endpoint Protection on the same host. This BSOD occurs rarely when Symantec Endpoint Protection denies read access to the Airlock kernel driver (HAS-2396) (v4.6.4);
- Fixed an AppCrash after the initial installation and during discovery phase, if a system wide WinHTTP proxy is configured. This could prevent an enforcement agent from successfully discovering the server after installation (v4.6.4);
- Fixed a non-critical AppCrash if Airlock -stop is called during the upgrade process from a previous version of Airlock. This crash has no impact as the Airlock process is already closed (v4.6.4);
- Fixed a deadlock which may occur in the event that the Airlock Enforcement Agent is unable to perform a Certificate Revocation Lookup on a catalog signed file (v4.6.5);
- Modified the SysPrepHostname registry key to a 'contains' match rather than an 'exact' match to support multi-step build SOE build processes (v4.6.5).

2. Enforcement Agent Linux (4.6.1.0)

New Features

- Linux Automatic kernel reload;
- Linux secure boot support;
- OTP Codes now remain active through system reboots.

3. Server (4.6.0.0-Camby)

New Features

- SAML Authentication Support;
- Global 2-Step Verification Enforcement;
- Multiple Relay Agent Support;
- RHEL / CentOS 8.1 & 8.2 support (when the podman dependency is installed);
- Computer list export;
- Sumo logic & local logging support.

Improvements / Fixes

- Added an e-mail 'domain' field to the e-mail configuration screen to allow users control over the e-mail 'return-path' (HAS-1920);
- LDAP Users can now have 2-Step Verification enforced (HAS-1807);
- Fixed an issue where renaming a policy group results in the dashboard no longer seeing historical events (HAS-1934);
- Fixed an issue where Baselines could be uploaded to the server, from a registered Baseline Builder even if the credentials supplied were invalid (HAS-1713);
- Fixed an issue where some characters were not being treated literally in the publisher filter, resulting in incorrect results being returned (HAS-1999);
- Renamed Blacklists to Blocklists throughout the product (HAS-1915);
- Details of service crashes / panics are now written to each service's respective log file (HAS-1810);
- Fixed an issue where the 'Restart All Services' function would not restart the services (HAS-2077);
- Fixed an issue where exporting a CSV from a scheduled search would return blank (HAS-2140);
- Fixed a 2-Step Verification bypass for LDAP authenticated users where if usernames were provided in certain formats the 2-Step Verification requirements may not be enforced (HAS-2193);
- Airlock MSI installers are no longer signed, due to a patch released by Microsoft in August 2020, under CVE-2020-1464 where authenticode signature checking was modified and Airlock installers were seen as having an invalid digital signature. The Airlock server now automatically trusts installers by their hash value upon download, instead of relying on digital signatures (HAS-2191);
- Added new REST API endpoints to export Baselines, Applications and Blocklist packages (HAS-2212);
- Updated the /v1/agent/download REST API endpoint to allow downloading of Linux installers (HAS-2233);
- Fixed an issue where usernames in e-mail address format could cause login issues when the account was protected by 2-Step Verification (HAS-2266);
- Fixed an issue where disabling proxy authentication, would not remove the associated username and password in the database, which may cause a proxy settings 'mismatch' warning when moving computers between groups (HAS-2284);
- Fixed an issue where group renames could revert to old names when multiple user sessions are open, the group is renamed in one and then a setting is changed in the other (HAS-2283);
- Added a computer filter to the Self-Service Management page to allow for computers to be found faster when large numbers of Self-Service OTP codes have been issued (HAS-2297);
- Fixed an authenticated XSS issue on the Self-Service Management page (HAS-2298);

- Fixed a character sanitisation issue where if a tab character was entered into a policy rule it would cause a ‘invalid character’ error on downstream relay agents (HAS-2342);
- Fixed an issue where the path rule tester would not display results (HAS-2352).

4. Relay Agent (4.6.0.0)

New Features

- Relay Agents can now operate behind a third-party network load balancer;
- Relay Agents now support a -ReSync flag for troubleshooting.

5. Baseline Builder (4.6.0.0)

New Features

- The Baseline Builder now supports online capture via a proxy server;

Improvements / Fixes

- Online baseline captures can now be performed via the command line (HAS-1707).

6. Application Capture (4.6.0.0)

New Features

- The Application Capture Agent now supports online capture via a proxy server.

Improvements / Fixes

- Fixed an issue where Application Captures would fail to upload when the FQDN of the Airlock Server was unable to be resolved and communication was relying on the fallback IP address (HAS-2089).

Airlock Change Log v4.5.1 (rapid release)

Released 17th July 2020

Overview

This incremental release of Airlock v4.5.1 fixes issues in the Airlock server and also updates the Linux and Windows Enforcement Agents with stability fixes and minor improvements.

1. Server (4.5.1-Bryant)

Improvements / Fixes

- Fixed an issue where users with Two-Step Verification enabled would be unable to see their user groups assignments on some logins;
- Fixed an issue where CSV, XML and PDF reports would not correctly send via e-mail and would log a failed job error in the resque log;
- Fixed an issue on the REST API where reference baselines would not correctly import;
- Fixed an issue where OTP codes were not correctly revoked upon request;
- Fixed an issue where if a client was updated from v4.1 -> v4.5, the upgraded agent would not update policies until a new policy database was generated (through making a policy change), the update logic will now correctly handle upgraded clients;
- Fixed an issue where trusted logging would not correctly log events to the server when path rules were used;
- Fixed an issue where if a server was connected to LDAP for authentication and a blank password was entered, the user may be permitted login when Anonymous Simple Binds are enabled;
- Fixed an issue where directory separators in paths are not correctly handled in blacklisting, resulting in the path not being respected;
- Fixed an issue where self-modifying account details could result in user permissions being revoked from the users account; and
- Downloaded Linux clients now have no spaces in the filename, making installations easier;
- Fixed an issue where client Self-Service OTP secrets may fail to synchronise resulting in invalid Self-Service OTP codes on clients;
- Fixed an issue where Linux file paths may not be correctly displayed in the application capture file browser.

