Extending Identity Protection Beyond the Perimeter

MFA, Securing High Risk Access and Service Account Protection

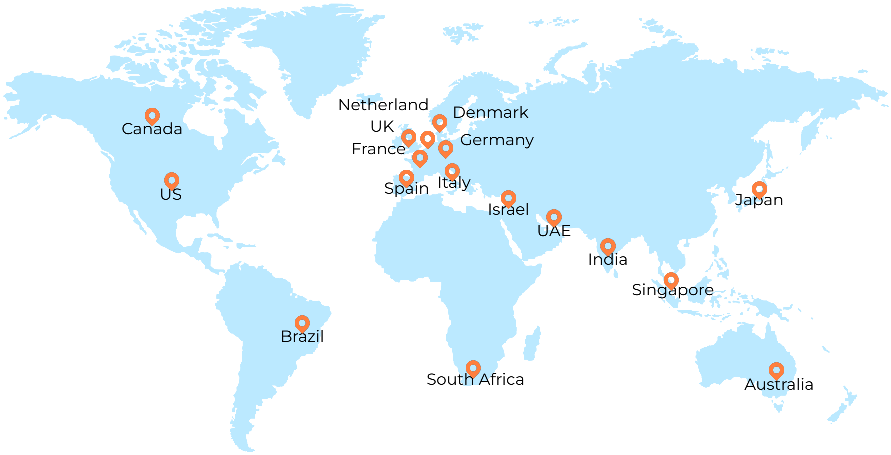
Tomáš Jilík
Regional Sales Manager
tomas.jilik@silverfort.com

Paweł Jakacki
Sales Engineer CEE
pawel.jakacki@silverfort.com

Identity security done right.

Silverfort

Silverfort — The Identity Security Platform Company



2024 Microsoft Partner of the Year Award

Microsoft

2024 Microsoft Partner of the Year

Winner

Microsoft is proud to recognize

SILVERFORT
Microsoft for Startups Award

With gratitude,

Nicole Dezen
Chief Partner Officer and Corporate Vice President
Global Partner Solutions
Microsoft Corporation

Silverfort ranks 4.8 out of 5 stars

★★★ Gartner peerinsights™

2025 Fast Company Most Innovative Companies List

FAST COMPANY Most Innovative Companies 2025

Silverfort customers 1,000+

Funding (Series D) $222m

Employees around the world 500+

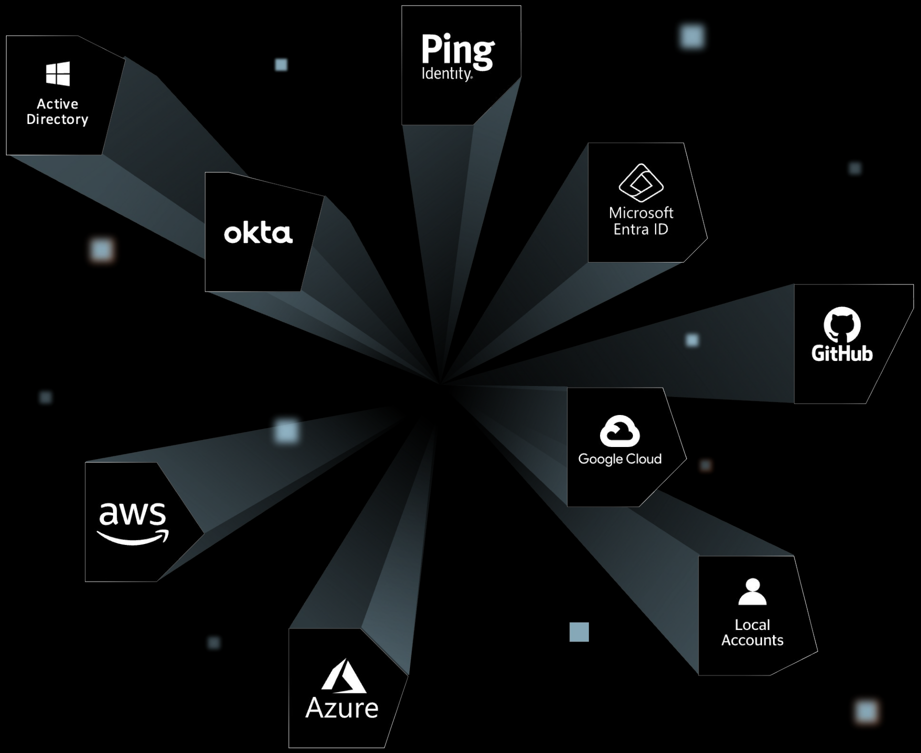
gm NVIDIA AIRBUS BHP Johnson&Johnson TESCO AAA

Key Technology Partnerships

Microsoft
okta
Ping Identity
splunk>
cisco
CROWDSTRIKE
yubico
aws
servicenow
HYPR
DUO
paloalto NETWORKS
RSA
Check Point SOFTWARE TECHNOLOGIES LTD.
SentinelOne

The IAM infrastructure in most companies is hybrid and fragmented.

As a result, identity security controls work in silos, with inconsistent visibility and enforcement, redundant costs, and bad user experience.



Current solutions also leave critical identity security blind spots.

