Silverfort

Securing Privileged Access at Scale: From Blind Spots to Resilience

How to discover and protect every privileged account – simply and quickly – across your environment.

Why securing privileged identities matters now more than ever

Talk to any security or identity leader in any organization, and they'll all say the same thing: securing privileged access is a major concern and a major challenge.

Looking at the numbers, this isn't surprising. Around 80% of breaches involve privileged accounts at some stage of the attack lifecycle. Attackers target them because they're an effective option for lateral movement, persistence, and rapid escalation after gaining an initial foothold.

For years, the standard for securing this critical attack surface has relied on Privileged Access Management (PAM) solutions. In practice, they leave most privileged identities in modern enterprises exposed to risk.

Traditional PAM solutions were designed over two decades ago for a simpler IT environment, mainly to support compliance by controlling admin access to servers. They weren't designed to cope with today's hybrid environments, where thousands of human, machine and AI agent identities are scattered across cloud, SaaS, and legacy systems. This misalignment leaves critical security gaps for attackers to exploit.

What you'll learn from this ebook

Why legacy PAM can't keep up with modern security needs

The five essential capabilities for securing privileged access in modern environments

A new vaultless approach to protecting privileged access at runtime

A simpler way to deploy and manage privileged access security at scale

Why is protecting privileged identities so difficult?

Nowadays, organizations seeking to protect their privileged identities rely mostly on traditional PAM solutions, centered on vaulting, password rotation, and session recording.

But the reality is hard to ignore. The vast majority of organizations that deploy PAM admit they struggle to move their projects forward. Only 10% get to the finish line.[1] Others simply avoid implementing them in the first place, due to notoriously high costs and operational overhead.

[1] *The State of the Identity Attack Surface, Osterman Research*

Complex and lengthy onboarding

PAM solutions are infamous for their long, painful onboarding process. Most PAM projects never reach full coverage, leaving large portions of privileged identities outside protection. Identity teams manage a costly, operationally heavy solution that still fails to deliver the expected risk reduction. Meanwhile, PAM licenses remain underutilized, and project costs continue to grow.

Manual discovery

Before you can *protect* privilege accounts, you must be able to *discover* them. While some are visible in Active Directory (AD) groups, many operate outside of them. Discovering service accounts, shadow admins, and growing numbers of NHIs and AI agents requires time-consuming manual investigation across logs and systems, creating a telemetry nightmare.

Coverage gaps that quietly erode your security posture

Traditional PAM solutions prioritize human admins, leaving service accounts and other non-human identities exposed. Bringing these accounts under management is often complex and risky, leading teams to delay onboarding or exclude them altogether. The result is partial coverage and a false sense of security—tools may be in place, but meaningful protection is not.

Easy to bypass

Admins often bypass PAM by checking out credentials and logging in directly, sometimes outside their access tier. Meanwhile, PAM itself is a high-value attack target. When compromised, it becomes a single point of failure, granting adversaries unlimited access to resources.

THE RESULT:

A posture attackers exploit

PAM projects are often too complex to fully deploy or scale, leaving a large portion of privileged identities unprotected and ripe for exploitation.

Four perspectives on traditional PAM's shortcomings

Identity

Head of IAM:

Continuous operational inefficiency

"My team has spent hundreds of hours trying to get our PAM project on wheels and we're still encountering issues and have gaps. This project consumes critical resources while pushing aside other critical tasks."

Identity Engineer:

Daily friction and workload overload

"I'm drowning in the task of manually discovering each and every privileged account and their access paths, integrating systems one by one, and chasing admins who refuse to use the tool at all . We're constantly playing catch up instead of reducing risk."

Security

CISO:

Persistent exposure and unmitigated risk

"The fact that we cannot confidently say all privileged accounts are protected keeps me up at night. One exposed account is enough for threat actors to move laterally, deploy ransomware, and disrupt our business."

Security Architect:

Critical resilience gap

"I don't know which privileged identities are exposed and how they are used. There are too many blind spots. If an admin account is compromised, I can't detect it or block lateral movement across the environment."

