Secure Endpoint Private Cloud Release Notes

Version 3.5

14 October 2021

Secure Endpoint Private Cloud Administration Console 3.5.2

Bugfixes/Enhancements

- Fixed API bug resulting in increased number of files sent to Secure Malware Analytics.

28 September 2021

Secure Endpoint Private Cloud Administration Console 3.5.1

Bugfixes/Enhancements

- Fixed failure to download connector when upgrading Linux connector to 1.16.0.
- Update console help to reflect rebranding.
- Fixed failure to register new FMC integration.
- Enabled iOS in standalone airgap mode.

7 September 2021

IMPORTANT! A reboot is required after the upgrade to 3.5.0 for all the changes to take effect.

Secure Endpoint Console v5.4.20210831

New

- AMP for Endpoints has been renamed to Cisco Secure Endpoint.
- Policy Product Update Dates can now use a predefined range of this month, next 7 days, or next 30 days in addition to a custom date range selection.
- The following processes are no longer monitored by Secure Endpoint Windows connector exploit prevention because of compatibility issues:
  - Webex Meetings Troubleshooting Assistant
  - Webex Meetings Manager

IMPORTANT! This change will take effect the next time you save a policy with exploit prevention enabled.

Bugfixes/Enhancements

- Changing the policy for a group triggers a message with a link to the computers page filtered to display all affected connectors.
- Minor bugfixes and performance enhancements.
- Minor dark mode fixes and usability enhancements.
- Eliminated redundant time periods on the reports page.
- Fixed rendering of the legend on dashboard page.
- Improved organization of policy page. (Relocated the event tracing for Windows option)
- Improved rendering at narrow browser window widths.

Secure Endpoint Windows Connector v7.4.3

New

- AMP for Endpoints Windows connector has been renamed to Cisco Secure Endpoint Windows connector.
- New Behavioral Protection engine available.
- Added support for side-grade updating to newer builds of the same version.
- Updated ClamAV to 0.103.2

7 September 2021

Bugfixes/Enhancements

- Addressed an issue when upgrading from 7.3.x to 7.4.x that could cause the connector to be left in a bad state. (CSCvy41367)
- Fixed an issue where the connector would not correctly quarantine malicious files using expired digital certificates.
- Fixed an issue where behavioral protection exclusions sometimes wouldn't work as expected.
- Fixed performance issues with the malicious activity protection driver when used on network drives.
- The connector no longer enables Windows event tracing for Windows 10 version 1803 and earlier.
- Debug logging when enabled in the user interface will now persist through a computer restart.
- Stability updates for TETRA, supporting Windows 21H2 (Preview build 21376.1)
- Connector no longer sends excessive metric events affecting the performance of the Private Cloud Console. (CSCvx99844)
- Fixed exploit prevention engine compatibility issues with the following applications:
- NetOp remote control
- Fortinet
- Sentinel LDK
- Improved compatibility with Microsoft Control Flow Enforcement (CEAT)
- ServiceNow (CSCvy802888)
- VuGen extension for Google Chrome
- Improved stability during connector startup and shutdown.
- Suppress Windows Security Center alerts during future upgrade processes.
- Fixed issue where the user name field was not rendered correctly in MAP detection events.
- Resolved an issue where endpoint isolation state was not honored after a reboot. (CSCvx48035)

Secure Endpoint Mac Connector v1.16.0.841

Bugfixes/Enhancements

- Fixed an issue where the product update time could differ between the Mac endpoint and the console.
- Update libxml2 to 2.9.12, including changes related to the following vulnerability: CVE-2021-3541
- Added a workaround for a network interference issue that exists in macOS 11.3 and 11.4 when network monitoring was enabled. (CSCvy93372)
- Fixed an issue that can cause a high number of disk writes when scanning. (CSCvy75080)
- Fixed an issue that would cause the connector to interfere with IPv6 network traffic on macOS 11.3 and later when network blocking was enabled in the policy.

7 September 2021

Secure Endpoint Linux Connector v1.16.0.768

New

- Added support for sysadmins to build the connector's filesystem and network kernel modules for unsupported kernels.

Bugfixes/Enhancements

- The connector command line interface (ampcli) has been updated to Cisco Secure Endpoint (formerly AMP for Endpoints). This is a display-only change; the connector filenames and directory paths remain the same.
- Fixed an issue that would cause increased CPU usage during mount and unmount operations on the computer. (CSCvy75353)
- Fixed an issue where the connector may log to the syslog at a high volume on RHEL/CentOS/OEL 6 computers. (CSCvz01177)
- Update libxml2 to 2.9.12, including changes related to the following vulnerability: CVE-2021-3541

Secure Endpoint Private Cloud Administration Console 3.5.0

Bugfixes/Enhancements

- Fixed a bug in airgap environment where VirusTotal information was displayed incorrectly.

Secure Endpoint Private Cloud Hardware Appliance 3.5.0

New

- UCS firmware is updated to 4.1(3c).
- Appliance wipe-out now keeps the recovery partition.
- Serial console is now also available over tty.
- Improvements in logging and error handling in the Private Cloud recovery RPM.
- Log rotation for journald logs are now enabled.
- Block all incoming connections to port 80 on the public interface (eth1).

Secure Endpoint Private Cloud Virtual Appliance 3.5.0

New

- Journaling enabled in the /data partition.
- Root partition is now set to 35GB.
- Log rotation for journald logs are now enabled.
- Block all incoming connections to port 80 on the public interface (eth1).

23 July 2021

Secure Endpoint Private Cloud Console 5.4.20210720

Bugfixes/Enhancements

- Fixed failed upgrades from v3.0.1 to 3.4.0 due to ERROR: execute[run_migrate_db_smbe].

Secure Endpoint Private Cloud Admin Console 3.4.1

Bugfixes/Enhancements

- Fixed an issue where retrospective was broken for ESA/WSA integration.

2 June 2021

Secure Endpoint Private Cloud Console 5.4.20210602

New

- Users can now enable and disable the file fetch from the Features section of the Organization Settings page.

Bugfixes/Enhancements

- Fixed an issue where SHA256 values were incorrectly considered unknown.
- Added ExPrev events to the list of the displayed events.
- Fixed display issue about lacking metadata information for iOS apps.
- Fixed asynchronous CSV export of events.
- Fixed preset policies to match recommended settings.
- Added controls to quickly apply recommended workstation and server settings for modes and engines in Windows policies.
- Conviction modes for new Windows policies now default to the recommended workstation settings.
- Added descriptions for each engine's conviction mode settings.
- Updated Advanced Custom Detection signature validation to stop errors when uploading custom clamAV signatures.
- Fixed a timestamp issue with low prevalence executables that was causing errors when generating reports.
- Endpoint IOC scheduled scan times are now displayed without a time zone on the scan summary page because scans start in the connector local time zone.
- Filtering by the statistics at the top of the Computers page now stacks the filters when clicking each one instead of clearing the previous filtered view.
- Added the IP pivot menu to the Audit page.

- Fixed an issue where the Quarantine Failed error reason wasn't displayed in Quarantine Failed Events. (CSCvw45177)
- Exported System Process Protection events now show the parent process path.
- Fixed an issue where Low Prevalence Detections were not rolling over to Threat Detected as expected. (CSCvw49000)
- The context menu allows you to create new outbreak control lists in place through a dialog.
- Added connector scan requests to audit logs.
- Fixed style and alignment issues on various pages
- The default setting for Script Control in new Windows policies is now Audit mode.

Secure Endpoint Mac Connector 1.15.4

New

- The connector now runs on ARM architecture without Rosetta emulation. See Secure Endpoint Mac Connector OS Compatibility for more information. (https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214849-amp-for-endpoints-mac-connector-os-compa.html)

Bugfixes/Enhancements

- " System Extension Blocked" or "System Extension Updated" pop-ups are no longer displayed after connector upgrades on macOS Big Sur.
- Connector installation/uninstallation no longer triggers a Rosetta installation pop-up on ARM architecture Macs.
- Fixed an issue where an invalid proxy policy setting in the connector install package prevented events from being sent to the cloud.
- Temporary files created by the connector scan service are now properly removed if the scanner restarts unexpectedly. (CSCvy06341)
- Fixed an issue where ampcli failed to timeout for long periods of time after attempting to process a command in non-interactive mode.
- Fixed an issue where the connector would monitor lock files, preventing other applications from gaining the lock.
- The scan service no longer restarts when hashing large files.
- Fixed an issue where the connector no longer recognizes macOS binaries as signed with a trusted certificate, resulting in increased CPU usage and possible
- Time Machine failures on the endpoint. (CSCvy01803)
- Added support for wildcards in process exclusions.
- Fixed an issue where the connector was not sending Execution Blocked events in active mode for programs executing in deep directories.
- Fixed a memory leak when running on macOS 11 that can occur when onexecute mode is set to active in policy.
- Improved URL flow visibility for HTTPS and HTTP/3 protocols on macOS 11.
- Added new command for checking connector posture to ampcli.

- Fixed a bug where the AMP Security Extension was incorrectly translated into Korean in the System Preference Full Disk Access window.
- Fixed a memory growth issue when monitoring connections made with Apple's NSURL API with macOS System Extensions. (CSCvx09259)

Secure Endpoint Linux Connector 1.15.4

New

- Added official support for Ubuntu 20.04.0 LTS and 20.04.1 LTS. See Secure Endpoint Linux Connector OS Compatibility for supported operating systems and kernel versions. (https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/215163-amp-for-endpoints-linux-connector-os-com.html)

Bugfixes/Enhancements

- Improved performance when running on systems with kernel modules that frequently spawn a large number of threads.
- Improved file monitoring performance on RAM drives.
- Improved performance when using process exclusions.
- Fixed an issue where an invalid proxy policy setting in the connector install package prevented events from being sent to the cloud.
- Fixed an issue where temporary files created by the connector's scan service were not removed if the scanner restarted unexpectedly, consuming disk space. (CSCvy01076)
- Fixed an issue where ampcli failed to timeout for long periods of time after attempting to process a command in non-interactive mode.
- Fixed an issue that could trigger the scan service to restart when hashing large files.
- Reduced kernel memory usage when monitoring file activity on a system under heavy load.
- The connector will now raise fault 5, amp-scan-svc-user unavailable if its directory privileges have been revoked.
- Added patches for libxml2 version 2.9.10 to address the vulnerability described in CVE-2020-7595.
- Fixed a crash related to the use of process exclusions.
- Fixed an issue where Advanced Custom Detection updates were not processed until connector restart.
- Reduced installer size to further mitigate an issue where 1.12.0-1.12.5
- Connectors may fail to upgrade via policy on slow networks. (CSCvv07225)
- Fixed issue with upload timeouts for remote file fetch and snapshot uploads over slow networks. (CSCvv17811)
- Fixed a kernel panic that can occur when unloading the ampnetworkflow kernel module on CentOS/RHEL 6/7. (CSCvv58039)

- Fixed a bug where the required kernel modules might not load on older CentOS/RHEL distributions, depending on the host kernel version. (CSCvv49913)
- Fixed a problem that would cause the connector to consume significant amounts of memory on CentOS/RHEL 8.1 and 8.2.
- Updated ClamAV to 0.102.4, including changes related to the following vulnerabilities:
  - CVE-2020-3327
  - CVE-2020-3481

Private Cloud Administration Portal 3.4.0

Bugfixes/Enhancements

- Fixed issue loading large support session logs.
- Fixed TLS validations to take into account the whole certificate chain that was passed.

Private Cloud Hardware Appliance 3.4.0

New

- Added a wipe option that retains the recovery partition.

Bugfixes/Enhancements

- Updated appliance firmware to address security and bug fixes.
- Fixed support snapshot generation from console.

1 April 2021

Secure Endpoint Private Cloud Console 5.4.20210330

Bugfixes/Enhancements

- Fixed compatibility issue with computers with Intel Tiger Lake processors running Windows 10 20H2.
- Device trajectory correctly shows data for all event types when accessed from the events page.
- Fixed administration console crash that was caused by very long support session log files.
- Improved reliability for exporting events.
- Fixed issue that prevented users from setting an email address from reset password email.

- Fixed issue where the connector detected and attempted to quarantine allowed files.
- Fixed issue that prevented upgrading to Private Cloud 3.3 after failed migration.

Secure Endpoint Windows Connector 7.3.15

Bugfixes/Enhancements

- Stability updates for Exploit Prevention.
- Fixed Exploit Prevention engine compatibility issues with the following applications:
  - Firefox (CSCvx49567)
  - Powershell (CSCvx47570)
  - Lenovo Smart Standby (CSCvx54732)
  - Microsoft Control Flow Enforcement (CET)
  - Cortex XDR
  - Office Plus
  - Thinapp
- Addressed vulnerability described in CVE-2021-1386. (CSCvw77090)

9 February 2021

Secure Endpoint Private Cloud Console 5.4.20200923

New

- A new Indicators page maps Cloud Indications of Compromise (IOCs) to the MITRE ATT&CK knowledge base of tactics and techniques. You can search the knowledge base by indicator name, tactics, and techniques.
- The Indicators page includes links to the Dashboard, Events, and Inbox tabs filtered to computers that observed the specific Cloud Indications of Compromise.
- You can save and recall filters on the Computers page.
- Added support for Cisco Security Connector and the Clarity module that allows you to investigate incidents and device activity across your iOS devices.
- iOS Clarity tab on the Dashboard provides access to the new Cisco Security Connector features such as App Trajectory and tracking of App usage through Recently Observed Apps.
- MDM Integration settings added to the Accounts > Business page.

