IBM PowerSC 2.1

Designed for enterprise security and compliance in cloud and virtualized environments

Highlights

Manage security, compliance and patch management with a centralized UI

Enhance security with multifactor authentication

Improve audit capabilities against security exposures in virtual environments

Security control and compliance are some of the key components needed to defend virtualized data center 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, labor-intensive and costly activity especially when it comes to cloud and virtualized IT environments. IBM® PowerSC provides a security and compliance solution optimized for virtualized and cloud environments on IBM Power® servers.

PowerSC manages the security and compliance of IBM Power Systems and runs on IBM AIX®, Linux®, or IBM i systems. It 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 to the virtualization and operating system, 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.

Manage security, compliance, and patch management with a centralized UI

PowerSC has a centralized UI, which makes managing security and compliance significantly easier while reducing costs, saving time and lowering the risk for human error. The user friendly, web-based UI manages the four main functions of PowerSC: Compliance, Security, Patch Management and Multifactor Authentication.

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

PowerSC provides solutions for highly regulated industries by automating compliance in pre-built profiles to comply with industry standards for General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPPA), the Payment Card Industry Data Security Standard (PCI DSS), the Department of Defense (DoD), the Center for Internet Security (CIS), the North American Electric Reliability Corporation (NERC) and many other industries.

The UI in PowerSC enables dashboard and drill-down capability in order to view and investigate endpoint compliance status and details about compliance rule failures. These profiles are frequently updated in PowerSC to keep up with changes to industry standards. The PowerSC GUI also provides extensive profile editing and reporting capabilities.

Security

For real-time security, the PowerSC dashboard shows a summary of statuses from security event sources and includes File Integrity Monitoring (FIM), Endpoint Detection and Response (EDR), Allow Listing, Block Listing and Anti-Virus capabilities.

File Integrity Monitoring (FIM)

File Integrity Monitoring (FIM) validates the integrity of key system files by recognizing and alerting when monitored files have content or permission changes. FIM makes use of underlying operating system hooks and features such as the Linux Audit daemon, IBM i Audit, and the AIX event infrastructure via the Real Time Compliance (RTC) component of PowerSC. Through the PowerSC GUI users can configure and view real-time events.

Endpoint Detection and Response (EDR)

With the recent increase in ransomware and cybersecurity attacks, PowerSC has added endpoint detection and response (EDR) capabilities. Aspects of EDR include intrusion detection and prevention, log inspection and analysis, anomaly detection, correlation, incident response, event triggers, and event context and filtering. These features provide an additional layer of security and protection to IBM Power Systems.

Allow Listing

This kernel-based “allow listing” approach is an anti-malware capability of PowerSC. It uses digital signatures to cryptographically verify important files haven’t been corrupted and prevents the execution of altered files. This zero-trust approach is a key aspect of locking down and securing systems.

Block Listing and Anti-Virus

Basic block listing in PowerSC is a selective, on-demand capability that allows for the matching of a customer-selected set of virus signatures at the file level using hash searches. PowerSC also provides a full-fledged anti-virus engine to scan, detect and quarantine viruses by checking files against a database of known malware and by searching for recognizable patterns or suspicious file structures.

Patch Management

The Patch Management status for all managed VMs can be found on the Security tab of the PowerSC UI. It highlights the non-compliant VMs and shows which security patches are missing. Updates can be triggered directly from the PowerSC GUI for AIX and Linux on Power logical partitions (LPARs). For AIX, the UI integrates closely with the policy-based patch management component of Power SC called Trusted Network Connect (TNC).

Enhance security with Multifactor Authentication

Multifactor Authentication (MFA) leverages two or more factors that are used to confirm separate pieces of evidence to grant access to the system. The first factor is something you know, such as a password or a PIN code. The second factor is something you have, such as an ID badge, email or phone number. The third factor uses something you are, such as a fingerprint, a retinal scan or facial recognition.

For more information on IBM PowerSC MFA, visit the IBM PowerSC MFA Data Sheet.

Improve audit capabilities against security exposures in virtual environments

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 IBM 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 the disk, the entire operating system, and the application layers. Each virtual machine has its own separate 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 IBM POWER8® technology or on systems running eFW7.4 firmware or higher.

Harden audit trails in virtual environments
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 IBM PowerVM Virtual I/O Server (VIOS). This secure VIOS virtual machine protects the 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, the 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 can 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.

Conclusion
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 while reducing costs, simplifying administration, accelerating compliance audit preparation and reducing risks by increasing visibility of security threats.

Why IBM?
IBM has over 105 years of aligning continuous innovation with our customers' business needs. With IBM's focus on delivering high performance secure systems and software, PowerSC ensures the highest level of security and compliance across all layers of the system.

For more information
To learn more about IBM PowerSC, please contact your IBM representative or IBM Business Partner, or visit ibm.com/products/powersc.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2022