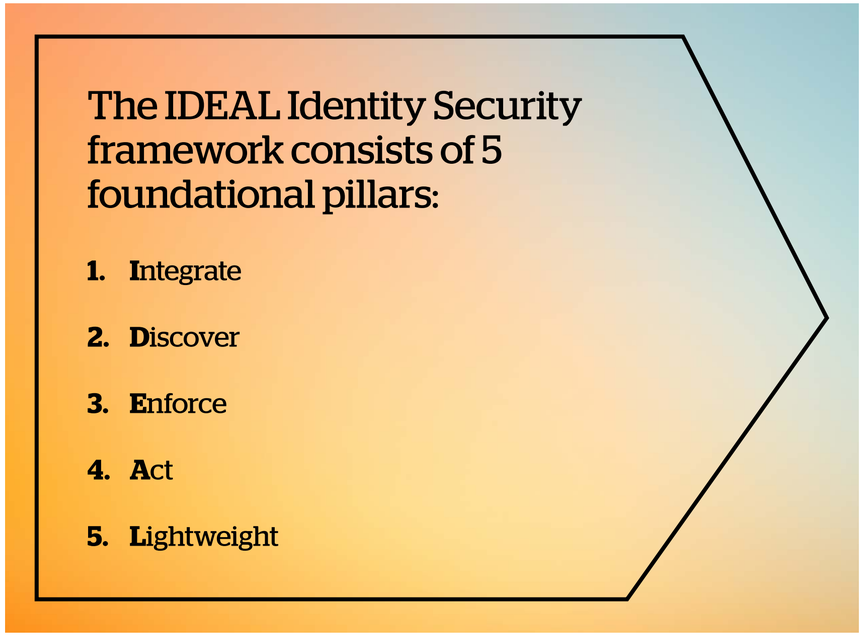
"We might be compliant, but we're definitely not secured."

– CISO of large manufacturing company

I
D
E
A
L

Paradigm shift: Applying the IDEAL Identity Security approach to privileged access protection

When the old way doesn't work anymore, we need to shift our mindset. This is where the IDEAL approach to identity security comes in.



The five capabilities below can help you choose a privileged access security solution that can holistically deliver the visibility, coverage, and enforcement to secure every privileged identity, on-prem, in hybrid environments, and in the cloud:

Integrate: Become a native part of the IAM authentication flow, allowing privileged access security controls to apply to every authentication attempt, across all environments.

Discover: Continuously identify and classify all privileged access across all identity types, including workforce users, admins, external contractors, NHIs, and AI agents, along with their configurations, attributes, and resource access.

Enforce: Actively secure risky authentications and access attempts at runtime with adaptive controls such as MFA step-up authentication, Just-In-Time (JIT) access, and access blocking when risk is detected.

Act: Immediately respond to real-time events and potential identity threats, such as credential exposure, privilege escalations, and lateral movement attempts, blocking malicious access at runtime before it completes.

Lightweight: Deploy and operate the solution quickly and easily, without disrupting users, systems, or automated processes.

What is Vaultless PAM?

