Release Notes for Threat Protection Appliance v3.4

Applies To:	Forcepoint Threat Protection Appliance v3.4.0

Use these Release Notes to find information about what's new and improved for Threat Protection Appliance v3.4.

New in Threat Protection Appliance v3.4

Release Notes | TPA | 28-Nov-2016

Applies To:	Forcepoint Threat Protection Appliance v3.4.0

The new v3.4 version of the Threat Protection Appliance (formerly known as SureView Threat Protection) includes the following new features:

New product name

For v3.4, SureView Threat Protection has been renamed to Threat Protection Appliance. The Threat Protection Appliance console and documentation have been updated to reflect the new product name. This change does not affect product functionality.

Look and feel enhancements

To support the ongoing transition from Raytheon Cyber Products and Raytheon|Websense to Forcepoint LLC, Threat Protection Appliance has a new look and feel. The colors and logos have been updated to reflect the Forcepoint brand. These changes do not affect product functionality.

Automated software updates

Threat Protection Appliance v3.4 supports the ability to check for software updates and to automatically upgrade the software to a newer release. The system can periodically check for updates automatically, or the check may be completed manually at any time. An Internet connection is required for this feature to work.

To manually check for new software updates, open the Help menu (**?** icon) in the upper right corner of the TPA console, and then select the **About Threat Protection Appliance** option. In this About window, TPA indicates whether the installed software is up to date or if updates are available. If updates are available, click the **Upgrade** button to download and install the latest software.

ThINK custom hypervisor sandbox

The Honey Monkey behavioral node has been renamed to the ThINK behavioral node. The new ThINK node implements the latest sandboxing technology developed by Forcepoint. The new sandboxing implementation, known as ThINK v1.1, permanently replaces the Honey Monkey project and KI2 hypervisor technology. The Operating System has also been upgraded from Windows 2008 Server to CentOS 7 64-bit.

The new ThINK node provides the following upgrades over the old Honey Monkey system:

- Able to run two different baselines in the same behavioral node.
- Able to run more analysis virtual machines than the previously used Honey Monkey node.
- Implements heap-spray analytics. ThINK will flag entropy changes to the process heap which are indicative of a heap spray attack. Heap sprays are a common component of browser and Acrobat Reader exploits.
- Flags hardware and software exceptions that are likely to indicate that an exploit is being attempted.
- Flags detection of sandbox signature tools. Malware will not be able to detect that it is being executed in a virtualized environment.
- Flags software that requests elevated privileges (UAC) from the user.
- Improves stability and scalability.
- Implements emulator fixes, including updates to the guest timer subsystem.
- Implements a REST API for easier integration with other technology.

Deployment improvements

Threat Protection Appliance deployments has been streamlined to include improvements within the Configuration Wizard. This feature allows the user to make routine changes to the system without needing a command-line session.

A main menu screen has been added to the Configuration Wizard to list the category screens (e.g., External Services, Network, Behavioral Servers) from which you can make changes to the system.

License manager

Threat Protection Appliance v3.4 includes the ability to extend maintenance coverage for the application remotely, through Forcepoint Sales.

After Threat Protection Appliance v3.4 is installed, and after the initial license period expires, you can now automatically re-enable the maintenance coverage without local administrator intervention. You can extend your support period through Forcepoint Sales, which will automatically re-enable periodic updates and will enable full application functionality consistent with your sales agreement(s).

End user license agreement

The End User License Agreement (EULA) is now presented through the Configuration Wizard during installation. If you do not accept the EULA, the installation will shut down.

After installing the software, you can view the EULA from the TPA Console by opening the Help menu (? icon) in the upper right corner, selecting the **About Threat Protection Appliance** option, and then clicking **Terms of Use**.

Installation and Upgrade

Release Notes | TPA | 28-Nov-2016

Applies To:	Forcepoint Threat Protection Appliance v3.4.0

Licensing

All installations of Threat Protection Appliance v3.4 require a valid license key. Obtain this license key from Forcepoint Sales prior to beginning the installation. The installation will fail without a valid license key.

New Installation

A step-by-step guide to installing Threat Protection Appliance can be found in the Quick Start Guide and the Threat Protection Appliance Installation Guide provided with the product.

Upgrading Threat Protection Appliance

The Threat Protection Appliance upgrade process varies per installation, depending on the hardware profile. Existing customers wishing to upgrade to v3.4 must contact Forcepoint Support. Forcepoint Professional Services will then work with the customer to determine the system requirements and the installation process.

Resolved and known issues for Threat Protection Appliance

Release Notes | TPA | 28-Nov-2016

Applies To:	Forcepoint Threat Protection Appliance v3.4.0

A list of resolved and known issues in this release is available to Threat Protection Appliance customers in the Forcepoint [Knowledge Base.](#) Access to the Knowledge Base requires that you log on to My Account.