Silverfort

Privilegierten Zugriff im großen Maßstab absichern: Von Blind Spots zu mehr Resilienz

So entdecken und schützen Sie jedes privilegierte Konto – einfach und schnell – in all Ihren Umgebungen.

Warum der Schutz privilegierter Identitäten heute wichtiger denn je ist

Fragen Sie irgendeinen Security- oder Identity-Verantwortlichen in einem x-beliebigen Unternehmen, und alle werden Ihnen dasselbe sagen: Die Absicherung privilegierter Zugriffe ist ein zentrales Anliegen und eine große Herausforderung.

Ein Blick auf die Zahlen zeigt, warum das kaum überrascht. Bei rund 80 % aller Sicherheitsverletzungen sind privilegierte Konten an irgendeiner Stelle im Angriffsverlauf beteiligt. Angreifer nehmen sie gezielt ins Visier, weil sie sich hervorragend für Lateral Movement, Persistenz und eine schnelle Eskalation eignen, sobald ein erster Zugang erlangt wurde.

Jahrelang galt Privileged Access Management (PAM) als Königsweg für die Absicherung dieser kritischen Angriffsfläche. In der Praxis bleiben jedoch dadurch die meisten privilegierten Identitäten in modernen Unternehmen Risiken ausgesetzt.

Traditionelle PAM-Lösungen wurden vor mehr als zwei Jahrzehnten für eine einfachere IT-Umgebung entwickelt – vor allem, um Compliance-Anforderungen zu erfüllen und den administrativen Zugriff auf Server zu kontrollieren. Sie wurden nicht dafür entwickelt, mit den heutigen hybriden Umgebungen zurechtzukommen, in denen Tausende menschliche, maschinelle und KI-Agenten-Identitäten über Cloud-, SaaS- und Legacy-Systeme verteilt sind. Diese strukturelle Fehlausrichtung hinterlässt kritische Sicherheitslücken, die Angreifer ausnutzen können.

Was Sie in diesem E-Book erfahren werden

- Warum bestehende PAM-Systeme mit modernen Sicherheitsanforderungen nicht Schritt halten
- Die fünf wesentlichen Funktionen zur Absicherung privilegierter Zugriffe in modernen Umgebungen
- Ein neuer, vault-loser Ansatz zum Schutz privilegierter Zugriffe zur Laufzeit
- Eine einfachere Möglichkeit, den Schutz privilegierter Zugriffe in großem Maßstab zu implementieren und zu verwalten

Warum ist der Schutz privilegierter Identitäten so schwierig?

Heute verlassen sich Organisationen, die ihre privilegierten Identitäten schützen wollen, meist auf traditionelle PAM-Lösungen, die auf Vaulting, Passwortrotation und Sitzungsaufzeichnung basieren.

Doch die Realität lässt sich schwer ignorieren. Die überwältigende Mehrheit der Organisationen, die PAM einführen, gibt zu, dass sie Schwierigkeiten haben, ihre Projekte voranzubringen. Nur 10 % bringen sie tatsächlich zum Abschluss.[1] Andere verzichten von vornherein auf eine Implementierung – aufgrund der bekanntermaßen hohen Kosten und des operativen Aufwands.

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

Komplexe und langwierige Implementierungsprozesse

PAM-Lösungen sind bekannt für ihren langwierigen und mühsamen Implementierungsprozess. Die meisten PAM-Projekte erreichen nie eine vollständige Abdeckung, sodass große Teile privilegierter Identitäten ungeschützt bleiben. Identity-Teams verwalten eine kostspielige und betrieblich aufwendige Lösung, die dennoch nicht die erwartete Risikominderung erzielt. Gleichzeitig bleiben PAM-Lizenzen unzureichend genutzt, und die Projektkosten steigen weiter.

Manuelle Erkennung

Bevor Sie privilegierte Konten *schützen* können, müssen Sie sie *erkennen* können. Einige sind zwar in Active-Directory (AD)-Gruppen sichtbar, viele sind jedoch außerhalb dieser Gruppen tätig. Das Aufspüren von Service Accounts, Shadow-Admins und einer wachsenden Zahl von NHIs und KI-Agenten erfordert zeitaufwendige manuelle Untersuchungen in Protokollen und Systemen, was zu einem Albtraum in Sachen Telemetrie führt.

