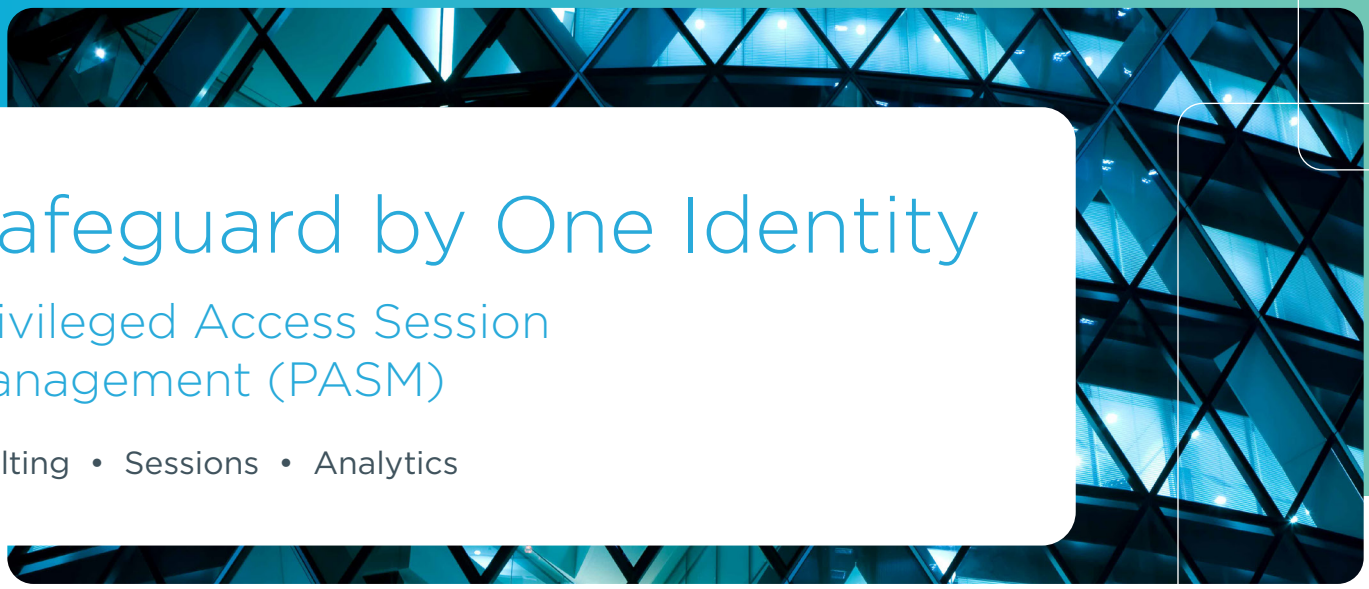
ONE IDENTITY



Safeguard by One Identity

Privileged Access Session Management (PASM)

Vaulting • Sessions • Analytics

Secure, control, monitor, analyze and govern privileged access for every identity. Safeguard is available as SaaS, on-prem or hybrid, and flexible enough to grant full credentials when needed or enforce least privilege for human and non-human identities, across every environment.

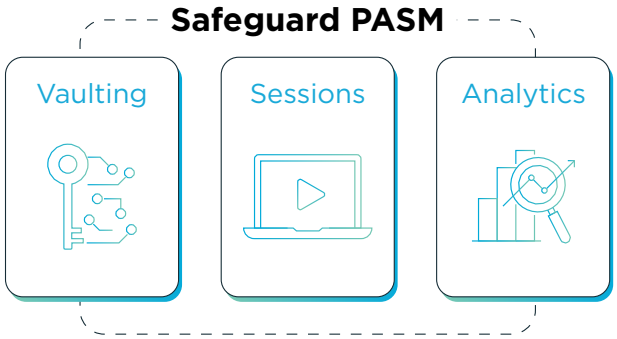
Overview

Privileged accounts are the primary target in nearly every major breach. Safeguard is a fully integrated PASM platform uniting three capabilities: a hardened password safe, a proxy-based session recording engine, and a machine-learning analytics layer, giving complete visibility, control and auditability over every privileged interaction.

One integrated solution. Sessions feed Analytics for behavioral modeling; Passwords inject credentials into sessions so they're never exposed; Analytics findings terminate risky sessions in real time.

Key Business Outcomes

- **Reduce breach risk** by eliminating uncontrolled privileged access
- **Prove compliance** with tamper-proof, signed session records
- **Realize fast ROI** with appliance-based deployment; recording in days
- **Detect insider threats** and hijacked accounts via behavioral analytics
- **Simplify administration** with a low-learning-curve, user-centered design



Safeguard PASM Core Capabilities

PAM in one solution: vaulting, sessions, analytics.

Vaulting: Privileged Passwords

Automates and secures privileged credential release through role-based workflows, reducing administrative burden.

