Version 5.3.x (Latest)

Version 5.3.3

Released 25th October 2024

Overview

This is a critical maintenance release fixing a known security issue for customers using SAML authentication (CVE-2024-45409) and adds incremental capabilities such as support for friendly application names on Windows Store applications.

Upgrade Notes

- Upgrading to v5.3.3 of the Airlock Server is only supported from v5.2.5+ or v5.3.0+ due to database requirements. If the Airlock Server being upgraded is on an earlier release, you must first upgrade to v5.2.5+ or v5.3.0+ before upgrading the server to v5.3.3 please see Software Upgrade Paths for more information.

Detailed Changes

Server (5.3.3.2251-Kemp)

🔧 Improvements / Fixes

- Add Allowlists & Blocklists UI search functionality (HAS-6619);
- Policy and Blocklist path rules are now sorted by inheritance and ascending order (HAS-6620);
- Fixed an upstream SAML security vulnerability CVE-2024-45409, and update application dependencies (HAS-6678);
- 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);
- Improved enqueue handling on DB Policy Generation Tasks (HAS-6709);
- Fixed Crowdstrike Falcon LogScale form fields appearing missing on v5.3.2 (HAS-6631);
- Fixed an issue where backup tabs and server controls could appear under certain cloud deployment scenarios (HAS-6669);
- Refactor a number of search fields and operators to return more reliable results particularly for Linux and macOS file paths (HAS-6490);
- Add additional Browser Extension File Execution fields to REST API and SIEM logging (HAS-6604);
- Add the local ip address to the /agent/find REST API endpoint (HAS-6638);
- Fixed an issue where generating an OTP on the policies page, if the first custom OTP duration was blank, would cause the generation to fail (HAS-6641);
- Removed the 'per script type' option which was cosmetic only, as it is intended for the upcoming v6.0 branch release (HAS-6666);
- Added additional fields to the /group/policies REST API endpoint to ensure the response is feature complete with the latest features (HAS-6668);

- Fixed an issue where exporting CSV results from a saved search would error (HAS-6670);
- Fixed an issue when trying to export clients from the All Clients view would fail if all computers were selected (HAS-6673);
- Updated policy tester guidance on the file repository page (HAS-6675);
- Removed the input sanitisation of forward slash characters within search criteria, to support Linux and macOS file paths (HAS-6677);
- Add support for displaying the publisher friendly name of applications for Windows Store applications in file repository and publisher lists (HAS-6380);
- Fix typo on external logging event types list (cosmetic only) (HAS-6711);
- Added new reference baselines for latest Windows 11 & macOS releases (HAS-6712).

Enforcement Agent Windows (v5.3.3.0)

🔧 Improvements / Fixes

- Improved handling of files containing control characters (HAS-5628);
- Fixed a notifier exception when exporting agent logs (HAS-6402);
- Optimised the submission of file details to the server to use less network bandwidth (HAS-6544 / HAS-6547);
- Support log bundle collection can now be performed from the command line, by running airlock -support target\zip\path.zip (HAS-6458);
- Fixed an issue where the Relay Agent could not be installed alongside the Airlock Enforcement Agent (HAS-6461);
- Fixed an issue where the agent may fail to enforce Constrained Language mode for certain x86 PowerShell sessions (HAS-6484);
- Fixed an issue where using the emailbutton or urlbutton messages for notifications could insert the button text into the message (HAS-6496);
- Grandparent processes for browser extension executions are now reported in Windows (HAS-6548);
- Fixed an unexpected usermode service termination when attempting to re-check a publisher for a temporary file (HAS-6553);
- Fixed an issue, where under high event rates and with large user Domain Security Group membership, a metarule check for dll files may rarely fail to match at file execution time (HAS-6632);
- Driver optimisations for performance (HAS-6556, HAS-6085, HAS-6549);
- Improved the closure of the notifier processes when Windows is detected to be shutting down (HAS-6557);
- Fixed an issue where certain Chrome browser extensions could not be parsed (HAS-6566);
- Added additional debug log messages for Airlock Cloud to assist troubleshooting (HAS-6571);
- Improved Assembly Reflection Prevention to detect additional file load techniques (HAS-6283);
- Add support for reading the friendly publisher name of applications for Windows Store applications (HAS-6380);
- Fixed an issue where calling notifier -mode could return non standard return codes (HAS-6452);
- Additional agent hardening against tampering (HAS-6462);
- Fixed a rare fltmc hang during driver unload (HAS-6681);
- Added support for dll files being read as resources rather than directly loaded (HAS-6573);
- Fixed a regression where an Airlock Notifier shortcut is incorrectly created in the start menu after install (HAS-6593).
- Fixed a rare occurance where catalog digital signatures could fail validation for catalogs that use memberTags (HAS-6595);