AD and Cloud identity security blind spots

Lack of visibility, bad configurations, vulnerable protocols, risky accounts, etc.

Systems that don't support MFA

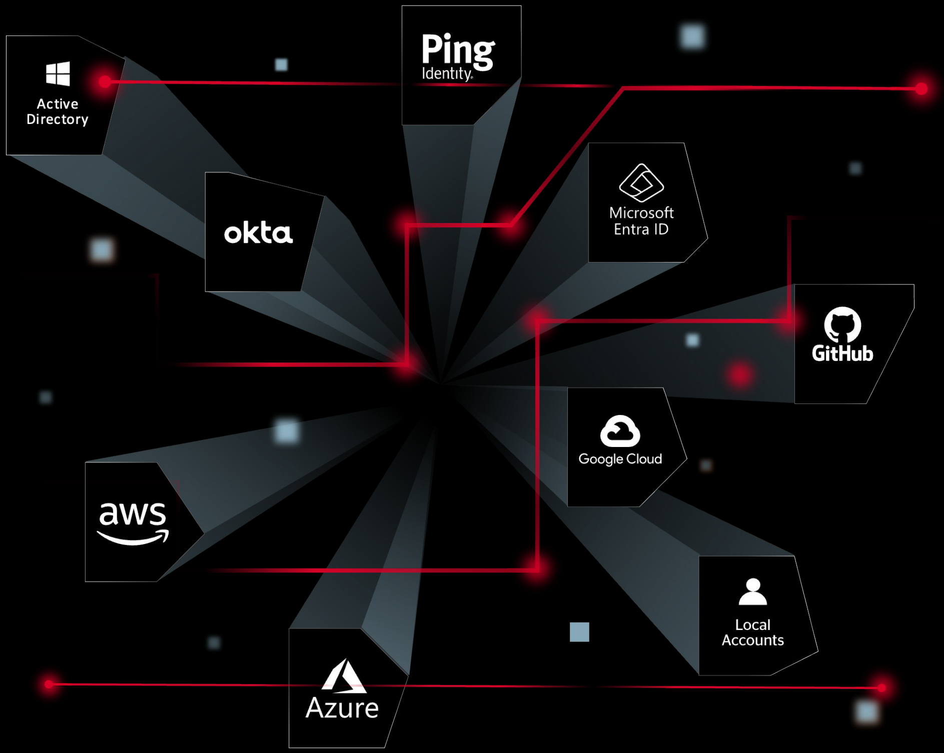
Legacy systems, command-line interfaces (e.g., PsExec), IT/OT infrastructure and more.

Service accounts and other NHIs

Very difficult to map them, understand where they are being used, and protect them at scale.

Ineffective controls for privileged access

Traditional PAM is complex to implement and use, expensive, and easily bypassed by admins and attackers.



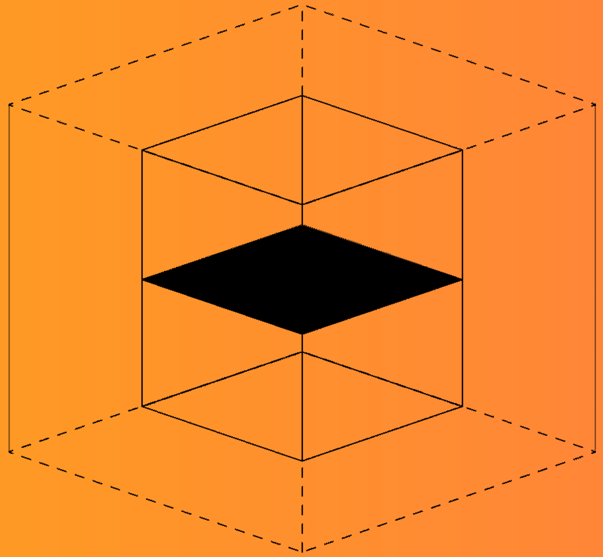
THE SILVERFORT IDENTITY SECURITY PLATFORM

Secure every dimension of identity.

Discover
Every identity across every environment—from one platform.

