SOLUTION BRIEF

RSA® IDENTITY GOVERNANCE & LIFECYCLE

UNIFY ACCESS MANAGEMENT FOR PRIVILEGED ACCESS

UNIFY ACCESS MANAGEMENT

Many organizations have historically managed their non-privileged user access with identity access management solutions like RSA® Identity Governance & Lifecycle, and their privileged access with a separate point solution. While privileged access management (PAM) providers do a great job at securing privileged access, utilizing point solutions that aren't connected to identity governance makes it difficult to enforce holistic access policies and consistent provisioning and authorization processes. This can create gaps in management and oversight that might result in access violations, leading to costly security and audit failures.

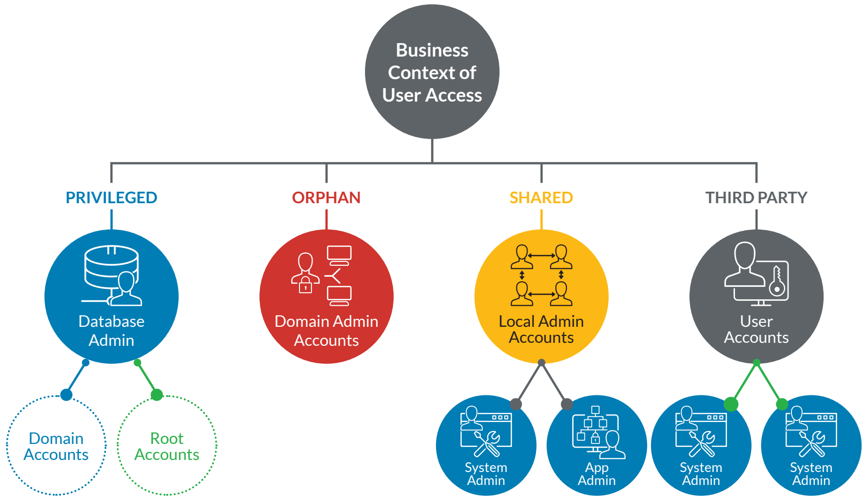

Figure 1: Understanding who has access to critical data and applications is key in taking a holistic approach to access management.

TAKE A CENTRALIZED APPROACH

To address identity risk gaps, instituting a centralized policy-based process for privileged and non-privileged users will provide efficient management of access requests, approvals, provisioning and remediation of out-of-band privilege escalations.

RSA Identity Governance & Lifecycle interoperability with PAM solutions optimizes existing PAM services by combining their strengths with the power of full identity lifecycle management, including risk and business context. This is achieved in two ways:

1. Standard governance processes can be applied to PAM access including reviews, requests, policy enforcement and certification. This ensures that privileged access is consistently monitored and adheres to security best practices.
2. Greater visibility and control to all privileged access can be realized from the PAM solution. This includes leveraging the PAM credentials vault so that credentials no longer have a hardcoded connection to applications and can comply with corporate credential management security policies, such as password rotation, to minimize risk for these highly sought-after identities.

Interoperability between RSA Identity Governance & Lifecycle and a PAM solution maximizes the power of both tools. It means organizations can leverage best-in-class solutions that work together to mitigate identity risk, reduce security blind spots and help improve their overall security posture.

OPERATIONALIZE PAM INTEROPERABILITY WITH RSA IDENTITY GOVERNANCE & LIFECYCLE

Through built-in connectors within RSA Identity Governance & Lifecycle, administrators can easily configure interoperability with PAM solutions. The interoperability delivers secure bidirectional data exchange that allows RSA Identity Governance & Lifecycle to ingest the privileged access data from PAM providers and allow for automated provisioning and deprovisioning back to the provider.

With this connection established, RSA Identity Governance & Lifecycle can centrally manage identity and access governance of privileged users throughout the user and application lifecycles.

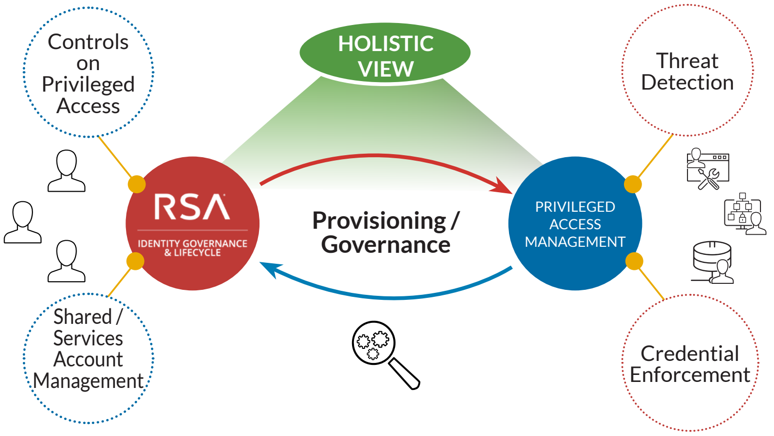
Controls on Privileged Access
HOLISTIC VIEW
Threat Detection
RSA
IDENTITY GOVERNANCE & LIFECYCLE
Provisioning / Governance
PRIVILEGED ACCESS MANAGEMENT
Shared / Services Account Management
Credential Enforcement

Figure 2: RSA Identity Governance & Lifecycle interoperability with PAM providers automates privilege access governance and provisioning while providing the business a holistic view into all identities and access.

KEY BENEFITS OF THE COMBINED SOLUTION

Connecting a PAM solution to RSA Identity Governance & Lifecycle helps organizations reduce identity risk and improve the overall security posture. The following are the key benefits:

- Reduces identity risk by providing centralized visibility and control of privileged accounts and access
- Ensures privileged users are granted appropriate access permissions in accordance with policies
- Streamlines compliance by identifying Segregation of Duties violations, auditing all identities and access permissions, and providing centralized reporting
- Maximizes time and dollar investments with existing providers while enhancing the organization’s security posture

The interoperability enables organizations to gain unified, policy-driven identity and access governance across all users and access. It effectively arms organizations with the information they need to quickly identify and respond to security access risks involving the organizations most powerful identities—privileged users. Learn more at rsa.com/igl

ABOUT RSA IDENTITY GOVERNANCE & LIFECYCLE

RSA Identity Governance & Lifecycle provides organizations the ability to act with insight to reduce identity risk and drive informed security decisions. RSA Identity Governance & Lifecycle simplifies how access is governed and streamlines access requests and fulfillment to deliver continuous compliance assurance by automating the management of user entitlements throughout the user's lifecycle.

Dell Inc. or its subsidiaries believe the information in this document is accurate as of its publication date. The information is subject to change without notice.