9 February 2021

Bugfixes/Enhancements

- Simplified Device Trajectory filters so that selecting none of the flags is now the same as selecting all of them.
- Fixed a cosmetic issue where the Device Trajectory filter button was hidden on wide-screen monitors.
- The default setting for Script Control in new Windows policies is now Audit mode.
- Fixed an issue where the Quarantine Failed error reason wasn't displayed in Quarantine Failed Events. (CSCvw45177)
- Exported System Process Protection events now show the parent process path.
- Fixed an issue where Low Prevalence Detections were not rolling over to Threat Detected as expected. (CSCvw49000)
- The context menu allows you to create new outbreak control lists in place through a dialog.
- Fixed alignment in device trajectory time lines.
- Improved device trajectory scaling for higher resolution monitors.
- Renamed Business Settings to Organization Settings.
- Fixed an issue where the computer scan dialog would not close after a scan was started.
- Fixed an issue where the Diagnose button wasn't working when you navigate to a computer from the Groups page.
- System Process Protection events now display the path for parent files when available.
- Minor UI improvements to the users page.
- Product name is displayed correctly in the vulnerable software report (in console and exported CSV files).
- Fixed an issue where SHA-256 info was missing from quarantine failed events. (CSCvv77863)
- Improved filter view on the Computers page.
- It is easier to make selections in the Device Trajectory interface.
- Fixes to dark mode in Device Trajectory.
- Events arriving at the same time appear in the correct order on the Events page.
- Fixed layout issues on the Computers page when the filter panel is collapsed.
- Fixed alignment issues on the Dashboard and Inbox when items are muted.
- Fixed a discrepancy between the Vulnerable Software page and the CSV export. The CSV export only showed one of the observed groups even if there was more than one group.

Known Issues

- Some built-in iOS apps appear in the interface without icons associated with them.
- The Export CSV button downloads the .csv file directly from the page, but you will not receive an email with the download link.
- Files whose dispositions were changed from malicious to clean are still detected and will generate events for retrospective detection.

- Certain event types are not displayed when Device Trajectory is accessed from the events page.

Private Cloud Administration Portal 3.3

New

- Added options to enable mounting an ISO file on an NFS server using `amp-ctl iso`.
- Added a new page for mounting an ISO file on an NFS share.
- Updated Base OS to CentOS 7.8.2003.

Bugfixes/Enhancements

- CIMC console functionality on serial TTY.

IMPORTANT! Appliance Reinstall and Appliance Wipe operations do not provide output of their progress to the CIMC console. When one of these operations are performed, the user must wait for the appliance to reboot to ensure that these operations have completed successfully.

- Improved TLS certificate validations.
- HTTP Strict Transport Security Header is enabled for sites served off eth1.
- Connectors can quarantine PowerShell files and others on file creation.
- TLS 1.0/1.1 will be deprecated in favor of TLS 1.2 in a future Private Cloud release. If you wish to restrict your appliance to TLS 1.2 for PC-3.3.0, see the AMP-CTL Commands section of the user guide for information on the tls-insecure command. Integrations will require the following minimum versions that support TLS 1.2:
  - Firepower Management Center: 6.4.0+
  - Email Security Appliance: 13.5.2+
  - Web Security Appliance: No TLS 1.2 support

Secure Endpoint Windows Connector 7.3.9 (supersedes 7.3.3 and 7.3.5)

New

- Added support for the Windows 10 October 2020 update.

Bugfixes/Enhancements

- Improved cloud registration process to prevent deadlock under high system activity. (CSCvw34067)
- Addressed an issue where the connector would have trouble shutting down in a timely manner.

- Script Control can now be set to audit, block, or disabled independently from your Exploit Prevention settings. This can be changed in policies under Advanced Settings -> Engines. (CSCvv87628)
- Connector no longer holds on to connections longer than necessary, avoiding network resource exhaustion on Windows. (CSCvv85169)
- Addressed a local privilege escalation vulnerability. (CSCvv53346, CVE-2021-1280)
- The connector now sends separate notifications for script control detections with the Exploit Prevention engine.
- Fixed a bug where the connector is disconnected for the length of the heartbeat interval after configuration changes.
- The connector now attempts to reconnect with the Private Cloud appliance faster after a failure instead of waiting for the next heartbeat interval.

Secure Endpoint Mac Connector1.14

New

- Added official support for macOS 11 (Big Sur). This release supports macOS 10.14, 10.15, and macOS 11. Mac connector versions prior to 1.14.0 are not compatible with macOS 11.

IMPORTANT! New full disk access approvals are required after upgrading to this release on all versions of macOS. Install and grant all required permissions to the 1.14.0 Mac connector before upgrading macOS to ensure continued protection of the endpoint.

- The Mac connector requires new approvals for full disk access. MDM profiles must be updated to ensure continued protection. If MDM profiles are not being used the connector will be unable to provide full protection until access has been granted by the end user. See this TechNote for details on these changes.
- This TechNote has been updated with descriptions of new Mac connector faults.

Bugfixes/Enhancements

- New alert icon for the menulet user interface.
- Use legacy kernel extensions on all versions of macOS 10.15. This fixes third-party software compatibility issues seen when the new system extensions API is used on macOS 10.15.
- Fixed an issue that could result in high CPU/memory usage when the connector is unable to connect to the AMP Network Extension on macOS 11.
- Improve fault guidance when unable to connect to the AMP Network Extension on macOS 11.0.
- Connectors on macOS 11.0 now report the operating system version correctly.
- Fixed an issue that could cause Time Machine backups to a remote drive or Time Capsule to fail.

- When running the uninstaller from a service, users will now be prompted twice to remove the AMP System Extensions, allowing the connector to uninstall cleanly.
- Updated ClamAV to 0.102.4, including changes related to the following vulnerabilities:
  - CVE-2020-3327
  - CVE-2020-3481

29 January 2021 Release Notes

Secure Endpoint Windows Connector 7.3.9

Bugfixes/Enhancements

- Addressed an issue where the connector would have trouble shutting down in a timely manner.
- Script Control can now be set to audit, block, or disabled independently from your Exploit Prevention settings. This can be changed in policies under Advanced Settings -> Engines. (CSCvv87628)
- Connector no longer holds on to connections longer than necessary, avoiding network resource exhaustion on Windows. (CSCvv85169)
- Improved cloud registration process to prevent deadlock under high system activity. (CSCvw34067)
- Addressed a local privilege escalation vulnerability. (CSCvv53346)
- The connector now sends separate notifications for script control detections with the Exploit Prevention engine.
- Fixed a bug where the connector is disconnected for the length of the heartbeat interval after configuration changes.
- The connector now attempts to reconnect with the private cloud faster after a failure instead of waiting for the next heartbeat interval.

15 October 2020 Release Notes

AMP for Endpoints Private Cloud Console 5.4.20200923

New

- The Automated Actions page lets you set actions that trigger when compromise events occur on Windows endpoints in selected groups. See the user guide for details.
- Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation.

- There is a new Endpoint Isolation IP Allow list type under Outbreak Control > Network – IP Block & Allow Lists. Policies and groups using the Endpoint Isolation IP Allow lists will appear in the IP List details panel. All IP allow lists for Endpoint Isolation must be created using this new list type.
- Endpoint Isolation is available on Demo Data computers. The group policy for the Demo Data computers must have Endpoint Isolation enabled. Endpoint Isolation is available for Windows connector versions 7.0.5 and later.
- If you enter the unlock code incorrectly 5 times during an Endpoint Isolation session, you will not be able to make another attempt to unlock it again for 30 minutes.
- Filtering for Endpoint Isolation has been added to the audit log.
- Added ability to stop endpoint isolation in bulk.
- Added block, audit, and disable conviction modes for Exploit Protection.
- New processes protected by Exploit Protection:
  - Microsoft HTML Application Host
  - Windows Script Host
  - Microsoft Assembly Registration Tool
  - Zoom
  - Skype
  - Slack
  - Cisco Webex Teams
  - Microsoft Teams
- The engine also monitors the following directories:
  - Windows AppData Temp Directory (\Users\[username]\AppData\Local\Temp)
  - Windows AppData Roaming Directory (\Users\[username]\AppData\Roaming)
- Processes excluded from Exploit Protection monitoring for compatibility:
  - McAfee DLP Service
  - McAfee Endpoint Security Utility

IMPORTANT! This change will be included when you change the Exploit Prevention conviction mode to block, or the next time you save a policy that already has Exploit Prevention set to block. Until then the existing list will be used.

- The Exploit Prevention feature, Script Control prevents certain DLLs from being loaded by a list of monitored applications and their child processes. The engine will kill a process if it or one of its child processes attempts to load one of the blocked DLLs.
- Added a policy setting to enable a button in the Windows connector UI to update TETRA definitions on demand. Only available for Windows connector 7.2.11 and higher.
- IP List Create and Update Audit Logs show the specific IP addresses that were added and deleted from the list.

- When exporting events to a CSV file, you will now receive an email containing a link to download an archive file containing one or more CSV files depending on the number of events.
- Added a policy setting to allow the MAP engine to monitor network drives.

> **IMPORTANT!** This setting will be enabled when you change the MAP conviction mode to audit, block, or quarantine or the next time you save a policy that already has MAP set to audit, block, or quarantine. Until then, it will not be enabled.

Bugfixes/Enhancements

- The “Need Connector Update” metric on the Computer Management page counts unsupported connectors.

> **IMPORTANT!** The number of connectors that need updates are higher than before because unsupported connectors are now counted.

- Fixed a time stamp discrepancy between events in the console and the downloaded CSV files.
- Event export CSV files were renamed when the export consists of a single file.
- Fixed discrepancies between license information displayed on the license page vs. displayed on the weekly/monthly/quarterly reports.
- To make the presentation of events more consistent between the Events tab, CSV export and the API, all events are displayed as separate independent events. (Before this version, a detection event followed by a quarantine event was displayed as a single event. As of this version, these events are displayed separately.)

Private Cloud Administration Portal 3.2

- Implemented new restrictions on certificates compatible with the following:
  - https://support.apple.com/en-us/HT210176
  - https://support.apple.com/en-us/HT211025
- Changed email notifications to be from “AMP for Endpoints”.
- Prevent backups from starting when another backup is already in progress.
- Prevent backups from starting when Cloud Log Replay is running.
- Removed all but two support snapshot options.
- Updated authentication service help message.
- Error is now displayed when an appliance reconfiguration fails.

AMP for Endpoints Windows Connector 7.3.1

New

- Exploit Prevention engine with Audit mode support.

- Exploit Prevention engine with Script Control support.
- Added support for Windows 10 May 2020 Update (Version 2004).
- Improved secure communication between the connector and Private Cloud.

Bugfixes/Enhancements

- Increased the number of process exclusions honored by the connector to 500.
- Improved stability of local UI notifications.
- Addressed an issue where System Process Protection exclusions would not work for processes that start before the connector. (CSCvt63211)
- Changed connector driver altitudes to officially registered altitudes.
- Removed connector-related events and logs from a computer when the connector is uninstalled.
- Addressed issues with file exclusions.
- Addressed an issue with low prevalence uploads of portable executable files. (CSCvv52410)
- General performance and stability improvements for Exploit Prevention engine.
- Fix for the vulnerability described in CVE-2019-0708.
- Fixed Exploit Prevention engine compatibility issues with the following applications:
  - APTA Connect
  - MS PowerPoint 2016/2013
  - FSLogix
  - Internet Explorer and different plugins
  - CIG
  - ACG
  - MS Office App-V applications
  - Visual Studio debugger
  - Vizient and Open Text IRM
  - Black Knight
  - Powershell System.Management.Automation.Runspaces.LocalRunspace
  - PDF API and HTML to PDF Converter for .NET (EO.Pdf.dll)
  - ExOpen
  - Outlook VBA plugin
  - CyberArk
  - Forcepoint Insider Threat
  - Diva Client
  - AppV
  - Universal Windows Platform apps
  - Articad
  - Macros In Excel 365
  - BIFIT signer plugin in Microsoft Internet Explorer

- Product upgrades no longer fail under a rare condition when the Network Flow Monitoring (NFM) driver was left behind from an old connector that required reboots on upgrades. (CSCvv20713)

  IMPORTANT! A reboot will be required for this upgrade on any computers where the connector meets this condition.