2. Enforcement Agent Windows (4.5.13)

New Features

- Multiple criteria support for Blacklist Parent Processes & Paths. Simply specify multiple conditions in a criteria separated by a pipe character, for example explorer.exe|powershell.exe.

Improvements / Fixes

- Fixed a rare notifier connection loop which caused TCP exhaustion and high memory usage in Airlock & Notifier;
- Fixed an unexpected service termination, which may occur if Airlock accesses the database during policy update operations;
- Masked text entered into the Airlock ASC entry box;
- Fixed blacklist rule caching where if a blacklist execution was triggered, the result could be remembered for the cache duration. This can result in the same file being handled by the same rule, even when conditions change;

- Fixed an issue where the client communication thread may get stuck in poor or heavily congested network conditions, the client now has a timeout on all communication sockets;
- Fixed a rare single thread high CPU condition upon launch of Airlock;
- Fixed a string comparison issue when using the 'product version' less than or greater than blacklisting criteria, which could cause the resulting blacklisting match to be incorrect;
- Added interoperability improvements with Symantec Endpoint Protection;
- Fixed a timing bug, where if the agent was disconnected from the network between the client check-in function and then subsequently during the event upload function, the events may become stuck until the client is next restarted or a new file is seen;
- Fixed an issue where usernames may appear as a single '@' character in the web interface instead of displaying the correct username;
- Fixed a high CPU issue in the Notifier Launcher where the airlock.exe process may use high CPU on a single thread. This could occur when a user logs in to the system while another interactive session is in progress and the notifier launcher is used (rather than Windows launching the notifier component upon login). Fixed a logic issue in the agent which was presenting the Notifier Launcher from successfully connecting to the main airlock.exe component (v4.5.12);
- Fixed an issue where clients could get stuck in Safe Mode if an invalid baseline was applied, the client would require a restart or group move to exit this condition;
- Fixed an issue where if 'Do not process the legacy run one list' is disabled in group policy, the Notifier UI would not launch correctly (v4.5.12);
- Fixed an unexpected service termination in the agent if a blacklist rule comparison was made where the product version contains a combination of lexographic and integer matching methods. Opening a file containing the same parameters triggers an agent crash (v4.5.13);
- Fixed an issue where the agent may fail to check-in in the event the Airlock license is exceeded, requiring a re-seat of the server license to resolve (v4.5.13).

3. Enforcement Agent Linux (4.5.7.0)

New Features

- Status switch that responds with what enforcement mode the agent is operating in. Simply type 'airlock -status' in a bash shell. This feature will also print the time left on an OTP code if there is one currently active;
- Safe Mode for Linux, prevents the client from loading potentially unsafe policies on the system if core system binaries are not included in the whitelist when moving to enforcement mode;
- Reload switch that reinstalls the driver after a kernel update has been performed, simply type 'airlock -reload' after a kernel update to restore operation;
- Secure Boot Support for CentOS / RHEL 7.x, the driver is now digitally signed and includes a public key;
- Added support for communication via the Airlock Relay agent;
- Support for CentOS / RHEL 6.x

Improvements / Fixes

- Fixed a deadlock condition when Linux systems booted into RunLevel 5;
- Improved the stability and performance of the driver;
- Fixed an issue where OTP codes may not successfully activate;
- Agent upgrade without uninstall / re-install is now supported (from v4.5.4 onwards);
- Fixed a crash during policy validation failure;

- Fixed an issue where file repository entries may not upload correctly;
- Fixed an issue where policy diffs may not apply correctly leading to some files not being trusted, even though they are in policy;
- Fixed a file cache issue where some files may be reported as untrusted during database changeover when policies are updated;
- Fixed an issue where new file sightings were not correctly uploaded;
- Fixed a crash when the Airlock client applies a blank database due to Safe Mode;
- Added support for the Airlock Relay Agent;
- Fixed an issue where event uploads could be delayed in poor network conditions unless the client saw a new event or was restarted.

Upgrade Instructions

- In order to update the agent from v4.5.3 or less, you must:
    - Uninstall the agent; and
    - Then install the new version of the agent.

4. Relay Agent (4.5.2.0)

New Features

- Alrelay -resync flag, which enables the rebuilding of the Relay Agent database without having to re-install.

Improvements / Fixes

- Fixed an issue where if the v4.5.0 relay agent was connected to an Airlock server, it could trigger the re-generation of OTP codes on behalf of a client. This would cause invalid OTP codes on all client agents connected to the Airlock server globally;
- Fixed an issue where if more than one v4.5.0 relay agent was connected to an Airlock server, it could trigger the re-generation of a newly registered computers OTP codes. Causing invalid OTP codes on the newly registered client;
- Improved the reliability of the relay agent by updating database handling routines;
- Fixed an issue where Linux clients may appear to be registered in a different group to the currently operating policy when talking via a relay agent.

5. Baseline Builder (4.5.1.0)

Improvements / Fixes

- Fixed an issue where the builder may present an ‘Upload Failed: Invalid credentials’ message during Stage 4 of the Online Capture.

Airlock Change Log v4.5

Released March 2020

Overview

Airlock v4.5 improves scalability, adds new policy trust features and initial Linux enforcement agent support. Highlights include:

- **Airlock Enforcement Agent for Linux:** Enables application whitelisting to be performed on Linux hosts using the same workflow as Windows agents;
- **Parent Process Whitelisting:** Whitelist applications based on the parent process which executed them, making whitelisting significantly easier in scenarios such as development;
- **Offline Application Capture:** The Application Capture agent now supports captures of Applications without a server connection, with capture initiation now allowed from the agent side;
- **Group Filtering & Restriction:** Prevent users from seeing and managing computers in certain policy groups;
- **CrowdStrike Falcon Integration:** CrowdStrike customers can now manage and deploy the Airlock agent from within the CrowdStrike Falcon platform;
- **User Permission Groups:** User permission groups can now be used to assign functionality to users within the product. Making management of large user groups significantly easier.