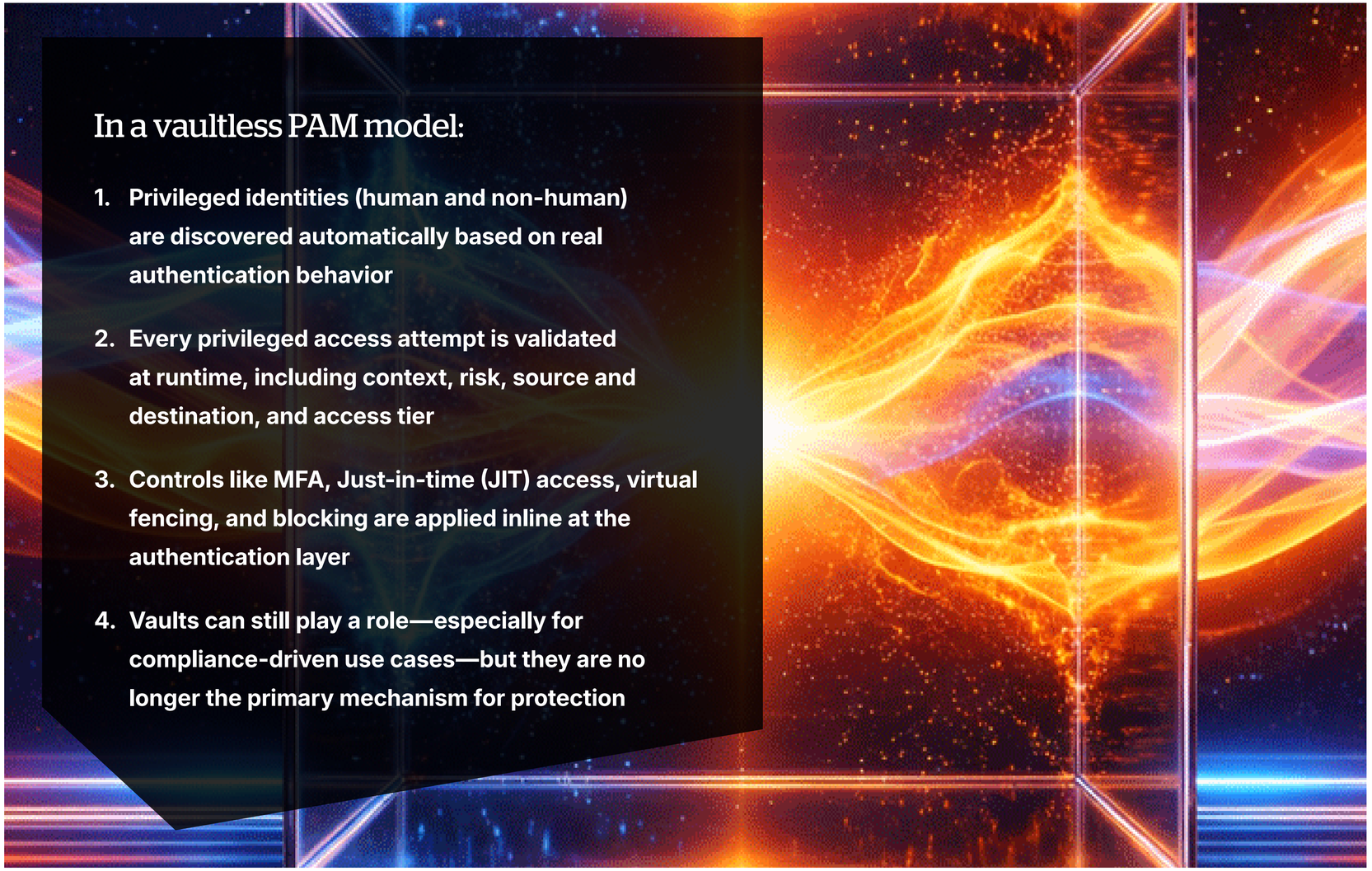
Vaultless PAM is a modern approach that protects privileged access when it happens without relying on credential vaults, password rotation projects, or disruptive onboarding.

Instead of asking,

> “Have we successfully forced every privileged account into a vault?”