Sicherheitslücken, die Ihre Sicherheitslage still und heimlich schwächen

Klassische PAM-Lösungen priorisieren menschliche Admins und lassen Service Accounts sowie andere nicht-menschliche Identitäten ungeschützt. Die Übernahme dieser Konten in die Verwaltung ist oft komplex und risikobehaftet, was dazu führt, dass Teams die Einführung verzögern oder ganz darauf verzichten. Das Ergebnis ist eine lückenhafte Abdeckung und ein trügerisches Gefühl der Sicherheit – zwar sind die Tools vorhanden, doch ein wirksamer Schutz fehlt.

Leicht zu umgehen

Administratoren umgehen PAM häufig, indem sie sich Anmeldedaten anzeigen lassen und sich direkt anmelden, manchmal sogar außerhalb ihrer Zugriffsebene. Gleichzeitig ist PAM selbst ein besonders attraktives Angriffsziel. Wird es kompromittiert, wird es zum Single Point of Failure und gewährt Angreifern uneingeschränkten Zugriff auf Ressourcen.

DAS ERGEBNIS:

Eine Sicherheitslage, die Angreifer ausnutzen

PAM-Projekte sind oft zu komplex, um vollständig implementiert oder skaliert zu werden, sodass ein großer Teil der privilegierten Identitäten ungeschützt bleibt und angreifbar ist.

Vier Perspektiven auf die Schwächen klassischer PAM-Lösungen

Identity

IAM-Leitung:

Anhaltende operative Ineffizienz

„Mein Team hat Hunderte von Stunden damit verbracht, unser PAM-Projekt voranzubringen, und dennoch stoßen wir immer noch auf Probleme und haben Lücken. Dieses Projekt beansprucht wichtige Ressourcen und verdrängt dabei andere wichtige Aufgaben."

Identity Engineer:

Tägliche Konflikte und Arbeitsüberlastung

„Ich versinke in der Aufgabe, jedes einzelne privilegierte Konto und dessen Zugriffspfade manuell zu ermitteln, Systeme nacheinander zu integrieren und Administratoren hinterherzulaufen, die sich rundweg weigern, das Tool zu nutzen. Wir hinken ständig hinterher, statt Risiken zu reduzieren."

Security

CISO:

Anhaltende Gefährdung und ungemindertes Risiko

„Die Tatsache, dass wir nicht mit Sicherheit sagen können, dass alle privilegierten Konten geschützt sind, lässt mich nachts nicht schlafen. Ein einziges ungeschütztes Konto reicht aus, damit Angreifer sich im Netzwerk lateral bewegen, Ransomware einsetzen und unseren Geschäftsbetrieb unterbrechen können."

Security Architect:

Kritische Resilienzlücke

„Ich weiß nicht, welche privilegierten Identitäten exponiert sind und wie sie genutzt werden. Es gibt zu viele Blind Spots. Wenn ein Admin-Konto kompromittiert wird, kann ich das weder erkennen noch laterale Bewegungen in der Umgebung blockieren."

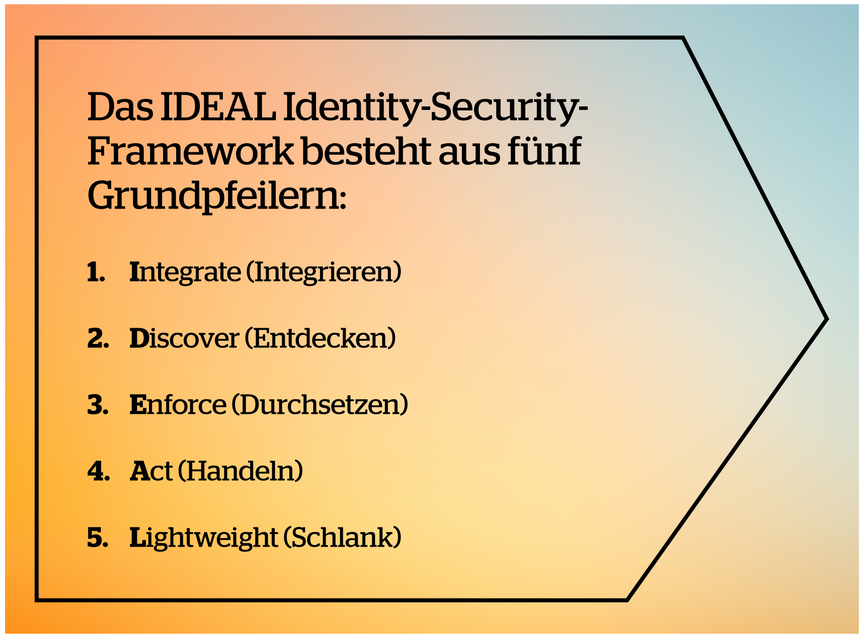
„Wir sind möglicherweise compliant, aber sicher sind wir definitiv nicht."