Upgrade Instructions:

- You must follow the instructions in this article to perform the upgrade process, upgrading without these instructions may result in an inability to access your Airlock instance post upgrade: https://support.airlockdigital.com/support/solutions/articles/9000182529-v4-5-group-permission-management-changes
- Client compatibility is unchanged from the previous releases, however to use new features such as Parent Process Whitelisting you must upgrade agents to v4.5.5 or newer;
- Relay agents must be updated to v4.5.0.0 (if applicable) before upgrading clients to v4.5.5, otherwise policy download issues may occur.

Detailed Changes:

1. Enforcement Agent (Windows 4.5.7.0 / Linux 4.5.0.0)

New Features

- Parent Process whitelisting and blacklisting support;
- Linux Agent.

Improvements / Fixes

- Diffing optimisations to further reduce network bandwidth;
- Now you can press ‘Enter’ to click OK after an OTP input;
- Fixed multiple issues which resulted in OTP’s being invalid and not accepted;
- Increased the overall reliability of OTP code usage;
- File cache security is improved with more strict validation;
- Fixed an issue where .MSI files were not correctly enforced;
- Limit notifier to display a maximum of 5000 results, preventing long load times in the event of 5000+ exceptions;

- Improved the file ‘greater than’ and ‘less than’ comparison operators for blacklisting, by detecting when a file is using standard version numbering and comparing numerically rather than using lexicographic comparison;
- The Airlock agent now loads earlier during system boot;
- Fixed an issue where if a v3.x agent is upgraded to v4.x, path rules may be ignored temporarily after installation. This is caused by a database structure mismatch between the v3.x and v4.x clients. The agent now correctly detects this condition and recreates the local database in the correct format;
- Improved the reliability of path and publisher rule processing when updating policies by guarding critical database sections;
- Fixed an issue where if a relay agent is configured and the relay agent is not online at the time of initial agent installation, the agent service may unexpectedly terminate;
- Enforcement Agents can no longer register as an Application Capture agent if installed on the same machine in quick succession with each other;
- Fixed an issue where signed files may be missed and seen as Unsigned when an individual system catalog (.cat file) has entries removed. Note that this update will trigger a catalog database reindex when upgrading from v4.x agents, which may result in a few minutes before enforcement commences upon first installation;
- Fixed unreachable SQL Injections in the Airlock Service (medium vulnerability severity as the injection points were unable to be reached by users). These issues were found during an independent security source code review of the agent;
- Fixed an issue where high CPU usage of the agent occurs when policy group names contain specific strings;
- Fixed an issue where .bat files would not respect the Script Enforcement Mode setting and instead would use the ‘main’ policy enforcement setting;
- Fixed an issue where the ‘OTP Activated’ label may get stuck in Notifier after an OTP has expired;
- Fixed a number of unexpected service termination conditions;
- Fixed an issue where CSV Export from Notifier would stop prematurely if the command line of a process used hidden Unicode characters;
- Fixed an issue where the Agent will detect a database mismatch on client restart, causing a full database definition download to occur;
- Fixed high Non-Paged memory usage due to notifier launcher excessively creating large amounts of file handles;
- You can now customise an installation at install time by placing a ‘AirlockClientAgentConfig.xml’ file in the same folder as the MSI installer. The installer will detect this file when launched and use the file settings for installation;
- The client now has the ability to read ‘Client to Server’ proxy settings stored in the ‘AirlockClientAgentConfig.xml’, this makes client recovery far easier in environments that require proxy configuration for agent communication
- Added the ability to disable the notifier launcher feature for troubleshooting and workloads where the launcher is not required;
- Fixed an issue where 7-day OTP codes may not be accepted on the client computer due to a HOTP algorithm calculation error. The 7-day algorithm code has now been updated to correctly accept 7-day OTP codes.;
- Fixed an issue where MSI installers may fail and present a notification “Notifier.exe is not marked for installation”. This was fixed by removing a MSI custom action that launched the Notifier component upon completion of the installer;
- Fixed a rare issue where a database update could lead to a machine deadlock or unexpected service termination if a blacklist rule check was performed during the same millisecond.

2. Server (4.5.0.0-Bryant)

New Features

- Parent process whitelisting and blacklisting support;
- User permissions can now be grouped;
- Computer groups can now be restricted from being viewed by users;
- Airlock Roadmap is now available from the User Dropdown menu;
- Export TXT function for publishers and path rules;
- You can now filter on parent and child policies in the dashboard;
- Common Event Format (CEF) external logging support;
- New REST API endpoints enabling complete removal of hashes from Airlock;
- CentOS 7.7 & CentOS 8.0 installer support;
- Added more information on the execution history section of the repository page;
- Added Linux Baselines and updated Windows baselines to January 2020;
- You can now right click on Publisher Names in the Bulk Add window and add Publishers directly into policy;
- The server can now support 50% higher density of client agents with the same resource usage;
- All computers view;
- The dashboard now has a month option for filtering criteria.

Improvements / Fixes

- Redesigned the Settings page to be less cluttered;
- Improved user input validation to prevent unintentional whitespace in numerous product locations;
- Removed the 'Show/Hide' filter from the dashboard page, so filters are shown all the time;
- Modal boxes can no longer be dismissed by clicking outside of the modal window (preventing accidental dismissal);
- Fixed an authenticated XSS vulnerability on the Bulk Add screen;
- Fixed an issue where the filter would be reset on the real-time activity viewer whenever the page data refreshed;
- Added a check to notify the user when moving computers between groups that have different 'client to server proxy settings',
- The Restart and Shutdown Server panels are now hidden when installed on Microsoft Azure IaaS machines;
- Added additional database indexes to improve repository load performance;
- The server now automatically expires the OTP code status if they are activated and never de-activated by the client (due to uninstallation or off network status etc.);
- Fixed an issue where the REST API /v1/agents/find endpoint could return invalid JSON if an endpoint being returned reports a null value for free disk space;
- Prevent carriage returns from being put into notification messages, to prevent partial messages from being seen by users;
- Reinstated the ability to paste data into multiple text fields within the product;
- Fixed an issue where the Airlock installer will detect docker as being out of date;
- Fixed an issue where the Airlock installer free disk space check would only target the home volume, rather than the installation location;
- Fixed a policy issue where a file may appear to be added to an application capture, however the policy version will never increment to generate a new policy, resulting in the file not being trusted until the next policy generation;
- Fixed an issue where clients may not re-register if they have an invalid or corrupt Client ID;