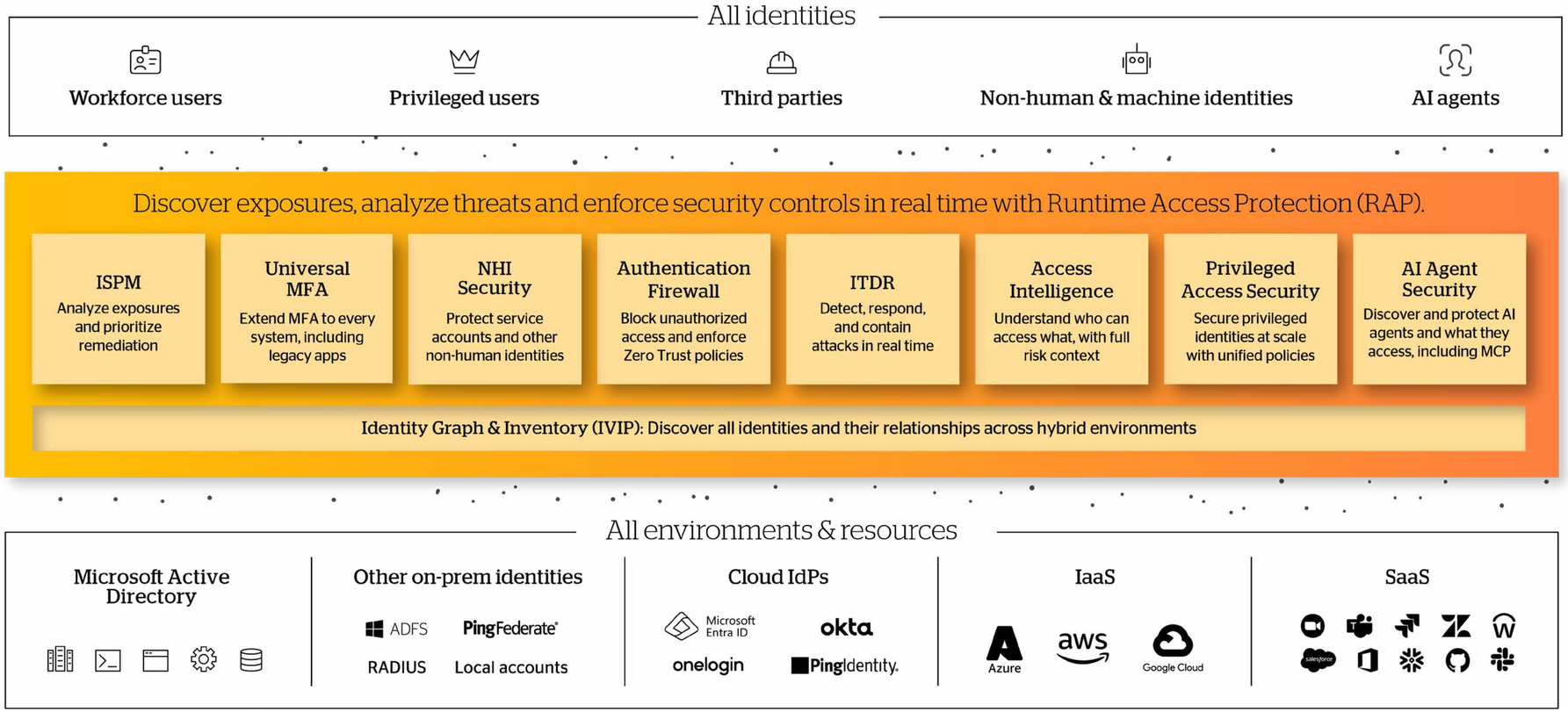
the core question becomes:

> “Are all privileged authentications evaluated and protected at runtime?”



The Silverfort Identity Security Platform

Silverfort has pioneered the first Identity Security Platform that fully implements the IDEAL framework across the identity stack, from on-prem Active Directory to cloud IdPs, IaaS, and SaaS. With Silverfort, organizations can apply automated discovery, continuous monitoring, risk analysis, and runtime enforcement on every authentication attempt.



I
D
E
A
L

How Silverfort delivers Vaultless PAM

Integrate:

Accelerate time to protection.

Thanks to our unique Runtime Access Protection (RAP) technology, Silverfort integrates seamlessly into existing authentication flows, so organizations can:

- → Quickly onboard all privileged identities and reduce deployment timelines from years to weeks
- → Monitor and evaluate authentications across Kerberos, NTLM, LDAP, RDP, PowerShell, PsExec, SSH, and more
- → Apply policies at the point of authentication, before access is granted

Discover:

Gain complete visibility across all privileged identities.

Silverfort continuously discovers:

- → Domain, cloud, server, and application admins
- → Break-glass accounts
- → Service accounts and other NHIs
- → AI agents that access privileged resources

Discovery is driven by both configuration and *actual behavior*, eliminating manual log-stitching and one-off discovery projects.

Enforce:

Apply runtime controls on admins and service accounts.

