NetIQ Privileged User Manager

Secure Your Server Infrastructure with Actionable Risk Management

With NetIQ Privileged User Manager, your organization can monitor and manage superuser access across its heterogeneous network.

You are responsible for securing your organization's data and your biggest security threat may be sitting down the hall. Experts estimate that as many as half of all security breaches come from inside organizations. Because organizations often grant employees and IT administrators higher access privileges than they need, you can manage this risk by closely managing superuser access.

Product Overview

NetIQ® Privileged User Manager eliminates the need to distribute UNIX, Linux and Windows 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. NetIQ Privileged User Manager records user activity down to the keystroke and displays this information in an intuitive interface with color-coded risk ratings that alert you to take action when suspicious activity occurs.

With the industry's only GUI-based, drag-and-drop interface, NetIQ Privileged User 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. You can simply drag rules into nested hierarchies to build sophisticated control structures that provide granular control for even the most demanding environment.

The unique NetIQ Privileged User Manager risk-profiling capability enables you to quickly and easily identify high-risk user inputs, allowing you to mitigate potential damage from malicious activity or accidental misuse. You can play back any part of a recorded session through an intuitive DVR-like interface that streams UNIX and Linux sessions, plays second-by-second snapshots of Windows sessions or allows line-by-line analysis. In addition, you can search and select activities according to multiple criteria.

Capabilities

Control unauthorized and unmonitored superuser 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.
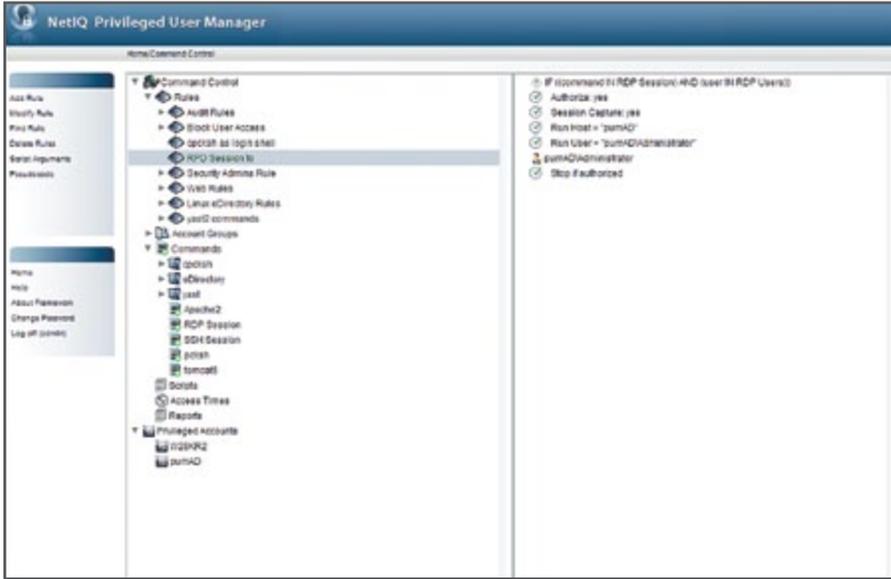
NetIQ®

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

Key Differentiators

Build the most comprehensive audit trail available. With NetIQ Privileged User Manager you have the ability to audit all user activity with 100-percent keystroke logging and video capture for Windows environments. It records every keystroke that users type while they're authenticated to Unix, Linux and Windows servers.

For specific access events, auditors can 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 NetIQ Privileged User Manager, or to start a trial, go to **www.netiq.com/pum**.

Features

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

- Smart risk ratings built on potential threat analysis

- Comprehensive audit capabilities for complete compliance management and forensic analysis

- Integrated rules testing that verifies consistency across UNIX, Linux and Windows servers

- Risk profiling that quickly identities high-risk users

- Keystroke logging that lets you audit all user activity

- Robust and scalable architecture with built-in redundancy to provide 100-percent availability