- Fixed an issue where REST API Policy changes may not trigger a client policy update;
- Fixed an issue where Renaming Policies or Enabling / Disabling Communication lists may not take effect;
- Fixed an issue where Application Capture Categories could not be renamed and would display ‘capture name is required’;
- Fixed errors in PDF generation when sending reports via e-mail in scheduled searches;
- Fixed an issue where if an empty baseline was uploaded twice within the product it would cause a baseline naming loop to occur;
- Fixed an error where ‘$’ characters would not be treated literally by the policy tester or database exclusion tester, resulting in issues viewing results for paths that contain this character;
- Fixed an issue where deleting a dashboard user would not remove associated multi-factor authentication information for the user in the product;
- Fixed an issue where Bulk Add would cause an error if called from the Quick Search feature;
- Fixed an issue where Self-Service OTP codes could not be scanned by Apple iOS devices;
- Fixed an issue where if a Publisher contains an ‘&’ character on the Bulk Add screen and is selected, the publisher filter would not correctly apply;
- The ‘Average Approval Time’ metric on the Server Health page has been removed as it was not widely used;
- Fixed an issue where the policy tester may interpret some path rules incorrectly and display inconsistent results;
- Fixed numerous search issues which resulted in an Airlock ‘error’ page being presented upon search execution;
- Allowed the * / and . characters to be added into path rules when using Swiss German keyboard layouts;
- Fixed an issue where renaming a parent policy would cause a web server error;
- Fixed an infinite loop condition where if scheduled searches were set to the ‘Now’ timeframe, it would result in 100% CPU usage in QueueScheduler;
- Improved prevention of auto filling the User Settings page by browser extensions such as LastPass. However, in testing the fix has only partial effectiveness due to these extensions often ignoring page fill requests;
- Reversing Labs threat levels now use English names, rather than threat ‘numbers’ on the repository page;
- Fixed an issue where moving an Application Capture between folder categories (from unapproved folders, to approved) doesn’t trigger a generation;

3. Application Capture Agent (4.5.0.0)

New Features

- The Application Capture can now be used in an offline mode, without connection to the Airlock Server;
- Application Captures can now be initiated from the client side, rather than requiring a server login to capture applications.

Improvements / Fixes

- Application Capture now supports the capture of all script file types the Airlock Enforcement Agent supports;
- Files are now captured on disk write rather than execution, resulting in more ‘complete’ Application Captures;

- Fixed a deadlock that may occur when running on systems with McAfee Anti-Virus installed or on some application virtualisation platforms;
- o Removed the Application Capture agent third-party networking driver to improve reliability of application captures.

4. Baseline Builder (Windows 4.5.0.0 / Linux 4.5.0.0)

New Features

- Linux Agent.

Improvements / Fixes

- Ability to set the Baseline Builder thread intensity via the command line, allowing for ‘slower’ captures to occur that consume less system resources.

5. Relay Agent (4.5.0.0)

Improvements / Fixes

- The relay agent has updated version numbers to be consistent with the main product versioning;
- Fixed a number of issues where the relay agent could not correctly process policies under certain conditions. This would cause downstream agents to be unable to update policies;
- The relay agent has been updated to support v4.5 clients.

Airlock Change Log v4.0

Released 22nd July 2019

Overview

Airlock v4.0 improves policy flexibility, increases reliability and performance, highlights include:

- **Blacklisting:** Enables undesired software, malware and other code to be proactively blocked, even if the software would otherwise be allowed to run by the existing application whitelisting ruleset;
- **Multi-Factor (2-Step) Authentication:** Provides extra security for user interface logins;
- **REST API:** Manage Airlock from third party applications by using Airlocks REST interface;
- **Policy Tester:** Easily see if a file would be blocked or allowed using the policy tester on any file repository page;
- **Trusted Logging:** Enable granular logging for any path or publisher rule, to see what files have been executed by the rule;
- **Self-Service OTP:** OTP Codes can now be issued in a self-service mode using any mobile application that supports Time Based One-Time Pad (TOTP) codes.

Upgrade Instructions:

- Run the installer package on the server as per the manual to upgrade from the previous release of the Airlock Server;
- NOTE: If LDAP authentication is configured in an existing installation of Airlock v3.x, these settings will be lost upon upgrade to v4.0. Please ensure you have local account access to the Airlock server before upgrading. This is due to an overhaul of the LDAP permission model within Airlock for increased flexibility;
- Client compatibility is unchanged from the previous v2.0 release, however to use new features such as Blacklisting you must upgrade agents to v4.0 or newer.

Detailed Changes:

1. Enforcement Agent (4.0.5.0)

New Features

- Script support for Python files;
- 30% improved endpoint performance using new file hashing libraries;
- Blacklisting support;
- Per-Rule Trusted Logging support;
- OTP code activation via the command line;
- DirectAccess IPv6 VPN Support;
- PowerShell Constrained Language Mode (CLM) enforcement;

Improvements / Fixes

- Support two new VB Script file types (.vbe and .wsf);
- Reduced the amount of bandwidth used by the agent by more intelligently queuing file uploads to the server. If a new file is seen by an agent the details will be immediately uploaded to the server, all subsequent executions of the same file will be uploaded in bulk at the next check-in time. This reduces the number of connections made to the Airlock server;
- The Enforcement Agent now captures the ‘Original Filename’ of files;