For privileged authentications, Silverfort can:

- → Enforce MFA to human admins and on admin tools (PowerShell, PsExec, WMI, RDP, SSH, etc.)
- → Implement JIT access and zero standing privilege for admins
- → Apply virtual fencing to constrain service accounts to known hosts, destinations, and behaviors
- → Block or challenge risky cross-tier or lateral movement attempts at runtime

Because enforcement happens at authentication, there's no need for credential checkout workflows, new proxies, or route changes.

Act:

Immediately detect and contain identity threats.

Using continuous authentication telemetry, Silverfort spots credential theft, misuse, and abnormal privileged behavior. When risky activity is detected, and before an attacker can weaponize privileged access, the platform can:

- → Block the request
- → Step up MFA
- → Restrict access paths and tiers

Lightweight:

Simplify deployment and daily operations.

Silverfort's approach avoids complex infrastructure changes, so you can benefit from:

- → Quick deployment and easy operations
- → No app rewrites
- → No multi-year vault onboarding plans
- → Fast time to value and proven ROI

Organizations commonly go from first connect to meaningful privileged access controls in days, including in large enterprise environments.

How Silverfort's Identity Security Platform scales protection & risk reduction to privileged access

Key capabilities:

Discover identities and understand risks with complete visibility and actionable intelligence

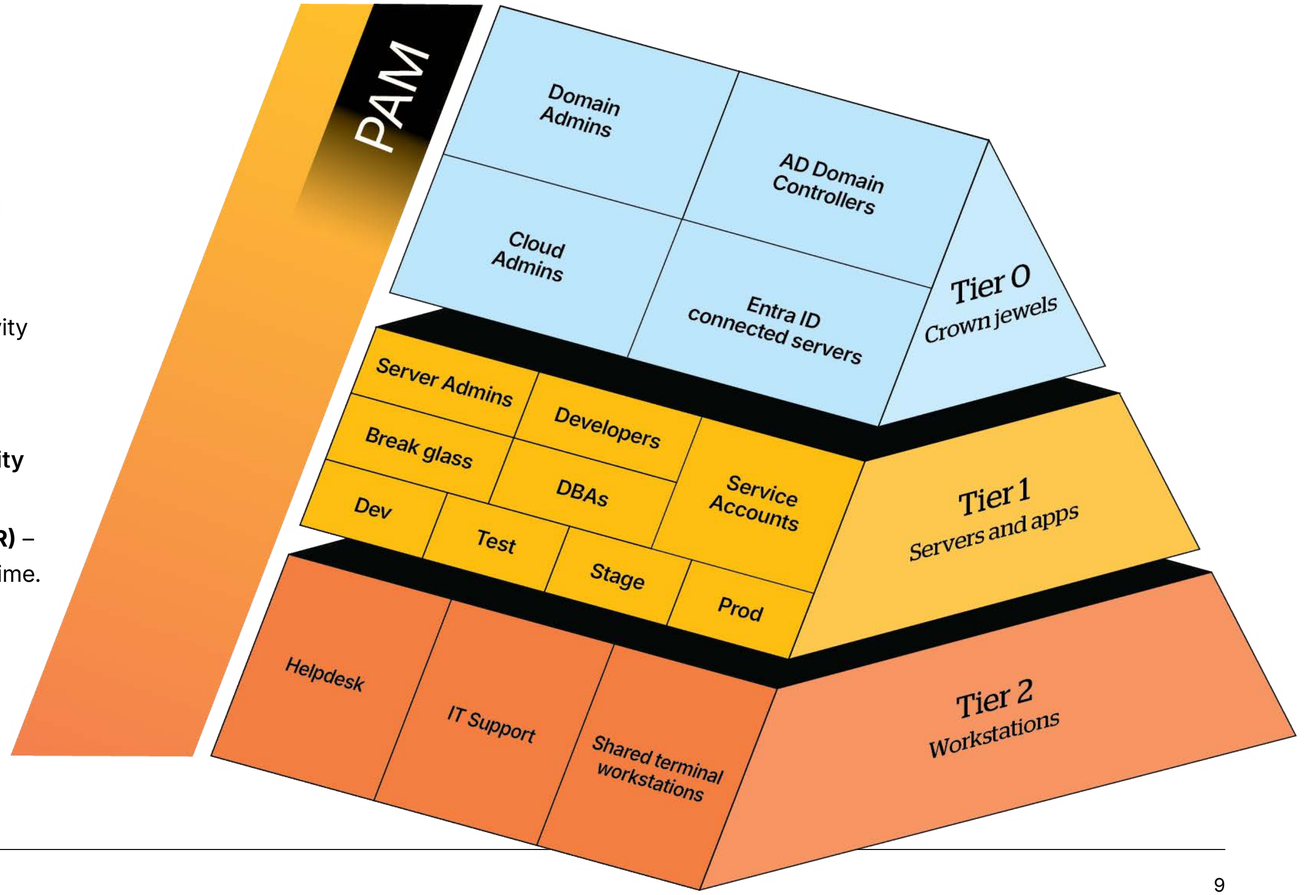
- → **Full visibility** – Automatically discover all privileged identities, human and non-human, based on both configuration and real authentication behavior, ensuring no privileged account is left unprotected.
- → **Access Intelligence** – Analyze authentication activity to identify risky behavior and unneeded privileges to reduce.
- → **Identity Security Posture Management (ISPM)** – Uncover, map, and prioritize Identity Security exposures and hygiene issues.

