Protect Servers with Privilege Controls

Enforce least privilege principles by centralizing authorization controls across identities

Privileged accounts with administrative rights are a major target for cyber criminals. These accounts have elevated permissions and access to confidential information and can modify system configurations. Because these accounts often have excessive privileges that never expire, they create opportunities for significant damage if compromised.

To protect access to servers, organizations need visibility and consistent oversight of all privileged accounts and the identities that access them. Discovering and eliminating excessive and unnecessary privileges allows organizations to support zero trust and least privilege best practices that reduce the risk of a breach. Ongoing monitoring of privileged activities is critical for mitigating cyber incident risk and meeting compliance requirements.

Privilege Control for Servers in the Delinea Platform increases security and streamlines operations for organizations with Windows, Unix, and Linux systems in a hybrid cloud environment. It builds on an enterprise vault by layering security directly on servers.

HOW IT WORKS

Identity Consolidation and elimination of local accounts

Leverage centralized enterprise identities for the administration of Windows, Unix, or Linux infrastructure with precise policies that determine the scope of privileged activities that can be performed.

Zero Standing Privileges

Grant administrative rights and privileges at the start and eliminate them at the end of each administrative session, providing just-in-time (JIT) and just enough privilege (JEP).

Prevent Lateral Movement

Enforce MFA on direct system access to validate identities, discover and contain threat actors, and eliminate lateral movement. Layer MFA on privileged commands provides peace of mind that activities are performed by the intended administrator.

Auditing and Monitoring

Record all sessions directly on the host system so you have full visibility into all privileged activities tied to an individual user. Because users can't bypass security controls, you can confidently prove compliance.

Privilege Control for Servers Benefits

DECREASE RISK
Remove unnecessary privileges on servers, enforce MFA, eliminate lateral movement, and improve visibility to reduce your attack surface.

INCREASE EFFICIENCY
Consolidate identities and easily apply privilege controls on servers with simplified tools.

CENTRALIZE MANAGEMENT
Manage all privileged access from login through privilege elevation across all servers with the ability to enforce MFA from all major identity providers.

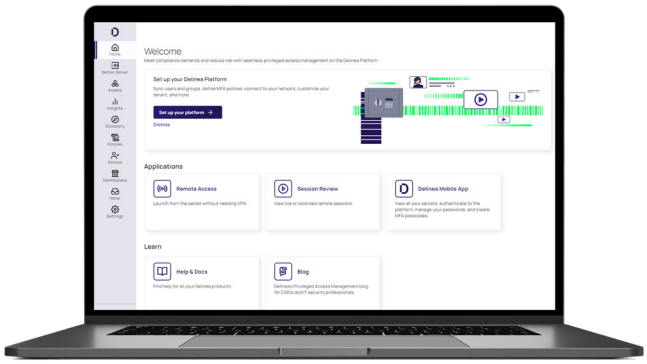
SEAMLESS SCALABILITY
Manage PAM controls through an intuitive interface as your IT infrastructure evolves and privileged identities increase.

REALIZE FAST ROI
Save time with out-of-the-box templates, verified integrations, and cloud-native infrastructure.

Privilege Control for Servers is delivered on the Delinea Platform for centralized administration

Unify privilege management for all identity types so your team can work more efficiently to optimize productivity. Strengthen security and reduce the risk of a breach with privileged session monitoring and centralized policy administration.

Removing excessive or unnecessary privileges for users accessing servers allows organizations to support zero trust and least privilege best practices that reduce the risk of a cybersecurity breach. Ongoing monitoring of privileged activities on servers is critical for lowering the risk of a cyber incident and lateral movement.



OBSERVE: Audit and Monitor

Identify abuse of privilege, thwart attacks, and easily prove regulatory compliance with a detailed host-based audit trail and video recordings that capture all privileged activity on servers tied to unique identities.

CONTROL: Privilege Elevation

Manage privileges consistently across all server types continuously through a single intuitive interface. Elevate privileges as needed with governance workflows and flexible, granular rules and MFA.

ADAPT: Authenticate

Accommodate all major identity providers such as Active Directory, Open LDAP, and cloud directories such as Azure AD, Okta, and Ping. Secure access to Linux, Unix, and Windows virtual systems and containers. Enforce MFA for stronger identity assurance.

An edition designed for every type of organization

The flexibility, and agility to scale PAM security controls on your own terms

DELINEA PLATFORM
Essentials

Get started by discovering privileged accounts, vaulting and requesting access to secrets, and managing and auditing sessions.

DELINEA PLATFORM
Standard

Continue your PAM journey with Privilege Control for Servers by managing remote access, enhancing discovery, implementing MFA enforcement, and granting just enough privilege on endpoints.

DELINEA PLATFORM
Enterprise

Extend PAM across your enterprise by governing service and cloud accounts, implementing adaptive MFA enforcement and analytics, and situational just-in-time privilege.

Learn more about the Delinea Platform at Delinea.com

Delinea

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**