DATASHEET

One Identity privileged access management

Eliminate the "keys to the kingdom" problem with privileged access management

Benefits

- Enterprisewide control of administrative access
- Improved efficiency, security and compliance
- Simple tracking and auditing for all privileged activities

One Identity identity and access management (IAM) solutions empower you to control administrative access enterprise-wide. One Identity solutions for privileged access management improve efficiency while enhancing security and compliance; administrators are granted only the rights they need—nothing more, nothing less— and all activity is tracked and audited.

Specifically, One Identity solutions include granular, policy-based delegation for superuser credentials; session audit and replay; keystroke logging; and secure and automated workflows for issuing privileged credentials to administrators and in application-to-application and application-to-database scenarios. The One Identity suite of privileged access management solutions includes both network-based and host-based solutions:

ONE IDENTITY

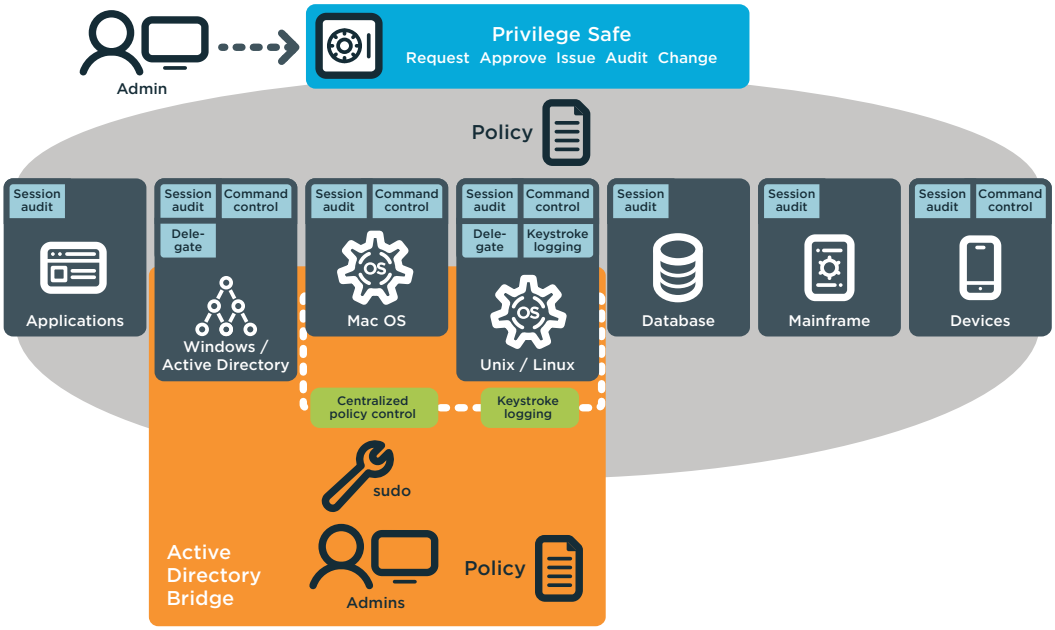
One Identity solutions for privileged access management include granular, policy-based delegation for superuser credentials; session audit and replay; keystroke logging; and secure and automated workflows.

Network-based solutions These powerful solutions provide "privilege safe" functionality, session audit and replay from a single, secure, hardened appliance that maximizes economy, ease of deployment and system coverage.

One Identity Safeguard for Privileged Passwords provides secure storage, release control and change control for privileged passwords for individual accountability across highly diverse deployments of systems, devices and applications. It ensures that when administrators require elevated access (typically through shared credentials such as the UNIX root or Windows Administrator account), that access is granted according to established policy, with appropriate approvals. All actions are fully audited and tracked and the password is changed immediately upon its return. One Identity Safeguard for Privileged Passwords application password management capabilities replace hardcoded application and database passwords with programmatic calls that dynamically retrieve account credentials.

One Identity Safeguard for Privileged Sessions provides session control, proxy, audit, recording and replay of high-risk users such as administrators and remote vendors. It gives you a single point of control from which you can authorize connections, limit access to specific resources, view active connections, record all activity, alert if connections exceed preset time limits and terminate connections.

Host-based solutions These powerful solutions deliver maximum security and control through agents deployed on target systems. For those systems with the heaviest compliance burden, One Identity's host-based options provide the depth, granularity and "forensics-ready" visibility your auditors require.



One Identity solutions enable you to secure, delegate, control and audit access for superuser accounts and shared administrative credentials—across a variety of platforms and systems.

ONE IDENTITY

One Identity solutions empower you to control administrative access enterprise-wide.

Privilege Manager for Sudo helps UNIX/ Linux organizations take privileged access management through sudo to the next level. Its plug-ins enhance sudo 1.8.1 (and newer with a central policy server, centralized management of sudo and the sudoers policy file, centralized reporting on sudoers access rights and activities, as well as keystroke logging of sudo activities. It makes administering sudo across the entire enterprise easy, intuitive and consistent— eliminating box-by-box management. Authentication Services enhances Privilege Manager for UNIX by unifying UNIX/Linux identities into Microsoft® Active Directory®, enabling you to use a common management interface and policy set to control delegation of UNIX root. Authentication Services is the pioneer in the now ubiquitous "Active Directory bridge" space.

All privileged activities can be audited with single-click reports.

Privilege Manager for UNIX protects the full power of root access from potential misuse or abuse. It helps you define a security policy that stipulates who has access to which root functions, as well as when and where individuals can perform those functions. It also controls access to existing programs as well as any purpose-built utilities used for common system administration tasks. In addition, Privilege Manager provides comprehensive auditing of all activities, down to the keystroke level.

Active Roles Server provides granular delegation of the Active Directory Administrator account and central control of administrative access using a single, well-defined set of roles, rules and policy.

Privilege Manager grants user accounts the least privileges necessary according to best practices, yet elevates specific applications and ActiveX controls as needed. You can set elevated execution privileges for just those applications, features and controls you choose. Access rights can be targeted to a specific user, user group, organizational unit, operating system, computer group, office or application. All privileged activities can be audited with single-click reports.

For more information

To learn more about Privileged Access Management visit oneidentity.com/privileged-access-management/

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged access management.

Learn more at OneIdentity.com

DataSheet-PrivilegedAccountMgmt-US-KJ

ONE IDENTITY