OpenText NetIQ Privileged Access Manager

Control and monitor privileged user access across databases, applications, and the cloud

Benefits

- Mitigates the risks associated with privilege abuse
- Simplifies administration, enhancing security and operational efficiency
- Enables quick responses to suspicious activities
- Aligns with your current infrastructure while supporting growth

Managing privileged access is one of the biggest challenges organizations face, as it often leads to security vulnerabilities, insider threats, and compliance risks. Without proper control over who can access critical systems and data, IT departments and security teams in industries such as finance, healthcare, and government are at high risk of breaches.

OpenText™ NetIQ™ Privileged Access Manager (NetIQ PAM) helps organizations enforce strict access controls, mitigate risk, and meet regulatory requirements efficiently. It provides comprehensive tools to monitor, manage, and audit privileged user activity, ensuring visibility into who accesses critical systems and when. By automating policy enforcement and streamlining compliance reporting, it helps organizations reduce administrative overhead, minimize security risks, and ensure adherence to regulatory requirements with ease.

Comprehensive privilege management

NetIQ PAM offers robust privilege management that centralizes and secures privileged accounts across your organization. With a unified platform for managing privileged access, including advanced controls for monitoring and auditing activities, OpenText NetIQ PAM mitigates the risks associated with privilege abuse and simplifies administration, enhancing overall security and operational efficiency.

Cybersecurity journey drastically reduces workload, improves user productivity, and enhances security.

Read the success story ›

Associated services options available

- Consulting Services
- Learning Services

Enhanced security and compliance

Benefit from advanced security features designed to protect sensitive information and ensure compliance with regulatory requirements. NetIQ PAM includes real-time threat detection, automated alerting, and detailed audit trails, providing visibility into privileged account activities. These features support regulatory compliance and enhance your security posture by enabling quick responses to suspicious activities and offering comprehensive reporting capabilities.

Streamlined access controls

NetIQ PAM's sophisticated access control mechanisms streamline the management of privileged access. Granular policy definitions ensure access is granted based on roles, contexts, and risk levels. This precise control minimizes the potential for unauthorized access and reduces the complexity of managing access permissions across diverse systems, maintaining a secure and compliant IT environment.

Automated privilege management

Automation is a key strength of NetIQ PAM, designed to reduce the administrative workload associated with privileged access management. Critical tasks such as provisioning, de-provisioning, and credential rotation are automated, enhancing operational efficiency and ensuring consistent application of privilege changes, reducing the risk of errors and improving overall management accuracy.

