# 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
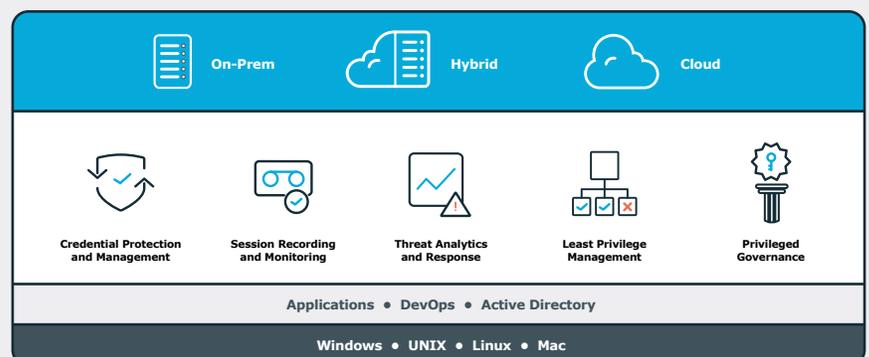- Simple tracking and auditing for all privileged activities

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:

**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. Content of the recorded sessions is indexed to make

One Identity security solutions include comprehensive offerings that address the privileged access management needs of even the most diverse and demanding enterprises.

| On-Prem | Hybrid | Cloud | | |
|---|---|---|---|---|
| Credential Protection and Management | Session Recording and Monitoring | Threat Analytics and Response | Least Privilege Management | Privileged Governance |

Applications ● DevOps ● Active Directory

Windows ● UNIX ● Linux ● Mac

searching for events and automatic reporting simple so you can easily meet your auditing and compliance requirements. In addition, Safeguard for Privileged Sessions serves as a proxy, and inspects the protocol traffic on the application level and can reject any traffic that violates the protocol – thus it is an effective shield against attacks.

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

**One Identity Safeguard for Privileged Analytics** monitors questionable behaviors and uncovers previously unknown threats from inside and outside of your organization. By using user behavior analytics technology, Safeguard for Privileged Analytics detects anomalies and ranks them based on risk so you can prioritize and take appropriate action -- and ultimately prevent data breaches.

**One Identity Safeguard 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.

**One Identity Safeguard Authentication Services** enhances Safeguard for Sudu 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. Safeguard Authentication Services centralizes authentication and provides single sign-on for UNIX/Linux

unifying identities and consolidating directories simplifying management and easing compliance.

**Active Roles** 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 for Windows** 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.

**Identity Manager** integrates with Safeguard to provide Privileged Access Governance (PAG). Account provisioning, lifecycle management and access governance capabilities of Identity Manager can be used while continuing to leverage the privilege account and session management capabilities of Safeguard.  PAG ensures that privilege account users gain and maintain the appropriate level of access to accounts, while periodic attestations ensure the privileged access is regularly attested and assigned correctly.

## For more information

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

## About One Identity

One Identity by Quest, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of the program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com