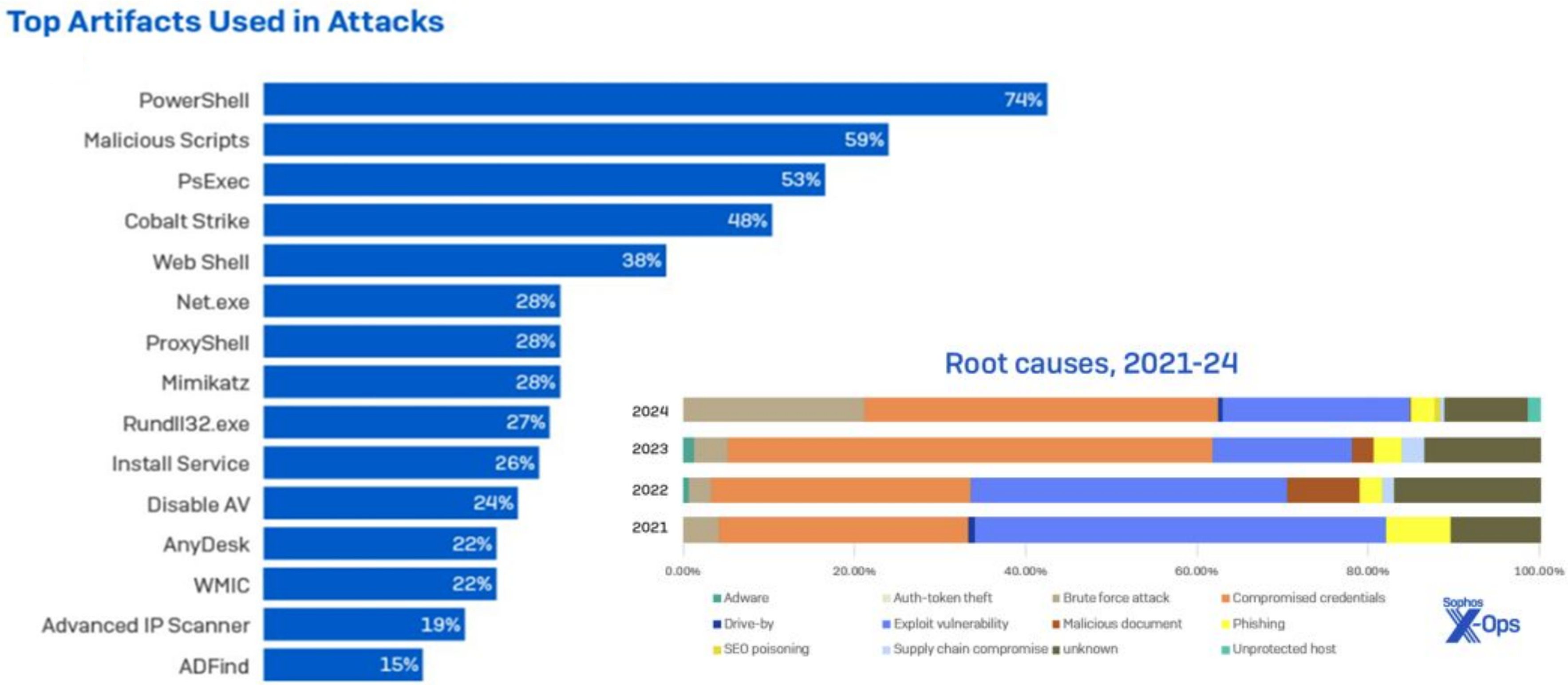
Analyze
All access attempts and uncover exposures and threats in real time.

Enforce
Security controls inline to prevent attacks and address compliance gaps, even on systems that couldn't be protected before.



PAWEL’s PART…

“Impossible to MFA” low level CLI interfaces are top attack vectors



*Source: Sophos, The Adversary Playbook

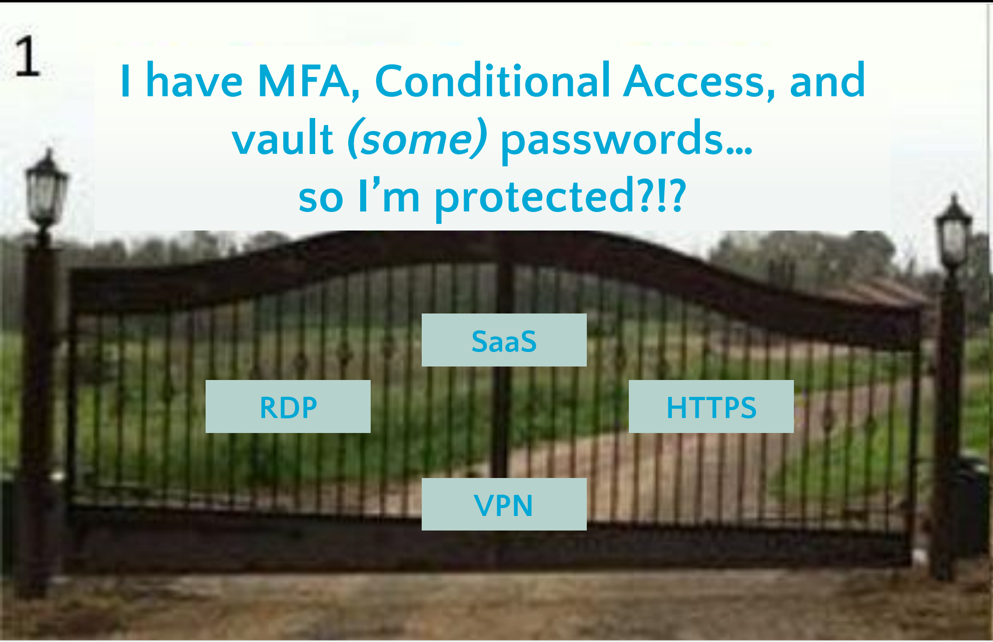
90% of cyber incidents investigated involve **Active Directory (AD)** in one way or another*

MFA reduces account compromise by **99.9%****

95% of companies require MFA…**so what's the problem**? Most things against AD don't support MFA or have to do various integrations with agents and attackers know this.