- Fixed a privilege escalation vulnerability. (CVE-2020-3350, CSCvt98752)
- Improved TETRA definition update mechanism by dropping buggy ciphers from the update servers. (CSCvu75358)
- Made stability and efficacy improvements to the Malicious Activity Protection engine.
- For policy upgrades the connector honors the time zone on the endpoint rather than assuming UTC-0. (CSCvt59185)
- File properties are filled out for AMP connector DLLs.
- Addressed crash that could sometimes occur when connector is configured to use a proxy to communicate with the Private Cloud.
- Addressed issue where connector upgrades could hang indefinitely.
- Addressed issue where an identity sync error could cause the connector to hang on shutdown.
- Addressed issue where some DLL files were not removed after uninstalling the Windows connector.
- Connector generates driver logs on agent start up if configured to in the policy.
- Cleaned up signal handling in Proxy Discovery.
- Performance improvements for Script Protection.
- Addressed issue where System Process Protection exclusions would not work for processes that start before the connector. (CSCvt63211)
- Update driver altitude to fix compatibility issue against other AV. (CSCvt99262)
- Fixed connector crash caused by long network interface names. (CSCvu15646)
- Fix to prevent ClamAV log files from filling up disk space. (CSCvu65043)
- Updated Exploit Prevention Engine to include changes related to the vulnerability described in CVE-2020-0796.
- Malicious Activity Protection (MAP) engine performance improvements.
- Resolved an issue where the connector service would freeze on startup under certain circumstances. (CSCvt38340)
- Fixed an installer issue that failed to send reboot completed and update completed events when a reboot is required on upgrade.
- Windows connector now reports the correct processor ID of the computer.
- Fixed an issue where the connector could cause a fatal system error when used in conjunction with software that use file system locks as part of their normal operation. (CSCvt56075)
- Improved uninstall logic to gracefully handle Orbital uninstall failures that could block the connector uninstall.
- Updated Connectivity Test Tool with new command line arguments and output.
- Script protection across the local endpoint, attached storage, and network.

- Fixed an issue where ClamAV was taking long time in scanning PDF files resulting into longer high CPU usage. (CSCvs33228)
- Addressed issue where Windows connector would fail to upgrade when installed alongside BitDefender AV. (CSCvs58858)
- Fixed an issue with ClamAV where scanning a certain zip file was crashing Windows connector. (CSCvs34538)
- Resolved an issue where having %temp% path set to different drive than primary drive will fail the Windows connector upgrade. (CSCvs62397)
- Updated Exploit Prevention engine to address the vulnerability described in CVE-2020-14418. (CSCvu61848)
- Updated ClamAV to 0.102.1, including changes related to the vulnerability described in CVE-2019-15961.

AMP for Endpoints Mac Connector 1.12.7 (supersedes 1.12.0-1.12.4)

Bugfixes/Enhancements

- Reduce installer size to further mitigate issue where 1.12.0-1.12.4 connectors may fail to upgrade via policy on slow networks. (CSCvv37020)
- Fixed issue with upload timeouts for remote file fetch and snapshot upload over slow networks. (CSCvv17808)
- Patched ClamAV 0.102.3 to include changes related to the following vulnerabilities:
  - CVE-2020-3481
  - CVE-2020-3327
  - CVE-2020-3341
- Fixed a timeout issue that could cause failures when upgrading the connector via policy on slow networks. (CSCvv07225).
- The installer removes stale database files when upgrading from an older version of the connector. (CSCvu98581).
- The connector now scans all local storage devices and logical volumes during a full scan.
- Reduced connector CPU and disk space usage when the associated user of a process exclusion does not exist on the system.

AMP for Endpoints Linux Connector 1.13.2

New

- Added official support for RHEL/CentOS/Oracle Linux 8.1 and 8.2. The kernel-devel package must be installed on these systems to enable realtime network and file monitoring. A connector fault will be raised if this package cannot be found. See Linux Kernel-Devel Fault for more information.

- Automatic crash reporting is available when the connector is running on RHEL/CentOS/Oracle Linux 7 and 8. The setting is enabled by default and can be found in Administrative Features under Advanced Settings in Linux connector policies.

Bugixes/Enhancements

- Reduced installer size to further mitigate an issue where 1.12.0–1.12.5 connectors may fail to upgrade via policy on slow networks. (CSCvv07225)
- Fixed issue with upload timeouts for remote file fetch and snapshot uploads over slow networks. (CSCvv17811)
- Fixed a kernel panic that can occur when unloading the ampnetworkflow kernel module on CentOS/RHEL 6/7. (CSCvv58039)
- Fixed a bug where the required kernel modules might not load on older CentOS/RHEL distributions, depending on the host kernel version. (CSCvv49913)
- Fixed a problem that would cause the connector to consume significant amounts of memory on CentOS/RHEL 8.1 and 8.2.
- Updated ClamAV to 0.102.4, including changes related to the following vulnerabilities:
  - CVE-2020-3327
  - CVE-2020-3481
  - CVE-2020-3341
- Reduce installer size to further mitigate issue where 1.12.0–1.12.5 connectors may fail to upgrade via policy on slow networks. (CSCvv07225)
- Fixed issue with upload timeouts for remote file fetch and snapshot upload over slow networks. (CSCvv17808)
- Fixed realtime filesystem and network monitoring when running the connector on RHEL 7.9 beta releases.
- Fixed a timeout issue that could cause failures when upgrading the connector via policy on slow networks (CSCvv07225).
- The installer removes stale database files when upgrading from an older version of the connector (CSCvu98581).
- The connector now scans all local storage devices and logical volumes during a full scan.
- Reduced connector CPU and disk space usage when the associated user of a process exclusion does not exist on the system.

1 June 2020 Release Notes

AMP for Endpoints Private Cloud Administration Portal 3.1.2

Bugfixes/Enhancements

- VPC devices with 1.8 TB or more disk space won't be incorrectly recognized as appliances.
- Fixed invalid JSON parsing in support snapshots.
- Fixed a bug where the BIOS update would fail after updating the BMC firmware.
- Fixed a bug where the log file for Event Log Replay would get deleted.
- Corrected an invalid RabbitMQ hostname for Event Streams API.

AMP for Endpoints Mac Connector 1.12.4

Bugfixes/Enhancements

- Fixed a memory leak that could occur when setting up a proxy.

AMP for Endpoints Linux Connector 1.12.4 (supersedes 1.12.3)

- Fixed an issue in the redirfs kernel module affecting connector version 1.12.3 on RHEL/CentOS 6 that could cause the computer to hang with high CPU utilization. You must reboot the computer after upgrading for the changes to take effect. (CSCvu07130)
- Fixed a memory leak that could occur when setting up a proxy.

IMPORTANT! Linux connector 1.12.4 and earlier does not have official support for RHEL/CentOS/Oracle Linux 7.8. connector does not protect computers that are running unsupported versions of Linux.

6 May 2020 Release Notes

Private Cloud Administration Portal 3.1.1

New

- Upgraded UCS BMC and BIOS.
- The portal is Cisco AMP for Endpoints-branded.
- Updated EULA.
- The support snapshot progress bar updates in real-time.
- A notification displays progress during data migration.
- You are notified if a reboot is required after applicable system updates.

- The changelog has moved to the 'details' section in the Notifications Catalog.
- Newly created passwords must pass new policy guidelines.
- Password recovery instructions are accessible from the log-in page.
- Support snapshots have been simplified. All formerly available options are included in support snapshots by default.
- Support session parameters are read-only.
- The backup limit is 1.
- New option to check for IP address conflicts on the Network Configuration page.
- Private Cloud has been updated to CentOS 7.6.

IMPORTANT! Private Cloud 3.1.1 requires 1.1 TB free disk space and 128 GB RAM. See this TechZone article for information on adding disk space and RAM to your virtual machine: http://go2.cisco.com/PC311AddDiskSpaceRAM

Bugfixes/Enhancements

- Email Configuration page validates upstream hostname.
- "Create snapshot" button is disabled while a snapshot is in progress.
- Support snapshot list shows "missing file" if the snapshot file does not exist.
- User is redirected from the login page if already authenticated.
- Notification when a support session is running.
- User is redirected to the setup page when restore fails.
- Certificate upload is disabled if no file is present.
- Certificate requirements checklist is updated when a file is removed.
- Cisco Cloud metrics are only displayed in Cloud Proxy mode.
- Tabbing between fields on the "Change Password" page does not cause an error.
- System password is preserved when a backup has been restored.
- 'Perform backup' button is disabled while either backup or data migration is in progress.
- License validity is now based on date, not time-of-day.
- Fixed support for non-English characters in licenses.
- The administration portal can be accessed after an eth0 IP change.
- The CD-ROM is always ejected after the disk is unmounted.
- Support sessions persist through network losses and reboots.
- An error is displayed if a backup fails due to lack of disk space.
- The update changelog correctly shows special characters.
- False positive executables that were recently seen are restored from quarantine.

AMP For Endpoints Private Cloud Console 5.4.20200429

New

- The heat map is now displayed in the Dashboard tab.

- Redesigned Overview tab displays an interactive view of statistics.
- Redesigned Prevalence page.
- Redesigned Policies page.
- Redesigned Exclusions page.
- Redesigned Users page with new filter interface.
- The Business pages in the Accounts menu have been combined into a single Business Settings page.
- AV Definitions Threshold on the Business Settings page enables the user to set the threshold for out of date definitions.
- Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation.
- Added AV Definition Summary page under the Management tab to view recent AV updates.
- Users can configure SSO on Business Settings page.
- Users can directly access License Information from the Accounts menu.
- Users can create an IP list by uploading a CSV file containing IP addresses/CIDR blocks.
- Users can edit and manage their IP lists in the console.
- IP List types have been renamed to Block and Allow lists.
- Users can view and configure quarterly reports in addition to monthly and weekly reports. Quarterly reports aggregation is based on calendar quarters.
- Redesigned reports with new data summaries.
- The following events are now hidden to reduce the number of extraneous events visible to the user.
- Quarantine Item Deleted
- Failed to Delete from Quarantine
- Attempting Quarantine Delete
- Users can select which types of announcements to receive through email notifications by clicking the Announcement Email Preferences link.
- Emails now come from no-reply@amp.cisco.com.
- A summary of metrics is displayed at the top of the Computers page.
- You can filter the computer list by operating system by selecting the respective tab on the Computers page.
- New Device Trajectory interface with navigator for quickly pinpointing events.
- When editing Windows exclusion sets, there is a check box to apply the wildcard exclusion to all drive letters.
- Users can enter or paste a list of multiple exclusions to add to exclusion sets.
- This release introduces a new UI for Exclusions.
- Users can choose specific date ranges instead of only predefined ranges with the date/time picker on the Dashboard, Inbox, and Overview tabs.
- Added Cisco-Maintained Exclusions to the Exclusions page to allow more granular control of application-specific exclusions for certain applications. You can now add both Cisco-Maintained Exclusions and your Custom Exclusions to policies.

- Connector Diagnostics enable users to remotely request a support package from a computer. Requested diagnostic files will be available in the File Repository, so you must have Two-step verification and Remote File Fetch enabled to use this feature.
- Redesigned Overview tab displays the status of your environment and highlights recent threats and malicious activity in your AMP for Endpoints deployment. Users can click on the headings of each section to navigate directly to relevant pages in the console to investigate and remedy situations.
- Threat severity provides quick insight into the most important compromises and is now visible in the Dashboard, Inbox, and Event tabs. Threat severity also appears in exported CSV reports, CTA events, subscription email, and the streaming API.
- Users can use the Audit Logs API to retrieve audit logs.
- Added a new field called av_update_definition in the REST API response for single computer queries that include AV version and status values.
- Users now have the ability to delete a group using the REST API.
- Calls to start, stop, and retrieve Endpoint Isolation status are available in the API.
- Endpoint Isolation APIs have been added.
- Vulnerabilities API now enables you to filter by group GUID.
- Vulnerabilities API now enables you to get a list of computers with a specific vulnerable application by passing the SHA-256 of the application.
- Added a REST API for querying vulnerabilities observed in the last 30 days.
- Command line data is now available in the API.
- REST API for Event Streams added.
- Export CSV on event page is limited to 100,000 events.
- Updated EULA.

Bugfixes/Enhancements

- The Console can be accessed after an eth1 IP change.

AMP for Endpoints Windows Connector 7.1.5

New

- Added support for the Windows 10 November 2019 Update (version 1909).
- Added support for Windows Server 2019
- Upgrading and uninstalling the Windows connector no longer requires a reboot in most situations.

IMPORTANT! No reboot upgrades only apply when upgrading from connector version 7.x.x to a later version. While most upgrades will not require a reboot, there may be occasional instances where a reboot is still required.

- Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation.

- New installer command line switch to skip registration and startup of connector in order to use the Windows operating image as a deployable golden image:
- /goldenimage = 1 (Skip initial connector registration and startup on install)
- /goldenimage = 0 (Do not skip initial connector registration and startup on install)
- Support for scanning Windows shortcut (.lnk), RAR5 compressed and Postscript file types.
- System Process Protection engine detections generate Console events and Windows Event Viewer messages.
- Added to the Exploit Prevention engine:
- 64-bit process support.
- Process-hollowing protection.
- Adware injection protection.
- Exploit Prevention engine sends detection notifications for VBScript attacks.
- Windows connector support package is now a ZIP file instead of 7zip so that Windows can natively unpack the support package.
- New certificate for the Early Launch Antimalware (ELAM) driver.
- New Cisco Anti-Malware Protected Process Light (AM-PPL) services “Cisco Security connector Monitoring Service(CSCMS)” to register with WSC on Windows 10 19H1 and beyond.
- Connector supports launching the AMP UI from WSC, and also shows statuses. (CSCvo61707)
- Windows connector Crash is now handled by the Cisco Security Connector Monitoring Service (CSCMS) Server.

Bugfixes/Enhancements

- Updated TETRA license key.

  IMPORTANT! The TETRA license for Windows connector versions 5.1.11, 5.1.15, and 6.1.7 will expire on May 13, 2020. To continue using the TETRA engine you must upgrade to connector version 7.1.5 or newer, or trigger the license update on the connectors by modifying every Windows policy (this could be a minor change, such as simply renaming the policy).