- Fixed a regression where notifier could not have OTP codes activated when called from the 'SYSTEM' user (HAS-6605);
- Added operating system detection logic for Windows Server 2025 (HAS-6614);
- Fixed an issue where agents upgraded from older versions may fail to properly recognise the new Allowlist Metarule and/or Browser Extensions policy settings (HAS-6628);
- Improved the reliability of self upgrading agents through refactoring agent uninstallation logic, upgrade detection and failover logic (restart existing install on failure) and modification of agent unload mechanisms (HAS-6626: HAS-6429, HAS-6615, HAS-6616, HAS-6617, HAS-6624, HAS-6625, HAS-6672, HAS-6636);
- 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 agent crash upon activation of Self Service OTP, while under heavy processing load. This was observed during internal stress testing (HAS-6676).

Enforcement Agent Linux (v5.3.3.6177)

🔧 Improvements / Fixes

- Fixed a delay after upgrade where Browser Extension Control and Allowlist Metarules would not be functional until a new policy generation is performed (HAS-6610);
- Limited the error size written out to log files in standard logging (HAS-6640).

Enforcement Agent macOS (v5.3.3.8177)

🔧 Improvements / Fixes

- Fixed a delay after upgrade where Browser Extension Control and Allowlist Metarules would not be functional until a new policy generation is performed (HAS-6610);
- 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).

Relay Agent (v5.3.3)

🔧 Improvements / Fixes

- Added support for source application and publisher description fields for Windows Store applications (HAS-6679).

Version 5.3.2

Released 5th September 2024

🚀 Headline Features

Airlock Digital v5.3.2 significantly improves server performance and fixes a number of known issues.

- **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.

Upgrade Notes

- Upgrading to v5.3.2 of the Airlock Server is only supported from v5.2.5+, v5.3.0 or v5.3.1 due to database requirements. If the Airlock Server being upgraded is on an earlier release, you must first upgrade to v5.2.5, v5.3.0 or v5.3.1 before upgrading the server to v5.3.2 please see Software Upgrade Paths for more information.

Detailed Changes

Server (5.3.2.2113-Kemp)

🔧 **Improvements / Fixes**

- Stale Client Management can now be configured in hours (previously it was limited to days) (HAS-6177);
- Dashboard performance has been substantially improved (HAS-6588);
- Dashboard now displays 'No Results' instead of blank values when no results are available (HAS-6596);
- The Airlock SSH menu now has improved readability (HAS-6589);
- ‘Unmanaged’ clients now have their own audit mode value in the products internal database. This provides more accurate REST API counts relating to the number of clients actually running in audit mode (HAS-6010);
- Server scheduled restarts have now been made less frequent to improve in memory database performance (HAS-6453);
- Improved consistency when creating a new child policy group to 'mirror' the Group Settings from a parent group, rather than resetting to defaults (HAS-6455);
- Export List on the policies tab now exports the selected agents, rather than all agents. If users want to export a list of all agents they can simply select all first (HAS-6459);
- Exporting and Importing of allowlist metarules via XML files is now supported (HAS-6471);
- Fixed screen layout issues on the repository page File Packages tab when specific event counts are populated (HAS-6497);
- Quotes are now supported in Blocklist command line metarule criteria (HAS-6527);
- Added additional validation when uploading of XML / ALF files to Allowlists (HAS-6568);
- Fixed an issue where the Local User Management table would populate slowly or in some cases fail to populate at all (HAS-6569);
- Fixed a regression where sort by clicking the column headers on bulk add was disabled (HAS-6572);
- Fixed a log entry error in the ClientAPI where the a username error would refer to hostname in a particular error message which was misleading (HAS-6574);
- Fixed an issue where a colon is still added to Crowdstrike Falcon LogScale URL when no port is provided (HAS-6576);
- Fixed a search issue relating to the Grand Parent Process field (HAS-6577);
- Implemented additional error handling for Airlock Client msi management (HAS-6578);
- Reduced verbosity of certain rails log entries (HAS-6579);
- Fixed an issue where scheduled backup jobs could fail and report there is insufficient disk space free even though enough disk is available (HAS-6580);

- Improved handling of resource locks that could result in segfaults on a number of server side components when placed under extremely heavy load (HAS-6585);
- Fixed an issue where creating a blank allowlist does not populate the hostname and user fields that can cause future import and export errors (HAS-6567);
- Fixed the date picker when formatted with mm/dd/yyyy date formats (HAS-6612);
- Fixed a regression where authenticode hash was missing from the metarules criteria list on v5.3.0 & v5.3.1 (HAS-6608);
- Fixed an authenticated XSS issue (HAS-6527) - reporting credit to Qusai Alhaddad (Honeywell).