- Added an MSI installer switch for the v4.0 installer that allows a stop code to be specified, this enables existing Airlock Agents that are protected by stop codes to be upgraded;
- Numerous improvements in policy download and hash database verification reliability, hash databases now fail integrity checking much less often;
- Prevented double popup notifications during definition updates and OTP activation operations;
- The ‘Update Policy’ button is now greyed out during an in-progress policy update operation, this is intentional to prevent the user from triggering multiple policy update jobs;
- Added ‘Input OTP Code’ to the Airlock tray icon right click menu;
- Increased the size of Input OTP & Clear Log prompts for better viewing on high resolution screens;
- Added a -Mode switch to the Airlock Notifier that allows third party applications to determine the enforcement state of the Airlock Agent;
- Server 2019 is now detected as an operating system type (previous clients showed Server 2016 as the Operating System);
- The enforcement agent installer no longer requests a restart;
- The enforcement agent will no longer download a policy from the server if no changes have been made to the policy, this results in bandwidth improvements;
- Fixed a deadlock that could occur when installed on the same machine as McAfee Endpoint Security 10.x;
- Fixed an issue where .vbs files and other script types may trigger an exception however fail to prevent the file execution;
- Fixed two BugChecks (BSOD) that could occur during low resources or the computer waking from sleep;
- Fixed an issue where in bad network conditions (such as slow DNS or slow Airlock server responses) the agent may fail to enter enforcement mode till after the user had logged in, this could allow users to execute untrusted files. The Airlock enforcement agent no longer waits for connection timeouts to occur before entering enforcement mode;
- Fixed an issue where files could be seen as Not Signed, when they are actually signed by a publisher. This occurred due to file lock conditions when the files were in use by the system, preventing the Airlock agent from reading the digital signature information. Airlock database and caching routines have been improved to prevent this from occurring and additional logging has been added to detect file lock conditions;
- Updated SQLite libraries to remove a known security vulnerability;
- Fixed an issue where if ‘Export Log’ was clicked in the Airlock Notifier and the user’s desktop was redirected, the export would fail. The Airlock Notifier now correctly reads the environment variable for the current users’ desktop;
- The local hash cache will no longer be dumped upon a computer waking from sleep mode. Previously if a computer had been asleep for longer than the cache dump time, Airlock would dump the cache upon waking from sleep mode, causing slow boot performance;
- Fixed an issue where upon installation the Airlock Server details would not be correct, this was due to the server configuration failing to copy the server details during MSI installation. Fixed the installer so that administrative elevation occurs at the correct install time;
- Fixed an issue where loading the Eclipse IDE triggered a .JAR file execution, modified checking of file access flags to prevent this issue;

- Fixed an issue where if DNS responded with an IPv6 address of the Airlock server, the client would fail to contact the IPv6 address. Updated the connection method to correctly communicate with an IPv6 address. NOTE: The Airlock server is still unable to have an IPv6 address natively, however this fix supports transit over IPv6 networks such as when a DirectAccess VPN is in use.
- Fixed an issue where the Airlock Enforcement Agent did not validate the Airlock server correctly during communication. This could have potentially allowed an attacker to create a fake Nginx server and communicate with an Airlock Enforcement Agent. Updated the certificate checking routine to explicitly validate the presented server-side certificate;
- Fixed an issue where if more than one OTP code was activated offline, the OTP details would not be correctly uploaded to the server. Fixed the handling of multiple OTP code sessions in a single upload;
- Fixed an issue where the client couldn't correctly recover in all circumstances from a corrupt factivity.db, moved the database repair to a different thread to prevent file locking during the repair operations.

2. Server (4.0.0.0-Artest)

New Features

- Dashboard loading performance has been improved;
- LDAP group roles are now granular;
- Policy Tester;
- Blacklisting Support;
- REST API;
- Per-Rule Trusted Logging;
- Self-Service OTP;
- Multi-Factor (2-Step) Verification;
- CentOS 7.6 installer compatibility.

Improvements / Fixes

- The header row in the Bulk Add screen no longer scrolls to make it easier to use;
- Added the ability to delete entire drive letters within an application capture;
- Fixed an error where Airlock backups would not function correctly or backup far more frequently than the set schedule. Fixed the scheduler jobs to ensure backups run at the correct time;
- You can now paste usernames into the main Airlock login username field;
- There is a new popup window that appears whenever trusted logging for all rules is enabled, this is to warn the user that the action could cause significant server load issues if this feature is enabled at scale;
- Airlock's friends at Reversing Labs now have their logo on the repository page to show where we get our file reputation information from;
- Multiple wording updates across the UI to better explain a number of components;
- Added a help page within the product that contains a number of helpful resources;
- The Airlock installer now detects port conflicts if the user tries to assign the web interface to an already allocated port;
- The Airlock installer now backs up the existing client and web server certificates on every upgrade to prevent accidental deletion;
- Changed the layout of the repository page to accommodate the new Policy Tester feature;

- The trusted publisher list on the Policies screen is now sorted alphabetically, rather than the order in which the publishers were added;
- The OTP screen is now paginated to better display and manage large numbers of OTP codes;
- There are new Server Activity Messages for user role modifications and deletions;
- The file uploading policies option has been removed in v4.0 as this was a rarely used feature. This is planned to return in a future release when Malware Analysis Sandboxing integration is added;
- Screens that display large amounts of file data now have loading icons;
- The server now displays a low disk warning when there is less than 15% of disk space free on the Airlock host;
- The Airlock installer will no longer run if there is under 10GB of free disk space;
- Added an OTP Purpose input box, to allow users to specify the reason for issuing an OTP code;
- Overhauled the OTP algorithms to use HOTP & TOTP which improves reliability, this has also shortened server issued codes to 8 digits.
- Improved the filters on the Bulk Add screen so that reputation and publisher filters can now be applied at the same time;
- When the Airlock SSH interactive menu was loaded on a machine with restricted privileges (root account disabled) the functions in the SSH menu did not work. The menu now detects the account context it is running in and only appears if it has the correct privileges, if it does not the SSH message of the day states how to open the menu;
- Fixed an issue where Airlock Policy groups with a space character at the end could not be renamed;
- Updated web UI code to remove deprecated elements reported by Google Chrome;
- Fixed a filtering error when using the parent process selector in the activity viewer;
- Fixed an issue where folders that contain files in a Baseline capture were unable to be deleted;
- Fixed an issue where leading or trailing whitespace on either side of proxy settings (for Airlock Cloud or Client) was not trimmed, this would cause the proxy configuration to fail and make debugging difficult (as the correct proxy details appeared in the debug logs);
- Fixed an issue where underscores and hyphen characters within a username were not permitted, this was caused by us trying to sanitise input a little too much;
- Fixed an issue where if you renamed a group the same as an existing group, it broke the policy tree;
- Fixed an issue where if you filtered for a folder path that contains brackets in the activity viewer, these files would not appear in the Bulk Add process (for example Program Files (x86));
- Fixed an issue where if Parent Process was selected as an output column in search and that search was exported to a file, the Parent Process column would appear blank in the external file;
- Fixed an issue where if a comma was used in the LDAP scoping filter, the LDAP connector would not resolve any users. The LDAP controller now appropriately escapes the comma character;
- Fixed an issue in Internet Explorer 11 where changes to policy settings would not take effect. Internet Explorer 11 does not like blank form inputs, so we changed the submission code to specify a null value instead of a blank field;
- Fixed an issue where if you only have the create_otp role and browsed to the policy page, the page would refresh continually;