- System Process Protection notifications
  - are less verbose. (CSCvn41948)
  - are no longer sent when the process in question is excluded by process exclusions. (CSCvo90440)
- A failing System Process Protection rule no longer prevents the Self Protect driver from starting.
- Addressed System Process Protection (SPP) event notification issue which was being triggered under certain conditions, even if the SHA-256 is allowed (CSCvn41948).
- Fixed System Process Protection (SPP) exclusions issue which was triggering event notifications for certain processes, even if they are excluded via process exclusion (CSCvn30222).

- Improved evaluation of System Process Protection (SPP) event notifications.
- Fixed Exploit Prevention engine from blocking Windows 10 updates
- Fixed an Exploit Prevention engine issue that could cause Google Chrome v78 and later to crash or display a renderer code integrity error.
- Stability improvements in the Exploit Prevention engine.
- Improved Exploit Prevention engine to prevent deadlock during initialization in rare cases.
- Multiple Exploit Prevention detection engine fixes and performance improvements [CSCvi60967].
- Fixed Exploit Prevention engine access violation issue which crashed the connector.
- Improved Exploit Prevention engine with added protection against BlueKeep security vulnerability discovered in Microsoft's Remote Desktop Protocol. (CVE2019-0708)
- Exploit Prevention events will now contain parent process information.

- Resolved Exploit Prevention engine compatibility issue with the following applications:
  - SAP SSO Addon
  - Microsoft Excel 2016
  - XLSLINK software
  - Kronos ERP add-on (CSCvq76698)
  - ExOpen plug-in (CSCvq73086)
  - .NET applications (CSCvq74953)
  - Adobe Acrobat (CSCvq46250)
  - WIDOS Application
  - Micro Focus Unified Functional Testing (UFT) Application (CSCvq18773)
  - Insider Threat/Web Insider (CSCvq09279)
  - MS Excel plugin Aspen
  - Fasoo DRM
  - Trusteer Rapport
  - ivanti application
  - MS Excel plugin ResQ
  - Tavos Taxport web app
  - MalwareBytes AV
  - Java installer.
  - Adobe add-on PitStop Pro
  - Internet Explorer with VBScript running on local machine (CSCvo91932)
  - Skype Meetings App
  - IPFX plug-in for Outlook
  - MS PowerPoint Presentations (CSCvn69111)
  - Litera ChangePro add-on for Outlook
  - RDP (RD web access)
  - Eden add-on for Outlook (CSCvg00086)
  - Trend Micro
  - Office 365 32-bit on Windows 10 October 2018 Update (Version 1809) (CSCvn54432)
  - Intel HD Graphics
  - Outlook add-on iManage
  - Excel plugin KuTools v19 - 64bit/32bit (CSCvq02201)
  - Nuance EditScript MT 11 (CSCvq02237)
  - Symantec PGP (CSCvq02223)
  - Symantec DLP Plugin (CSCvq02211)
  - SKYSEA Client (CSCvp84312)
  - AppV container
- Reduced false positives with the Malicious Activity Protection engine.
- Stopped Malicious Activity Protection (MAP) from monitoring network drives (CSCvo32112)

- Addressed an issue where the connector could cause a BSOD in MAP driver under rare conditions (CSCvp03825)
- Fixed issue in Malicious Activity Protection (MAP) engine which caused the computer to freeze or crash after starting Visual Studio in debug mode (CSCvn52070).
- Malicious Activity Protection (MAP) engine performance improvements (CSCvm37593).
- Malicious Activity Protection engine no longer incorrectly detects Google Chrome.
- Reduced false positives with the Malicious Activity Protection engine.
- Addressed an Endpoint IOC engine crash for non-English versions of Windows (CSCvs09940).
- Endpoint indication of compromise (IOC) driver stops gracefully when uninstalling Windows connector.
- Improved stability for the Protect driver.
- Memory leak fixes and other stability improvements in the Self-Protect driver.
- Fixed a crash on shutdown issue.
- Fixed issue where the support tool would sometimes fail to include all necessary files.
- Support tool is more stable and supports long file paths (CSCvh97231).
- Fixed Cisco AMP for Endpoints crash on startup when Windows Management Instrumentation (WMI) service is disabled. (CSCvq39434)
- Fixed Cisco AMP for Endpoints Windows Command Injection Vulnerability (CVE2019-1932, CSCvp53361).
- Fixed BSOD caused when connector, under some circumstances, incorrectly requests a file to be quarantined from a different volume than where it was originally detected. (CSCvo11650)
- Fixed incompatibility with MS Sysprep.
- Windows connector Installer can now handle special characters in the install path. (CSCvk54455)
- Improved stability for the connector installer.
- Increased connector installer resource size to accommodate large policies (CSCvk03811).
- Windows connector no longer protects itself when the connector service is set to ‘disable’, thereby allowing users to modify the connector’s service status. (CSCvj72318)
- Fixed logic around deleting quarantine files that exceed the TTL and have already been deleted. (CSCvo00165)
- Added a new check for the end-of-file on non-Microsoft file systems which will prevent a custom app from hanging when running through a network share with Windows connector installed.
- Enhanced Identity Sync logic to prevent Windows connector from falling back to the default group (CSCvo23266)
- Improved Identity Sync logic to prevent duplicate connectors in the Console and dropping to the default group [CSCvi92800].
- Improved hash calculation process to prevent deadlock under certain conditions (CSCvn99024).

- Include mitigation for the Windows DLL preloading vulnerability (CVE-2018-15452) (CSCvm93525).
- Address Scanning Denial of Service Vulnerability (CVE-2018-15437) (CSCvk70945).
- Limit the number of quarantined items to reduce quarantine folder growth (CSCvk22403).
- Fixed Windows Security Centre (WSC) registration issue around TETRA settings.
- Enhanced kernel logging.
- Improved performance of Process Exclusions.
- Fix to mitigate connector high CPU usage.
- Fixed a bug where duplicate connectors were created when cloning a virtual machine.
- Improved performance of Support Diagnostic Tool.
- Addressed an issue where the connector could cause Blue Screen of Death
- (BSOD) under rare circumstances (CSCvo24869).
- Fixed incompatibility with MS Sysprep.
- Fixed compatibility issue with Kaspersky Real-Time Engine which prevented
- it from starting (CSCvq22483).
- Fixed an issue where currently running rootkit scans continued to run after the connector service was stopped.
- Fixed incompatibility with Kaspersky Real-Time Engine.
- Windows connector gathers the BIOS serial number more reliably when it is needed to detect hardware changes for registration with Private Cloud.
- Updated curl to v7.66.0, including a fix for an integer overflow vulnerability in NTLM password authentication (CVE-2018-14618).
- Updated ClamAV to 0.101.4. This version addresses the following vulnerabilities:
  - CVE-2019-1010305
  - CVE-2019-12625
  - CVE-2019-12900
  - CVE-2019-1787
  - CVE-2019-1788
  - CVE-2019-1789
  - CVE-2018-0360
  - CVE-2018-0361

AMP for Endpoints Mac Connector 1.12.3

New

- This release supports macOS 10.13, 10.14, and 10.15.
- Improved connector authentication when connecting to Private Cloud services.
- Added support for Process Exclusions.
- Added RARv5 archive extraction support.

- Connector now runs ClamAV file scans using an unprivileged process. A new cisco-amp-scan-svc user will be created by the installer. File scan operations are now run as an independent process.
- Enabled PCRE definitions in ClamAV.
- Added menu item and CLI command /opt/cisco/amp/ampcli defupdate to initiate ClamAV definition update.
- Added support for user data protection in macOS 10.14 and 10.15.
- Added Apple notarization to connector install package.
- The installer is now packaged using the Disk Image (.dmg) file format.

Bugfixes/Enhancements

- Added ID numbers to fault information displayed in the command line.
- Fixed an issue where deleting a file on a locally-hosted network share was incorrectly identified as an execute event.
- Fixed an issue where scripts were incorrectly identified as Mach-O files in execute events.
- Report the connector's unique hardware identifier as part of connector registration.
- Performance improvements for systems with many repeating execute events.
- Improved handling of corrupt AMP kernel extension files detected on the system during install/upgrade.
- Made stability improvements in the connector installer.
- Reduced install time when using Active Directory/LDAP.

- Updated ClamAV to 0.102.1, including changes related to the following vulnerabilities:
  - CVE-2019-15961
  - CVE-2019-1010305
  - CVE-2019-12625
  - CVE-2019-12900
  - CVE-2019-1787
  - CVE-2019-1788
  - CVE-2019-1789
  - CVE-2018-0360
  - CVE-2017-16932
  - CVE-2018-14679
  - CVE-2018-0361
  - CVE-2018-15378
  - CVE-2018-14680
  - CVE-2018-14681
  - CVE-2018-14682
- Updated third-party libraries, including changes related to these vulnerabilities:
  - Curl:
    - CVE-2018-16840
  - CiscoSSL:
    - CVE-2018-0732
    - CVE-2018-0737
    - CVE-2018-5407
  - SQLite:
    - ORDER BY LIMIT fix http://www.sqlite.org/cgi/src/info/9936b2fa443fec03ff25
  - XML2:
    - CVE-2018-14404
- Improved detection events to include download source URL when available (CSCve69181).
- Changed virus definition update download protocol from HTTP to HTTPS.
- Fixed incorrect known virus count in virus definition update event.
- Fixed memory leak affecting systems with low filesystem and network activity.
- Fixed memory leak that may occur after a detection event.
- Fixed memory leak that may occur after applying virus definition update.
- Improved UI stability.
- Reduced CPU usage by optimizing file scan algorithm.
- Reduced error log messages when file scan processing queue is full.
- Fixed memory leak when disconnected from the Private Cloud.
- Improved handling of file activity from system processes like Spotlight.

- Delete stale ClamAV temporary files when file scan terminates abnormally (CSCvo74969).
- Fix intermittent file scan failure if debug logging has been enabled for a long time.
- Fixed scheduled full scan incorrectly processed as single file scan(CSCvn36511).
- Fixed connector status may be stuck at "Offline" after system time change.
- Fixed unintended quarantine when a retro quarantine request is received in Audit mode.
- Reduced overhead on system, especially when compiling software.
- Fixed memory leak when reading certificates from config.
- Fixed missing log messages for file-op command line logging.
- ClamAV definition information is now displayed in CLI and menulet.
- Improved stability of Cloud network connections.
- Improved tracking and reporting of connector faults.
- Improved descriptions for connector events reported in the CLI and history pages.
- Added filter for network events in the Event list.
- Reduced volume of NetworkFlowLib logs generated in some situations.
- Improved execute monitoring performance.
- Clicking on a fault in the menulet now opens the relevant System Preferences.
- Updated menulet status icons.

AMP for Endpoints Linux Connector 1.12.3

New

- Added official support for RHEL/CentOS 7.6/7.7.
- Added official support for RHEL/CentOS 6.10.
- Added official support for Oracle Linux 6.10 Red Hat Compatible Kernel (RHCK). Oracle UEK is not supported.
- Added official support for Oracle Linux 7.7 Red Hat Compatible Kernel (RHCK). Oracle UEK is not supported.
- Connectors are now signed.
- Improved connector authentication when connecting to Private Cloud services.
- Added kernel modules built with a Retpoline-enabled compiler for RHEL/CentOS 6.
- Added support for Process Exclusions.
- Added lightweight Linux-only ClamAV definition configuration option.
- Added RARv5 archive extraction support.
- Connector now runs ClamAV file scans using an unprivileged process. A new cisco-amp-scan-svc user will be created by the installer. File scan operations are now run as an independent process.

- Added CLI command /opt/cisco/amp/bin/ampcli defupdate to initiate ClamAV definition update.
- Connector now reports a fault when filesystem monitor or network monitor fails to start (CSCvm10710).

IMPORTANT! There is an incompatibility between Linux connector version 1.12.3 and RHEL/CentOS/Oracle Linux 6 that can cause the host to lock up. We recommend using an older version of the connector on RHEL/CentOS/Oracle Linux 6 systems until the Linux connector is updated. RHEL/CentOS/Oracle Linux 7 is unaffected by this.