Enforcement Agent Linux (v5.3.2.6163)

🔧 Improvements / Fixes

- Removed some occurances of sudo on install if the user is already root (HAS-6483);
- Log files now print CPU core count to assist debugging (HAS-6584);

Enforcement Agent macOS (v5.3.2.8163)

🔧 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);
- When sideloading a configuration XML via the UI on macOS a manual agent restart is no longer required for the new settings to load (HAS-6460);
- Fixed an issue where the notifier would display the wrong execution type for cached blocked events, this is a cosmetic issue only and file handling was correct (HAS-6599);
- Fixed an issue where Browser Extensions added via an Allowlist metarule may not be correctly processed (HAS-6609);
- FIxed an issue where Browser Extensions added individually to an Allowlist may not be correctly processed (HAS-6600).

Relay Agent (v5.3.2)

🔧 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).

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);

Application Capture Agent (v5.3.2)

🔧 Improvements / Fixes

- Improved handling of files containing control characters (HAS-5628);

Version 5.3.1

Released 18th July 2024

> ⚠ **NOTE**
>
> NOTE: From v5.2.5 / v5.3.1 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.

> ⚠ **NOTE**
>
> 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 v5.3 Documentation under System Requirements.

🚀 Headline Features

Airlock Digital v5.3.1 introduces two new major product features and a number of bug fixes.

- **Browser Extension Control:** Airlock Enforcement Agents now have the ability to control the installation of Browser Extensions in Chrome, Edge and Firefox browsers. This feature is supported on Windows & macOS Enforcement Agents;
- **Trusted Installer:** Trusted Installer is a feature which automatically trusts files written to disk from centralised software deployment sources such as Microsoft SCCM, InTune, BigFix etc. This reduces friction when deploying software within enterprise environments. This is supported on Windows Enforcement Agents.

Upgrade Notes

- Upgrading to v5.3.1 of the Airlock Server is only supported from v5.2.5 and v5.3.0 due to database requirements. If the Airlock Server being upgraded is on an earlier release, you must first upgrade to v5.2.5 or v5.3.0 before upgrading the server to v5.3.1 please see Software Upgrade Paths for more information;
- Please note that Relay Agents must be updated to v5.3.1 to support Browser Extension Control and must be performed before downstream enforcement agents are upgraded to v5.3.1.

Detailed Changes

Server (5.3.1.1942-Kemp)

🚀 New Features

- Browser Extension Control support (HAS-4621);
- Trusted Installer support (HAS-6180);

