helpsystems

DATASHEET *(Cybersecurity)*

Powertech Security Auditor

In today's world of overworked administrators, you need a product that allows you to automate your security administration and compliance tasks across multiple servers and storage areas on-premises and in the cloud. You need Powertech Security Auditor. Security Auditor is a server and S3 storage bucket security auditing and compliance reporting product. It simplifies and automates security administration tasks and compliance reporting requirements all from an easy-to-use, web-based console.

What Security Auditor Does

Security Auditor allows you to define your security requirements, whether for auditing a server or storage bucket. After defining your requirements, you compare them (run a 'compliance check') to the actual settings on the systems you manage. You can have the same requirements for all servers and manage them as a group, manage them individually depending on their function, or do a bit of both—it's your choice.

Security Auditor identifies the configuration settings that don't match your requirements. You can make the changes yourself to bring the settings into compliance, or you can run the FixIt function and let Security Auditor do the work for you.

The checks can be run interactively through the web-based console, or you can set them to run automatically through the integrated scheduler feature. This allows you to review your configurations as often as you need to. You can assess the results of the automated jobs interactively using the console. Or you can choose to have the results automatically emailed. The exception-based report is concise, listing only the items which do not match your requirements. The compliance reports are suitable to hand to you auditors. You can even create customized reports with the built-in report writer.

PRODUCT SUMMARY

KEY FEATURES

- Documented security configuration
- Automatic compliance checks on-premises and in the cloud
- Exception-based reports
- Security auditing for multiple systems on-premises and in the cloud via a single screen
- Automatic remediation of out-of-compliance settings
- Create custom audits

SYSTEM REQUIREMENTS

- IBM AIX 5.3 and higher
- Red Hat Linux
- Ubuntu Linux
- SUSE Linux
- CentOS Linux
- Oracle Linux
- Windows 7 or later
- Windows Server 2008R2 or later

PLATFORMS SUPPORTED

- Linux
- AIX
- HP-UX
- Solaris
- IBM i
- Windows
- AWS
- Azure
- Google Cloud
- OpenStack
- IBM Cloud
- And more!

PUBLIC CLOUD INTEGRATIONS

- Amazon EC2
- Amazon S3

Regularly Define and Check Policies on These Server Areas

- **Directory and file permissions:**
  - Read, Write, and Execute
  - Ownership and Group access
  - Special security attributes
    - SUID/SGID/SVTX
  - Extended permissions
  - File contents changed
  - Directory contents changed
- **Global security settings:**
  - Auditing attributes
  - Group attributes
  - Login defaults
  - Password attributes
  - User account creation defaults
  - And more
- **User account settings:**
  - Auditing attributes
  - Group attributes
  - Login defaults
  - Password attributes
  - And more
- **Services and daemons whitelist/blacklist**
- **Exported directory shares**
- **User-defined policies**
- **User account settings:**

Automating Security Administration

Here are just a few ways you can use Security Auditor to automate your security administration tasks:

- Apply your organization's security configuration as new on-premise or cloud servers come online, including global configuration settings, daemon settings, file/directory permissions, and exported directories
- Ensure cloud storage areas are secure and not leaking critical data to outside attackers
- Manage the permissions and ownership of files and directories, including those with no owner
- Establish a baseline of files with SUID or SGID and discover new ones as they are created
- Run compliance checks to identify new files or changes to settings such as ownership or permissions
- Determine when files' contents or executables have changed
- Adjust global security settings to comply with your requirements using FixIt
- Find user accounts with non-unique UIDs, or UIDs of 0 (other than root)
- Identify inactive local user accounts
- Ensure local user accounts remain configured correctly

Automating Compliance Requirements and Reporting

- Detailed and Summary reports, including the capability to add additional notes which can be used to document corporate policy adherence, justification for deviations from best practices, etc.
- Compliance reports, showing the details of out-of-compliance items or the fact that the security status is checked regularly, and all items are in compliance
- Reports on FixIt usage, including the command used to make the change and the previous value
- Consolidated reports—the results from multiple servers rolled into one report
- Elimination of the manual process of gathering data from multiple servers, consolidating it, comparing values, and generating a compliance report for auditors
- Confirmation that reports have been run as scheduled
- Automation and management of the security policies and compliance with those policies on multiple systems via a single screen in an easy-to-use browser-based GUI interface
- All reports—including consolidated reports or an individual server report—can be emailed to individuals (such as yourself or your compliance officer) or accessed through the console
- Report format options: PDF, CSV

User-Created Audits

The Scripts function in Security Auditor makes it possible for users to upload custom audits into the Security Auditor console and run them as part of their regular compliance checks. This allows administrators to consolidate specialized auditing unique to their organization in a central location and run those audits across multiple servers.

Administrators can take advantage of Security Auditor's built-in reporting capabilities to provide documentation of when the specialized auditing was run and whether it was successful. (When defining a script policy, administrators define what constitutes successful audit values.) The built-in scheduling function of the Security Auditor console can be used to run scheduled scripts across multiple servers and email administrators a report with the result. The Integrated Script Management feature includes the ability to:

- Import existing audit scripts into the Security Auditor console
- Define script conditions and return codes to be included in the compliance report
- Automate running of scripts (compliance checks) across multiple servers
- Define a "FixIt script" to be run when an audit is found to be non-compliant
- Provide proof to auditors that scripted audits were run on a regular basis
- Determine whether a script's contents have changed since the last time it was run
- Create user-defined policies to check unique requirements not pre-defined within Security Auditor

Additional Features

- Admin console allows you to administer individual servers or groups of servers on-premises and in the cloud at the same time using agentless technology
- Admin console allows you to administer one or more cloud service accounts at the same time, automatically discovering and applying security configurations to servers and storage as they come online
- All connections from the console to the servers are over an encrypted connection to ensure no data flows in cleartext. This connection is established using certificates so no passwords are ever stored.
- Comprehensive message log for tracking of Security Auditor administration and activity
- To get started, configurations can be initialized—that is, the current settings of a server can be automatically discovered and used as the initial settings to be applied to other servers in the environment, or just use one of the included security audit settings

Let's Get Started

To find out what Security Auditor can do for you, request a demo. We'll review your current setup and see how HelpSystems products can help you achieve your security and compliance goals.

helpsystems

www.helpsystems.com

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.