IBM Systems
Data Sheet

IBM PowerSC

Designed for Enterprise Security & Compliance in Cloud and Virtualised environments

Highlights

- Simplify management and measurement for security & compliance
- Quickly view security compliance of an entire data centre (DC) from a centralised user interface (UI)
- Reduce time and administration costs of meeting compliance regulations
- Improve the audit capabilities for virtualised systems while reducing time and skills required for preparation
- Improve detection and reporting of security exposures in virtualised environments.

Security control and compliance are some of the key components needed to defend virtualised DC and cloud infrastructure against evolving new threats. Ensuring that IT systems are compliant with common industry security standards and maintaining system security can be a challenging, labour-intensive and costly activity especially when it comes to cloud / virtualised IT environments. IBM® PowerSC provides a security and compliance solution optimised for virtualised and cloud environments on Power Systems servers, running PowerVM.

PowerSC is an integrated offering, ensuring high levels of security and compliance by taking advantage of all the features of the IBM Power Systems Software stack, from the hypervisor and firmware through the virtualisation layer to the operating system (OS), including network traffic between the layers.

The PowerSC functionality reduces cost, simplifies administration, accelerates compliance audit preparation and reduces risk by increasing visibility to security threats.

Automate systems settings for optimal security and compliance

Many IBM Power System clients must adhere to strict security compliance standards for their particular industry. Regulatory compliance requires setting security on systems in a uniform manner in order to comply. Understanding all the rules and applying a particular standard is tedious, time consuming and error prone. Compliance standards are typically long, complex documents containing hundreds of rules that are difficult to translate into the appropriate operating system settings. Plus, because standards often encompass many different areas of OS and virtualisation software, they may have required using several different administrative interfaces to configure a system appropriately.

PowerSC Compliance Automation provides pre-built profiles that are certified to comply with industry standards like the Payment Card Industry Data Security Standard (PCI) v3, HIPAA (Health Insurance Portability and Accountability Act Privacy and Security Rules) for Healthcare, NERC (North American Electric Reliability Corporation) for Utilities like the energy sector, DoD STIG (US Department of Defence Security Technical Implementation Guide for UNIX) for our Federal clients or support for SOX-COBIT (Sarbanes- Oxley best practices specified by the Control Objectives for Information and related Technology). PowerSC also provides a security automation profile to automate configuration of optimal security for database servers. In addition, it provides out of the box (OOTB) levels for Low, Medium and High security levels.

PSCxpert (an enhanced version of AIXpert) is the underlying mechanism to apply security policy settings and check for compliance. These have always been great tools for managing compliance. However, to manage the profiles, you had to log in and execute commands on each system individually. The new centralised UI for Compliance Automation, first delivered with PowerSC 1.1.5, makes security compliance significantly easier to manage (see ‘New centralised UI for Security & Compliance’ below)

Continuous monitoring and alerting of changes

Real Time Compliance allows monitoring a list of files and provides notification when compliance violations occur or when a monitored file changes. Usually, regular compliance checks are conducted on a scheduled basis. So, if your system runs into a violation situation, this typically won’t be noticed prior to the next scheduled scan. Real Time Compliance closes this gap by adding real-time notifications of any possible policy violation to your server. Whenever a change is made that violates the compliance profile policy, a message can be sent to the administrators or security officers via Short Message Service (SMS) or email. It is also possible to send Syslog and Simple Network Management Protocol (SNMP) messages to your monitoring server, integrating the feature into your IT monitoring system. Products, such as IBM QRadar, can accept these alerts for integration into your existing infrastructure.

PowerSC Real Time Compliance provides two monitoring options:

1. *Content monitoring* checks whether the content of a file is modified

2. *Attributes monitoring* verifies whether the file permissions changed

New centralised UI for Security & Compliance

The new centralised UI for security and compliance – first introduced with PowerSC 1.1.5 and hugely extended with PowerSC 1.1.6 - makes security & compliance significantly easier to manage and thus reduces cost, saves time and lowers the risk for human error.

- **Compliance Automation**
  Understand & manage the security compliance of all PowerSC managed AIX endpoints across your Power environment with minimal discovery effort and in a centralised location. It allows checking and applying PowerSC profiles, using both built-in and custom profiles, on multiple endpoints simultaneously. In addition, it enables organising and grouping PowerSC endpoints, enabling custom filtering.
- **RTC / TE Integration**
  Improved Malware intrusion prevention / detection capabilities due to centralised configuration and monitoring capabilities for File Integrity Monitoring (PowerSC RTC & AIX TE)
- **PowerVC Integration**
  This allows to protect your clouds right from the beginning. We semi-automated the process to connect new endpoints being deployed with PowerVC as new managed endpoints within the new PowerSC UI
- **Security & Compliance Dashboard**
  Providing a consolidated view of all relevant AIX security tracking and protection components
- **Reporting to support audits**
  PowerSC 1.1.6 ships with five OOTB reports to support to prepare for / pass audits. It provides capability to generate formatted html or csv files, that can even be scheduled to be sent regularly via email at a certain time
- **Profile Editor Enhancements**
  While the Profile Editor in 1.1.5 just had limited capabilities to create custom profiles, the extended profile editor delivered with 1.1.6 allows clients to aggregate rules of various profiles into a custom profile. In addition, it enables to change parameters of specific rules within these custom profiles
- **Northbound Integration (QRadar)**
  In 1.1.6 we worked on integration with higher level security tools via syslog information, so that it can be consumed by QRadar and made available there
- **UNDO Improvements**
  The process to UNDO a profile is a rather complex process. In PowerSC 1.1.6, improved UNDO behaviour is provided for the PCIv3 profile. (The UNDO behaviour of the remaining profiles will be improved in subsequent releases as well)
- **Compliance GUI Scalability**
  PowerSC used to support 500 endpoints per UI server in 1.1.5. In PowerSC 1.1.6, we are doubling that number, so that 1000 endpoints per UI server are supported.