🔧 **Improvements / Fixes**

- The application container operating environment has been upgraded (HAS-6089);
- Exporting policy group process rules now include the type of rule (grandparent / parent) (HAS-6079);
- Product documentation now includes a health check guide for self hosted customers and other documentation updates (HAS-6395, HAS-6463, HAS-6467 & HAS-6431);
- The REST API documentation has been overhauled and can be found at https://api.airlockdigital.com;
- The REST API /v1/otp/usage endpoint has been updated to support status filtering (HAS-6306);
- Updated the REST API group setting endpoints to bring functionality up to feature parity with what is shown in the UI (HAS-6377 & HAS-6383);
- Fixed an issue where the REST API /v1/getexechistory limit parameter was not respected (HAS-6387);
- Updated the /v1/otp/retrieve REST API endpoint to accept clientid which is standard across the other endpoints (HAS-6388);
- Added additional REST API endpoints for process exclusion management (HAS-6393);
- 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);
- REST API /v1/group/policies now returns the parent process type on a rule (HAS-6403);
- Added a database index count to the Server Health page (HAS-6376);
- Uplifted the version of the underlying database system (HAS-6398 & HAS-6406);
- Perform additional input validation on Agent Stop Codes to prevent unsupported characters from being entered (HAS-5992);
- Fixed a number of UI issues when the policy settings window was viewed with a narrow screen width (HAS-6054 & HAS-6415);
- Fixed an error when changing the Show Unique selection to 'no' on the activity viewer screen (HAS-6384);
- Fixed an issue where the allowlists file browser could fail to load when rendering large data sets (HAS-6482 & HAS-6485);
- Fixed an issue where API key generation restrictions could be circumvented by authenticated users (HAS-6475);
- Fixed an authenticated XSS issue (HAS-6476);
- Fixed a service failure if the REST API is unable to connect to the external logging source when using TCP Syslog (HAS-6385);
- Fixed a count discrepancy between the dashboard and activity viewer unreviewed count (HAS-6379);
- Fixed an issue won the Bulk Add screen, which could see filtered file events persist on the screen even after they have been added to an allowlist (HAS-6401);
- Fixed an issue where Bulk Add returned to the top of the screen upon performing a bulk add (HAS-6438);
- Increased the application container shutdown timeout to improve graceful application restarts (HAS-6532);
- Fixed an issue where the bulk add screen may not load events when scrolling to the bottom of the page (HAS-6486);
- Fixed an issue where publishers containing a forward slash were unable to be selected on the Bulk Add screen (HAS-6307);
- Fixed an issue where zero width spaces would appear in various places within the product, particularly on the Bulk Add screen (HAS-6313);
- Fixed an issue where an invalid time error could occur when switching between time filters on the dashboard (HAS-6465);
- Fixed an activate / deactivate OTP loop that could occur if the ClientID of the submitting agent could not be found

(HAS-6435);

- Fixed an issue where exporting an allowlist CSV could terminate early if repository data was not available for files in the allowlist (HAS-6528);
- Fixed an issue where the publisher listing on the Policies page could occasionally fail to display updated publishers for selection (HAS-6529)
- Upgrade application dependencies (HAS-6493);
- The PDF versions of the REST API, User Manual and Change Logs have been removed from the product (HAS-6501);
- Fixed an issue where custom OTP durations were reset to default values (in the UI) when restarting Airlock (HAS-6405);
- Removed an unsafe rule warning that was shown incorrectly when configuring Allowlist metadata rules (HAS-6358);
- Fixed an issue where 'add multiple hashes' did not work on Allowlists (HAS-6407);
- Fixed an issue where the Microsoft recommended block rules 10.1.0.2 would contain empty values for product versions (HAS-6478);
- Fixed an issue where documentation links could not be directly accessed using a URL (HAS-6359);
- Fixed an issue where OTP's were unable to be issued from the All Clients View on the Policies tab if custom OTP durations were in use (HAS-6362);
- Fixed an issue where the dashboard policy filter would not correctly display results for child policy groups when a parent is selected and subgroups are set to yes (HAS-6365);
- The height of the invalid publishers window has been reduced to fit on widescreen displays (HAS-6367);
- Fixed an authenticated 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 v5.3.0 (HAS-6481);
- 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-6375);
- Fixed an error that could occur when performing database maintenance tasks (HAS-6410);
- Updated an installer check to ensure future server upgrade paths are enforced (HAS-6411);

Enforcement Agent Linux (v5.3.1.6151)

🔧 Improvements / Fixes

- Support full file path trust for both Parent and Grandparent processes (HAS-6326);
- Fixed a crash when the user was viewing the shell based notifier interface and the agent was placed under sustained heavy load (HAS-6333);
- Fixed an issue where custom OTP durations were not respected when using an OTP code (HAS-6356);
- Fixed an issue where the poll time on Linux was not adhering to the policy setting (HAS-6394);
- Fixed an issue where the agent was unable to retrieve publishers on Ubuntu 22.0.4+ (HAS-6440);
- 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);
- Fixed an issue where if script control is disabled the agent could miss certain non-script file executions (HAS-6536).

Enforcement Agent macOS (v5.3.1.8151)

🚀 New Features

- Browser Extension Control support (HAS-4621);

🔧 Improvements / Fixes

- The uninstall agent option now prompts for administrator re-authentication before proceeding (HAS-6213);
- The macOS agent now supports sideloading with a configuration file for discovery (HAS-6305);
- Support full file path trust for both Parent and Grandparent processes (HAS-6326);
- Fixed an issue where custom OTP durations were not respected when using an OTP code (HAS-6356);
- 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);
- Reverted publisher checking logic to match v5.2 branch to avoid "(Invalid Signature)" issues reported by some customers, additional logging has been added to assist with forward investigation (HAS-6538).