– CISO eines großen Fertigungsunternehmens

I
D
E
A
L

Paradigmenwechsel: IDEAL-Identity-Security-Ansatz auf den Schutz privilegierter Zugriffe anwenden

Wenn die alte Methode nicht mehr funktioniert, müssen wir unsere Denkweise ändern. Hier kommt der IDEAL-Ansatz zur Identity Security ins Spiel.



Die fünf nachfolgenden Fähigkeiten helfen Ihnen dabei, eine Security-Lösung für privilegierte Zugriffe auszuwählen, die ganzheitliche Transparenz, Abdeckung und Durchsetzung bietet, um jede privilegierte Identität On-Prem, in hybriden Umgebungen und in der Cloud abzusichern:

Integrate (Integrieren): Werden Sie zu einem nativen Teil des IAM-Authentifizierungsablaufs, damit Sicherheitskontrollen für privilegierte Zugriffe bei jedem Authentifizierungsversuch in allen Umgebungen greifen können.

Discover (Entdecken): Identifizieren und klassifizieren Sie kontinuierlich alle privilegierten Zugriffe über alle Identitätstypen hinweg, einschließlich Workforce-Nutzern, Admins, externen Auftragnehmern, NHIs und KI-Agenten, zusammen mit ihren Konfigurationen, Attributen und Ressourcenzugriffen.

Enforce (Durchsetzen): Sichern Sie risikobehaftete Authentifizierungs- und Zugriffsversuche zur Laufzeit aktiv durch adaptive Kontrollmechanismen wie MFA Step-up-Authentifizierung, Just-in-Time (JIT)-Zugriff und die Sperrung des Zugriffs bei Erkennung eines Risikos ab.

Act (Handeln): Reagieren Sie sofort auf Ereignisse in Echtzeit und potenzielle Identitätsbedrohungen wie die Offenlegung von Anmeldedaten, die Ausweitung von Berechtigungen und laterale Bewegungsversuche und blockieren Sie böswillige Zugriffe zur Laufzeit, bevor sie erfolgreich abgeschlossen werden.

Lightweight (Schlank): Setzen Sie die Lösung schnell und einfach ein und betreiben Sie sie, ohne dass es zu Beeinträchtigungen für Benutzer, Systeme oder automatisierte Prozesse kommt.

Was ist Vaultless PAM?

Vaultless PAM ist ein moderner Ansatz, der privilegierte Zugriffe in Echtzeit schützt, ohne auf Credential-Vaults, Passwort-Rotationsprojekte oder störende Implementierungsprozesse angewiesen zu sein.

Statt zu fragen:

„Haben wir erfolgreich jedes privilegierte Konto in einen Vault gezwungen?“

lautet die Kernfrage:

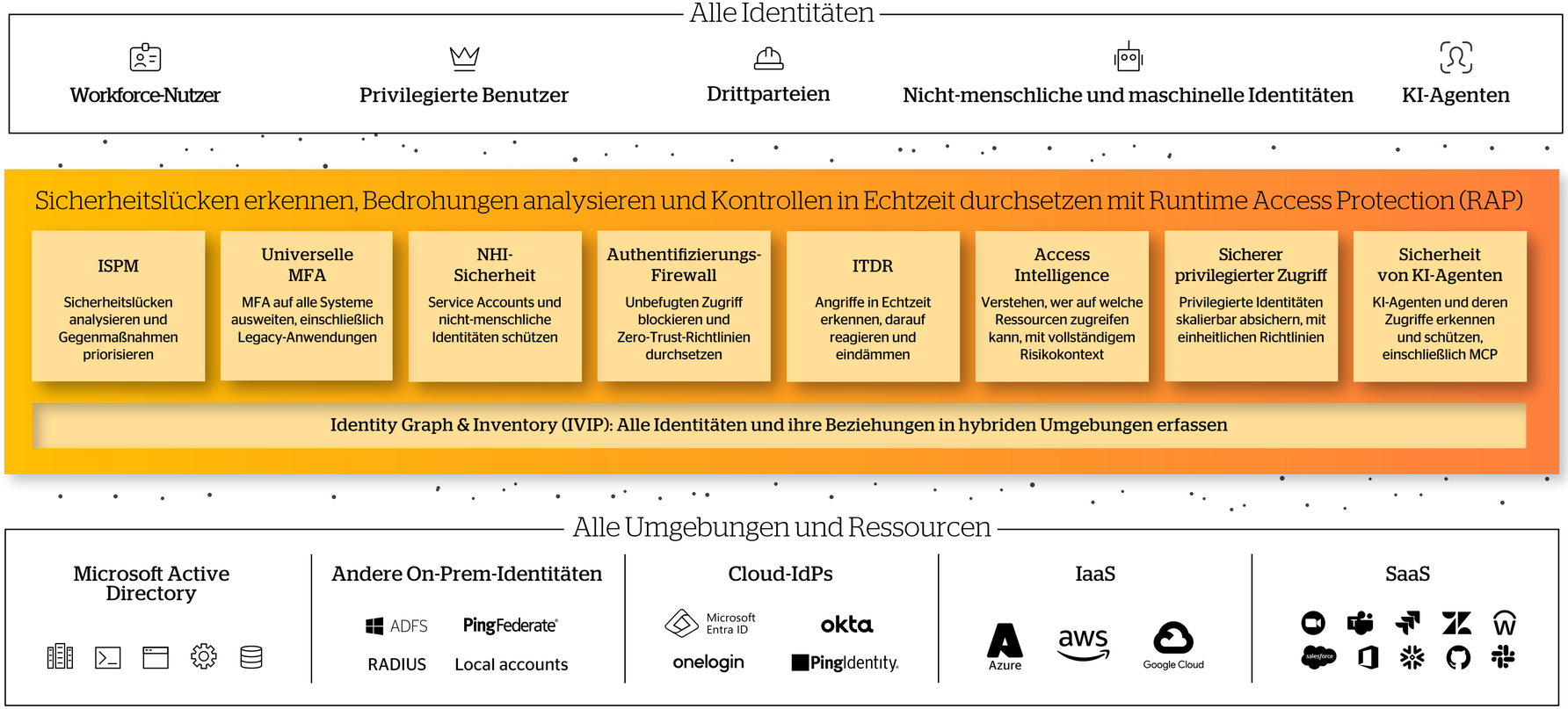
„Werden alle privilegierten Authentifizierungen zum Zeitpunkt des Zugriffs bewertet und geschützt?“

