Endpoint Protector Release History

Learn about the current and previous Endpoint Protector updates. Information regarding changes and enhancements is detailed in chronological order below.

25-April-2016

Endpoint Protector – Product Update

(Version 4.4.1.0)

Server Version: 4.4.1.0

Improvements:

- EasyLock Enforced Encryption for USB storage devices has been significantly extended. It now provides features like:
  - The option for deployment and use only in networks when Endpoint Protector is present
  - Automatic deployment to connected USB storage devices
  - Master Password, assisting in business continuity in various circumstances
  - Changing users' passwords remotely
  - Sending messages to EasyLock users' directly from the UI
  - Resetting devices in cases like lost or stolen devices
  - Automatic updates for EasyLock
  - Logs, Alerts and SIEM integration have also been added
- Continuing with the changes in the latest releases relating to a better user experience, several UI improvements have been made, including the ones below:
  - The Content Aware Protection Blacklists and Whitelists have been restructured and renamed in a more intuitive way
  - Adding new Whitelists and Blacklists or Editing them has been simplified, eliminating unneeded steps
  - The Endpoint Protector Client download section has been redesigned
  - A new option has been added to uninstall the Endpoint Protector Client by right clicking on the desired entity from Endpoint Management > Computers
- Audit Log Backup has been added, providing a new option to manage and export logs in a more visual way

Device Control

- Trusted Device Level 1+ was added, providing additional features in correlation with EasyLock Enforced Encryption

- For Mac OS X, a more granular way to control Bluetooth devices has been added and includes devices like Smartphones, Tablets, Keyboards, Mice and Others
- Performance improvements in the Networking section of the Endpoint Protector Appliance Console

Content Aware Protection

- The Content Aware Protection module has been enhanced to support the most popular Linux versions and distributions. Currently in Private Beta, the available features include the below:
  - Monitoring and controlling file transfers through various exit points like E-mails, Web Browsers, Cloud Services, File Sharing Services and more
  - Creating Filters based on Predefined Content, Custom Content, Regular Expressions and File Extensions etc.
  - Thresholds, Whitelists and Blacklists
- File Location Blacklists and Whitelists have been added, allowing file transfers from a specific location to be automatically blocked or allowed, regardless of the general Content Aware Policy
- The Predefined Content Filters within the Content Aware Policies have been extend to include new PIIs for Australia, Netherlands, Italy, UK, USA and Canada like Australian Medicare Numbers, Burgerservicenummer BSNs, Codice Fiscale, ABA Routing Numbers and more
- Slack has been added to the list of monitored applications
- Lotus Notes new add-on has been implemented for versions 8.5 and 9.0.1, bringing benefits like E-mail body shadowing, logging sender and receiver. In addition to these, the managed applications versions for Lotus Notes have been merged to simplify administration
- The Whitelists and Blacklists menu has been restructured for easier access

Bug fixes:

- In some cases, E-mails generated by the System Alerts were showing negative remaining or expired days. Fixed
- An error occurring when deleting multiple Computers that were part of large networks has been fixed
- Fixed broken string and blank page that sometimes appeared when deleting entities
- Special characters could not be used in certain passwords. Fixed
- For File Tracing Reports, unchecking some columns would only hide the header. Fixed

Windows Client Version: 4.5.3.7

Improvements:

- The VID, PID and Serial Number of a removable device is now displayed in the Endpoint Protector Client Notifier when the user hovers the device, simplifying the Offline Temporary Password generation process
- The file extensions from within the Exclude Extensions from Shadowing and Exclude Extensions from CAP Scanning are no longer case sensitive
- Improved E-mail address detection to reduce some false positives

Bug fixes:

- After a Client Upgrade, the Notifier did not start automatically. Fixed
- Fixed the blocked message displayed in some cases when an unauthorized device was connected

- Fixed invalid device names reported on some Content Aware Protection and File Tracing events

Mac Client Version: 1.4.9.7 (for MAC OS X: 10.6+)

Improvements:

- The Vendor ID, Product ID and Serial Number of a removable device is now displayed in the Endpoint Protector Client Notifier when the user hovers the device, simplifying the Offline Temporary Password generation process
- New Devices are now recognized as a direct result of the extended granularity of Bluetooth devices
- EasyLock now starts automatically if TD1 or TD1+ rights are set
- Improved E-mail address detection to reduce some false positives
- The list of IPs for a single entity was enlarged, providing the option to view various Computer IPs (internal, external, routed, gateway etc.)

Bug fixes:

- Some localized translations for the Notifier were fixed
- In certain circumstances, device rights were not applied correctly due to the available Vendor information. Fixed

Linux Client Version: 1.2.9.1

Improvements:

- Content Aware Protection has been added for multiple Linux versions and distributions (Ubuntu 14.04, CentOS and RedHat 7.0 up to 7.3, openSUSE 12.1 and SUSE 12.1) including features like:
  - Thresholds, Controlled Storage Device Type, Application Filters, File Type Filters, Predefined Content Filters, Custom Content Filters, Regex Filters, File Whitelist, etc.
- The list of controlled devices now also includes WiFi, Bluetooth, Webcam and Media Transfer Protocol devices (Android phones and tablets, iPhones, iPads etc.)
- Offline Temporary Password has been added

Note: The Endpoint Protector Client currently supports Gnome and KDE Desktop Environments.

EasyLock Enterprise: 1.0.0.1

Improvements:

- EasyLock Automatic Deployment has been added, offering the option to enforce encrypt any USB storage device that is plugged into any computer where the Endpoint Protector Client is present
- Added the option to create a Master Password, providing continuity in various circumstances like resetting the user's password, sending messages, resetting devices and more

Bug fixes:

- Fixed Offline File Tracing to display accurate information in real time.