Enforcement Agent Windows (v5.3.1)

🚀 New Features

- Browser Extension Control support (HAS-4621);
- Trusted Installer support (HAS-6180);
- Fixed a buffer overrun crash in the notifier GUI (this does not impact allowlist enforcement) (HAS-6508);
- Fixed an issue where if Windows Explorer crashes the notifier fails to re-open itself on the task bar (HAS-6523);
- Minor Notifier UI improvements (HAS-6409, HAS-6366, HAS-6369, HAS-6370 & HAS-6374);
- Fixed an issue where if the -register command line is called, the old ClientID would still be used for registration if the agent previously had one set (HAS-6352);
- Fixed an issue where OTP codes starting with a leading zero were seen as invalid by the agent (HAS-6355);
- Removed official support for Windows Vista & Server 2008. These operating systems still function however are not fully quality assured (HAS-6443).

Relay Agent (v5.3.1)

🚀 New Features

- Browser Extension Control support (HAS-6524);

🔧 Improvements / Fixes

- Certificate thumbprint fields, grandparent process fields and TBS hash fields are now uploaded by the relay agent (HAS-6540, HAS-6541 & HAS-6542).

Version 5.3.0

Released 21st April 2024

🚀 Headline Features

Airlock Digital v5.3 significantly improves the flexibility of Airlock’s rule engine and contains a number of highly requested product features.

- **Rename Application Captures to Allowlists:** Application Captures are now called Allowlists to better reflect their purpose: Allowlists are for allowing files, Blocklists are for blocking them;
- **Multi Rule Matching through Allowlist Metadata:** Allowlist Metadata significantly improves flexibility by enabling administrators to trust files based on multiple criteria. For example: folder paths rules can be combined with user groups or publishers to only allow files to execute in specific scenarios;
- **Allowlist Package Summary:** Administrators can now see statistics relating to their Allowlist packages, with breakdowns of data including file types and publishers;
- **Customisable OTP Durations:** OTP code durations can now be customised to specific lengths of time to better match organisations individual requirements, such as change windows;
- **Modern Toast Notifications on Windows:** The Airlock Enforcement Agent on Windows has an entirely rebuilt UI component (called notifier). This rebuild contains visual improvements and supports modern toast notifications for Windows 8 onwards;
- **Notification Buttons:** Notifications now support action buttons on macOS & Windows, which provide clickable 'mailto' & URL links whenever a file is blocked;
- **Modern Documentation:** PDF User Manuals are very last decade. To make the information more accessible, easy to read and scalable for the future we have overhauled the documentation in the product. Documentation also supports both light and dark mode.
- **Dashboard Custom Time Selector:** The Airlock Server Dashboard now allows for custom times and dates to be selected for event data.

Upgrade Notes

- v5.3 server deprecates support for v3.x Airlock Enforcement Agents and below, which are now five years old;
- v5.3 server + only supports installation on CPUs that support AVX instructions (most modern CPU's post 2011 will support this) (HAS-5767);
- Upgrading to v5.3 of the Airlock Server is only supported from v5.2.x. If the Airlock Server being upgraded is on an earlier release, you must first upgrade to v5.2.x before upgrading the server to v5.3;
- Please note that Relay Agents must be updated to v5.3 to support new client features and must be performed before downstream enforcement agents are upgraded.

Detailed Changes

Server (5.3.0.1597-Gobert)

🚀 New Features

- Renamed Application Captures to Allowlists (HAS-5794);
- Customisable OTP Durations (HAS-5037);
- Added the ability to upload a custom LDAP public certificate for LDAPS (HAS-5491);
- Allowlist (formerly Application Capture) and Baseline summaries (HAS-5627);
- Added a new Constrained Execution reporting type, so when PowerShell scripts are executed in Constrained Mode they are tagged uniquely from Untrusted Executions or Blocked Executions (HAS-5687);
- Authenticode Hash is now a Blocklist Metadata Criteria (HAS-5689);
- Added a Custom Time Selector in the Dashboard (HAS-5864);
- Added a new server diagnostic script to assist support with server environment troubleshooting (HAS-5965);

- Modern documentation (HAS-6342).