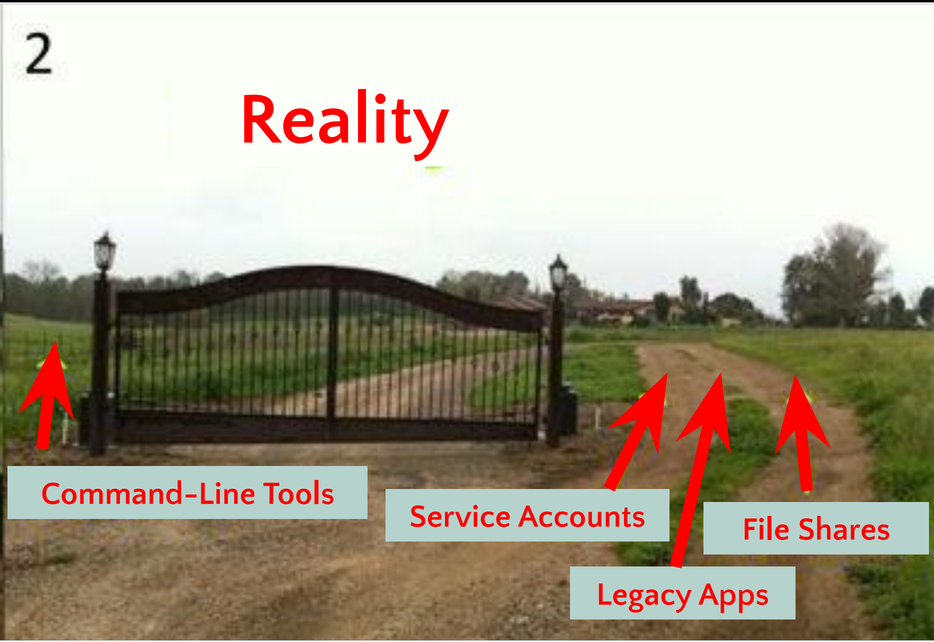
Source:
* Mandiant
** Microsoft

Attackers know about these gaps, these blind spots, and are leveraging them in over 80% of all data breaches to easily bypass the existing protection



1

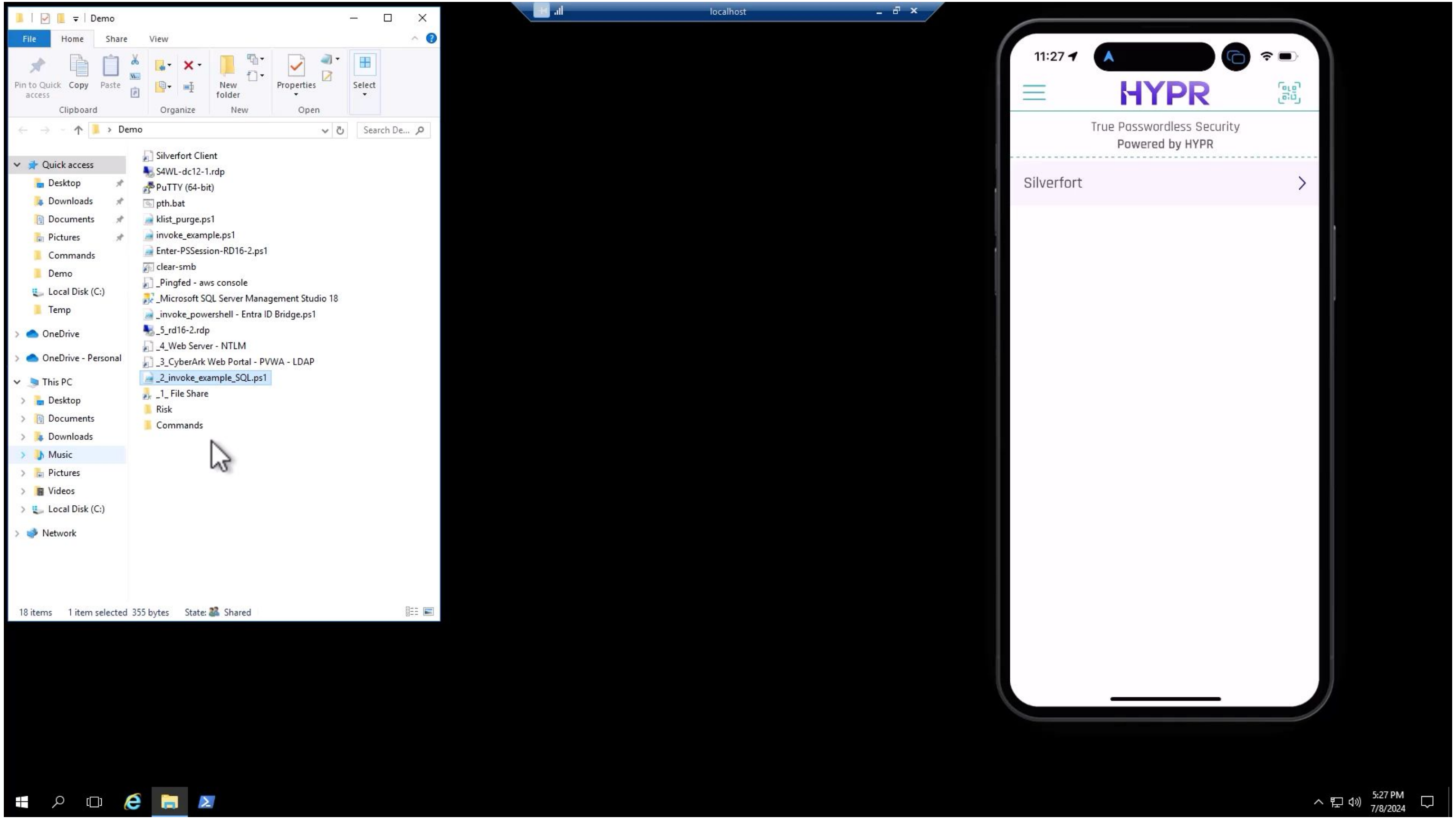
I have MFA, Conditional Access, and vault *(some)* passwords… so I'm protected?!?