Bugfixes/Enhancements

- Fixed a rare kernel panic on RHEL/CentOS 6 when the connector service is frequently restarted (CSCvt54122).
- Added ID numbers to fault information displayed in the ampcli.
- Fixed an issue where some rename operations would not trigger an on-access scan.
- Fixed a CentOS/RHEL 6 kernel panic from the redirfs kernel module that can occur when drives are frequently mounted and unmounted.
- Fixed a CentOS/RHEL 7 kernel panic from the ampfsm kernel module that can occur when unloading the kernel module while performing a rename operation (CSCvt13313).
- Fixed a situation that could add unnecessary delay in quarantining malicious files when the Cloud connection is unreliable. (CSCvs75040)
- Fix restart issue when scanning CIFS mounts with Kerberos authentication (CSCvs45576).
- Fixed a rare crash on RHEL/CentOS 7 which could occur when monitored files on a network drive were removed. (CSCvr43285)
- Updated ClamAV to 0.102.1, including changes related to the following vulnerabilities:
  - CVE-2019-15961
  - CVE-2019-1010305
  - CVE-2019-12625
  - CVE-2019-12900
  - CVE-2019-1787
  - CVE-2019-1788
  - CVE-2019-1789
  - CVE-2017-16932
  - CVE-2018-14679
  - CVE-2018-15378
  - CVE-2018-14680
  - CVE-2018-14681
  - CVE-2018-14682

- Update third-party libraries, including changes related to these vulnerabilities:
  - libxml2:
    - CVE-2019-19956
  - Curl:
    - CVE-2018-16840
  - CiscoSSL:
    - CVE-2018-0732
    - CVE-2018-0737
    - CVE-2018-5407
  - SQLite:
    - CVE-2018-20346
  - SQLite:
    - ORDER BY LIMIT fix: http://www.sqlite.org/cgi/src/info/9936b2fa443fec03ff25
  - XML2:
    - CVE-2018-14404
- Changed virus definition update download protocol from HTTP to HTTPS.
- Improved performance when processing execute-triggered scans.
- Improved performance on systems with multiple mount namespaces.
- Fixed incorrect known virus count in virus definition update event.
- Fixed install failure due to error creating new user group.
- Fixed memory leak affecting systems with low filesystem and network activity.
- Fixed memory leak that may occur after a detection event.
- Fixed memory leak that may occur after applying virus definition update.
- Reduced CPU usage by optimizing file scan algorithm.
- Reduced error log messages when file scan processing queue is full.
- Fixed memory leak when disconnected from the Private Cloud.
- Delete stale ClamAV temporary files when file scan terminates abnormally (CSCvo74969).
- Fix intermittent file scan failure if debug logging has been enabled for a long time.
- Fixed scheduled full scan incorrectly processed as single file scan (CSCvn36511).
- Fixed memory leak when updating cached mount table (CSCvo35582).
- Fixed issue where CPU usage may remain high even after stopping AMP service.
- Fixed RedirFS-related kernel panics (CSCvj44170, CSCvo74991).
- Fixed incorrect exclusion on devtmpfs from on-access scan.
- Fixed connector status may be stuck at 'Offline' after system time change.
- Fixed unintended quarantine when a retro quarantine request is received in Audit mode.
- Fixed a bug which caused segmentation faults in RHEL/CentOS 7.5 (CSCvn39498).

- Fixed a bug where files renamed or moved to a non-root mount are not always scanned.
- Improved handling of mount namespaces with shared subtrees.
- ClamAV definition information is now displayed in the CLI.
- Reduced demand on kernel memory when running on RHEL/CentOS.
- Reduced ampnetworkflow logging.
- Improved stability of Private Cloud network connections.
- Improved tracking and reporting of connector faults.
- Improved descriptions for connector events reported in the CLI.
- Fixed a procfs-related memory consumption issue that could lead to an out of memory error (CSCvm42255).
- Changed server authentication to align with the Red Hat ca-certificates package update.
- Improved network flow monitor kernel module logging.

10 December 2018 Release Notes

Private Cloud Administration Portal 3.0.2

Bugfixes/Enhancements

- Fixed an issue where error logs were not handled correctly during a restore from backup.

16 November 2018 Release Notes

Private Cloud Administration Portal 3.0.1

New

- In Private Cloud 3.0.1, Airgap Mode has been deprecated; however, existing customers with Airgap Mode will be grandfathered in.

IMPORTANT! To upgrade to Private Cloud 3.0.1 you must do a Backup/Restore from a 2.4.0 or newer device, and have Disposition Server Extended Protocol enabled, which may require several system migrations. Users performing a Backup/Restore from a 2.4.x device will be exempt from the Trusted Certificate requirement during install. Any new services (such as the Authentication) will be subject to the new mandatory hostname requirements. Users will have to set valid hostnames and upload a cert/key pair for all new services during the initial install wizard.

- Hostnames and a certificate/key pair are now required for all services:
  - Administration Portal
  - Authentication (new in Private Cloud 3.0.1)
  - FireAMP Console
  - Disposition Server
  - Disposition Server – Extended Protocol
  - Disposition Update Service
  - Firepower Management Center
- Users can upload the root certificate for custom Certificate Authorities during the initial install wizard.
- Wildcard certificates are permitted.

Bugfixes/Enhancements

- There is no longer a distinction between manual and scheduled backups. This means that both kind of backups are subject to the same retention policy.
- We no longer allow backups to fill the disk. As backups can become very large, we perform a check and do not allow backups to be done if they will fill a disk above 90%. We will also remove the oldest backups if required.
- We do not allow multiple backups to be triggered at the same time.
- We do not allow a backup to be performed on an Airgapped device if a ProtectDB import is running.
- A new license type has been added. This is to support the hardware device, but can be used on a virtual appliance.

FireAMP Console 5.3.20180910

New

- Add “Upload Successful” message when uploading endpoint IOC.

Bugfixes/Enhancements

- Fixed a problem with portal file_repository page breaking when one of the fetched file checksum is in an application control blocking list.
- Allow OOXML_* files to be cloud queried.
- CVEs are now limited to 45 per event.
- CVEs are now emitted weekly, instead of daily.

Secure Endpoint Windows Connector 6.1.7

Bugfixes/Enhancements

- Fixes for multiple ClamAV vulnerabilities:
  - CVE-2018-0360
  - CVE-2018-0361

IMPORTANT! Malicious Activity Protection and Exploit Prevention are not yet supported in Private Cloud.

Secure Endpoint Mac Connector 1.8.2

Bugfixes/Enhancements

- Fixed a bug introduced in 1.8.0 that could cause the AMP service to restart unexpectedly.
- Fixed a kernel panic on macOS 10.12 when accepting TCP connections from malicious hosts. (CSCvk08192)
- Disabled unsupported command line capture when running on OS X 10.11 and earlier.
- Improved command line capture with macOS 10.12.4 and later.
- Improved Support Tool command line arguments, descriptions, and optimized data collected when generating a support snapshot.
- Improved file execute activity monitoring to ensure appropriate SHA value generation.
- Corrected display of policy information when connector starts without network connection.
- Updated third party libraries including changes related to these vulnerabilities (CSCvj56731):

- ClamAV:
  - CVE-2017-12380
  - CVE-2017-12379
  - CVE-2017-12378
  - CVE-2017-12377
  - CVE-2017-12376
  - CVE-2017-12375
  - CVE-2017-12374
  - CVE-2017-11423
  - CVE-2018-0361
  - CVE-2018-0360
- Curl:
  - CVE-2018-1000300
  - CVE-2018-1000301
  - CVE-2018-1000122
  - CVE-2018-1000121
  - CVE-2018-1000120
- SQLite:
  - CVE-2018-8740

IMPORTANT! We strongly advise Mac connector 1.3.0 users to upgrade to 1.3.1 then reboot the system before upgrading to 1.8.2. Upgrading directly from 1.3.0 to 1.8.2 may cause a kernel panic.

IMPORTANT! If your connectors are deployed with Mac connector v1.8.0, we recommend upgrading to v1.8.2. If you previously disabled the command line capture feature due to the v1.8.0 announcement regarding connector restarts, you can reenable the command line capture feature after completing the upgrade.

13 June 2018 Release Notes

Private Cloud Administration Portal 2.4.4

New

- Added the ability to surface data around bad cloud lookups within support snapshots.

Bugfixes/Enhancements

- Fixed an issue where certain cloud lookups with bad data sent by integrations were not stored in the database, so no retrospectives could be performed on these lookups.
- Increased the performance of the Events page by limiting the size and frequency of certain large events.

25 April 2018 Release Notes

Secure Endpoint Windows Connector 5.1.15

New

- Added /kb4072699 installer switch to automatically set the registry key necessary to receive the Windows Security Update for KB 4072699.

IMPORTANT! Test and ensure compatibility of all AV products installed before using this installer switch. See Cisco AMP for Endpoints Compatibility with Windows Security Update KB4056892 for important details in the Caveats and Considerations section that apply to use of the installer switch for setting the registry key.

Bugfixes/Enhancements

- Improved compatibility with TrendMicro (CSCvi07080).
- Addressed a Clam AV issue that was triggering false positive detections against PDF files (CSCvi01400).
- Fixed an issue where Windows connector updates may fail with password protection enabled.
- Patched a DLL hijacking vulnerability in the connector installer (CVE-2017-12312).
- Extremely long process command line arguments are now properly captured.
- The connector UI accurately displays Cloud connectivity status.
- Improved ability of the connector to detect and repair configuration issues during regular usage and on connector upgrade.

- Improved performance of Process Exclusions for operating systems prior to Windows Vista.
- Addressed an issue where the connector is unable to upgrade directly from version 5.0.9 or older to 5.1.11 when connector Protection is enabled.
- Reliability of Support Package generation has been improved.
- connector will not generate new identity on machines where the BIOS serial number contains white spaces.
- Addressed issue where the connector service does not automatically start after multiple upgrades without a reboot.
- Improved reliability of system reboot after upgrades in Windows Server 2003.
- Improved security of the connector Protection password.
- Improved Windows proxy discovery.
- Improvements to make connector upgrades more robust going forward.
- Addressed an issue where the connector would leave many temporary files behind, filling up the disk.
- The History page on the connector user interface now shows the proper detection name for quarantined files that were already in the local cache.
- Improved reliability when an Endpoint IOC scan is launched.
- Updated SQLite version to prevent high CPU usage.
- Improved connector user interface responsiveness.
- connector service now functions properly when installed on Windows 10 Fall Creators Update.
- The connector no longer causes a warning to appear when opening the Computer Management window.
- Improved TETRA file detection parsing. (CSCvh54783, CSCvh77705)
- Addressed an issue where the connector could cause a blue screen under rare conditions. (CSCvh56811)
- Fixes for multiple Clam AV vulnerabilities:
  - CVE-2017-6420
  - CVE-2017-12378
  - CVE- 2018-0202
  - CVE-2017-6418

IMPORTANT! Starting from Windows connector 5.1.13, we will no longer be supporting the addition of new features for Windows XP, Windows Vista, Windows Server 2003 and Windows Server 2008 (non-R2) operating systems. Critical bug fixes and security patches will still be made to the 5.x.x branch of the connector for a limited time. For more information, please refer to the End of Support Announcement.

Secure Endpoint Mac Connector 1.7.0

New

- Digitally signed malware will now be quarantined by the Mac connector.
- Support macOS High Sierra (10.13).
- Resume filesystem scans after AMP service daemon restarts.
- Hide exclusion list in UI based on policy configuration.
- Added automatic crash reporting.
- ClamAV virus definition file versions are now displayed.

IMPORTANT! The AMP for Endpoints Mac connector no longer supports OS X 10.10 and earlier as of version 1.7.0.

Bugfixes/Enhancements

- Improved DMG container handling.
- Addressed race condition that would result in failed quarantine restores.
- Custom or scheduled scans that result in 0 files being scanned no longer report as a failed scan.
- Installs of the connector on a system with multiple users will no longer be incorrectly reported as failed.
- Remove old quarantined files automatically.
- Restrict access permission of some internal files.
- Update Third Party libraries.
- Fix memory leak.
- Optimize how exclusions are applied.
- Improve Cloud Recall Restore error handling.
- Scan full contents of archives that contain malware.
- Addressed memory leak when scanning plist files.
- Fixed potential crash during a failed retrospective quarantine.
- Fixed a bug that caused retrospective quarantine failure events to be displayed even though it succeeded.
- Improved compatibility with macOS 10.13.
- Updated third-party libraries.
- Reclassified some error messages that were being logged frequently under normal circumstances so they are only seen when running the connector with Debug Logging enabled in policy.
- Increased the size of the retrospective database from 50MB to 500MB with better pruning efficiency to decrease disk reads and writes.
- Reduced disk write activity. (CSCvd15950)
- Reduced the number of duplicate network detection events sent.
- Enhanced scanning of larger files on execution.
- Improved formatting of information in the UI.

- Added SupportTool option for specifying maximum size of output archive.
- Reclassified error messages that can be logged frequently under normal operation.
- Updated third party libraries.
- Patched ClamAV vulnerabilities:
  - CVE-2018-1000085
  - CVE-2012-6706
  - CVE-2017-6419
  - CVE-2017-6418
  - CVE-2017-6420
  - CVE-2018-0202

Secure Endpoint Linux Connector 1.7.0

New

- Update Linux signed file quarantine guardrail.
- Resume filesystem scans if the daemon restarts.
- Hide exclusion list in UI based on policy configuration.
- Remove old quarantined files automatically.
- Official support for RHEL/CentOS 7.4.
- Official support for RHEL/CentOS 6.9.
- ClamAV virus definition file versions are now displayed.

Bugfixes/Enhancements

- ClamAV vulnerability fixed.
- Update 3rd party libraries.
- Bypass proxy when unable to connect to AMP registration server.
- Fix execute not being excluded from scan when it should be.
- Fix custom scan misbehavior.
- Disable unintended auto-start of ampmon after reboot in CentOS 6.
- Scan full contents of archives that contain malware.
- Do not treat directed or scheduled scans which processed zero files as failed.
- Fix restore from quarantine failure.
- Fix CLI crash when displaying very long exclusion lists.
- Fix intermittent failure where CLI is stuck in initializing phase.
- Fixed HTTP parsing for certain processes.
- Improved upgrade process to protect against failures.
- Fixed a bug that caused retrospective quarantine failure events to be displayed even though it succeeded.
- Updated third-party libraries.

