Simplified Security Administration and Compliance Reporting for SUSE® Linux Enterprise

Poor system configuration is commonly exploited by attackers to gain access to valuable data. Several recent security incidents were caused by little more than a series of human errors, reminding us that simple misconfiguration can have a disastrous impact. It is extremely difficult to manage and maintain the security you need without the right tools in place.

Policy Minder helps organizations maintain proper security configuration by automatically applying the proper security controls and ensuring that those controls are maintained.

Policy Minder at a Glance:

+ *Automates compliance audits and meets regulatory mandates*
+ *Provides exception-based reporting that integrates with your syslog monitoring station*
+ *Supports easy identification and remediation of security policy discrepancies with compliance management from a centralized user-friendly, browser-based interface*
+ *Gives you visibility into DevOps with automatic system discovery and applies the security configuration as new on-premise or cloud servers come online*

Products:

SUSE Linux Enterprise Server

The Challenge

Misconfiguration is a leading cause of data loss. Therefore, system configuration is a key component of your security operations. With hundreds of settings across multiple servers, many organizations find themselves in a situation where manually maintaining and enforcing their security controls is nearly impossible. Complex or heavily regulated organizations feel this pain most acutely, but even smaller businesses struggle to find the time and resources to verify security compliance.

The purpose of a security policy is to provide more control and visibility into system settings and user activity, but that purpose is only achieved if you have an effective way to manage your security policy. Solutions that automate your security policy management are the most efficient way to ensure that your security controls stay up to date and that policy exceptions are identified and corrected quickly.

The Solution

Automating security policy management saves time and enhances your security posture by enabling you to identify and then correct security exceptions. Manual solutions introduce the possibility of human error, including failing to apply fixes everywhere they are needed. In addition, manual solutions can simply take longer to complete. While manual policy management might be better than defining a security policy and ignoring it until audit time, an automated solution with a single console view provides a level of visibility and control that enables you to maximize your protection and your cybersecurity investment. It is faster and more reliable. Policy Minder delivers automation for simplified

security policy management, security administration, and compliance reporting.

KEY FEATURES

Automated Security Compliance—Policy Minder saves security administrators countless hours of manual data analysis and reporting. With the ability to automatically compare security controls to actual server settings, you'll guarantee that system reports are 100 percent accurate—and dramatically increase your productivity. Centralized compliance reporting also meets audit requirements for third-party-generated reports versus reports that are compiled by hand.

Centralized Security Administration for On-Premises, Cloud and Hybrid Environments—Policy Minder centralizes security administration regardless of whether your infrastructure is on-premises or in public, private or hybrid cloud scenarios.

Elimination of Security Administration Blind Spots—Apply your organization's security configuration automatically as new on-premises or cloud servers come online.

Simplified Configuration Management Across the Enterprise—When server settings need to be changed, Policy Minder's admin console makes it easy to automatically administer changes on one or multiple servers, whether on-premises or in the cloud, at the same time using agentless technology. With Policy Minder, you'll stay compliant and avoid human error, making your system more responsive and secure.

Regulatory Mandates Maintained with Ease—Policy Minder can automatically fix out-of-compliance items. Its automated fix-it function is able to detect and remediate any exceptions to policies in order to maintain compliance. The fix-it function can also be executed manually if you prefer that a member of your team authorizes the fix before it is made. Maintaining compliance couldn't be easier.

Compliance & Reporting from a Single Screen—Managing security policies and compliance with those policies on multiple systems, and in hybrid environments, becomes much easier from a single screen with Policy Minder's user-friendly, browser-based interface. Policy Minder logs all checks, out-of-compliance settings and fixes so that you have a complete audit trail.

How It Works With SUSE

CERTIFIED AND SUPPORTED ON SUSE LINUX ENTERPRISE SERVER 11 AND 12 ON X86-64 AND ON SUSE LINUX ENTERPRISE FOR IBM POWER

Policy Minder uses agentless technology over secure SSH connections to configure, audit and report on system security configuration and compliance settings. Connections can be secured with traditional login and password combinations or public/private key pairs. As your DevOps teams deploy workloads into the cloud, Policy Minder discovers those servers over cloud service APIs and then automatically applies the security configuration audits that you have defined. This perfectly complements SUSE's flexibility and strength in supporting on-premises, hybrid cloud and wholly cloud-based deployments.

You can remove delays in remediating the exceptions discovered by Policy Minder's automated technology by using SUSE® Linux Enterprise advantages such as Live Patching.

For More Information

For more information about Policy Minder, or to schedule a free, no-obligation demo or software trial, please visit: **www.help systems.com/products/security-policy-management-software-ibm-i-unix-linux-and-aix**