



Privileged Access Management for On-Premise Infrastructure

Protect Your Servers Against Identity-Based Attacks

Digital transformation leads to fragmented identities across a hybrid enterprise infrastructure. A modern privileged access management (PAM) solution takes an identity-centric approach to protect your organization against new and evolving threats. Server Suite allows humans and machines to authenticate to on-premise infrastructure, enforcing least privilege with just-in-time privilege elevation, increasing accountability, and reducing risk.

✓ Easy to Deploy, Fully Integrated, Low Complexity Solution

- Centralized solution for enterprises with heterogeneous infrastructures

✓ Identity Consolidation with Advanced Active Directory (AD) Bridging

- Best-in-class, advanced AD bridging for complex architectures

✓ Just-in-Time (JIT) Privilege Elevation

- Flexible, fine-grained privilege elevation for zero standing privileges

✓ Identity Assurance Everywhere

- Multi-factor authentication (MFA) at system login and privilege elevation

✓ Full Visibility and Control of Privileged Activities

- Cross-platform auditing, session recording, and policy enforcement on the host
- Readily customizable means no need to spend extra time or money

Server Suite Benefits



ENHANCE SECURITY

Enforce zero standing privileges and reduce lateral movement



STREAMLINE POLICY MANAGEMENT

Centralize PAM policy management and enforce PAM policy on each server



IMPROVE PRODUCTIVITY

Protect your servers with MFA and JIT policy and controls



CENTRALIZE CONTROL

Centrally manage machine identities and their credentials within Active Directory



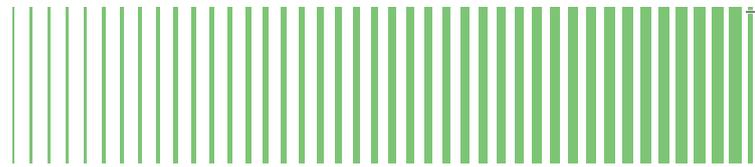
COMPLIANCE & INCIDENT INVESTIGATION

Advanced host-based session recording, auditing, and reporting



MITIGATE RISK

Achieve a stronger risk posture, lower costs, improve security, and reduce IT overhead



Minimize your attack surface and control privileged access

Server Suite minimizes the attack surface through advanced PAM capabilities such as identity consolidation, real-time password reconciliation, delegated machine credentials, brokered authentication, and just-in-time privilege with MFA, while auditing everything.

✔ Authentication Service

Extend Active Directory (AD) benefits to on-premise Linux and Unix servers by natively joining them to AD, turning the host system into an AD client. Secure access consistently, using the same authentication and Group Policy services deployed for Windows systems.

- Active Directory bridging
- Machine identity and credential management
- Brokered authentication
- MFA at system login
- Approval workflows for login
- Unified policy management

✔ Privilege Elevation Service

Control privilege elevation on on-premise Windows, Linux, and Unix servers. Instead of standing privileges, self-service workflows allow administrators to request temporary roles to complete legitimate tasks with just-in-time access.

- Approval workflows for privilege elevation
- Patented "Zones" technology for RBAC policy
- Delegated machine credentials

✔ Audit and Monitoring

Get a holistic view of all privileged activity across on-premise Windows, Linux, and Unix servers. Associate unique identities with all privileged activity to increase accountability. Leverage out-of-box reports for regulatory compliance and incident response investigations.

- Host-based audit and monitoring
- Gateway-based audit and monitoring
- Linux and Unix advanced monitoring at the shell and process levels

[Learn more at Delinea.com](https://delinea.com)



Delinea

Delinea is a leading provider of privileged access management (PAM) solutions that make security seamless for the modern, hybrid enterprise. Our solutions empower organizations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide, including over half of the Fortune 100. delinea.com