- Reclassified some error messages that were being logged frequently under normal circumstances so they are only seen when running the connector with Debug Logging enabled in policy.
- Increased the size of the retrospective database from 50MB to 500MB with better pruning efficiency to decrease disk reads and writes.
- Fixed installation failure when the system temporary directory is mounted without execute permission.
- Fixed issue where the system may hang during start up due to kernel module conflict.
- Reduced disk write activity.
- Reduced the number of duplicate network detection events sent.
- Enhanced scanning of larger files on execution.
- Removed CLI history file from user home directory on full uninstall.
- Added SupportTool option for specifying maximum size of output archive.
- Improved the handling of network mounted drives by the SupportTool.
- Improved CLI display formatting.
- Reclassified error messages that can be logged frequently under normal operation.
- Updated third party libraries.
- Patched ClamAV vulnerabilities:
  - CVE-2018-1000085
  - CVE-2012-6706
  - CVE-2017-6419
  - CVE-2017-6418
  - CVE-2017-6420
  - CVE-2018-0202

15 November 2017 Release Notes

Private Cloud Administration Portal 2.4.2

Bugfixes/Enhancements

- Fixed a bug where retrospective data was not processed in some situations.

FireAMP Console 5.3.20171105

Bugfixes/Enhancements

- Fixed a bug where some data displayed in an integrated Firepower Management Center may not reflect current endpoint network addresses.
- Fixed a bug where running ipsupporttool.exe on a computer after installing Secure Endpoint Windows connector 5.1.11 will temporarily disable File Fetch functionality on the endpoint.

24 October 2017 Release Notes

Private Cloud Administration Portal 2.4.1

Bugfixes/Enhancements

- Fixed an issue where Disposition Server - Extended Protocol registration fails if proxy authentication is set to none.
- Fixed an issue where slow DNS causes a timeout when registering with the Disposition Server - Extended Protocol.
- Relaxed certificate validity requirements.
- Fixed an issue that could cause increased memory use and impact stability.
- Fixed issues where files were not submitted for Threatgrid analysis from integrated FMC, ESA, and WSA devices.
- Fixed an issue where vulnerable applications were not being alerted on.
- Fixed issues related to malicious file detection on integrated FMC, ESA, and WSA devices.

Secure Endpoint Windows connector 5.1.11

IMPORTANT! Upgrading to 5.1.11 from a 4.4.5 or earlier connector will fail if connector Protection is enabled. To upgrade you must disable connector Protection in Policies and wait for the policy to be applied to your connectors before upgrading. connector Protection may be re-enabled once the upgrade has succeeded. This will be fixed in the next connector release.

30 August 2017 Release Notes

Private Cloud Administration Portal 2.4.0 (superseded by 2.4.1)

New

- Added the Disposition Server - Extended Protocol to support advanced connector features.

  IMPORTANT! A migration wizard has been added to transition to the Extended Protocol. To deploy new connectors you must first migrate to the Extended Protocol. Only upgrades from previous versions of Private Cloud need to run the migration wizard.

- Improved interface for certificate management.

Bugfixes/Enhancements

- Fixed a bug where a Private Cloud device in Air Gap mode could not enable remote file fetch due to Two Step Verification issues. Contact support to enable this.
- Advanced Custom Detections are now downloaded over HTTPS.
- Resolved an issue where backup size increased dramatically under some use cases.
- Addressed various security issues.

FireAMP Console 5.3.20170823

New

- Secure Endpoint Linux connector is now available for download in your Private Cloud device.

Bugfixes/Enhancements

- Fixed an issue with Identity Sync.
- Low Prevalence Executables will now display correctly when used in conjunction with rules-based access control.

Secure Endpoint Windows Connector 5.1.11

New

- Disposition Server - Extended Protocol has been enabled in the connector.
- Limited rebranding from Sourcefire FireAMP to Cisco AMP for Endpoints.

IMPORTANT! As part of the rebranding, the connector default installation path was changed to C:\Program Files\Cisco\AMP. Before upgrading your endpoints to this version, be sure to review any exclusions you have for 3rd party software that is installed alongside AMP for Endpoints.

- Updated the TETRA engine to add support for downloading signature deltas.
- A new Timed Diagnostic Tool option is available in the Cisco AMP for Endpoints connector Start Menu group.
- A utility to test connectivity from the endpoint to the Private Cloud device is now included in the installation directory.

- Connector binaries are now signed using the Cisco EV code signing certificate.
- The AMP for Endpoints Windows connector can now be installed on systems that have Secure Boot enabled.

IMPORTANT! Starting from Windows connector 6.0.1, we will no longer be supporting the addition of new features for Windows XP, Windows Vista and Windows Server 2003 operating systems. Critical bug fixes and security patches will still be made to the 5.x.x branch of the connector for a limited time. For more information, please refer to the End of Support Announcement.

Bugfixes/Enhancements

- Updated TETRA license key.

  IMPORTANT! The TETRA license for all Windows connector versions prior to 5.1.11 will expire on November 1, 2017. If you wish to continue using the TETRA engine you must upgrade before this date.

- The DFC driver now initializes more reliably.
- The connector now has an increased window for monitoring network connections.
- The local DFC cache is now being updated correctly.
- Certain IP ranges are no longer incorrectly whitelisted by the connector.
- Custom IP black/whitelist entries composed of CIDR block and port number combinations are now processed correctly by the connector.
- The connector Protection password is no longer logged during the uninstall process.
- Unnecessary TETRA definitions are no longer downloaded when the local definition set is up to date.
- Reduced the likelihood of the connector generating a new identity on upgrade.
- Scanning of container files (pdf, zip, tar, etc) is now more robust.
- Improved accuracy of parent process reporting.
- Performance of process exclusions has been improved.
- Patched a vulnerability in unrar (CVE-2012-6706)
- Addressed an issue where connectors installed on Windows SMB servers would cause shared, mapped drives to be inaccessible.
- Addressed issues where the connector could lose connection to the Private Cloud device when Identity Sync is enabled.
- Addressed an issue where the connector could be disabled by a user with admin privileges when connector protection is enabled.
- Addressed a crash that would occur when attempting to enable debug logging.
- Fixed a crash that could occur during the connector service shutdown.
- Addressed an issue where a password containing certain special characters was not being parsed correctly when attempting to uninstall the connector via command line with connector protection enabled.

- Improved system performance when the connector is installed on systems with VMware Persona Management.
- Addressed an issue where the connector could cause a BSOD under rare conditions.
- Fixed an issue where the connector could cause system freezes in some instances.
- Addressed an issue with Endpoint IOC scans consuming high amounts of CPU.
- The connector is now able to download TETRA definitions over SSL.
- Added a fix to address a vulnerability in bzip2 (CVE-2016-3189).
- Removed erroneous log lines that appeared when using the Connectivity Test Tool.
- Improved stability of the connector by addressing numerous reported crashes.
- Improved handling of local configuration files to reduce instability due to configuration errors.
- Addressed issue where the connector network driver could cause a BSOD when Windows Driver Verifier is used against it.
- Modified altitude of the AMP for Endpoints Windows drivers to be more in line with Microsoft software recommendations.
- Addressed an issue where the connector could become deadlocked.
- Addressed compatibility issues with LabLogic Debra.
- Addressed an issue where virtualized systems were not correctly being identified as unique.
- Addressed an issue where the installer would not complete successfully under certain circumstances.
- Addressed an issue where previously downloaded TETRA definitions couldn't be used after a partial uninstall followed by a re-install.
- Addressed an issue where the connector would not shut down in a timely fashion while TETRA definitions were being downloaded.
- Fixed an issue where Application Blocking events were not reporting parent process information properly.
- Addressed an issue where log files could grow beyond their maximum size.
- Fixed an issue where the connector would continue to apply Advanced Custom Detection definitions after they were removed from policy until the connector was restarted.
- Fixed an issue where HDB Advanced Custom Detection signatures would not be correctly applied when configured to use a wildcard for file size.
- Addressed an issue where the first scan after install would execute without network activity or before TETRA definitions were fully downloaded.
- Addressed an issue where the connector would negatively impact write performance when installed on machines with solid state drives (SSDs).
- Addressed an issue on Windows XP where the connector could not acquire the machine's IP address when configured with a static IP address and the "Register this connection's addresses in DNS" option was disabled.
- Updated curl to version 7.51.0.
- Addressed a vulnerability where connector protection could be bypassed during uninstall by entering a specific character in the password field.

- Improved the ability for the connector to upgrade/uninstall connectors that are in a crashed state.
- Fixed an issue where TETRA could incorrectly flag files as malicious.
- Fixed an issue where TETRA was not handling the detection of malicious archive files properly in certain situations.
- Fixed a rare issue where the connector would cause high CPU usage due to MTU and policy size.
- Addressed an issue where the connector process was able to be stopped via debugger access.
- Users are now able to configure which path to store temporary files during the installation process through a command line switch.
- Improved the uninstall process to better handle scenarios where the connector is in a bad state prior to uninstalling.
- Improved overall stability of the connector.
- Addressed a minor issue where the connector would report a successful custom scan for invalid paths.
- Improved error reporting.

IMPORTANT! Upgrading from certain connector versions will require a reboot. Downloading the new installer or performing an update via policy will provide a list of computers in the selected group or policy that will require a reboot.

Secure Endpoint Mac Connector 1.4.3

New

- Disposition Server – Extended Protocol has been enabled in the connector.
- Added Support for Mac OS X 10.12.

  IMPORTANT! Users running macOS 10.12 (Sierra) should upgrade to 10.12.4 or later. There are compatibility issues that affect system stability which are resolved in macOS 10.12.4.

- Rebranded product from Sourcefire FireAMP to Cisco AMP for Endpoints.

  As part of the rebranding, the connector installation paths have changed to:

  - /Applications/Cisco AMP
  - /Library/Application Support/Cisco/AMP for Endpoints Connector
  - /opt/cisco/amp

  Before upgrading your endpoints to this version, be sure to review any exclusions you have for 3rd party software that is installed alongside AMP for Endpoints.
- Added support for Advanced Custom Detections.
- A command line interface has been added to the AMP for Endpoints Mac connector. This can be used to initiate scans, sync policies, show the connector history, and more.

- The connector will now send queries for LZMA compressed Adobe Flash files, MSO attachments within MS Office 2003 XML files, and Hancom Office files.
- Added scanning of files referenced by startup and launch related plists.
- Upgraded ClamAV engine to 0.99.2.

IMPORTANT! The AMP for Endpoints Mac connector no longer supports OS X 10.7 as of version 1.3.0.

Bugfixes/Enhancements

- Addressed issue where a different folder may be inadvertently deleted during the uninstall process when a subdirectory in the "/Users" directory contains a subdirectory with a space character.

  Note that most systems are not affected as macOS System Preferences prevents creating a user with a space character in the account name.

  To trigger this issue, two similarly-named user directories must exist (e.g. "/Users/JohnDoe" and "/Users/JohnDoe Copy"). If "/Users/JohnDoe Copy" contains the path to AMP connector log files (e.g. "/Users/JohnDoe Copy/Library/Logs/Sourcefire/"), uninstalling or upgrading will result in the user directory "/Users/JohnDoe" being deleted.
- Fixed a bug in the AMP network kernel extension that can cause a kernel panic.
- Patched a vulnerability in unrar (CVE-2012-6706)
- Applied security fixes from 3rd party libraries used by the connector including OpenSSL, cURL, and xmlsec.
- Fixed a bug where a user-initiated scan could interfere with detections in real-time file operations.
- Strengthened guards against misbehaving UI clients.
- Fixed a bug to ensure that files found to be malicious by the offline engine are scanned using the Private Cloud device before generating a detection event.
- Fixed a bug where file paths are included in queries even when the feature is disabled in policy.
- Fixed a bug causing a "too many open files" error after parsing MSXML files.
- Fixed a bug where user information for some events are missing.
- Fixed a bug causing a UI lockup when performing flash scan.
- Improved the readability of quarantine failure messages.
- Improved resiliency against corrupt ClamAV definition files.
- Removed a dependency on perl in the installer.
- Resolved an issue where the connector could not quarantine malicious resource forks.
- Applied security fixes from third party libraries including OpenSSL, Jansson and Libxml2.
- Fixed a bug that stopped ClamAV from scanning files when disconnected from the Private Cloud device.
- Addressed an issue where certain file activity could cause scans to stop prematurely.