In einem Vaultless-PAM-Modell:

1. **Privilegierte Identitäten (menschlich und nicht-menschlich) werden automatisch auf Basis des tatsächlichen Authentifizierungsverhaltens erkannt.**
2. **Jeder privilegierte Zugriffsversuch wird zum Zeitpunkt des Zugriffs überprüft, einschließlich Kontext, Risiko, Quelle und Ziel sowie Zugriffsebene.**
3. **Kontrollmechanismen wie MFA, Just-in-Time (JIT)-Zugriff, Virtual Fencing und Zugriffssperren werden direkt auf der Authentifizierungsebene angewendet.**
4. **Vaults können nach wie vor eine Rolle spielen – insbesondere bei Anwendungsfällen, bei denen es um die Einhaltung von Vorschriften geht –, doch sie sind nicht mehr der wichtigste Schutzmechanismus.**

Die Identity-Security-Plattform von Silverfort

Silverfort hat die erste Identity-Security-Plattform entwickelt, die das IDEAL-Framework über den gesamten Identitäts-Stack hinweg vollständig umsetzt – vom lokalen Active Directory über Cloud-IdPs bis hin zu IaaS und SaaS. Mit Silverfort können Unternehmen bei jedem Authentifizierungsversuch automatisierte Erkennung, kontinuierliche Überwachung, Risikoanalyse und Durchsetzung zur Laufzeit einsetzen.



Wie Silverfort Vaultless PAM umsetzt

I
D
E
A
L

Integrate (Integrieren):

Beschleunigung der Time-to-Protection

Dank unserer einzigartigen Runtime-Access-Protection (RAP)-Technologie integriert sich Silverfort nahtlos in bestehende Authentifizierungsabläufe, sodass Organisationen:

- → alle privilegierten Identitäten zügig einführen und die Bereitstellungszeiten von Jahren auf Wochen verkürzen können
- → Authentifizierungen über Kerberos, NTLM, LDAP, RDP, PowerShell, PsExec, SSH und mehr überwachen und auswerten können
- → Richtlinien bereits bei der Authentifizierung anwenden können, bevor der Zugriff gewährt wird

Discover (Entdecken):

Vollständige Transparenz über alle privilegierten Identitäten

Silverfort erkennt kontinuierlich:

- → Domänen-, Cloud-, Server- und Applikationsadmins
- → Break-Glass-Konten
- → Service Accounts und andere NHIs
- → KI-Agenten mit Zugriff auf privilegierte Ressourcen

Die Erkennung basiert sowohl auf der Konfiguration als auch auf *dem tatsächlichen Verhalten* und macht manuelles Zusammenführen von Logs sowie einmalige Erkennungsprojekte überflüssig.