Control privileged access with Runtime Access Protection:

- → **MFA for admin tools** – Extend MFA to admin tools and protocols such as PowerShell, PSexec, WMI, and RDP.
- → **Authentication Firewall** – Enforce Zero Trust access controls, tier segmentation, and Least Privilege policies to prevent unauthorized privileged access.
- → **Just-In-Time (JIT) access** – Eliminate standing privilege by granting privileged access only when required.
- → **Virtual fencing** – Restrict service account activity to known sources and destinations, preventing unauthorized use.

Detect and stop attacks in their tracks with Identity Threat Detection and Response:

- → **Identity Threat Detection and Response (ITDR)** – Detect and stop identity-based attacks in real time.



Whether you have a PAM or not, Silverfort ensures all your privileged identities are protected.

Vaultless PAM is not anti-vault—it's pro-outcome. We know different environments are at different points in their PAM journey, so we support several models to protect privileged identities regardless of the existing architecture.

WITH PAM:

Extend coverage and maximize your existing investment

Many organizations deploy PAM but struggle to extend coverage to all privileged identities. Silverfort enhances existing PAM deployments by acting as a security enforcement layer across the authentication flow.

This allows organizations to protect privileged identities that remain outside the vault, including accounts that have not yet been onboarded or service accounts that can't undergo rotation. By extending protection beyond the vault, Silverfort helps organizations achieve full coverage while reducing the operational burden of onboarding every account into PAM.

Right-size your PAM scope, effort, and investment. Vault only what is truly required and decommission unused licenses.

WITHOUT PAM:

Secure privileged access without deploying a vault

For organizations without an existing PAM deployment — either because PAM was never implemented or a previous rollout was abandoned — Silverfort can serve as the primary control plane for securing privileged identities.

The platform automatically discovers privileged identities, applies runtime security controls such as MFA, Just-In-Time access, and access restrictions, and detects identity-based threats such as credential abuse, privilege escalation, and lateral movement attempts.

Secure privileged access across the entire environment without deploying vault infrastructure or running complex onboarding projects.

Evaluating PAM solutions?

Below is a condensed checklist adapted from a recommended RFP framework for privileged access security—so you can be sure you're buying the outcomes your organization needs.

A solution that scores strongly across these dimensions delivers what modern environments need: full visibility, broad coverage, and real-time control over privileged access.

Get the guide

Get the full Identity Security Buyer's Guide and RFP Checklist

Integration & coverage

- ☐ Can the solution integrate directly with Active Directory and major cloud IdPs without agents or proxies?
- ☐ Does it see all authentication flows, including CLI, RDP, SSH, and legacy protocols?
- ☐ Can it cover human admins, service accounts, NHIs, and AI agents across on-prem and cloud?
- ☐ Can it scale across the entire environment and cover all privileged accounts?
- ☐ Can it easily support the growth of privileged users and accounts as the environment expands?

