IBM PowerSC

Security and compliance solution designed to protect virtualized datacenters

Highlights

- Simplify security management and compliance measurement
- Reduce administration costs of meeting compliance regulations
- Ensure virtualized environments meet same security levels as physical servers
- Improve the audit capabilities for virtualized systems
- Reduce time and skills required for preparation of security audits
- Improve detection of security exposures in virtualized environments

Security and compliance are vital to many businesses, especially now that they must adhere to regulatory requirements designed to safeguard personal data and company information from security attacks. Ensuring that IT systems are compliant with common industry security standards and maintaining system security can be a challenging, labor-intensive activity especially with today's virtualized IT infrastructures. IBM® Power Security and Compliance (PowerSC™) provides a security and compliance solution optimized for virtualized environments on Power Systems™ servers, running PowerVM®.

Automate systems settings for optimal security and compliance

Ensuring system compliance with third-party security standards is often a labor intensive and time consuming process. Compliance standards are typically long, complex documents that are difficult to translate into the appropriate AIX® or Linux operating system settings. And, because standards often encompass many different areas of operating system and virtualization software, they may have required using several different administrative interfaces to configure a system appropriately.

With its simple administration interface and preconfigured compliance profiles, PowerSC is designed to simplify the administrative effort associated with complying with some of the most common external standards

for security and compliance. PowerSC security and compliance automation provides profiles for the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act Privacy and Security Rules (HIPAA) and US Department of Defense Security Technical Implementation Guide for UNIX (DoD STIG) standards, as well as supporting the implementation of best practices specified by the Control Objectives for Information and related Technology (COBIT) standard. Public companies that are subject to the U.S. Sarbanes-Oxley Act of 2002 often adopt the COBIT best practices. PowerSC also provides a security automation profile to automate configuration of optimal security for database servers.

Since all external security standards include aspects outside the realm of system configuration settings, the use of the security and compliance automation will not, by itself, ensure standards compliance. Nonetheless, PowerSC security and compliance automation does significantly simplify systems configuration settings management, allowing security administrators the time to focus on the other aspects of standards compliance.

Improve visibility and hardening of the virtual infrastructure

PowerSC provides a range of capabilities to ensure a root of trust for virtual machines, including "Trusted Boot," a virtual implementation of the Trusted Platform Module (TPM) from the Trusted Computing Group. The PowerSC Trusted Boot feature provides virtual TPM functionality for AIX virtual machines running with the PowerVM hypervisor on Power Systems.

The TPM functionality measures the system boot process in each virtual machine, and with cooperation from the AIX Trusted Execution technology, provides security, trust and assurance of the boot image on disk, the entire operating system and the application layers. Each virtual machine has its own separate virtual TPM that holds its unique measurement data used to validate the root of trust. This functionality is available on all IBM Power Systems built with POWER8™ technology or on systems running eFW7.4 firmware or higher.

A trust monitor, OpenPTS, is also provided with PowerSC that enables administrators to monitor and attest to the trust of their AIX virtual machines. The monitor makes clear the trust and security level of Power Systems running PowerVM virtualization.

Comply with site security policies for virtual machines

Maintaining virtual machines across multiple systems presents different administrative challenges to traditional physical systems deployment. For example, virtual machines may be suspended or powered off or even moved to other servers during a patch application process. Moving a virtual machine, for example, may open a window of vulnerability by potentially having a different patch level than is required on a target physical system.

Trusted Network Connect (TNC) and Patch Management in PowerSC can detect AIX virtual machines that do not meet the corporate patch policies that have been established for a virtualized data center. Alerts are triggered if a noncompliant virtual machine is detected. TNC and Patch Management analyzes data from both the Service Update Manager Assistant (SUMA) and the Network Installation Manager (NIM) to check each virtual machine during network activation.

TNC and Patch Management also monitor the IBM Electronic Customer Care system and provide alerts for new security patches or updates that affect AIX systems. Alerts can also be configured simply to send SMS messages to mobile devices.

Harden audit trails in virtual environments

One of the foundations of compliance is the ability to audit an environment and to guarantee that audit trails, such as audit logs and system logs cannot be altered. These logs help provide transparency and prevent covering of security breaches. Trusted Logging in PowerSC centralizes the AIX system logs across all virtual machines on a server, enabling the logs to be kept on a single instance of the PowerVM Virtual I/O Server (VIOS). This secure VIOS virtual machine protects the entire log data received from each AIX virtual machine. No administrator of any AIX virtual machine can remove or alter the system logs held on the secure VIOS Server.

With the introduction of centralized logging and administration provided by Trusted Logging, backup, archive and audit of system logs is significantly simplified for the security administrator.

Control and enforce compliance for virtual networks

The Trusted Firewall feature in PowerSC provides a virtual firewall that allows network filtering and control within the local server virtualization. The virtual firewall improves performance and reduces resource consumption of network resources by allowing direct and secure local VM to VM network traffic. The Trusted Firewall has the ability to monitor traffic and provide advice as to which traffic should be added to the firewall. This advisor can generate the appropriate commands to add the VM network segments to the Trusted Firewall.

Feature	Benefits
Security and compliance automation *AIX, Linux*	• Reduces administration costs for complying with industry security standards
Real-time compliance monitoring *AIX*	• Continuous monitoring and alerting if changes occur that cause AIX systems to be non-compliant to security policies.
Compliance reports *AIX, Linux*	• Reduces time and cost to provide security and compliance reports to auditors
Preconfigured profiles for PCI,DOD STIG,HIPAA, COBIT security standards and database servers *AIX all profiles, Linux PCI & HIPAA*	• Saves time, cost and risk associated with deploying industry security standards
Trusted Boot *AIX*	• Reduces risk of compromised security by guaranteeing that an AIX operating system image has not been inadvertently or maliciously altered
Trusted monitoring *AIX*	• Ensures high levels of trust by displaying the status of all AIX systems participating in a trusted system configuration
Trusted logging *AIX*	• Prevents tampering or covering security issues by storing AIX virtual machine system logs securely on a central PowerVM Virtual I/O Server • Reduces backup and archive time via storing audit logs in a central location
Trusted network connect and patch management *AIX*	• Ensures that site patch levels policies are adhered to in virtual workloads • Provides notification of noncompliance when back-level systems are activated
Trusted firewall *Any VM Type, AIX, Linux, IBM i*	• Improves performance and reduces network resource consumption by providing firewall services locally with the virtualization layer
Trusted Surveyor *Any VM Type AIX, Linux, IBM i*	• Provides visibility to ensure segregation of virtual networks to maintain security compliance

Monitor compliance to network segregation policies

PowerSC Trusted Surveyor provides the capability to monitor network configuration drift and to report on network compliance adherence to defined policies. This provides an independent audit and governance of virtualized network infrastructure which ensures consistent and controlled configuration change. The information that Trusted Surveyor provides lowers administration costs by automating the network compliance monitoring. The Trusted Surveyor compliance monitoring solution works for all Power VM types which include AIX, IBM i and Linux. Trusted Surveyor is sold separately. All other PowerSC functionality is offered in the PowerSC Standard Edition.

Why IBM?

IBM is the trusted security advisor to thousands of the world's leading businesses and governments. IBM offers a complete range of server, storage, application and services offerings that have been architected with security at the core of their design. IBM's depth and breadth of expertise in security and compliance with IBM Power Systems is virtually unmatched.

For more information

To learn more about IBM PowerSC, please contact your IBM marketing representative or IBM Business Partner, or visit the following website:
ibm.com/systems/power/software/security/index.html

IBM Systems and Technology Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2014