Enforce (Durchsetzen):

Anwendung von Kontrollen zur Laufzeit auf Admins und Service Accounts

Für privilegierte Authentifizierungen kann Silverfort:

- → die Zwei-Faktor-Authentifizierung (MFA) für menschliche Administratoren und bei Admintools (PowerShell, PsExec, WMI, RDP, SSH usw.) durchsetzen
- → JIT-Zugriff und Zero Standing Privilege für Admins umsetzen
- → Virtual Fencing anwenden, um Service Accounts auf bekannte Hosts, Ziele und Verhaltensweisen zu beschränken
- → riskante bereichsübergreifende oder laterale Bewegungsversuche zur Laufzeit blockieren oder hinterfragen

Da die Durchsetzung bereits bei der Authentifizierung erfolgt, sind keine Workflows zur Überprüfung von Anmeldedaten, keine neuen Proxys und keine Routenänderungen erforderlich.

Act (Handeln):

Identitätsbedrohungen sofort erkennen und eindämmen

Mithilfe kontinuierlicher Authentifizierungsdaten erkennt Silverfort den Diebstahl von Zugangsdaten, deren Missbrauch sowie ungewöhnliches Verhalten bei der Nutzung privilegierter Zugriffsrechte. Noch bevor ein Angreifer privilegierten Zugriff für böswillige Zwecke nutzen kann, reagiert die Plattform auf verdächtige Aktivitäten und:

- → blockiert die Anfrage
- → eskaliert MFA
- → schränkt Zugriffspfade und Ebenen ein

Lightweight (Schlank):

Bereitstellung und Vereinfachung des täglichen Betriebs

Der Ansatz von Silverfort macht komplexe Änderungen an der Infrastruktur überflüssig, sodass Sie von folgenden Vorteilen profitieren:

- → schnelle Bereitstellung und einfacher Betrieb
- → keine Neuentwicklung von Apps
- → keine mehrjährigen Vault-Implementierungspläne
- → schnelle Time-to-Value und nachweisbarer ROI

Unternehmen schaffen es in der Regel innerhalb weniger Tage, von der ersten Anbindung bis hin zu wirksamen Kontrollen für privilegierten Zugriff zu gelangen, und das auch in großen Unternehmensumgebungen.

Wie die Identity-Security-Plattform von Silverfort Schutz und Risikoreduzierung auf privilegierte Zugriffe skaliert

Wichtigste Funktionen:

Identitäten entdecken und Risiken erkennen dank umfassender Transparenz und umsetzbarer Erkenntnisse:

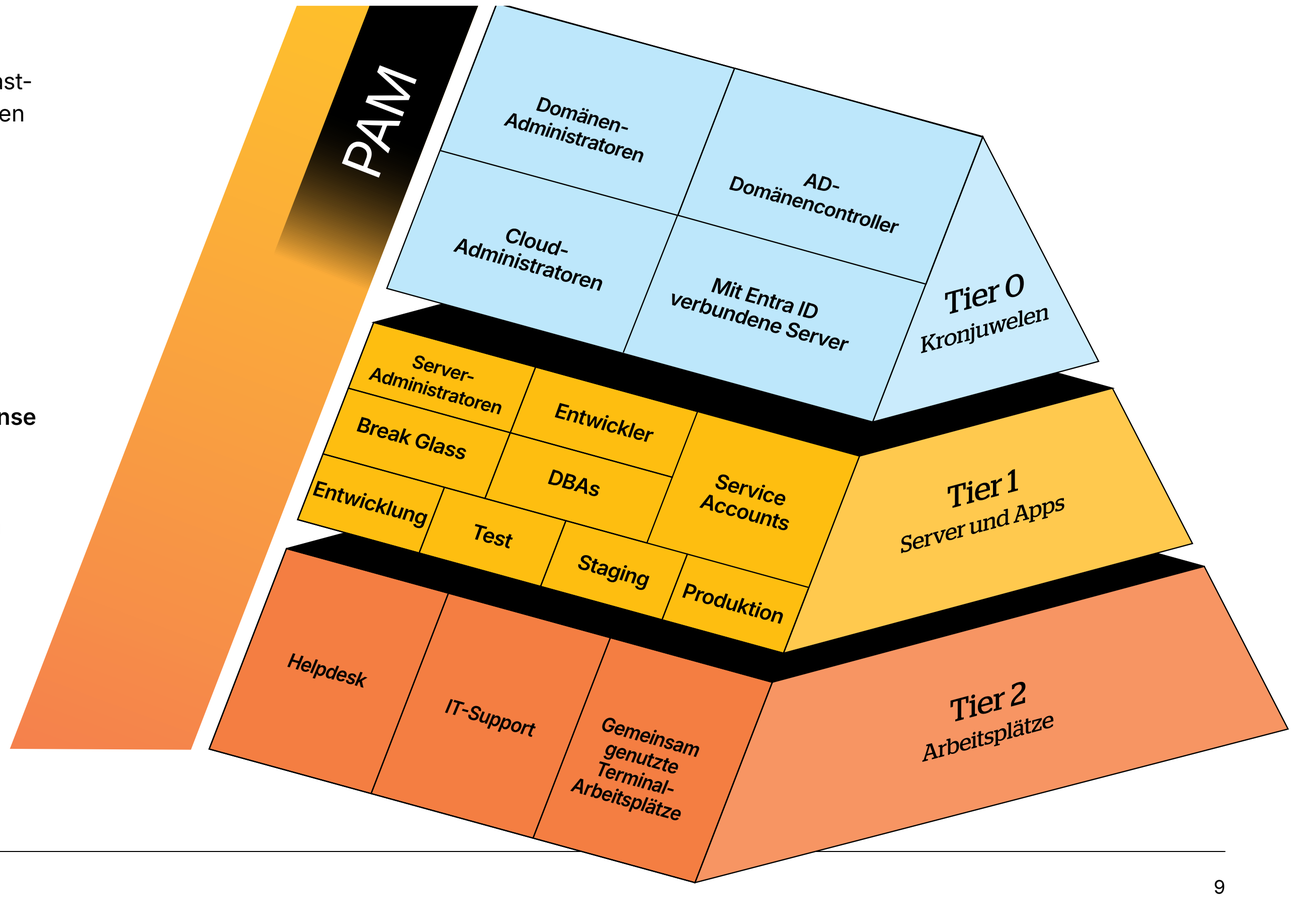
- → **Vollständige Transparenz** – Automatische Erfassung aller privilegierten Identitäten, menschlich und nicht-menschlich, auf der Grundlage von Konfigurationsdaten und tatsächlichem Authentifizierungsverhalten, um sicherzustellen, dass kein privilegiertes Konto ungeschützt bleibt
- → **Access Intelligence** – Analyse der Authentifizierungsaktivitäten, um riskantes Verhalten und überflüssige Berechtigungen zu identifizieren, die reduziert werden sollten
- → **Identity Security Posture Management (ISPM)** – Erkennen, Erfassen und Priorisieren von Sicherheitsrisiken und Mängeln im Bereich der Identity Security

Privilegierte Zugriffe mit Runtime Access Protection steuern:

- → **MFA auf Admin-Tools** – und Protokolle wie PowerShell, PsExec, WMI und RDP ausweiten
- → **Authentifizierungs-Firewall** – Zero-Trust-Zugriffskontrollen, Tier-Segmentierung und Least-Privilege-Richtlinien durchsetzen, um unbefugten privilegierten Zugriff zu verhindern
- → **Just-in-Time (JIT)-Zugriff** – Dauerhafte Zugriffsrechte verhindern, indem privilegierter Zugriff nur bei Bedarf gewährt wird
- → **Virtual Fencing** – Service-Account-Aktivitäten auf bekannte Quellen und Ziele beschränken und unbefugte Nutzung verhindern

Angriffe mit Identity Threat Detection and Response (ITDR) frühzeitig erkennen und stoppen:

- → **Identity Threat Detection and Response** – Identitätsbasierte Angriffe in Echtzeit erkennen und stoppen



Unabhängig davon, ob Sie PAM einsetzen oder nicht: Silverfort stellt sicher, dass alle Ihre privilegierten Identitäten geschützt sind.

Vaultless PAM ist nicht gegen Vaults gerichtet, sondern ein rein ergebnisorientierter Ansatz. Wir wissen, dass unterschiedliche Umgebungen an unterschiedlichen Punkten ihrer PAM-Entwicklung stehen. Deshalb unterstützen wir mehrere Modelle, um privilegierte Identitäten unabhängig von der bestehenden Architektur zu schützen.

MIT PAM:

Erweitern Sie Ihre Abdeckung und maximieren Sie Ihre bestehende Investition

Viele Organisationen führen PAM ein, haben aber Schwierigkeiten, die Abdeckung auf alle privilegierten Identitäten auszuweiten. Silverfort erweitert bestehende PAM-Implementierungen, indem es als Ebene zur Durchsetzung von Sicherheitsmaßnahmen im gesamten Authentifizierungsprozess fungiert.