Discovery & analytics

- ☐ Does it automatically discover all privileged identities (human and non-human) across all systems, applications, and environments?
- ☐ Does it discover privileged identity based on actual usage, not just static configurations?
- ☐ Can it discover shadow admins and unvaulted privileged accounts?
- ☐ Does it map privilege paths and lateral movement risks?
- ☐ Does it identify dormant and unused privilege accounts and recommend remediation plans?

Runtime control enforcement

- ☐ Can it enforce MFA on native admin tools and infrastructure access (not just web apps)?
- ☐ Does it support Just-In-Time elevation and zero standing privileges?
- ☐ Can it enforce Least Privilege access and restrict access to prevent unauthorized activity?
- ☐ Can it enforce access tier segmentation for admins?
- ☐ Can it enforce virtual fencing for service accounts?

Threat detection & response

- ☐ Does it provide ITDR capabilities for privileged identities, spotting abuse, lateral movement, and privilege escalation in real time?
- ☐ Can it automatically respond to threats (block, challenge, restrict) without manual intervention?

Simplicity & time to value

- ☐ What is the typical deployment and onboarding time?
- ☐ What is the typical time from initial deployment to meaningful privileged access protection?
- ☐ Does it require agents, application rewrites, or significant network changes?
- ☐ How does it impact operations for admins, DevOps, and application owners?

Silverfort: Identity Security done right

→ Full visibility across the hybrid IAM stack

Get Identity Security you deserve with comprehensive visibility and protection across all identities and all environments—human, AI, and machine, on-prem, cloud, and hybrid.

→ Security first with runtime enforcement

Simplify and consolidate identity protection for every identity type in one place with Silverfort's patented Runtime Access Protection (RAP) technology.

→ No more changes to your systems and apps—and no more hard conversations

Because Silverfort integrates directly into your existing IAM infrastructure, teams don't need to install agents on every machine, or recode, rearchitect, or change any application. No disruptions, no lengthy rollouts.

→ Protect systems that couldn't be protected before

Extend protection to previously unprotectable resources, including legacy systems, command-line interfaces, file shares, IT/OT infrastructure, air-gapped environments, and more.

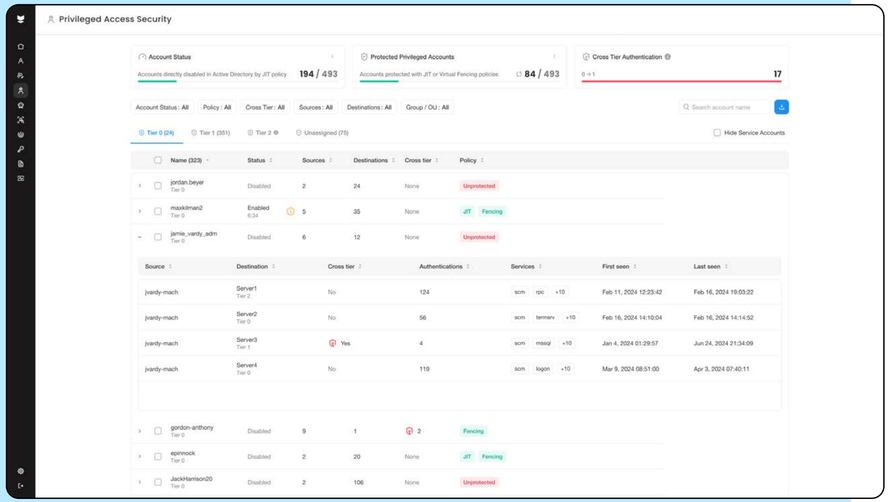
See it in action

Most organizations don't need yet another multi-year identity project.

They need a fast, easy, pragmatic path to better privileged access security.

Explore our interactive demos or book a personalized session to see how Silverfort protects privileged identities across your environment.

Product tour **Book a demo**



About Silverfort

Over 1,000 organizations trust Silverfort to secure every dimension of identity. We deliver end-to-end Identity Security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work.