Delinea

Invisible PAM

Balancing productivity and security behind the scenes

WHITEPAPER

Invisible PAM:

Balancing productivity and security behind the scenes

Enterprises are rapidly acquiring privileged access management (PAM) solutions that manage passwords and other digital credentials. PAM continues to be the number one priority for CISOs seeking to reduce cyber risk and meet security compliance requirements.

Unfortunately, many organizations struggle to maximize their PAM investment because traditional solutions are so complex. In fact, 32% of IT operations leaders name complexity as the main reason PAM programs fail.[1]

Traditional PAM solutions require people to interrupt their workflow in order to access credentials. As a result, people find ways to skirt security policies so they can stay productive. Their PAM investment sits on the shelf collecting dust.

We believe PAM complexity isn't just a pain, it's also downright dangerous. Usability and security go hand in hand to increase adoption and decrease risk.

To realize the promise of enterprise PAM, solutions must be easy to use, embedded in people's daily workflow, and orchestrated behind the scenes. For the average privileged user, PAM must be virtually invisible.

[1] https://delinea.com/company/blog/2020/04/14/global-state-of-least-privilege-report-2020/

Delinea is pioneering invisible PAM

What's invisible PAM?

With invisible PAM, organizations can seamlessly access and manage secrets of all kinds (traditional passwords as well as digital keys and credentials) without any friction or disruption. Invisible PAM works in the background to reduce cyber fatigue and empower happy employees.

Invisible PAM is a core requirement for our industry to achieve a "password-less" state. Password-less security doesn't mean digital credentials will cease to exist. It really means that people will no longer need to remember and manage traditional passwords. Instead, alternatives like ephemeral certificates will unlock and manage granular access.

Invisible PAM isn't some far-off future.

Even today, most Delinea users never need to interact directly with PAM technology at all. They work securely within the same IT and business productivity systems they already know and use every day.

Orchestration behind the scenes

Orchestration is key to invisible PAM. With orchestration, PAM can scale across a complex, growing enterprise by integrating privileged security and IT functions across multiple disparate systems. Identities, roles, permissions, and activities are all synched and security policies are followed consistently regardless of geography, business unit, or technology.

To make PAM orchestration a reality, Delinea has native integrations between our privileged security solutions and other enterprise tools. These integrations require zero code and are ready to go right away.

Privileged IT users

The work of IT teams traditionally involves lots of screen switching, fragmented information, and disjointed record keeping. Tedious, manual work increases human error and risk of a privileged account attack. It's not the most effective way to use the time of IT experts and it's impossible to scale.

Invisible PAM helps privileged IT users increase efficiency and reduce risk

IT users	Secure and manage privileged credentials via…
IT operations, provisioning, and helpdesk teams	**IAM and IGA systems such as SailPoint** Provisioning teams can provide contextual or time-bound access and permissions and maintain consistent role-based access across systems. **ITSM systems such as ServiceNow** IT teams can manage tickets for provisioning or troubleshooting within their preferred workflow tool. They can track completions, resolve issues, and document all activities. **Remote Desktop systems such as Connection Manager** IT teams can launch and manage multiple remote desktop sessions from a single interface. Credentials are injected directly into remote sessions without an IT admin needing to access or see a password. **Collaboration tools such as Slack** IT teams that use Slack can receive notifications, handle workflows such as approval requests, and launch secrets through PAM integration.
Database administrators	**Databases such as SQL and Oracle** Databases commonly contain confidential, highly sensitive, and irreplaceable data. They're also where logs of malicious behavior are stored, which makes them prime targets to be erased. Despite their importance, database access is often secured only by a password or at most SSO or MFA. Compromised database credentials could have tremendous impact on an entire organization, especially admin credentials that allow a user to access all data and create backdoor accounts. PAM solutions that secure database access reduce the attack surface. At the same time, they provide database admins and other teams the access they require, when they need it. Invisible PAM can automate approvals to provide people access to specific databases (not an entire server) and even granular access to what is inside a database. Proxy functionality means the IP address of the database as well as the password are never shown to users.
Developers	**Tools in the DevOps workflow and CI/CD toolchain** Invisible PAM solutions create ephemeral secrets instantly so DevOps teams can access tools for software and infrastructure deployment, testing, orchestration, and configuration. There's no need for developers to embed secrets into code or store them in insecure code libraries. In addition, PAM provides developers with SSH access to platforms they work with in the CI/CD pipeline and software development lifecycle.
Cloud admins	**Browser-based admin panels for AWS, Azure, and GCP** With invisible PAM, cloud admins can operate within their cloud consoles and automatically retrieve secrets needed to access and manage cloud resources.
InfoSec and incident response teams	**SIEM systems such as Splunk** Invisible PAM automates follow-up actions so IT teams can focus on exceptions where their expertise is most needed. For example, Delinea PAM can automatically assign incident severity based on threat scores and asset criticality, and quarantine suspicious files in sandboxes for malware analysis.