- Fixed a bug where files contained inside PDF files were not scanned.
- Fixed a bug where some UDP connections were not monitored.
- Fixed a bug where user information was missing from some events.
- Fixed a bug where some deferred scans were dropped because the deferred scan file was not written to correctly.
- Fixed a bug where the URL reported for some network events were malformed.
- Fixed a bug where Definition Update events were missing from the Events table.
- Fixed a bug where the known viruses count for Definition Update events was incorrect.
- Made automatic ClamAV definition updates more robust.
- Clarify in Execution Blocked events and notifications that no action was taken when the connector is running in audit mode.
- Removed stale files from ClamAV working directory at daemon start-up.
- Reduced the performance overhead of wildcard exclusions.
- Fixed a bug where a kernel extension could panic if there are active network connections when the daemon is stopping or retrying a failed initialization step.
- Fixed various logging issues.
- Updated curl version to 7.51.0.
- Addressed an issue where the connector would consume high CPU when a local database reached a certain size.
- Fixed a bug where the connector would consume high CPU when some local 3rd party software would periodically touch but not modify files.
- The connector is now able to successfully quarantine files that have immutable flags set.
- Addressed various issues with scan error reporting.
- Fixed an issue where you could not fetch a file from a computer after it was deleted even if other copies of the same file existed on the computer.
- Addressed an issue where the connector would only perform a Retrospective Quarantine on the first instance of a file on the computer.
- Fixed a bug where scans in progress when the computer was rebooted did not appear to complete in the Console.
- Fixed an issue where outdated ClamAV definitions were still being loaded by the connector in some instances. This could potentially cause an increase in false-positive detections.
- Patched ClamAV engine to address potential vulnerabilities when handling certain archive file types (CVE-2016-1371, CVE-2016-1372).
- Modified the connector installer to prevent downgrades when running the installer locally.
- Added more diagnostic information collected by the Support Tool.
- Improved performance when using Application Blocking lists on Mac OS X 10.8 and 10.9.
- Improved handling of nested archive files.
- Fixed an issue where the connector was not sending information about the current user for certain events.
- Fixed an issue where the connector wasn't cleaning up its child processes.

- Improved overall connector stability and efficiency.
- Addressed issue where ClamAV would download definitions more often then necessary.
- Resolved issue where connector sent extraneous file execute events.
- Addressed various memory usage issues.
- Improved DFC engine to robustly handle network events.
- Improved file move event detection data for better representation in Device Trajectory.
- Fixed issue where the connector was not clearing the file scan queue in some cases.
- Improved various UI messages and error notifications.
- Improved messaging for events displayed in the management console.
- Improved error messaging when attempting a custom scan for an invalid path.
- Improved connector upgrade functionality and console notifications.
- Connector updated to dynamically honor file scan size limits on policy change.
- Fixed various issues with exclusion handling.
- Improved handling of archive files.
- Improved ability of the connector to handle malicious forking executable files.
- Improved connector compatibility for OS X 10.10 and above.
- Addressed issue where upgrading OS X with the connector installed would sometimes freeze the system.
- Improved connector performance when installing from read-only media (e.g. DVDs).
- Addressed issue where cache TTLs were not expiring as expected.
- Changed Support Package creation process improving efficiency and flexibility.
- Added ability to specify custom output path for Support Package using "-o" option.

Secure Endpoint Linux Connector 1.3.1

New

- Disposition Server - Extended Protocol has been enabled in the connector.
- Added support for Red Hat Enterprise Linux and CentOS 7.2 and 7.3
- Added support for Red Hat Enterprise Linux and CentOS 6.7 and 6.8.
- Added support for Advanced Custom Detections.
- ClamAV upgraded to 0.99.2.
- The connector will now send queries for LZMA compressed Adobe Flash files, MSO attachments within MS Office 2003 XML files, and Hancom Office files.

Special Advisory

Important note for RHEL and CentOS 6.0-6.5 users

Confirm the installed version of procps is 3.2.8-30 or newer prior to installing this update. Older versions of procps are not compatible and users are advised to update to the latest version. Refer to the following Red Hat advisories for details:

https://rhn.redhat.com/errata/RHBA-2014-1595.html
https://rhn.redhat.com/errata/RHBA-2015-1407.html
https://rhn.redhat.com/errata/RHBA-2015-1812.html
https://rhn.redhat.com/errata/RHBA-2015-2643.html
https://rhn.redhat.com/errata/RHBA-2016-0904.html

3 August 2017 Release Notes

Private Cloud Administration Portal 2.3.6

New

- An alert (see below) has been added to the Administration Portal about the upcoming Private Cloud 2.4 release.

FireAMP Console 5.3.20170728

New

- An alert (see below) has been added to the FireAMP Console about the upcoming Private Cloud 2.4 release.

Upcoming Private Cloud v2.4 Release Alert

AMP Private Cloud v2.4 includes a new AMP Cloud protocol allowing us to bring more features to the AMP platform. Upgraded installs must run the included migration wizard to use the new AMP Cloud protocol.

IMPORTANT! To continue using the TETRA engine you must migrate to the new AMP Cloud protocol and upgrade to AMP for Endpoints Windows connector version 5.1.11.

The following TechZone article describes the full set of changes and benefits of migrating to the new AMP Cloud protocol.

http://cs.co/amppc24release

14 June 2017 Release Notes

Private Cloud Administration Portal 2.3.5

Bugfixes/Enhancements

- Fixed an issue where certain event types could cause the Events page to freeze.

11 May 2017 Release Notes

Private Cloud Administration Portal 2.3.4 (superseded by 2.3.5)

Bugfixes/Enhancements

- Resolved a performance issue by tuning an internal data store.
- Fixed a problem when automatically applying content updates.

IMPORTANT! A migration process has been added that must be completed after upgrading from previous versions to 2.3.3. The migration can take 12 to 24 hours and during this time connectors will be unable to perform lookups against the device.

8 March 2017 Release Notes

Private Cloud Administration Portal 2.3.2

Bugfixes/Enhancements

- Fixed an issue relating to retrospective and cloudlogs cron jobs. This only affects devices that have been updated, not fresh installs.

FireAMP Console 5.3.20170202

Bugfixes/Enhancements

- Fixed an issue where email from Event Subscription notifications were not being sent.

14 February 2017 Release Notes

Private Cloud Administration Portal 2.3.1

Bugfixes/Enhancements

- Fixed an issue where content updates fail when a proxy server is configured.
- Fixed an issue with excessive TokuMX logging.
- Fixed an issue where a logrotate cron job could interfere with backups.
- Limited the number of mysql binlog files to 15 to guard against filling up the /data partition.

FireAMP Console 5.3.20170202

Bugfixes/Enhancements

- Fixed an issue where immediate email from event notifications were not being sent.
- Updated documentation to include Secure Endpoint Mac connector for OS X 10.11 and 10.12.
- Fixed an issue where reports could timeout and create empty PDFs.

8 December 2016 Release Notes

Private Cloud Administration Portal 2.3.0

New

- New field in the Integrations tab for VirusTotal.
- UI Change for the Administration Portal to include Cisco Web Security Appliance integration.

Bugfixes/Enhancements

- Default collection has been removed from Storage Configuration.
- Defence Center has been renamed to Firepower Management Center.
- Validation added to Threat Grid hostname.
- Secure Malware Analytics integration now has show/hide buttons for the TG API key input field.
- Disposition update service password is now user configurable.
- Cloud server is renamed to Disposition server.
- Customizable From, Sender Name, and Device Name fields for notification emails.
- Bugfix to content updates which handles new yum behavior.
- Better help messages displayed for Firepower Management Center (formerly DC) Integration page.
- Support snapshots now contain additional information.
- The Server Keys upload form has been hidden when on a default (non-custom) upstream Disposition Server.
- SSL Keys page in the Administration Portal now shows data for default generated certs and user uploaded certificates.

FireAMP Console 5.3.20161013

New

- Added an API Credentials page to simplify 3rd party application management.
- The FireAMP API allows you to make changes to your business. API users can move computers, assign policies to groups, and make modifications to Application Blocking and Simple Custom Detection lists.
- New Reports are available under the Analysis heading. Old reports are still available.
- VirusTotal integration is enabled in proxy mode to allow files to be compared to VirusTotal on the right-click context menu. This must be enabled in the Administration Portal.
- Users can now specify their timezone so dates and times will be displayed in the chosen timezone throughout the Console.
- Clicking a date entry anywhere will show a pop-up menu with additional options.

- Added global search to the menu bar throughout the Console. This is the same as available under the Analysis header.
- Added filters to the Audit Log page. Added User links that will take you to a filtered view of the Audit Log.
- You can now select which VM operating system image to use for Cisco Secure Malware Analytics file analysis.
- Added information about reboot requirements to Product Update section of Policies and to the Download Connector page.

Bugfixes/Enhancements

- File Analysis page now displays threat report score on each result line.
- Fixed a bug that caused policy updates to fail in certain situations.
- Added Event Type filters for product updates.
- Fixed a bug that caused the incorrect file type to be displayed in trajectory data.
- Redesigned the Audit Log page for usability.
- Moved version number to Help dialog.
- Added support for Hangul Word Processor files.These files will now appear in File and Device Trajectory and can be submitted for File Analysis.
- The SHA-256 of archive files are now displayed when a detection is triggered by a file contained within the archive.
- Clarified detection events when a connector is in a group with a policy that uses Audit Mode.
- Fixed a bug where Advanced Custom Detections (ACD) were unable to add zmd signature.
- We now report the last policy serial number that a connector reported in with in the Device Trajectory.
- Fixed a bug where some events weren't showing in the dashboard unless filtered by GUID/computer.
- There is a new error code for consecutive agent crashes.
- Fixed a bug where cached File Trajectory data was being served to all users regardless of rules based access and control.
- Fixed a bug where aggregate IP Lists could fail silently.

Secure Endpoint Windows Connector 4.4.5

New

- Starting with upgrades from version 4.4.3 to future versions, the Secure Endpoint Windows connector no longer requires a reboot after every update.

  IMPORTANT! Updates that include major functionality changes or bugfixes may still require a reboot.

- Added support for Windows 10.

- The endpoint IOC scanner now supports the ability to only catalog changes in the filesystem, allowing IOC scans to complete faster after the first full catalog has been completed.
- Secure Endpoint Windows no longer requires Windows administrator credentials for scheduled scans.

Bugfixes/Enhancements

- TETRA definitions can now be downloaded when the connector is configured to use a proxy server.
- Addressed a bug where TETRA definition downloads did not appear to complete successfully even though they did.
- Fixed a rare issue where the connector would cause high CPU usage due to MTU and policy size.
- Addressed security issue where the connector process was able to be stopped via debugger access.
- Addressed security issue where connector protection could be bypassed on uninstall.
- Addressed issues where the connector install would occasionally fail.
- Enhanced scope of Endpoint IOC flash scan indexing to provide increased coverage. Please refer to the Cisco Endpoint IOC Attributes document for more information.
- Improved performance during the Endpoint IOC collection phase to reduce collection time.
- Addressed an issue where IOC Flash Scans were not correctly cleaning up files from previous scans.
- You can now stop the connector service via the command line when connector protection is enabled.
- Made improvements to the installer for preserving previous command line options.
- Various stability improvements and bugfixes.
- Improved connector reliability during installation and upgrades.
- The connector now dynamically honors file scan size limits when changed in policy. Previously the connector service would have to be stopped and restarted.
- Improved handling of archive files.
- Patched ClamAV engine to address potential vulnerabilities when handling certain archive file types.
- Fixed an issue where the connector was not sending information about the current user for certain events.
- Fixed a problem where the connector was not reporting the parent file type correctly in some cases.
- Fixed a bug where .elf file was not being found by windows agent but is being convicted by Mac.

Secure Endpoint Mac Connector 1.0.10

IMPORTANT! Mac connectors need to use port 32137 instead of 443, this is configurable via policy.

Bugfixes/Enhancements

- Fixed an issue where the connector could register with the FireAMP Console without an IP address.
- Addressed issue where the connector could potential get deadlocked and not be able to recover.
- Added new CPIO Archive (OLD), Master Boot Record, and GUID Partition Table File types.

6 September 2016 Release Notes

Private Cloud Administration Portal v2.2.3

Bugfixes/Enhancements

- Adjusted internal memory configuration for improved performance.
- Fixed a potential deadlock in the disposition service.
- Addressed an issue that could result in event data not being correctly stored.
- Performance enhancements to FireAMP Console when dealing with large amounts of historical data.

Secure Endpoint Windows Connector v4.1.9

Bugfixes/Enhancements

- Addressed an issue where policy updates could fail with specific endpoint MTU values.

9 August 2016 Release Notes

Private Cloud Administration Portal v2.2.2

Bugfixes/Enhancements

- Fixed an issue in Air Gap mode where a content update would fail when applied.
- Addressed an issue in Air Gap mode where updates could fill the data partition on the Private Cloud device.

- Addressed a bug in Air Gap mode where content updates were not queuing input files for retrospective.
- Fixed a Proxy Mode issue where content updates were not automatically being downloaded and applied when Apply/Install was selected from the Updates page.

31 May 2016 Release Notes

Private Cloud Administration Portal v2.2.1

Bugfixes/Enhancements

- Corrected an erroneous link in online help.

Secure Endpoint Windows Connector v4.1.7

Bugfixes/Enhancements

- Patched ClamAV engine to address vulnerabilities when handling certain archive file types (CVE-2016-1371, CVE-2016-1372).
- Addressed an issue where the TETRA engine was generating false-positive detections.

Secure Endpoint Mac Connector v1.0.9

Bugfixes/Enhancements

- Patched ClamAV engine to address vulnerabilities when handling certain archive file types (CVE-2016-1371, CVE-2016-1372).
- Addressed a rare issue where the connector logs could grow continually without bounds.

17 May 2016 Release Notes

Private Cloud Administration Portal v2.2.0

New

- Secure Endpoint Private Cloud now supports integration with Cisco Secure Malware Analytics appliances.
- Secure Endpoint Private Cloud now supports integration with Cisco ESA version 10.0 and higher.

