DATASHEET

RapidIdentity: Privileged Access Management (PAM)

Privileged users with elevated access are highly desired targets for intruders and malicious insiders and are closely watched by compliance auditors. With multiple approaches to privileged user access and identity management, RapidIdentity reduces the risk of security breaches and compliance violations.

How Secure Are Your Privileged Accounts?

Can you account for all of your privileged accounts? Are you confident prior employees, consultants, and partners no longer have access to your business critical systems? Do you have the automation in place to manage the workload required to pass increasingly demanding compliance audits? If you answered "**NO**" to any of these questions, you are not alone. Addressing the risk of "super" users and privileged accounts is a serious challenge for most organizations.

Privileged users and accounts are "the keys to the kingdom" and must be managed vigilantly. Still, according to Gartner, the adoption of PAM products is often partial, leaving gaps that put an organization at risk.

Securely Automating & Streamlining PAM

RapidIdentity secures your environment by serving as a repository of users' digital identities and entitlements (standard and privileged) across all connected systems, providing centralized control and visibility to managed entitlements. All associated events, including requests, approvals, and revocations are logged, capturing a complete audit trail.

RapidIdentity enables organizations to set time-based access expiration for all entitlements, which enforces security without being dependent on annual recertification campaigns. Access is granted only for the needed duration and certified on a continuous basis, rather than once or twice a year.

Automated Workflows

Easily Elevate Standard to Privileged Access

Time-Based Access to Shared Admin Accounts

Complete Audit Trail

CONTACT US TO SCHEDULE A DEMONSTRATION:

1.877.221.8401

sales@identityautomation.com

www.identityautomation.com

RapidIdentity Adapts to Existing Privileged Access Management Controls

RapidIdentity supports three different Privileged Access Control workflows, without requiring any third party PAM solutions. Simply choose the one that fits your established governance policy

1. ***Elevate Standard to Privileged Accounts***
   With RapidIdentity, temporarily elevating a standard account to a privileged account is fast, easy, and does not require IT involvement. When a user submits a workflow request for elevated access to a target system, an approval process is triggered with the appropriate system owners. The approval workflow can be dynamic, based on the requester's role, attributes, or currently held entitlements. Prior to the entitlement expiration, the entitlement owner is notified and can recertify or revoke the privileged access. If no action is taken, privileged access rights are automatically revoked.

2. ***Manage Multiple Accounts Per User, Per System***
   Create and manage multiple accounts per system, and link them to a single user ID. RapidIdentity applies the same entitlement controls and automated deprovisioning to privileged accounts as standard accounts. IT staff can have both a standard account for day-to-day use and a privileged account for administrator functions, without requiring compromises or manual workarounds. With other IAM systems that only support one account per user, per system, admin accounts must be created outside of the IAM system's control, often resulting in them being overlooked during the offboarding process.

3. ***Time Limit Access to Shared Admin Accounts***
   Give IT staff the ability to complete administrative tasks, without providing full-time, unlimited access to shared superuser or administrative accounts. RapidIdentity uses password vaulting that enables users to request login credentials for superuser accounts via streamlined approval workflow on an as needed basis. Once a request is approved, the recipient receives a valid credential that allows access for a predefined window of time. When the time expires, the credential is no longer valid, and the user must request access again with a newly provisioned credential.

Lock Down Your Privileged Access Controls with RapidIdentity

Contact us at 877-221-8401 or sales@identityautomation.com to request a demo today to see how RapidIdentity can dramatically reduce the security and compliance risks associated with legacy IAM solutions and manual processes.

Since 2004, Identity Automation has focused on intelligently automating provisioning, access, and account management. Our mission is to securely put control of these crucial tools in the hands of the users who need it most — employees and managers. RapidIdentity, our sophisticated, easy-to-use identity management software, makes every user a power user, increasing enterprise security and agility, boosting productivity across the board.

IDENTITY AUTOMATION