Auf diese Weise können Unternehmen privilegierte Identitäten schützen, die sich außerhalb des Vaults befinden, darunter Konten, die noch nicht integriert wurden, oder Service Accounts, bei denen keine Passwortrotation durchgeführt werden kann. Indem Silverfort den Schutz über den Vault hinaus ausweitet, unterstützt das Unternehmen Organisationen dabei, eine lückenlose Abdeckung zu erreichen und gleichzeitig den operativen Aufwand für die Einbindung jedes einzelnen Kontos in PAM zu reduzieren.

Passen Sie Umfang, Aufwand und Investitionen für Ihr PAM je nach Ihrem Bedarf an. Schützen Sie nur das, was wirklich benötigt wird, und deaktivieren Sie ungenutzte Lizenzen.

OHNE PAM:

Sichern Sie privilegierte Zugriffe ab, ohne einen Vault bereitzustellen

Für Organisationen ohne bestehende PAM-Bereitstellung – entweder weil PAM nie implementiert oder weil ein früherer Rollout abgebrochen wurde – kann Silverfort als primäre Steuerungsebene zur Absicherung privilegierter Identitäten dienen.

Die Plattform erkennt privilegierte Identitäten automatisch, wendet Sicherheitsmaßnahmen zur Laufzeit an, wie beispielsweise MFA, Just-in-Time-Zugriff und Zugriffsbeschränkungen, und erkennt identitätsbasierte Bedrohungen wie den Missbrauch von Anmeldedaten, die Ausweitung von Berechtigungen und Lateral-Movement-Versuche.

Sichern Sie privilegierten Zugriff in der gesamten Umgebung, ohne eine Vault-Infrastruktur bereitstellen oder komplexe Onboarding-Projekte durchführen zu müssen.

Sie evaluieren PAM-Lösungen?

Nachfolgend finden Sie eine komprimierte Checkliste, die auf einem empfohlenen Framework für Ausschreibungen im Bereich der Absicherung privilegierter Zugriffe basiert – damit Sie sicher sein können, dass Sie genau die Lösungen erwerben, die Ihr Unternehmen benötigt.

Eine Lösung, die in diesen Bereichen stark abschneidet, liefert genau das, was moderne Umgebungen benötigen: vollständige Transparenz, breite Abdeckung und Echtzeitkontrolle über privilegierte Zugriffe.

Leitfaden herunterladen

Holen Sie sich den vollständigen Identity Security Buyer's Guide und die RFP-Checkliste

Integration und Abdeckung

- ☐ Lässt sich die Lösung ohne Agenten oder Proxys direkt in Active Directory und große Cloud-IdPs integrieren?
- ☐ Erfasst sie alle Authentifizierungsabläufe, einschließlich CLI, RDP, SSH und Legacy-Protokollen?
- ☐ Kann sie menschliche Admins, Service Accounts, NHIs und KI-Agenten On-Prem und in der Cloud abdecken?
- ☐ Lässt sie sich auf die gesamte Umgebung skalieren und kann sie alle privilegierten Konten abdecken?
- ☐ Unterstützt sie problemlos die Zunahme privilegierter Benutzer und Konten, wenn die Umgebung erweitert wird?

Erkennung und Analytik

- ☐ Erkennt sie automatisch alle privilegierten Identitäten (menschlich und nicht-menschlich) über alle Systeme, Anwendungen und Umgebungen hinweg?
- ☐ Erkennt sie privilegierte Identitäten auf Basis der tatsächlichen Nutzung und nicht nur statischer Konfigurationen?
- ☐ Kann sie Shadow-Admins und privilegierte Konten außerhalb des Vaults erkennen?
- ☐ Erfasst sie privilegierte Pfade und Latera-Movement-Risiken?
- ☐ Erkennt sie inaktive und ungenutzte privilegierte Konten und schlägt sie Maßnahmen zur Behebung vor?

Durchsetzung von Kontrollen zur Laufzeit

- ☐ Kann sie die MFA für native Admin-Tools und den Zugriff auf die Infrastruktur (nicht nur für Webanwendungen) durchsetzen?
- ☐ Unterstützt sie Just-in-Time-Rechteerweiterung und Zero Standing Privileges?
- ☐ Kann sie das Prinzip der geringstmöglichen Berechtigungen durchsetzen und den Zugriff einschränken, um unbefugte Aktivitäten zu verhindern?
- ☐ Kann sie Zugriffsebenen-Segmentierung für Admins durchsetzen?
- ☐ Kann sie Virtual Fencing für Service Accounts durchsetzen?