- Fixed an issue where the Agent Stop Code (ASC) would not apply in policy unless it was changed in conjunction with another UI setting;
- Reduced the frequency of cloud reputation re-lookup to increase the lookup speed of new files within a customer's Airlock database. Previously on large databases the lookup queue would become delayed and prevent new file information from being looked up promptly;
- Fixed an issue where SysLog (UDP) messages would arrive out of order or not correctly line broken;
- Fixed an issue where both the edit_policies and edit_clients roles were required to move computers between groups. Now only the edit_clients role is required to move computers;
- Original Filename is now displayed on the file reputation page providing additional context;
- If a backlash character was used in the proxy password field, proxy authentication would not work. Updated the code to correctly treat backslash characters as non-special characters;
- Fixed a rare UI issue where if category approvals and inheritance are used to approve application captures, the UI could show that the package is approved in policy when it may not be. The approval tree code has been updated to ensure the correct application capture package state is displayed;
- Fixed an error when exporting a PDF, CSV or XML from Quick Search results;
- Fixed an issue on the Policies page where the last check in date column was not correctly sorted, now clients are sorted in the correct order;
- Fixed an issue with the installer where if /etc/hostname was marked as immutable, the installer would not correctly set the entered hostname. The installer now detects this condition and displays a notification;
- Fixed three authenticated Cross Site Scripting (XSS) vulnerabilities;
- Fixed an authenticated Command Injection vulnerability that allowed local files to be read from the Airlock server;
- Added the ability to specify the number of backup revisions to be stored on the server to ensure the server does not run out of disk space by indefinitely performing backups;
- Fixed an error where if the computer name or username contained UTF-16 characters (used in Danish character sets) the Enforcement Agent and Application Capture agents would fail to register and upload activity to the Airlock server;
- Fixed an issue where if a group was renamed to a blank name, the group tree would no longer display;
- The Airlock server now has an automated script to restore Airlock backups, please see the user manual for more information;
- Fixed an issue where the UI would get caught in a loop if the user attempted to edit a search without the edit_search role;
- Fixed an issue where path rules would not be correctly added to policy when importing from a predefined path rule set, this could cause path rules shown in the UI not applying in all circumstances in client policy.

3. Application Capture Agent (4.0.0.0)

Improvements / Fixes

- Significantly reduced the time it takes to upload Application Capture results to the Airlock server, particularly over high latency connections. The Application Capture Agent is now multi-threaded and performs a single bulk submission rather than uploading file information individually.

4. Baseline Builder (4.0.0.0)

Improvements / Fixes

- Improved the reliability of Baseline Builder to ensure all files on the target operating system are captured;
- Fixed an issue where Baselines would sometimes end in NUL characters causing the captured baseline to be invalid. This was due to early termination of the capture process without waiting for existing worker threads to return data. Now Baseline Builder waits for all threads to finish operation.

5. Relay Agent (1.7.0.0)

Improvements / Fixes

- The relay agent privileges have been reduced, it now runs as NETWORK SERVICE rather than SYSTEM. This reduces the potential attack surface of the agent;
- The relay agent will now recover from any crash conditions to ensure data continues to be served to clients;
- Fixed numerous policy parsing issues causing mismatched policy numbering on the client;
- Fixed a number of relay agent crashes due to invalid data;

Airlock Change Log v3.1

Released 22nd February 2019

Overview

Airlock v3.1 is a bugfix release.

Upgrade Instructions:

- Run the installer package on the server as per the manual to upgrade from the previous release of the Airlock Server;
- Client compatibility is unchanged from the previous v3.0 release;

Detailed Changes:

1. Enforcement Agent (3.1.0.0)

Improvements / Fixes

- Fixed an issue where CMD & BAT files were not blocked when executing files from the command prompt;
- Fixed an issue where CMD & BAT files may be blocked when script control is set to audit mode only;
- Fixed an issue where copying script files with the command prompt or PowerShell interpreter may trigger a file execution;
- Fixed an issue where the Airlock installer may clean-up unrelated files upon uninstallation of the agent;
- Added an interoperability fix to prevent crashing when the Airlock Agent is installed with McAfee Anti-Virus;
- Fixed an issue where executions were reported when Chrome_Software_Reporter.exe scanned the system and inspected .bat files;
- Fixed an issue where 'Export Log' in the notifier would assume the user Desktop was not redirected, the client now respects redirected desktops correctly.

2. Server (3.1.0.0-Wallace)

Improvements / Fixes

- Fixed an issue where backups would not write correctly;
- Fixed an issue where predefined path rules would not display when upgrading the server from the v2.2 branch;
- Usernames can now be pasted into the login field of the main login screen;
- Underscore and hyphen characters are now permitted in usernames;
- Fixed an issue where users that have unexpected comma's in their name can now authenticate;
- Fixed a compatibility issue with Internet Explorer 11 where form data was not being correctly submitted when updating policies;
- Fixed an issue where the LDAP OTP issuer role caused a page refresh when browsing to the policy tab;
- Updated the installer to be compatible with CentOS 7.6;
- Fixed an issue where Airlock certificates may be replaced upon upgrade of the server (certificates are now backed up upon every upgrade as an additional step);

- Fixed an issue where an Agent Stop Code update would not take effect unless another settings change was made at the same time;
- The Airlock interactive SSH menu now only activates for interactive terminal services (previously it caused an error using file copy utilities such as WinSCP);
- Fixed an issue where the group filter dropdown didn't filter correctly on the Activity Viewer screen;
- Fixed an issue where SysLog messages were sent out of order;
- Fixed an issue where backslash characters in some search criteria's were not escaped correctly;
- Updated the client database generation logic to prevent an issue where clients may download a database during generation, resulting in an incomplete update;
- Fixed a logic issue with the application policy tree where approved 'categories' may not actually approve the application package correctly;
- Fixed an error when exporting CSV/XML/PDF files from Quick Search;
- Removed the : character limitation in the Quick Search box, you can now search properly for file paths with drive letters;
- Server Backups are now processed outside of the application container, preventing a low disk space condition.