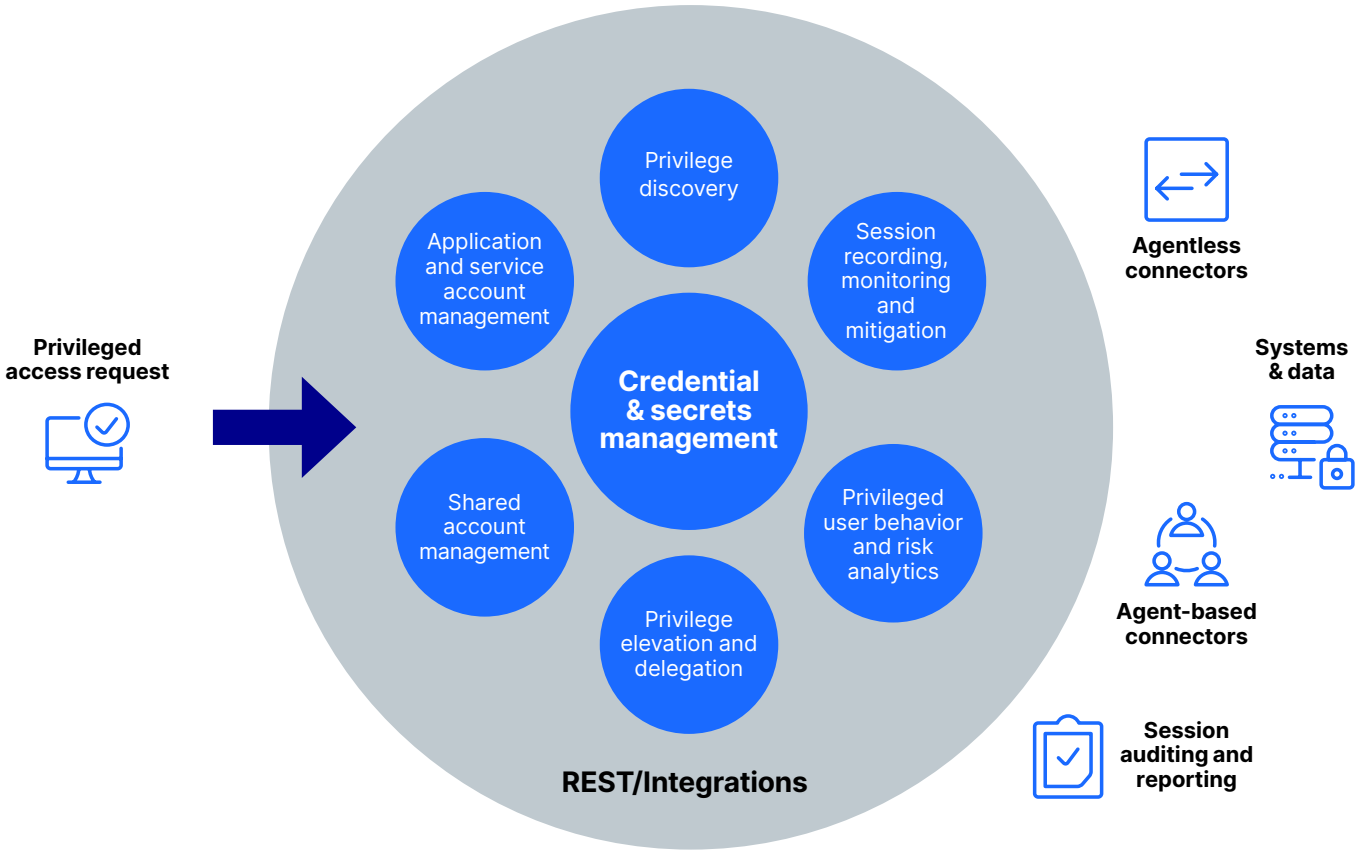
Scalable and flexible architecture

Built to accommodate the growing and changing needs of your organization, NetIQ PAM's scalable architecture supports both small and large deployments. It integrates seamlessly with existing IT systems, offering the flexibility to align with your current infrastructure while supporting future growth.

User-friendly interface

Enhanced with an intuitive, user-friendly interface, NetIQ PAM simplifies the administration of privileged accounts. The design focuses on ease of use, enabling administrators to quickly configure settings, monitor activities, and generate reports. This user-friendly approach reduces the learning curve for new users and enhances the efficiency of privilege management tasks.

NetIQ PAM stands out with its holistic approach to privileged access management, integrating robust security features, advanced automation, and a user-friendly design into a scalable platform. It simplifies access management by automating the identification of elevated rights, enhances security and compliance with dynamic access controls and real-time policies, and provides efficient monitoring to swiftly address potential threats, reducing risk and streamlining operations.



Resources

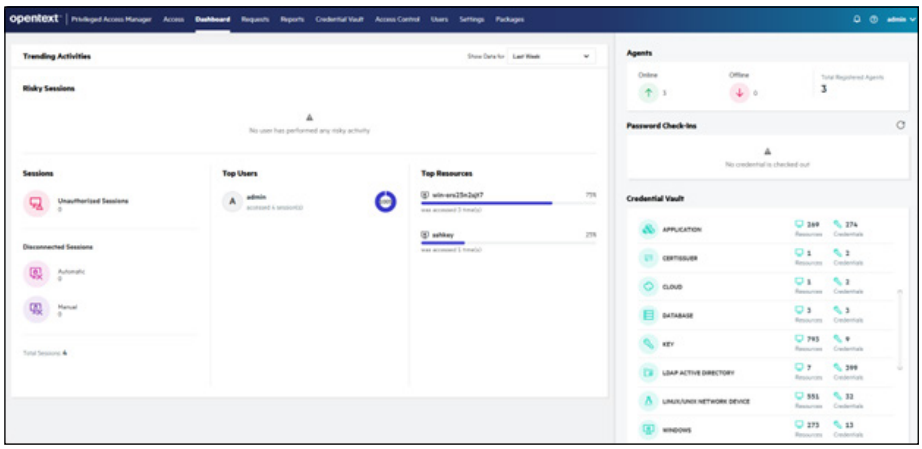
Understanding just-in-time access: The basics of privileged access management
Read the blog ›

Why is privileged access management important?
Read the blog ›

Staying secure in a cloudy world
Read the white paper ›

Learn about privileged access management
Read the What Is Privileged Access Management webpage ›

Product features	Description
Enterprise credential vault	Securely vault passwords for enterprise-level credentials, with monitoring for database privileged accounts across users, tools, and applications.
Single console	Manage privileged credentials for users, apps, and databases. Enable credential checkout, session recording, and keystroke logging for verification.
Risk-based intelligence and session control	Use real-time risk analysis to assess privileged activity and automatically terminate sessions or revoke access based on risk, ensuring swift enforcement and reporting.
Remote session management	Establish and control remote sessions for operating systems with full oversight.
Flexible deployment	Supports both agent-based and agentless deployments for Windows® and Linux® environments.
Privileged account discovery and onboarding	Automatically discover and onboard privileged accounts to streamline management.
Just-in-time (JIT) access	Grant real-time, temporary elevated privileges to users, ensuring secure, time-limited access to critical resources. Enforce least privilege by granting only the minimal permissions needed for a task.



opentext™