NetIQ

Product Flyer

Privileged Account Manager

NetIQ Privileged Account Manager: Secure Access from within Your Organization and to the Cloud

Experts estimate that as many as half of all security breaches occur as the result of insider activity. Insider threats are especially serious when associated with employees who have higher access privileges than needed. Whether the privilege misuse occurs due to employee error or is the work of a cyber-criminal who has leveraged the 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.

- **Solultion:**
  Access Management
- **Product:**
  NetIQ Privileged Account Manager

With NetIQ Privileged Account Manager, your organization can control and monitor privileged access and activity across physical and virtual environments.

Product Overview

NetIQ® Privileged Account Manager 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. You also eliminate the need to distribute root-account credentials to your entire administrative staff.

NetIQ Privileged Account Manager features an Enterprise Credential Vault, or an encrypted password "vault," that provides secure storage of your system, application, database and shared key credentials. 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 Microsoft SQL and Oracle DBMS), cloud services (such as Salesforce.com) and virtual servers.

To deliver an additional layer of data protection, NetIQ Privileged Account Manager integrates with advanced authentication solutions to support two factor authentication and step-up authentication while accessing critical resources and servers. When combined with solutions such as NetIQ Advanced Authentication, privileged users can be prompted for additional authentication credentials before being given privileged access to sensitive systems, databases, and applications.

NetIQ Privileged Account Manager also delivers improved security and reduced administrative overhead through single sign-on (SSO) capabilities. Authorized users can single sign-on to a Linux or UNIX server with elevated privileges directly from an intuitive user console. The GUI-based, drag-and-drop user interface also greatly simplifies the rule-creation process and virtually eliminates the need for complex, manual scripting.

Privileged Account Manager provides risk-based activity control using a unique risk-analysis engine that analyzes each user 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. If a user performs a risky activity, such as accessing restricted data, an administrator can configure Privileged Account Manager to disconnect the session automatically or revoke a user from accessing any privileged accounts.

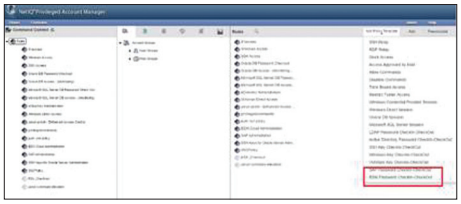

Figure 1. Enable password check-out for hypervisors easily by using out-of-box policy templates.

Capabilities

Reduce your risk of breach and audit failure by securing and controlling access to sensitive resources and assets.

- Control which commands can be run under elevated privileges, or restrict commands that can be executed.
- Provide secure access with step-up and multi-factor authentication.
- Use password vaulting to associate privileged user identity with activity.
- Monitor all privileged user access and activity using a policy-based approach.
- Centrally enforce consistent policy throughout physical and virtual environments.
- Enable access enforcement, analysis and reporting to comply with privacy laws and regulations.

Features

Design, configure, test and deploy a privileged account management solution from a single location.

- Broad authentication factor support includes one-time password (OTP), smartphone, SMS and more
- Granular control on when additional authentication must be invoked
- Enterprise Credential Vault for secure password vaulting
- Database privileged account monitoring and password checkout
- Secure privileged access to virtual servers (VMware ESXi)
- Risk-based session control to enable automatic session termination or access revocation
- Single Sign-On (SSO) to Linux and UNIX servers
- Integrated test-suite tool examines rules prior to production use
- Risk engine color-codes large amounts of event data to quickly detect policy violations
- Keystroke recording and playback of all privileged user session activity

Key Differentiators

Build the most comprehensive audit trail available and spot threats faster with NetIQ Privileged Account Manager. Audit all user activity with 100-percent keystroke logging and video capture across all credential-based physical and virtual environments. Video records are indexed, highly searchable and augmented with color-coded risk ratings.

Auditors can play back a specific event at a keystroke level—with color-coded, line-by-line detail—and apply a status of “authorized” or “unauthorized” to each event.

Color-coded risk reporting is highly customizable, enabling security teams to define and rapidly identify risky activity that could represent a threat. Additionally, you can configure Privileged Account Manager to provide automated policy enforcement, authorizing the solution to automatically terminate a session or revoke access in real time if risky or unauthorized activity is detected.

To learn more about NetIQ Privileged Account Manager, or to start a trial, go to: **www.netiq.com/pam**

www.netiq.com

Worldwide Headquarters
515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
+1 713 548 1700
888 323 6768
info@netiq.com
www.netiq.com
www.netiq.com/communities/

For a complete list of our offices
in North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit: www.netiq.com/contacts