Bugfixes/Enhancements

- Added FIPS-compliant TLS keys for the disposition server.
- Fixed a /tmp directory unmount error during reboot.
- Added a glibc fix for CVE-2015-7547.
- Added a Ruby on Rails fix for CVE-2015-7581, CVE-2015-7578, CVE-2015-0753, CVE-2015-0752, CVE-2015-7579, CVE-2015-7577, CVE-2015-0751, CVE-2015-7576, CVE-2015-3227.
- Fixed a problem with restores failing because the root directory was filled during restore from backup.
- Fixed an issue where the Private Cloud device loses boot configuration after a power failure.

FireAMP Console v5.2.20160509

New

- File Analysis is now available when a Cisco Secure Malware Analytics Appliance is integrated with your Private Cloud device. This allows analysis of files in the File Repository and automatic analysis of Low Prevalence Executables.

Bugfixes/Enhancements

- Policies automatically update after a license renewal, which adds updated certificates.

Secure Endpoint Windows Connector v4.1.6

Bugfixes/Enhancements

- Updated protocol version to support new TLS keys.

3 February 2016 Release Notes

Private Cloud Administration Portal v2.0.4

New

- Added notification about upgrading to Private Cloud version 2.1.

18 December 2015 Release Notes

Private Cloud Administration Portal v2.1.0

New

- Replaced MongoDB with TokuMX, this results in performance and reliability gains.

  IMPORTANT! To upgrade to version 2.1 existing customers must backup their version 2.0 Private Cloud device and restore it during the version 2.1 install.

- New and improved performance metrics.
- New notification on upstream cloud server ping failure.
- New hardware requirements page with shutdown VM option.
- Under new live support session, support identity is a click to expand.

Bugfixes / Enhancements

- Release notes for code updates are displayed in the Administration Portal.
- Default options for “Support Snapshot” when in airgap mode.
- Updated warning dialog on password change.
- Removed the errors tab from any areas that stream logs. Instead the errors are merged with the output.
- Change log added to software update details.
- Backups now use a .bak extension.
- Improved the option to replace a Private Cloud device license.
- Changed the scheduled backups pop-up when storage configuration is too large.
- Network settings page has been rearranged.
- Installation steps have been rearranged.

FireAMP Console v5.2.20151203

New

- Endpoint Indication of Compromise (IOC) feature added. You can filter based on the Endpoint IOC state and also activate, deactivate, and delete Endpoint IOCs in bulk.
- Added the ability to create administrator and unprivileged user accounts in the FireAMP Console. Administrators can assign unprivileged users access to view groups, edit policies, and create and edit outbreak control lists.
- Added an option to subscribe to individual event alert emails.
- Vulnerable Software functionality added. If an executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database that information is displayed on the Vulnerable Software page.
- Added the ability to search for computers by connector GUID.
- Export computer details to a CSV file from the Computers page.
- Added the ability to request file from any deployed FireAMP Connectors.

IMPORTANT! You must have Two-Step Verification enabled on your account to request files from your connectors and download them from the File Repository. Files can only be fetched from computers running version 4.1.2 or later of the Secure Endpoint Windows connector and version 1.0.6 of the Secure Endpoint Mac connector.

Bugfixes / Enhancements

- Added the ability to bulk delete computers from the Computers page.
- Improved bulk move operations on the Computers page.
- The Computers page can now be filtered by the last time an endpoint connected to the Cloud.

- Added a new UI feature to view all dates and timestamps in various formats by right-clicking the date to open a context menu.
- Fixed cross-site scripting issues on several pages.
- Added Group Filter to Dashboard, Threat Root Cause, and Deployment Summary pages that allow the view to be filtered based on selected Groups.
- Redesigned and consolidated the FireAMP Connector download page.
- Added Maximum Scan File Size and Maximum Archive Scan File Size items to Secure Endpoint Windows connector policies.
- SHA-256 values on File Repository page are now color-coded based on disposition.
- Removed Verbose Notifications policy item from Secure Endpoint Mac connector policies.
- Improved Groups page interface, including creating and editing groups.
- All user actions on Advanced Custom Detection lists are now recorded in the Audit Log.
- Secure Endpoint Mac connector policies updated to improve cloud query efficiency.
- Upgraded Secure Endpoint Mac connector protocol version to improve compatibility and reliability.
- Performance improvements to Device Trajectory load times.
- Fixes on various list pages and reports for when users who created the lists or reports have been deleted. The creator of these lists will now show as unknown.
- Fixed auto refresh on the Dashboard Overview tab.
- Redesigned Computers page with new computer view. You can now filter the view and move multiple computers to new Groups.
- Redesigned Users page with new layout. You can now search user accounts by name and email address and quickly access your own account.
- Better identification of Computers page for running scans for individual computers.
- Removed On Copy Mode and On Move Mode policy items and made these settings Passive for all FireAMP Connectors.
- Removed Unseen Cache TTL policy item as this was not used by the FireAMP Connector.
- Fixed an issue where event filters containing special characters could cause a javascript exception.
- Users can now specify a different email address to receive notifications.
- First Use wizard can now be accessed after initial setup from the Management > Quick Start menu item.
- Enhancements to Search page for better quality and clarity of results.
- Redesigned Business page.

Secure Endpoint Mac Connector v1.0.7

Bugfixes / Enhancements

- Added support for OS X 10.11
- Addressed issues causing Time Machine backups to take a long time over
- AFP.
- Fixed an issue where the connector would block applications while in Audit mode.
- Optimized Flash Scans for faster performance.
- Various bug fixes.

8 October 2015 Release Notes

Secure Endpoint Windows Connector v4.1.5

New Features

- Addressed an issue where the connector could become disconnected from the cloud. The computer may appear as a newly installed connector in the default group if this problem occurs. Secure Endpoint Windows connector version 4.1.2.10076 is affected.

8 September 2015 Release Notes

Private Cloud Administration Portal v2.0.20150904

New Features

- Added ISO split and reassembly functionality to the amp-sync utility.

Bugfixes / Enhancements

- Added guardrails to the amp-storage-container command to prevent accidental deletion of the /data container.
- Various bugfixes.

Secure Endpoint Windows Connector 4.1.2

New Features

- ClamAV engine updated to version 0.98.5.
- TETRA engine updated to version 3.0.0.71.
- connector process protection added for Windows Vista, Windows 7, Windows Server 2003, and Windows Server 2008.

Bugfixes / Enhancements

- Improved efficiency of the exclusion engine when handling wildcard exclusion types.
- Fixed a bug that would cause the connector crash reporting tool to fail.
- Fixed an issue where the connector would crash if left in debug mode for an extended period of time.
- Added enforcement of size limits for connector log files to a maximum of 10 files, each up to 50MB in size at any given time.
- Advanced Custom Detections can now be dynamically applied without restarting the connector.
- Improved error reporting during policy update failures.
- connector uninstall events are now properly reported from behind a proxy.
- connector is now able to perform Identity Synchronization from behind a proxy.
- Fixed a bug where the connector could crash when scanning certain file types.
- Fixed a vulnerability where an unprivileged user could cause the connector to crash through the UI.
- Fixed a bug where using the Microsoft Application Verifier tool could cause the connector to crash.

Secure Endpoint Mac Connector 1.0.6.292

New Features

- Added the ability to specify the output path of Support Packages with a command line parameter.
- Secure Endpoint Mac connector officially certified on OS X 10.10.
- Added Event History, Policy View, Local Scanning, and Headless Mode to the user interface.

IMPORTANT! If the user interface is not visible on a connector after the update, check the Start Client User Interface setting in your policy.

Bugfixes / Enhancements

- Performance improvements in the file scanning engine for more efficient calculation of file hashes and ClamAV scanning.
- Eliminated incorrect notifications when attempting a manual policy sync through the endpoint UI.
- Resolved issue where erroneous log messages appeared at system startup.
- Less ambiguous endpoint notifications by displaying “Off-line” when system is not connected to a network or the interface is disabled and “Service Unavailable” if there are problems connecting to the cloud.

- Addressed compatibility issue with OS X mail.app where malicious emails are continually downloaded and quarantined by the Secure Endpoint Mac connector. The connector now detects and notifies that malicious emails are present but does not quarantine malicious .emlx files created by mail.app. It is left to the administrator to remove the malicious email from the server manually. If mail.app is configured to automatically download attachments and those are determined to be malicious, the connector will continue to quarantine those attachments.

  IMPORTANT! This fix only affects OS X mail.app. Other email applications may behave differently.

- Resolved a rare issue where the connector is unable to sync policies for some period of time.
- Addressed a performance issue where users experienced high CPU usage after waking the computer from sleep or performing a reboot.
- Fixed high CPU usage issues on OS X 10.10 due to changes in Spotlight.
- Eliminated a race condition where kernel extensions were unable to successfully unload on shutdown or reboot.
- Improved connector validation of user-created exclusions.
- Fix for a WebDAV kernel panic issue.
- Fix for a race condition that would cause policy update failures.
- Significant performance improvement from file event queue optimization.
- Compatibility update for OS X 10.10 related to the metadata indexer.
- Cleanup of erroneous connector syslog messages.
- Added notifications for Device Flow Correlation, definition updates, Cloud Recall, and product updates.
- Updated ClamAV library to support scanning raw DMG files.
- Performance improvements.
- Various fixes for support cases.

28 May 2015 Release Notes

Private Cloud Administration Portal v2.0.20150525

Bugfixes / Enhancements

- Included a patch for the June 30, 2015 leap second.
- Improved user interface for device and content updates.
- Enhanced proxy support for retrieving updates.

31 March 2015 Release Notes

Private Cloud Administration Portal v2.0.20150325205338

New Features

- Secure Endpoint Private Cloud now supports air gap deployments.

Bugfixes / Enhancements

- Fixed an issue where disk performance and usage graphs were shown for removable devices.
- Fixed an issue where gaps in data were causing incorrect values for query failure rates.
- Added a sanity check for devices with insufficient memory.
- Additional information is now collected for support snapshots.
- Memory allocations for services are automatically adjusted based on VM memory at boot time.
- Patch for June 30, 2015 leap second.

24 February 2015 Release Notes

Private Cloud Administration Portal v1.5.20150206133846

Bugfixes / Enhancements

- Upgraded Secure Endpoint Mac connector protocol version to improve compatibility and reliability. This update is required to ensure future connectivity between the Private Cloud device and Secure Endpoint Mac connectors. All Secure Endpoint Mac connector policies will be updated to enable this change.

29 January 2015 Release Notes

Secure Endpoint Windows Connector 3.1.17.9685

Bugfixes / Enhancements

- Fixed an issue where saving an Excel file to a network drive could take an unusually long time.

Private Cloud Administration Portal v1.5.20150126112807

Bugfixes / Enhancements

- Improve accuracy for Private Cloud Administration Portal metrics reporting.

8 January 2015 Release Notes

FireAMP Console v4.5.2014112012

Bugfixes / Enhancements

- Resolved an issue with restoring quarantined files from the FireAMP Dashboard.

FireAMP Cloud Server 0.9.17-1

Bugfixes / Enhancements

- Resolved an issue with storage of cloud server lookups.

7 November 2014 Release Notes

FireAMP Console v4.5.2014110616

Bugfixes / Enhancements

- Performance improvements for file disposition lookups in Device Trajectory.

Secure Endpoint Windows Connector 3.1.16

Bugfixes / Improvements

- Fixed a bug caused by the accumulation of archived ClamAV logs that could result in computers running out of disk space. Archived ClamAV logs are now deleted hourly.

8 October 2014 Release Notes

Private Cloud Administration Portal v1.5.20141002

Bugfixes / Enhancements

- Security fixes for bash that address CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, and CVE-2014-6278.

18 September 2014 Release Notes

Private Cloud Administration Portal v1.5.20140916

Bugfixes / Enhancements

- Support for Cloud Recall functionality when a Defense Center is connected to Private Cloud.

Secure Endpoint Windows Connector 3.1.11

Bugfixes / Enhancements

- Fixed translation error in the Japanese version of the Secure Endpoint Windows connector.

20 August 2014 Release Notes

Private Cloud Administration Portal v1.5.20140814

Bugfixes / Enhancements

- Fixed a problem that would sometimes cause content updates to fail.
- Fixed a bug that would cause report generation to fail.
- Increased minimum RAM requirement for the Private Cloud VM to 16GB when the OVA is first installed.

15 June 2014 Release Notes

Private Cloud Administration Portal v1.5

New Features

- Added integration with Cisco Defense Center.

Bugfixes / Enhancements

- Fixed bug associated with growing storage containers from the same disk.
- Refresh DNS when switching from DHCP to static.
- Disabled multiple support sessions.
- Validate proxy server information.
- Fixed bug where an HTTP 502 response was returned after 40 seconds.
- Updated OpenSSL to address recent vulnerabilities including Heartbleed.

FireAMP Console 4.5.20140306

New

- Two-Step Verification will be an available option for all users.
- Secure Endpoint Mac connector now available.

Bugfixes / Enhancements

- Detailed file information can now be accessed from the File Trajectory page either by search or by right-clicking the filename or SHA-256 value.
- A single default exclusion set is now created during first use rather than one each for Audit, Protect, and Triage policies.
- Address an issue where policy scheduled scans created in the month of January would fail to run.
- New favicon for the FireAMP console.
- Added new Indication of Compromise event called Generic IOC to flag suspicious behavior.

Secure Endpoint Windows Connector 3.1.11

- Updated TETRA license key to avoid expiry on July 1, 2014.