2

Reality

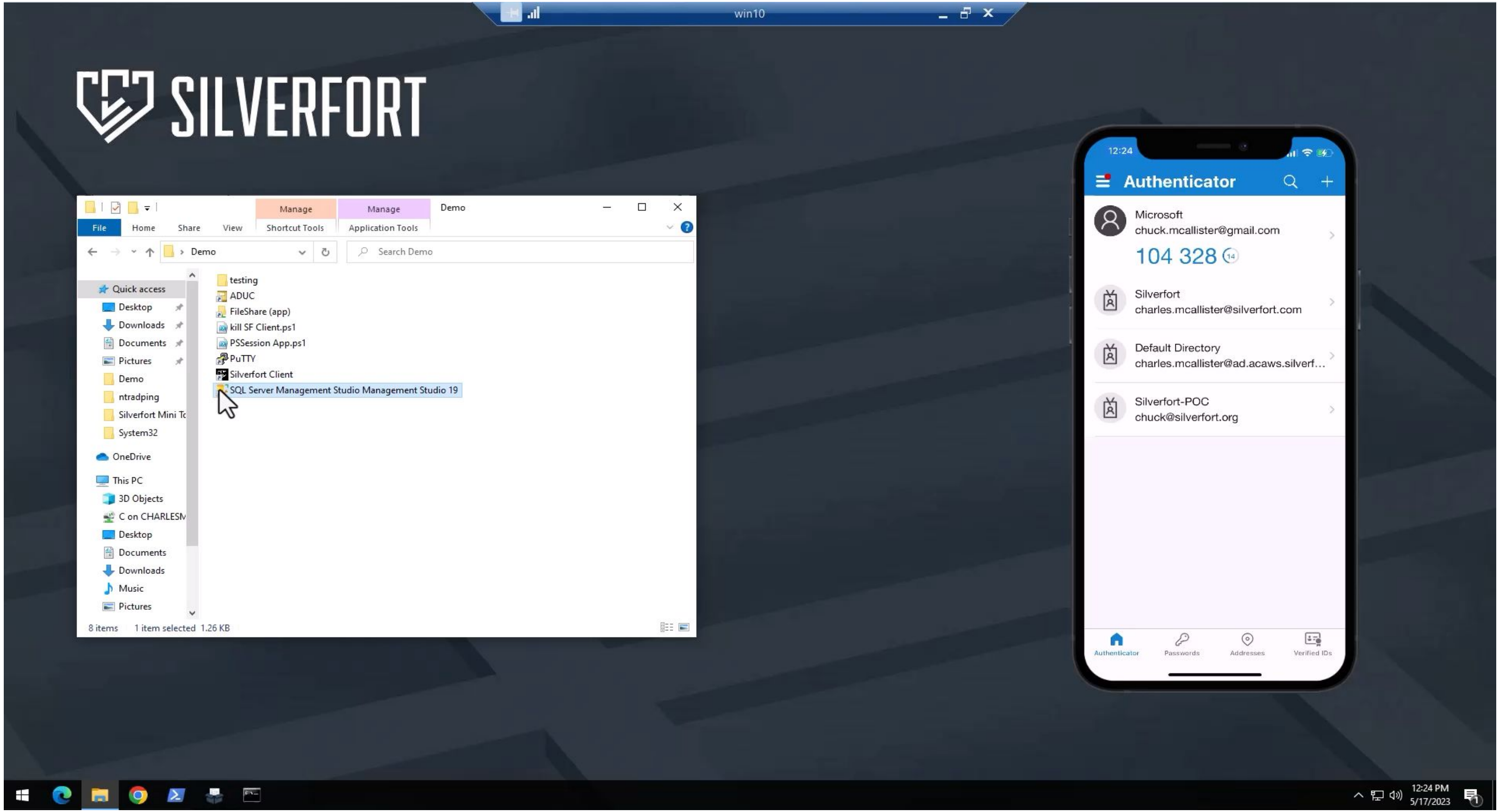
DEMO: Extending MFA to PowerShell



Silverfort Client
S4WL-dc12-1.rdp
PuTTY (64-bit)
pth.bat
klist_purge.ps1
invoke_example.ps1
Enter-PSSession-RD16-2.ps1
clear-smb
_Pingfed - aws console
_Microsoft SQL Server Management Studio 18
_invoke_powershell - Entra ID Bridge.ps1
_5_rd16-2.rdp
_4_Web Server - NTLM
_3_CyberArk Web Portal - PVWA - LDAP
_2_invoke_example_SQL.ps1
_1_ File Share
Risk
Commands

