Safeguard Privilege Elevation and Delegation Management (PEDM) by One Identity

Remove standing privileges and root rights across every endpoint and server

Full privileged access control with Safeguard by One Identity

Most privileged access controls stop at the vault. Standing local administrator and root rights on the host account for the largest part of the attack surface.

Safeguard Privilege Elevation and Delegation Management (PEDM) by One Identity extends least-privilege to the endpoint and server layers. It covers Windows, UNIX, Linux and macOS with one goal: Replacing always-on privilege with policy-based, audited elevation.

Safeguard PEDM runs alongside Safeguard Privileged Access and Session Management (PASM) by One Identity. Together, they give one team control over both privileged access and privileged rights for human and non-human identities (NHIs), from the vault to the endpoint.

Safeguard Privilege Elevation and **Delegation Management** (PEDM) by One Identity extends least-privilege to the endpoint and server layers.

Key business outcomes:

- Shrink the attack surface by removing standing local administrator and root rights.
- Utilize just-in-time with policy-based rules instead of permanent privilege.
- Prove compliance with keystroke-level logs, session records and access reporting.
- Reduce helpdesk load through self-service elevation with no user retraining.
- Consolidate identity across Windows, UNIX, Linux and macOS under AD and Entra ID.

One approach to least privilege across all systems

Safeguard PEDM for Windows lets users elevate and manage their own rights while the environment stays compliant with least privilege. It ships with prepackaged and community elevation rules for common needs. Validation Logic targets each rule to the right users, groups, platforms and applications. It integrates natively with Active Directory (AD) and Group Policy Objects.

- **Elevation on demand:** Utilize instant, self-service, requested, temporary session and no-elevation options for end-user administrative access.
- **Validation Logic targeting:** Apply rights by user, group, computer, OU, operating system, office or application.

- **Digital certificate verification:** Elevate every application signed by a trusted publisher automatically.
- **Discovery and remediation:** Find applications that require administrative rights and apply predefined elevation rules.
- **Reporting:** Report elevation activity, blacklist activity, rule deployment, instant elevation and temporary-session requests.
- **Blacklisting:** Deny access to unwanted or suspect applications.
- **Community Rules Exchange:** Use or extend more than 100 pre-existing rules.

Safeguard for Sudo

Most UNIX and Linux teams already use Sudo to delegate root rights. Sudo is proven but managing it box by box leaves policy inconsistent and activity unaudited.

Safeguard PEDM enhances Sudo 1.8.1 and newer with a central policy server, centralized file, consolidated reporting and keystroke logging. Because it enhances Sudo rather than replacing it, there is no user or administrator retraining and no increase in helpdesk calls.

- **Central Sudo policy:** Enforce one Sudo policy across all UNIX and Linux servers from a central service.
- **Keystroke logging:** Capture and replay every command run through Sudo with search and filtering.
- **Centralized reporting:** Track who changed what and when, with versioning and the ability to revert.
- **Offline policy cache:** Keep service running during a network or server outage.
- **Script compatibility:** Utilize continuous existing scripts with embedded Sudo commands.

Safeguard PASM by One Identity controls how **privileged access** is granted, brokered and recorded through vaulting, sessions and analytics.

How Safeguard PEDM completes PAM

Safeguard PASM by One Identity controls how privileged access is granted, brokered and recorded through vaulting, sessions and analytics. Safeguard PEDM by One Identity controls what privilege exists on the host by removing standing rights and elevating just in time.

Run together, they close the gap between the vault and the endpoint. Credentials are protected and sessions are recorded at the access layer, while removing local administrator and root rights and ensuring policy-driven elevation at the host layer. The result is automated least privilege for every human identity and NHI.

About One Identity

One Identity delivers trusted identity security for enterprises worldwide to protect every identity, human and non-human. With flexible deployment options and subscription terms, from self-managed to fully managed, our solutions plug directly into an organization's identity fabric to strengthen the identity perimeter, reduce breach risk and keep governance and compliance aligned at scale. Headquartered in Cork, Ireland, and trusted by 80 of the Fortune 100, One Identity is a leading provider of integrated identity governance and administration (IGA) and privileged access management (PAM) for identity security without compromise. Learn more at www.oneidentity.com.

© 2026 One Identity LLC ALL RIGHTS RESERVED. One Identity, and the One Identity logo are trademarks and registered trademarks of One Identity LLC in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.oneidentity.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners. Datasheet-SafeguardPEDM-KA-105654

ONE IDENTITY