- Policy-based release control: auto or multi-party approval by identity, time and resource, with ticketing integration
- Privileged account discovery: surface accounts and systems via host, directory, network discovery
- Change control: time-, use-based, manual or forced rotation for shared credentials
- Multifactor authentication: RADIUS 2FA, SAML 2.0 SSO, and built-in TOTP delivered at checkout
- Personal password vault: free employee vault for non-federated accounts, eliminating shadow IT
- RESTful API: every function exposed for any ITSM, SIEM or automation stack

Sessions: Privileged Session Management

A protocol-aware proxy gateway that controls, records and inspects every privileged session, rejecting anything that violates protocol before it reaches a target.

- Audit, recording & replay: keystroke-level capture in encrypted, signed trails; replay like video, search like a database
- Real-time alerting & blocking: log, alert or terminate on risky commands or screen patterns, with four-eyes override
- Two deployment modes: full workflow engine, or transparent Instant On proxy with zero workflow change
- Wide protocol support: agentless SSH, Telnet, RDP, HTTP(S),and VNC with granular service control
- Command & application control: allow- or deny-list commands and window titles without changing admin tools
- Full-text search with OCR: search command-line and graphical sessions; extract transferred files for forensics
- Auto-login (password injection): log in without ever exposing the credential to the user

Analytics: Privileged Analytics

Machine-learning behavioral analytics applied to session data, surfacing threats that rules-based tools miss.

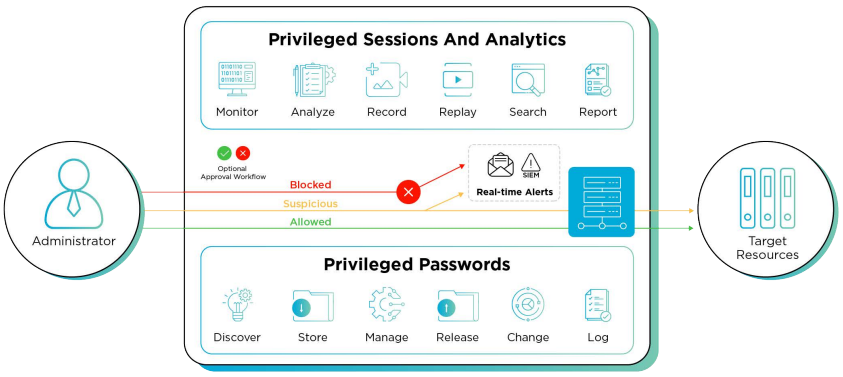
- Baseline behavioral modeling: ML learns each user's "normal" with no correlation rules required
- Behavioral biometrics: keystroke and mouse patterns give continuous, passive identity verification
- Risk-based alert prioritization: ranks events by risk to cut SIEM noise and focus analysts
- Real-time threat detection: catches external and insider activity rules-based systems miss
- Automated response: terminates sessions during reconnaissance, before damage is done

Technical Specifications

- **SESSION PROTOCOLS**
  - SSH, Telnet, RDP
  - HTTP(S), VNC
  - Agentless, no target agent
- **AUTHENTICATION**
  - RADIUS-based 2FA
  - SAML 2.0 Web SSO (federated IdP)
  - Built-in TOTP authenticator
  - Smartcard / strong auth gateway
- **DEPLOYMENT**
  - SaaS (Safeguard On Demand)
  - Self-managed on-prem
  - Hybrid
  - Hardened virtual / physical appliance
- **INTEGRATION**
  - Full REST API
  - ITSM & ticketing systems
  - SIEM
- **COMPLIANCE**
  - ISO/IEC 27001 certified cloud
  - Encrypted, signed audit trails

ONE IDENTITY

Safeguard PASM | Vaulting, Sessions, Analytics



EXTEND SAFEGUARD PASM

Safeguard Remote PAM (RPAM)

Cloud-native secure remote access for privileged users, without VPN or client software. All connection logistics handled in the cloud and controlled by Safeguard.

Safeguard Workforce Password Manager (WPM)

Enterprise password vault for workforce credentials that reduces shadow IT and password-reuse risk across the organization.

Safeguard PEDM: Privilege Elevation & Delegation Management

Extend least-privilege enforcement beyond the vault to Windows, UNIX and Linux endpoints and servers.

Privilege Manager for Windows

PMW

Enforce least privilege on Windows with granular application control and self-service elevation rules, integrated natively with Active Directory and Group Policy.

Safeguard for Sudo

SUDO

Centralize sudoer policy management across UNIX and Linux with full keystroke logging and access reporting, making open-source sudo enterprise-ready and compliant.

Authentication Services

AD BRIDGE (FORMERLY SAS)

Bridge UNIX, Linux and macOS to Active Directory so users authenticate with a single AD identity, extending AD security and compliance across the enterprise.

Privilege Manager for UNIX

UNIX

Delegate root access granularly with centralized policy control and reporting, protecting systems from the risk and abuse of unrestricted root.

"One Identity Safeguard provides outstanding privileged access control, helping us monitor privileged activities and secure administrative accounts."

R&D Manager, Manufacturing

Gartner Peer Insights™

Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

ONE IDENTITY