Airlock Change Log v3.0

Released 6th November 2018

Overview

Airlock v3.0 introduces new enterprise features along with significant improvements in scalability, usability and performance. Highlights include:

- **Relay Agent:** Enables policies to be relayed to clients in remote or high security network segments. This new agent provides greater flexibility of Airlock's product architecture for enterprise environments;
- **LDAP Authentication:** Provides integration with LDAP servers such as Active Directory for user authentication;
- **Unreviewed Activity:** Track which files have been seen through a bulk add process and know which files have / have not been added to policy. This feature also provides an audit trail for each file, showing which administrator added or removed files from policy;
- **External Logging:** Airlock's external logging engine has been re-written and now includes native connectors for Splunk and Graylog. Files can now be sent in a JSON format over TCP, UDP and HTTP(s);
- **Performance:** Airlock server now loads information five times faster than the previous release. The dashboard can now display over a million events;
- **Reference Baselines:** Airlock now ships with pre-captured baselines of all supported operating systems.

Upgrade Instructions:

- Run the installer package on the server as per the manual to upgrade from the previous release of the Airlock Server;
- Client compatibility is unchanged from the previous v2.0 release;
- NOTE: Customers using SysLog to send logs to an external logging solution will need to reconfigure external logging after upgrade. Native Graylog and Splunk apps are available at the Graylog Marketplace and Splunkbase.

Detailed Changes:

1. Enforcement Agent (3.0.2.0)

New Features

- Script support for Windows Script Component (.SCT) files;
- Support for Relay Agent communication;
- Parent process information is now uploaded to the Airlock server;
- Reporting of additional invalid publisher conditions (Verification Failure) and (Malformed Signature).

Improvements / Fixes

- Significantly reduced the number of TCP connections sent to the Airlock server by queuing execution activity and uploading the events in bulk upon check-in;
- Client logs are now automatically deleted after 30 days of age;
- Fixed a compatibility issue with Sophos Anti-Virus;
- Fixed a slow memory leak when Trusted Execution Activity Uploading was enabled;
- Fixed Script Blocking not working on Windows XP & Server 2003;
- Fixed execution's being logged when files are viewed using Windows Explorer tile view on Windows XP & Server 2003;

- Fixed ‘Export Log’ in the notifier so it now writes to a user writeable location;
- Fixed an issue where digital signatures may not be correctly validated on machines that are loading during an image build (SysPrep);
- Fixed an issue when clicking ‘Reboot Now’ on x64 systems at the end of the installer didn’t trigger a reboot;
- Removed the network driver from the enforcement agents to ensure greater compatibility with other endpoint protection products;
- Fixed an issue where the Notifier (user interface) would sometimes not load upon login;
- Overhauled client logging to assist with better problem diagnosis.

2. Server (3.0.0.0-Payton)

New Features

- Unreviewed activity;
- Dashboard and server performance is now five times faster;
- Native Splunk and Graylog external logging support;
- Database retention setting to limit database growth and ensure performance;
- Ability to force password resets and expire user passwords;
- LDAP support for user authentication;
- Parent processes can now be seen and filtered in the Activity Viewer;
- Reference baselines;
- Publisher summary is now shown on the Bulk Add screen;
- Predefined path rules now have rule descriptions explaining their purpose;
- SSH interactive menu for server management (on-premise only);
- Support for relay agents.

Improvements / Fixes

- Server activity events are now recorded whenever a client group is created, renamed or deleted;
- Confirmation dialogue has been put in place before allowing the deletion of an administrative user;
- Bulk Add, Activity Viewer and Policy screen columns are now sortable by clicking the header;
- File repository entry colours now change according to the file reputation status;
- SHA256 hash values are now truncated to allow for parent process to be shown in the Activity Viewer;
- File – Parent Process is now an option available in search;
- The server web interface now has a certificate chain that can be trusted by browsers to show as ‘valid’;
- Numerous text and UI look improvements;
- Policy inheritance colour has changed from orange and black. It is now blue;
- Parent process and command line fields are now sent to external logging solutions;
- Backups now store in tar.gz files, rather than flat JSON files;
- Backups now include the server certificates to allow for a complete server restore;
- Fixed an issue where backups would not run correctly on schedule;
- Fixed a number of Cross Site Scripting (XSS) vulnerabilities;
- Reduced the RAM usage of the server by 1 GB;
- Fixed an issue where baselines with / \ characters in their name could not be approved;
- Fixed an issue where the ‘File Status’ column would not be shown in search reports;

- Fixed an issue where application capture subcategories could not be renamed;
- Fixed an issue where pressing enter on the publisher search window would result in a ‘group not found’ error;
- Fixed an issue where the dashboard unreviewed count and activity viewer file count would not match if OTP codes had been used;
- Fixed an issue where repository entries were rarely shown as ‘File Not Found’ and the associated files could not be added to an application capture;
- Fixed an issue where Server 2003 x64 was shown as Windows XP x64;
- Fixed an issue where if the Cloud Reputation Service was disabled, it would start again upon the next boot of the Airlock server;
- Fixed an issue where clients could be shown as offline temporarily. Changed the behaviour of the ‘offline’ status so a client must be offline for at least two check-in periods before being marked as offline;
- Fixed an issue where quick search would often not show the desired results;
- Updated the Airlock server installer to force questions to be answered explicitly to reduce errors, also added the option to set the server time zone.