Note: All the remaining PowerSC components (TNC, Trusted Boot, Trusted Firewall, Trusted Logging) continue to exist in their native version (command line) in the current release;

The new centralised UI for security & compliance supports only AIX in the current release

Comply with site security policies for virtual machines

Maintaining virtual machines (VMs) across multiple systems presents different administrative challenges to traditional physical systems deployment. For example, a VM may be suspended or powered off or even moved to other servers during a patch application process. Moving a VM, 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 VMs that do not meet the corporate patch policies that have been established for a virtualised DC. Alerts are triggered if a noncompliant VM is detected. TNC and Patch Management analyses data from both the Service Update Manager Assistant (SUMA) and the Network Installation Manager (NIM) to check each VM 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.

In the latest release TNC and Patch Management also monitors the open-source software provided as a part of the base AIX for packages that have been downloaded from the AIX toolbox or other web download sites for AIX Open Source Packages.

Improve visibility and hardening of the virtual infrastructure

PowerSC provides a range of capabilities to ensure a root of trust for VMs, 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 VMs running with the PowerVM hypervisor on Power Systems.

The TPM functionality measures the system boot process in each VM and with cooperation from the AIX Trusted Execution technology, provides security, trust and assurance of the boot image on disk, the entire OS and the application layers. Each VM has its own separate virtual TPM that holds its extraordinary 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.

OpenPTS, a trust monitor provided with PowerSC enables administrators to monitor and attest to the trust of their AIX VMs.

Harden audit trails in virtual environments

Trusted Logging in PowerSC centralises the AIX system logs across all VMs on a server, enabling the logs to be kept on a single instance of the PowerVM Virtual I/O Server (VIOS). This secure VIOS VM protects the entire log data received from each AIX VM. No administrator of any AIX VM can remove or alter the system logs held on the secure VIOS Server.

With the introduction of centralised 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 virtualisation. 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.

PowerSC security and compliance functionality include the following components:

Compliance Automation incl. preconfigured profiles for various industry standards	• Security Compliance Automation provides pre-built profiles that are certified to comply with industry standards like PCIv3, HIPAA, NERC, DoD STIG, SOX-COBIT.
Real time compliance (RTC) incl. Reporting capabilities	• Simplifies management, by automating monitoring and providing immediate visibility to administrators sending alerts when a change to the system violates a rule that is identified in the configuration policy and thus lead to AIX systems being non-compliant.
Trusted Network Connect (TNC) and **Patch Management**	• Automatically detects any AIX system which boots, resumes or moves by live mobility into the virtual environment and ensures it is at the prescribed install and security patch level and provides alerts if a security patch is issued that affects the systems.
Trusted Boot	• Measures the boot image, OS and applications, and attests their trust and that it has not been inadvertently or maliciously altered by using the virtual trusted platform module (vTPM) technology.
Trusted Logging	• The logs of AIX are centrally stored on the Virtual input/output (I/O) Server in real time. This feature provides tamperproof logging and convenient log backup and management and eliminates the need for log-scraping agents running on the OS. Thus, it maintains the chain of trust for system and audit logs.
Trusted Firewall	• Trusted Firewall ensures that every VM has appropriate network isolation. It saves time and resources by enabling direct routing across specified virtual LANs (VLANs). By providing network firewall services within the server not requiring an external firewall for VM to VM traffic on the same CEC it improves performance as well.

For more information

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

IBM United Kingdom Limited
PO Box 41
North Harbour
Portsmouth
Hampshire
PO6 3AU
United Kingdom

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4

IBM Ireland Limited registered in Ireland under company number 16226.

The IBM home page can be found at **ibm.com**

IBM, the IBM logo, ibm.com, AIX, PowerSC, Power Systems, PowerVM, POWER8 and are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries.

A current list of IBM trademarks is available on the Web at 'Copyright and trademark information' at **ibm.com**/legal/copytrade.shtml

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product and service names may be trademarks, or service marks of others.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates.

Any reference to an IBM product, program or service is not intended to imply that only IBM products, programs or services may be used. Any functionally equivalent product, program or service may be used instead.

IBM hardware products are manufactured from new parts, or new and used parts. In some cases, the hardware product may not be new and may have been previously installed. Regardless, IBM warranty terms apply.

This publication is for general guidance only.
Information is subject to change without notice. Please contact your local IBM sales office or reseller for latest information on IBM products and services.

This publication contains non-IBM Internet addresses. IBM is not responsible for information found at these Web sites.

IBM does not provide legal, accounting or audit advice or represent or warrant that its products or services ensure compliance with laws. Clients are responsible for compliance with applicable securities laws and regulations, including national laws and regulations.

Photographs may show design models.

Please Recycle

PowerSC