Wind River's Advanced Security Program

Better Security, Easier Compliance

In today's day and age, avoiding cyber-attacks is a top priority for businesses across all industries. 80% of small businesses that suffer a breach go out of business after 18 months and so protecting both your business and your customers' data is essential. Thanks to Wind River, you now have access to all the tools you'll need to better protect your organization from cyber-attacks. Your TrustKeeper account in Wind River's Advanced Security Package (ASP) gives you access to the Endpoint Protection Suite, which includes 13 key tools such as Anti-Virus, File Integrity Monitoring, and Malware Monitoring. You don't have to be an IT expert to install Endpoint and you could easily *pay seven times more for these same capabilities if you purchased them independently*.

Wind River's Advanced Security Program helps you:

- Secure your business by providing a comprehensive toolkit that makes it easier to defend against hackers and malware
- Save money by bundling all the security solutions needed to secure your business in to one affordable package
- Simplify PCI compliance efforts with an automated workflow that reduces the number of questions to answer

Details of the ASP's Offerings

External Vulnerability Scans

- Certified external vulnerability scans designed to detect and report security shortcomings of the target physical location and/or website from the perspective of a would-be hacker.
- Applicable PCI/SAQ area: PCI DSS requirement 11.2

Security Health Check

- Monitors the basic health of the endpoints to ensure security settings are in-place and active.
- Applicable PCI/SAQ area: PCI DSS requirement 11

Security Configuration Monitoring

- Monitors the endpoint's security configuration against the relevant PCI Data Security Standard controls allowing you to discover and address policy and security weaknesses quickly and holistically on mobile and fixed endpoints.
- Applicable PCI/SAQ area: PCI DSS requirement 11

POS Application Detection Module

- Monitors the endpoints for known payment applications and reports on their compliance status.
- Applicable PCI/SAQ area: PCI DSS requirement 9

Credit Card Data Scanner (DLP)

- Inspects the endpoints for storage of sensitive or PCI-prohibited data including credit card data and full magnetic stripe data.
- Applicable PCI/SAQ area: PCI DSS requirement 3

Unauthorized Device Monitoring

- Inventories the local network as well as monitoring for unknown rogue devices.
- Applicable PCI/SAQ area: PCI DSS requirement 11.1

File Integrity Monitoring (FIM)

- Detects unexpected or malicious changes to critical system files, directories and registry settings for Windows and Linux OS endpoints.
- Applicable PCI/SAQ area: PCI DSS requirement 11.5

Trustwave Anti-Virus (AV)

- Prevents, detects and removes malicious computer viruses for Windows, Linux, and Android OS endpoints.
- Applicable PCI/SAQ area: PCI DSS requirement 5

Security Policy Generator

- Helps the merchant meet the relevant PCI SAQ requirements and speeds the process of showing that compliance.
- Applicable PCI/SAQ area: PCI DSS requirement 12

POS Tracker

- Helps track and monitor POS equipment for tampering and substitution.
- Applicable PCI/SAQ area: PCI DSS requirement 9

Remote Access Security

- Monitors and tracks remote access software installed and enabled on the endpoint; provides guidance on best practices for configuring remote access securely.
- Applicable PCI/SAQ area: PCI DSS requirement 8

Mobile Device Security

- Audits and reports on security and compliance of the device to enable proactive defense.

Web Malware Monitoring

- Regular monitoring for malware that may be present on the merchant's website. It also tracks other issues that may affect consumer confidence in the website, such as being listed on a search engine blacklist, domain hijacking, and expired SSL certificates.