18 items 1 item selected 355 bytes State: Shared

DEMO: Extending MFA to SQL server



Demo

- testing
- ADUC
- FileShare (app)
- kill SF Client.ps1
- PSSession App.ps1
- PuTTY
- Silverfort Client
- SQL Server Management Studio Management Studio 19

8 items 1 item selected 1.26 KB

12:24

Authenticator

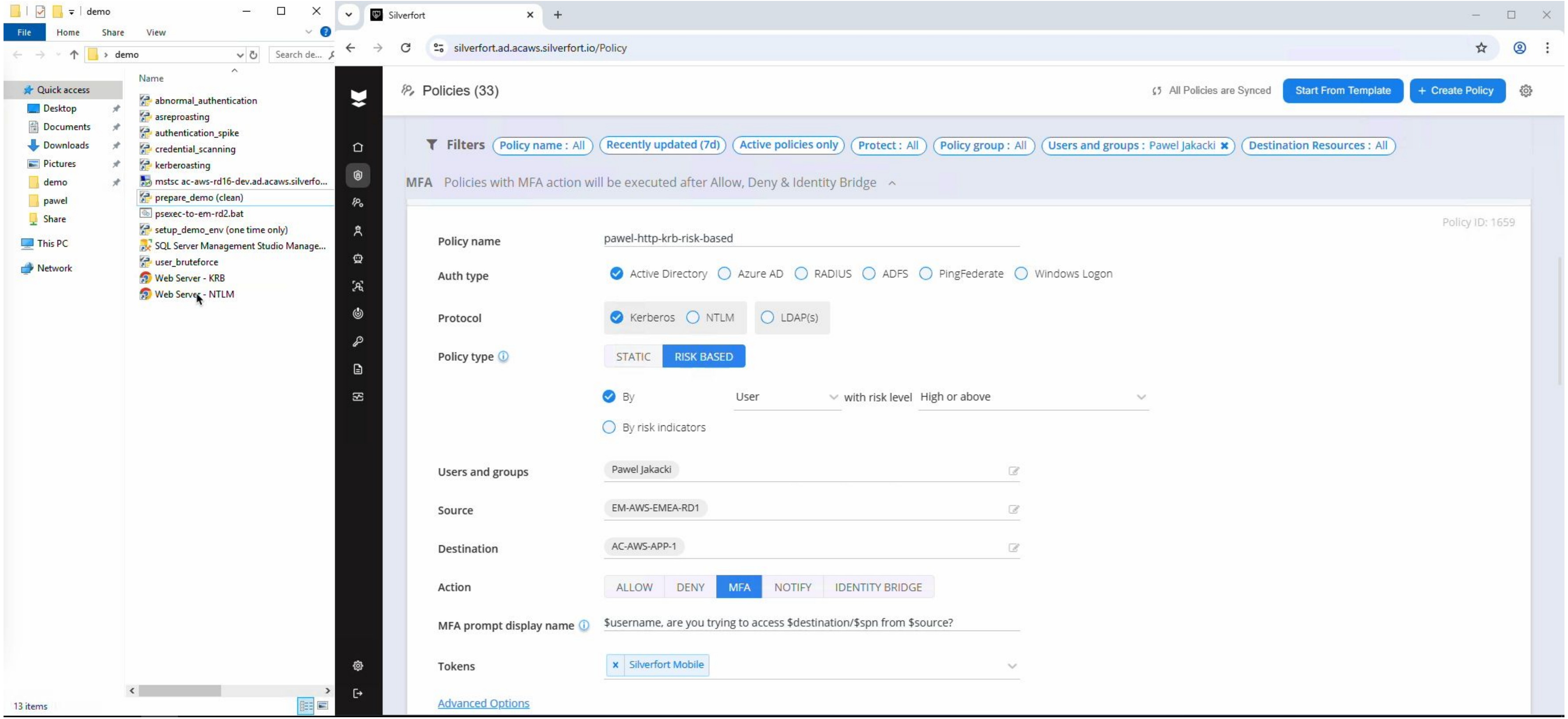
Microsoft
chuck.mcallister@gmail.com
104 328 14

Silverfort
charles.mcallister@silverfort.com

Default Directory
charles.mcallister@ad.acaws.silverf...

Silverfort-POC
chuck@silverfort.org

How to prevent lateral movement with Risk Based Policies?



Name

- abnormal_authentication
- asreproasting
- authentication_spike
- credential_scanning
- kerberoasting
- mstsc ac-aws-rd16-dev.ad.acaws.silverfo...
- prepare_demo (clean)
- psexec-to-em-rd2.bat
- setup_demo_env (one time only)
- SQL Server Management Studio Manage...
- user_bruteforce
- Web Server - KRB
- Web Server - NTLM

Policies (33)

Filters: Policy name : All | Recently updated (7d) | Active policies only | Protect : All | Policy group : All | Users and groups : Pawel Jakacki | Destination Resources : All

MFA Policies with MFA action will be executed after Allow, Deny & Identity Bridge

Policy ID: 1659

Policy name: pawel-http-krb-risk-based

Auth type: ☑ Active Directory ○ Azure AD ○ RADIUS ○ ADFS ○ PingFederate ○ Windows Logon

Protocol: ☑ Kerberos ○ NTLM ○ LDAP(s)

Policy type: STATIC [✓ RISK BASED]

☑ By User with risk level High or above

○ By risk indicators

Users and groups: Pawel Jakacki

Source: EM-AWS-EMEA-RD1

Destination: AC-AWS-APP-1

Action: ALLOW DENY [✓ MFA] NOTIFY IDENTITY BRIDGE

MFA prompt display name: $username, are you trying to access $destination/$spn from $source?

