Delinea

SERVER PAM

Enforce Principles of Least Privilege on Servers

Protect servers with seamless policy-based authorization controls and MFA at Depth

Digital transformation continues to disrupt organizations' with increasing complexity and fragmented identities across environments. It is critical to simplify and protect privileged access to servers with identity consolidation and centralized management of privileges across Windows, Linux, and Unix servers.

Delinea seamlessly and granularly controls privileged access to servers with just-in-time and just enough privilege elevation and provides identity assurance with layered MFA enforcement to prevent lateral movement while increasing accountability.

Enforce least privilege consistently

- Centrally manage privileged access and MFA enforcement policies in Active Directory (AD) (patented zones) or from most cloud identity providers. Single enterprise identity for user login.

Minimize risk with best practices

- Align with regulations and zero trust and least privilege best practices to protect against threats like ransomware and data breach attacks.

Elevate privileges granularly

- Apply policies at the host level for fine-grained control of privilege elevation. Implement self-service workflows for automating just-in-time access requests.

Enforce adaptive MFA

- MFA policies enforced at login and privilege elevation across Windows, Linux, and Unix for stronger identity assurance and cyber insurance demands.

More easily meet compliance requirements

- Forensic-level audit trails and session recordings for security review, incident response, compliance, and full accountability.

Server PAM Benefits

ENHANCE SECURITY & MITIGATE RISK

Centrally administer just-in-time (JIT) and just-enough (JEP) privileges and provide identity assurance with multi-factor authentication (MFA) enforcement at system login and at privilege elevation to prevent lateral movement and align with least privilege and zero trust best practices.

CONSOLIDATE IDENTITIES & IMPROVE PRODUCTIVITY

Eliminate the large number of unmanaged local accounts and use enterprise directory accounts to access Windows, Linux, or Unix on-premise or in the cloud to limit identity sprawl and simplify workflows.

MORE EASILY AUDIT PRIVILEGED ACTIVITIES

Leverage granular, host-based auditing and session recordings to identify potentially harmful privileged activities and demonstrate controls for compliance with unaltered audit data.

Control privileged access to servers, on-premise and in the cloud

Delinea protects privileged access to servers with identity consolidation and centralized management of just-in-time and just-enough privileges. Multi-directory brokering simplifies administrator authentication and consolidates identities, establishing trust between disparate identity providers and Windows and Linux instances across hybrid IT environments. MFA enforcement at server login and privilege elevation adds additional identity assurance for access to sensitive systems. Real-time session monitoring and recording on each server ensure complete visibility and actionable event details.

Authentication

Simplify user authentication to servers from any directory service, including Active Directory, Open LDAP, and cloud directories such as Azure AD, Okta, or Ping. Secure access to Linux, Unix, and Windows virtual systems and containers. Enforce MFA for stronger identity assurance.

- Multi-directory brokering
- Machine identity, delegated machine credentials, and credential management
- Authentication policy management
- MFA at system login
- Centrally manage the lifecycle of local accounts and groups

Privilege Elevation

Enforce the principle of least privilege across Windows, Linux, and UNIX infrastructure on-premise, in the cloud, and multiple clouds. Reduce standing privilege and prevent lateral movement to minimize the risk of a data breach or ransomware attack. Administrators can request just-in-time privilege elevation for a limited time.

- Consistent and automated security policy management
- Privilege elevation for least privilege enforcement
- Just-in-time privilege elevation workflow
- MFA at privilege elevation

Audit and Monitoring

Identify abuse of privilege, thwart attacks, and easily prove regulatory compliance with a detailed audit trail and video recordings that capture all privileged activity.

- Granular host-level event logging and auditing
- Searchable recordings for visual analysis
- Holistic view of privileged activity across Windows and Linux servers, IaaS, and databases
- Reports on every user's privileges and associated activity for compliance

Cloud Native

Delivery through the cloud-native Delinea Platform enables unified administration, driving fast time to value and lower total cost of ownership with comprehensive governance of privilege.

- Continuous discovery seamlessly identifies privileged accounts and identities across your network
- MFA at Depth provides identity assurance
- Audit privileged activity across privileged accounts and identities to increase accountability
- AI-driven analytics quickly identifies potentially dangerous privileged user activities
- Marketplace simplifies integrations with existing IT and security solutions

Learn more 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**