Bedrohungserkennung und Reaktion

- ☐ Bietet sie ITDR-Funktionen für privilegierte Identitäten, um Missbrauch, laterale Bewegungen und die Ausweitung von Berechtigungen in Echtzeit zu erkennen?
- ☐ Kann sie automatisch auf Bedrohungen reagieren (blockieren, abfragen, einschränken), ohne dass ein manueller Eingriff erforderlich ist?

Einfachheit und schnelle Rentabilität

- ☐ Wie lange dauern die Bereitstellung und die Einführung in der Regel?
- ☐ Wie lange dauert es in der Regel von der ersten Bereitstellung bis zu einem wirksamen Schutz vor unbefugtem Zugriff?
- ☐ Sind dafür Agenten, eine Neuprogrammierung der Anwendungen oder umfangreiche Netzwerkänderungen erforderlich?
- ☐ Welche Auswirkungen hat die Lösung auf den Betrieb für Admins, DevOps und Applikationsverantwortliche?

Silverfort: Identity Security, wie sie sein sollte

→ Vollständige Transparenz über den hybriden IAM-Stack

Sichern Sie sich die Identity Security, die zu Ihnen passt – mit umfassender Transparenz und Schutz für alle Identitäten und Umgebungen: ob menschlich, KI und maschinell, On-Prem, in der Cloud und in Hybridumgebungen.

→ Sicherheit an erster Stelle dank Laufzeitüberwachung

Vereinfachen und vereinheitlichen Sie den Identitätsschutz für alle Identitätstypen an einem Ort mit der patentierten Runtime-Access-Protection (RAP)-Technologie von Silverfort.

→ Nie wieder Änderungen an Ihren Systemen und Apps – und nie wieder schwierige Gespräche

Silverfort lässt sich direkt in Ihre bestehende IAM-Infrastruktur integrieren, sodass Ihre Teams weder Agenten auf jedem Rechner installieren noch Anwendungen neu programmieren, umgestalten oder ändern müssen. Keine Unterbrechungen, keine langwierigen Rollouts.

→ Schützen Sie Systeme, die zuvor nicht geschützt werden konnten

Weiten Sie den Schutz auf bisher nicht schützbare Ressourcen aus, darunter Legacy-Systeme, Befehlszeilenschnittstellen, Dateifreigaben, IT-/OT-Infrastruktur, Air-Gapped-Umgebungen und vieles mehr.

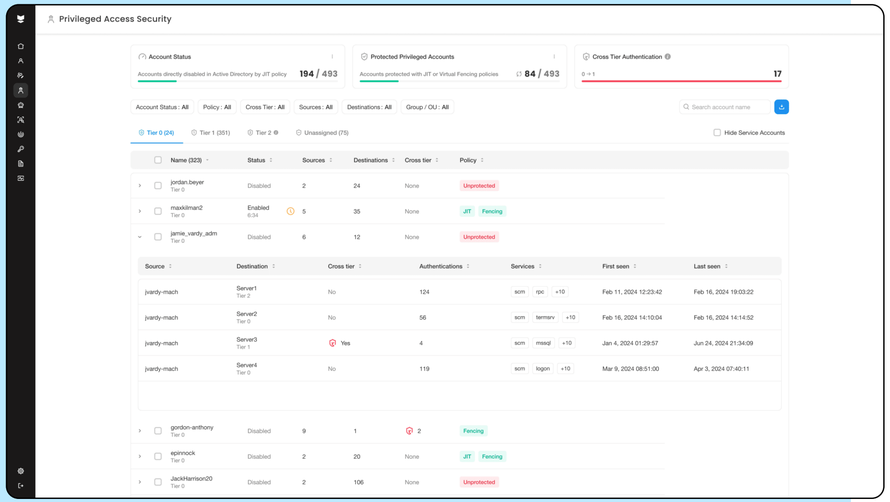
In Aktion erleben

Die meisten Unternehmen brauchen nicht noch ein weiteres mehrjähriges Identitätsprojekt.

Sie brauchen einen schnellen, einfachen und pragmatischen Weg zu besserem Schutz für privilegierte Zugriffe.

Entdecken Sie unsere interaktiven Demos oder buchen Sie ein persönliches Meeting, um zu sehen, wie Silverfort privilegierte Identitäten in all Ihren Umgebungen schützt.

Produkttour **Demo buchen**



Über Silverfort

Mehr als 1.000 Unternehmen vertrauen auf Silverfort, um alle Aspekte der Identity Security zu gewährleisten. Wir bieten eine End-to-End-Identity-Security, die sich einfach implementieren lässt und den Geschäftsbetrieb nicht beeinträchtigt, sodass Sie ohne großen Aufwand ein höheres Sicherheitsniveau erreichen.