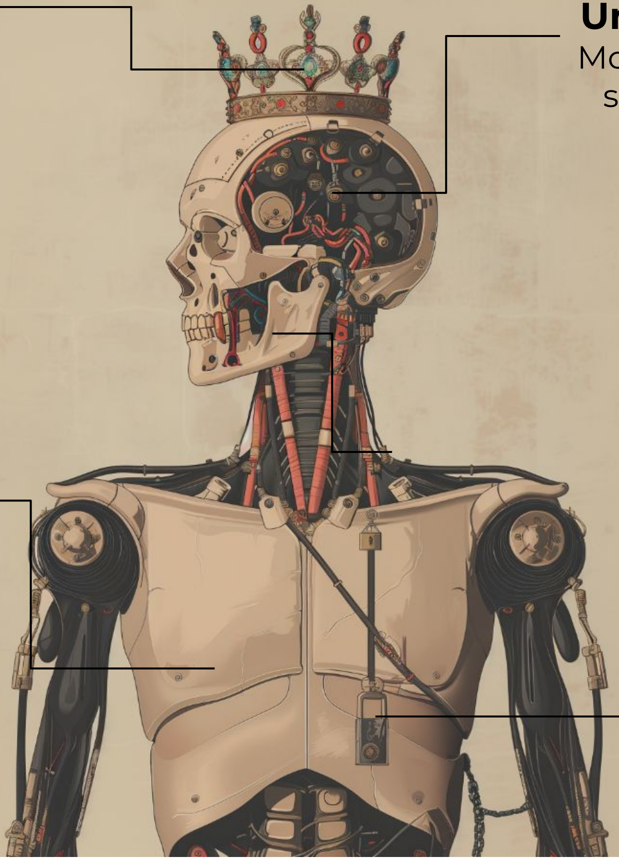
Tokens: Silverfort Mobile

Advanced Options

What are service accounts, and why are they so difficult to secure?

Highly privileged:
Can cause large damage
when compromised

Unknown Dependencies:
Most companies don’t know all
service accounts and where
they are used



Difficult to Protect:
Rotating their passwords
often breaks applications

Regularly Misused:
Service accounts are often used
by admins outside of their
intended purpose

Other common issues and bad practicies

Using personal admin accounts to run applications and scripts, instead of creating a service account

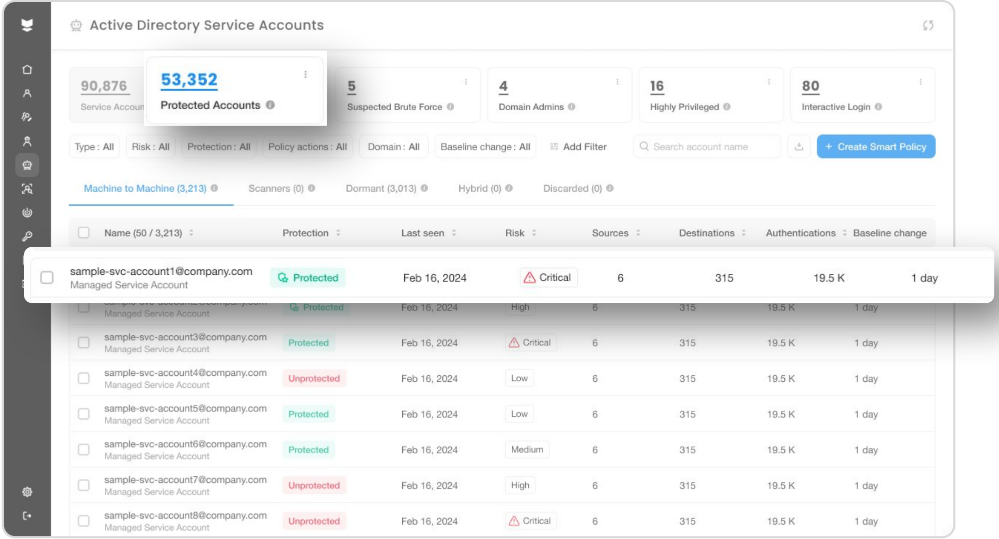
Admins using service accounts manually for their own needs, instead of asking for privileges

Reusing the same service account across many systems, and losing track of where it's being used

Providing service accounts with high privileges even if they only need to do a specific task

Silverfort’s Service Accounts Security

- **Automatically discover** all service accounts within your Active Directory
- **Prioritize & categorize** each service account based on its privileges and multiple other risk indicators
- **Protect with ‘Virtual Fencing’** to restrict access solely to intended sources and destinations, significantly reducing the risk
- **Automate this process** to secure service accounts at scale using CMDB (e.g. ServiceNow) integration and Smart Policy functionality



