Delinea

SERVER PAM

Server Privileged Access Management (PAM) for Least Privilege

Protect your servers against identity-based attacks

Digital transformation continues to disrupt the enterprise environment, increasing complexity and fragmenting identities. A modern Privileged Access Management (PAM) solution founded on the best practices of least privilege and Zero Trust is essential to protect your servers against new and evolving identity-based threats.

Server PAM facilitates large-scale digital transformation, modernizing how organizations secure privileged access to servers both on-premise and in the cloud. It allows humans and machines to seamlessly authenticate, enforcing least privilege with just-in-time privilege elevation, increasing visibility and accountability, while reducing administrative access risk.

✓ Centralized Identity and policy management

- Choose what's best for you. Manage privileged access, and MFA policies in Active Directory Patented Zone Technology consolidates complex and disparate non-Windows identities into Active Directory for greater security and centralized management.

✓ Identity consolidation with advanced Active Directory(AD) bridging

- Server PAM extends Active Directory policy and authentication benefits to Linux and UNIX, giving admins a single, accountable ID to log in cross-platform. Unify your IT infrastructure by consolidating identities, authentication, and access management for Linux and UNIX within AD.

✓ Multi-directory brokering

- Broker authentication to Active Directory, OpenLDAP, and cloud directories such as Azure AD, Okta, and Ping, without requiring direct connections from Linux or Windows Servers.

✓ Cloud-Native

- Capitalize on the cloud with a modern PAM solution purpose-built for hybrid cloud IT infrastructures. Don't be fooled by lift and shift.

✓ Multi-Factor Authentication (MFA) enforcement

- Block malware and ransomware and stop lateral movement by enforcing MFA at system login and privileged application and command elevation.

✓ Host-based auditing, reporting, and session recording

- Easily detect rogue activity used to circumvent security controls and attribute activity to users. Log all privileged session activity in forensic detail for security audit, corrective action, and compliance reporting.

Server PAM Benefits

ENHANCE SECURITY & MITIGATE RISK

Enforce just-in-time (JIT) least privilege access with multi-factor authentication (MFA) enforcement at system login and privilege elevation to prevent lateral movement and align with least privilege and Zero Trust best practices. Achieve a more robust posture, reduce costs and IT overhead, while improving efficiency.

CONSOLIDATE IDENTITIES & IMPROVE PRODUCTIVITY

Give administrators one account to access Windows, Linux or Unix on-premise or in the cloud by eliminating local privilege accounts to reduce the attack surface. Resulting identity centralization allows for consistent centralized authentication and authorization policies for privileged access to improve productivity.

MEET COMPLIANCE MANDATES & INCIDENT INVESTIGATION

Leverage granular, host-based auditing and session recording to prove compliance and to aid investigation of incidents across on-premise and cloud provider instances.

Control privileged access on-premise and in the cloud

Server PAM empowers organizations to take control of privileged access through centrally managed policies consistently enforced on servers. 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, OpenLDAP, 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

Learn more at Delinea.com

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**