Privileged business users

When PAM is too complex, many business users turn to browser-based password managers and vaults.

The problem is, personal password managers still depend on users to manage passwords and this means inconsistency and no central policies. People need to break their workflow to use them, so they lose productivity and find creative ways around them.

For an enterprise, password vaults are insufficient for many reasons. They don't provide oversight or control to ensure compliance requirements are met. They don't enforce, only recommend, password complexity, rotation or expiration policies, requirements for MFA, etc. With multiple password vaults in use throughout an organization, central IT security teams can't create consistent, comprehensive reports for execs or auditors.

If business users rely on password vaults, the responsibility for security falls on their shoulders. In contrast, with enterprise PAM solutions, the responsibility for privilege security is borne by IT.
All business users need to do is enjoy the benefits

Business users	Access privileged credentials via…
Web application users	**Web plugins** With Secret Server's Web Password Filler, people can access privileged credentials directly from their browser by authenticating directly from the web plugin. Support for 2FA options such as DUO, single sign-on, SAML and other multi-factor authentication mechanisms is included. **PAM designed for cloud applications** Invisible PAM solutions limit the accounts that can access applications, reducing your attack surface. Unlike a vault, in which users have access to system passwords, Access Controllers autofill passwords so they're never revealed to users. Only the administrators of Access Controllers set up the password that connects to the system.
Mobile users	**Mobile apps** Business users receive notifications and manage credentials via Delinea's mobile app.

No users, just code

Invisible PAM can operate without any human intervention at all.

Common trigger events can initiate a series of automated actions, saving IT time so they can focus on alerts that need more investigation or complex response.

For example, if a privileged credential's heartbeat fails, indicating a password has been changed outside of the central PAM solution, a triggered action in Delinea Secret Server can rotate that password automatically and bring control back into the central PAM vault.

Policies can apply triggered events to secrets, folders, or sets within folders. PAM administrators have tremendous flexibility to customize triggered events and follow-up actions, such as sending an email or running a script, in order to match their own IT systems, policies and workflows.

When you make PAM invisible, adoption skyrockets

Productive

- No context-switching or workflow disruptions
- No need to learn new interfaces

Painless

- No software installs
- No wrestling with VPNs

Secure

- No users storing passwords in their browser or using vaults where passwords are copied and pasted
- No users secretly using iCloud keychain or disconnected personal vaults
- No SSH users making secret backdoors

> “Organizations that use privileged task automation features will save 40% on staff costs...”
>
> → 2020 Gartner Magic Quadrant for PAM

Delinea

Defining the boundaries of access

Delinea provides seamless security based upon the principles of zero trust, least privilege, and just-in-time privilege elevation. If you're considering a migration to the cloud or worried that your existing cloud resources aren't properly protected, talk with one of cloud experts about PAM for the cloud.

Learn more about Delinea's solutions at **delinea.com.**