🔧 **Improvements / Fixes**

- Fixed an issue where Trusted Execution logging would not add files to the repository (HAS-5244);
- Fixed twenty issues relating to search where results may not be returned with certain search configurations (HAS-5271 -> HAS-5290);
- Fixed an issue where selecting a policy group could cause the include child dropdown menu to trigger (HAS-5312);
- Fixed an issue where offline clients could be reported incorrectly as stale, if stale client management was enabled (HAS-5441);
- Added a Server Activity History message for license expiry / over provisioning (HAS-5503);
- Upgrade application dependencies (HAS-5672, HAS-5676, HAS-5697, HAS-6077, HAS-6292);
- Added upgrade prevention from v5.1 and earlier releases to prevent not following correct upgrade paths (HAS-5674);
- Metarules when viewed in the browser are now force reloaded on save to prevent errors due to undefined or cached conditions (HAS-5773);
- Fixed an issue where resetting the admin account via the server shell would return an error, even though the reset was successful (HAS-5869);
- Fixed an issue where trusted logging flags for publishers were not correctly cleaned up if the publisher was removed (HAS-5874);
- Fixed an issue where the publisher list on the policies tab would sometimes need to be manually refreshed to load new publishers (HAS-5886);
- Fixed an issue where reference baselines imported via the REST API would all be visually tagged as Windows baselines (HAS-6053);
- The OTP ID column on the OTP tab has been renamed OTP Code (HAS-6165);
- Added an autocomplete dropdown for publisher match values on Allowlists and Blocklists (HAS-6212);
- Reduced load times on the Activity Viewer through database query optimisation (HAS-6268);
- 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 issue where under heavy database load small numbers (<0.5%) of external logs could be dropped (HAS-6332);
- Fixed an issue where the search bulk add capability could fail to load the reputation data overlay during the process (HAS-6353).

Enforcement Agent Linux (v5.3.0.6111)

🔧 **Improvements / Fixes**

- Support Allowlist Metadata rules (HAS-5982);
- Added additional checks to prevent misconfigurations from blocking critical files (HAS-5872);
- Added hostname retrieval on Windows Subsystem for Linux images (HAS-6280);
- The agent’s shell script detection has been improved to cover more detection scenarios (HAS-6121);
- Fixed an issue where a Secure Boot warning could be presented upon installation, even though the agent was operating in FANotify mode where the warning does not apply (HAS-6192);
- Added support for custom OTP durations (HAS-5037).

Enforcement Agent macOS (v5.3.0.8111)

🔧 Improvements / Fixes

- Support Allowlist Metadata rules (HAS-5982);
- Added additional checks to prevent misconfigurations from blocking critical files (HAS-5872);
- Added interoperability with Microsoft Defender for macOS, which improves performance (HAS-6153);
- Support action buttons in notifications (HAS-6269);
- Added support for custom OTP durations (HAS-5037);
- Reduce overall CPU usage when repeated executions occur (HAS-6293).

Application Capture Agent (v5.3.0)

🔧 Improvements / Fixes

- Fixed an issue where the Application Capture Agent would not capture any files in offline mode, if an initial client registration is not performed (HAS-5638);
- Updated the text in the application capture agent to refer to Allowlists instead of Application Captures (HAS-6150).

Enforcement Agent Windows (v5.3.0)

🚀 New Features

- Support Customisable OTP Durations (HAS-5037);
- Rebuilt Notifier UI with Modern Toast Notifications (HAS-5675);
- Support the Constrained Execution Reporting Type (HAS-5687);
- Support Authenticode Hash as a Blocklist Metadata Criteria (HAS-5689);
- Added a Collect Support Logs option in the notifier UI (HAS-5868);
- Support Allowlist Metadata rules (HAS-5982);
- Support action buttons in notifications (HAS-6269).

🔧 Improvements / Fixes

- Modified the digital signature checking precedence to 'fall back' to catalog signing in the event that a directly signed signature is invalid. This will reduce the impact when vendors mistakenly sign files using internal test certificates (HAS-6020);
- Improved memory management when file executions occur under sustained heavy load (thousands of executions per second) preventing memory growth (HAS-6032);
- Added additional validation when the usermode process attaches to the Airlock Driver to help prevent mismatch conditions (HAS-6117);
- Fixed a page fault BSOD identified through minifilter testing. This BSOD is unlikely to be seen under non-testing conditions (HAS-6147);
- Resolve issue where self-upgrade / downgrade would fail on Windows XP x86 (HAS-6340).

Relay Agent (v5.3.0)

🚀 New Features

- Added support for Allowlist Metadata on v5.3.0 Agents (HAS-6310).