3. Application Capture Agent (3.0.0.0)

Improvements / Fixes

- Updated the network capture libraries for improved compatibility

4. Baseline Builder (3.0.0.0)

New Features

- Baseline Builder will now use all available CPU cores

Improvements / Fixes

- Fixed an issue where Baseline Builder could not be installed on Windows XP x64 and Server 2003 x64 editions;
- Fixed a rare issue where Baseline Builder could miss files during capture and end prematurely.

5. Relay Agent (1.0.0.0) (Initial Release)

Airlock Change Log V2.2

Released 9th May 2018

Upgrade Instructions:

- Run the installer package on the server as per the manual to upgrade from the previous release of the Airlock Server;
- Client compatibility is unchanged from the previous v2.0 release;

Changes:

1. Enforcement Agent (2.2.1.0)

New Features

- Script support of the following file types - PowerShell, VBScript, Command Files, Batch Files, HTML Executables, JavaScript, Windows Installer Files and Java applications;
- Tamper detection has been introduced for the windows certificate validation bypass techniques described in the following whitepaper: https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf if tampering is detected, Airlock will fall-back to internal certificate validation.

Improvements / Fixes

- Re-engineered file digital certificate verification to be more robust, now digital certificates (publishers) of files on network shares are correctly validated;
- Digital certificates (publishers) signed with SHA-3 & SHA-5 certificates are now supported;
- Publishers are now cached during a policy update, reducing the risk of a file being seen as ‘untrusted’ during a policy update operation;
- ‘Not Signed’ files are no longer placed into the Airlock certificate cache. This reduces the risk of files been seen as perpetually ‘Not Signed’ after Windows updates or major operating system upgrades;
- Restored LocalSettings.xml file protection (not functional in v2.1);
- Both the policy and hash database versions are now reported to the server;
- Files with invalid digital signatures (publishers) are also no longer stored in cache, to reduce the risk of a file being perpetually seen as invalid.

2. Server (2.2.0-Mutombo)

Improvements / Fixes

- File – Threat Name is now an option in Search;
- Improved search reliability;
- References to ‘policy’ within the product are now called ‘group’;
- Numerous minor cosmetic and wording fixes;
- Application categories and their parents are now shown as yellow, unless the category is directly approved;
- Fixed a policy generation issue where multiple policies may be generated upon a single change.

3. Application Capture Agent (2.2.0.0)

New Features

- Script support;
- Application Capture now uploads all extended file metadata.

4. Baseline Builder (2.2.0.0)

New Features

- Script support;
- Baseline Builder now uploads all extended file metadata.

Improvements / Fixes

- Fixed an issue where Windows Server 2003 showed zero results during a baseline operation.

Airlock Change Log V2.1

Released 20th February 2018

Upgrade Instructions:

- Run the installer package on the server as per the manual to upgrade from the previous release of the Airlock Server;
- Client compatibility is unchanged from the previous v2.0 release.

Changes:

1. Enforcement Agent (2.1.0.0)

Improvements

- Fixed an issue where the agent was unable to be SysPrepped correctly.

2. Server (2.1.0-Olajuwon)

New Features

- The User Interface has been overhauled, improving readability;
- Reputation lookups now have proxy support;
- ‘New Files’ on the dashboard are now clickable to their repository page.

Improvements

- Fixed a policy inheritance issue, where policies in child groups were not processed correctly;
- Fixed an issue where quick search did not always return results;
- Fixed an issue in the path tester where results were invalid if file paths contained bracket characters;
- Fixed an issue where the server did not always install docker correctly;
- Fixed an issue where stopping application capture before clicking ‘start’ client side would result in an empty capture;
- Fixed an issue where clients would report an offline status, even though they were online;
- Fixed a number of minor UI bugs.

3. Application Capture Agent (2.1.0.0)

New Features

- Application Capture now supports AppX digital signatures (Win 8 / 10 Apps);

4. Baseline Builder (2.1.0.0)

New Features

- Baseline Builder now supports AppX digital signatures (Win 8 / 10 Apps);

Improvements

- Fixed poor performance and high memory utilisation during capture.

Airlock Change Log V2.0

Released 4th December 2017

Upgrade Instructions:

- Run the installer package on the server as per the manual to upgrade from the previous release of the Airlock Server;
- Client versions 1.0.0.0 - 1.2.4.0 are partially compatible with this build;
- Client versions 1.2.5.0 – 1.4.5.0 are fully compatible with this build;
- After upgrade the client interface will be accessible on a new port '3128'.

Known Issues:

- Baseline Builder performance is slow due to the collection of additional file metadata for all files. Optimisation will be performed for the next release.

Changes:

1. Enforcement Agent (2.0.0.0)

New Features

- Windows AppX Digital Signature support (Windows Store Apps);
- Process command line support;
- All file metadata (description, version, author etc. now captured);
- Character support for all languages;
- Citrix App Layering support;
- Customisable columns within Notifier.

Improvements

- Improved policy error checking and stability;
- File information appears faster within Notifier;
- New policy naming scheme 'policy.hash' instead of just 'policy';
- Fixed a memory leak and service termination on Windows Server platforms;
- Safe Mode is now triggered less often;
- Fixed a number of rare crashes.

2. Server (2.0.0-Robinson)

New Features

- Re-wrote the client API resulting in a significant performance improvement;
- Client API and Web Ports are now separate (improved architecture flexibility);
- Airlock Cloud reputation checking for all files (optional);
- Policy generation performance and error checking is improved;
- Stale client management (for VDI environments).

Improvements

- Publisher and Path rules are now exportable;
- Files can now be deleted from Baselines;
- Character support for all languages;
- Search performance and stability is improved;
- Compatibility with CentOS 1708;
- Numerous interface tweaks and improvements.

3. Application Capture Agent (2.0.0.0)

New Features

- Application Capture now captures all file metadata.

4. Baseline Builder (2.0.0.0)

New Features

- Baseline Builder now captures all file metadata.

Improvements

- Fixed an issue where Baseline Builder could not perform online captures.