Privileged Account Manager

With Privileged Account Manager, your organization can control and monitor privileged user access across databases, applications, and the cloud.

Product Overview

Experts estimate that as many as half of all security breaches come from inside organizations. Insider threats are especially serious when associated with employees who have higher access privileges than needed. Whether the privilege misuse occurs at the hands of an employee, or is the work of a cyber-criminal who has leveraged the access credentials of an insider to gain access to your IT network, you can best manage this risk by closely controlling and monitoring what privileged users, such as super-users and database administrators, are doing with their access.

NetIQ Privileged Account Manager eliminates the need to distribute root-account credentials to your entire administrative staff. It delegates administrative access using centralized policies. You configure these policies to allow or deny user activity based on a comprehensive “who, what, where, when” model that examines the user’s name, typed command, host name and time. By managing privileges this way, you can control what commands users are authorized to run, at what time and from what location.

Privileged Account Manager features an Enterprise Credential Vault, or an encrypted password “vault,” that provides secure storage of your system, application, and database passwords. The Enterprise Credential Vault helps you to centrally manage your organization’s privileged accounts and provides an intuitive interface for privileged users to check-out and return passwords. It also enables broader privilege account support for applications (such as SAP System), databases (such as Oracle DBMS), and cloud services (such as Azure, AWS, and Salesforce.com).

With the industry’s only GUI-based, drag-and-drop interface, Privileged Account Manager simplifies the rule-creation process and virtually eliminates the need for complex, manual scripting. An integrated test-suite tool allows you to model and test new rule combinations before committing them to production use.

Using a unique risk-analysis engine, Privileged Account Manager analyzes each command as it is typed and assigns it a risk level from 0 to 9 based on the command executed, the user who executed it, and the location. High-risk commands are color coded as red, and low-risk commands are color coded as green, with varying shades in between for instant identification of events that could pose a security risk. Additionally, you may view any recorded keystroke activity through an intuitive interface with play back functions. If an event requires further analysis, a workflow process escalates the event to the appropriate managers who can take immediate action.

Privileged Account Manager extends this risk-based activity control to deliver automated policy enforcement during privileged user sessions. If a user performs a risky activity, such as accessing restricted data or stopping a service, an administrator may configure Privileged Account Manager to disconnect the session automatically or revoke a user from accessing any privileged accounts.

System Requirements

For a detailed list of platforms that Privileged Account Manager supports, and requirements for installation, please see the Installation Guide here.

Key Benefits

Control and monitor unauthorized and un-monitored privileged user access across your entire heterogeneous environment.

- Centrally manage security policies from a single point.
- Continuously support compliance with internal policies and external regulations.
- Virtually eliminate the need for complex manual scripting.
- Enforce a consistent policy throughout your environment via centralized management.
- Enable access enforcement, analysis and reporting to comply with privacy laws and regulations.
- Integration with ArcSight Intelligence provides risk-aware services that considers risk associated with the activity when elevating an identities privileges.
- Instantaneous real-time monitoring of privileged sessions

Key Features

Design, configure, test and deploy a privileged account management solution across your entire environment from a single location.

- Enterprise Credential Vault for secured password vaulting
- Database privileged account monitoring for users, tools, and applications
- Risk-based session control to enable automatic session termination or access revocation
- Remote session establishment and control for operating systems
- Risk profiling that quickly identities high-risk users
- Smart risk ratings built on potential threat analysis
- Deployment flexibility with both agent-based and agentless support for Windows and Linux.

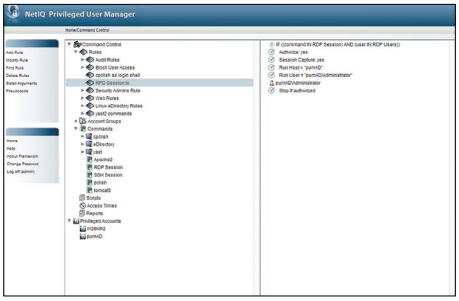

Figure 1. The Command Control Console enables administrators protect and control user commands.

Key Differentiators

Build the most comprehensive audit trail available. With Privileged Account Manager, you have the ability to audit all user activity with 100-percent keystroke logging and video capture for all credential-based environments, including applications such as SAP System, databases such as Oracle DBMS, and cloud services such as Azure, AWS and SalesForce.com.

For specific access events, auditors may play back the entire event at a keystroke level—with color-coded, line-by-line detail—and apply a status of “authorized” or “unauthorized” to each event.

To learn more about Privileged Account Manager, go here.

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes

A Micro Focus line of business