Active Directory Service Accounts

90,876 Service Accoun

53,352 Protected Accounts

5 Suspected Brute Force

4 Domain Admins

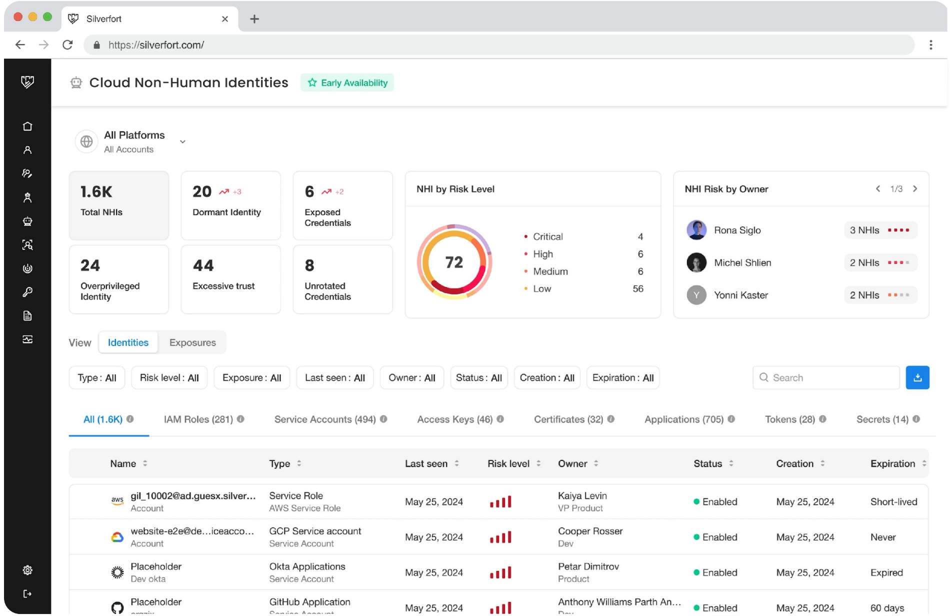
16 Highly Privileged

80 Interactive Login

Name (50 / 3,213)	Protection	Last seen	Risk	Sources	Destinations	Authentications	Baseline change
sample-svc-account1@company.com Managed Service Account	Protected	Feb 16, 2024	Critical	6	315	19.5 K	1 day
Managed Service Account	Protected	Feb 16, 2024	High	6	315	19.5 K	1 day
sample-svc-account3@company.com Managed Service Account	Protected	Feb 16, 2024	Critical	6	315	19.5 K	1 day
sample-svc-account4@company.com Managed Service Account	Unprotected	Feb 16, 2024	Low	6	315	19.5 K	1 day
sample-svc-account5@company.com Managed Service Account	Protected	Feb 16, 2024	Low	6	315	19.5 K	1 day
sample-svc-account6@company.com Managed Service Account	Protected	Feb 16, 2024	Medium	6	315	19.5 K	1 day
sample-svc-account7@company.com Managed Service Account	Unprotected	Feb 16, 2024	High	6	315	19.5 K	1 day
sample-svc-account8@company.com Managed Service Account	Unprotected	Feb 16, 2024	Critical	6	315	19.5 K	1 day

Silverfort's Cloud NHI Security

- **Discover and classify** different types of Non-Human Identities across IdPs, cloud infrastructure and SaaS applications
- **Gain visibility into effective privileges** of your entire NHI inventory and reduce unnecessary permissions
- **Prioritize and mitigate the most critical exposures** to minimize your attack surface and address compliance gaps
- **Remediate** security & lifecycle gaps by **identifying account ownership** and actionable recommendations



Silverfort

https://silverfort.com/

Cloud Non-Human Identities ☆ Early Availability

All Platforms
All Accounts

1.6K	Total NHIs
20 +3	Dormant Identity
6 +2	Exposed Credentials
24	Overprivileged Identity
44	Excessive trust
8	Unrotated Credentials

NHI by Risk Level

72

● Critical	4
● High	6
● Medium	6
● Low	56

NHI Risk by Owner < 1/3 >

Rona Siglo	3 NHIs
Michel Shlien	2 NHIs
Yonni Kaster	2 NHIs

View: Identities | Exposures

Type : All | Risk level : All | Exposure : All | Last seen : All | Owner : All | Status : All | Creation : All | Expiration : All | Search

All (1.6K) | IAM Roles (281) | Service Accounts (494) | Access Keys (46) | Certificates (32) | Applications (705) | Tokens (28) | Secrets (14)

Name	Type	Last seen	Risk level	Owner	Status	Creation	Expiration
gil_10002@ad.guesx.silver... Account	Service Role AWS Service Role	May 25, 2024	▮▮▮▮	Kaiya Levin VP Product	● Enabled	May 25, 2024	Short-lived
website-e2e@de…iceacco... Account	GCP Service account Service Account	May 25, 2024	▮▮▮▮	Cooper Rosser Dev	● Enabled	May 25, 2024	Never
Placeholder Dev okta	Okta Applications Service Account	May 25, 2024	▮▮▮▮	Petar Dimitrov Product	● Enabled	May 25, 2024	Expired
Placeholder	GitHub Application	May 25, 2024	▮▮▮▮	Anthony Williams Parth An…	● Enabled	May 25, 2024	60 days

How it works:
Runtime Access Protection (RAP)

1 User requests access from the IAM infrastructure

2 IAM infrastructure forwards request to Silverfort using patented RAP technology

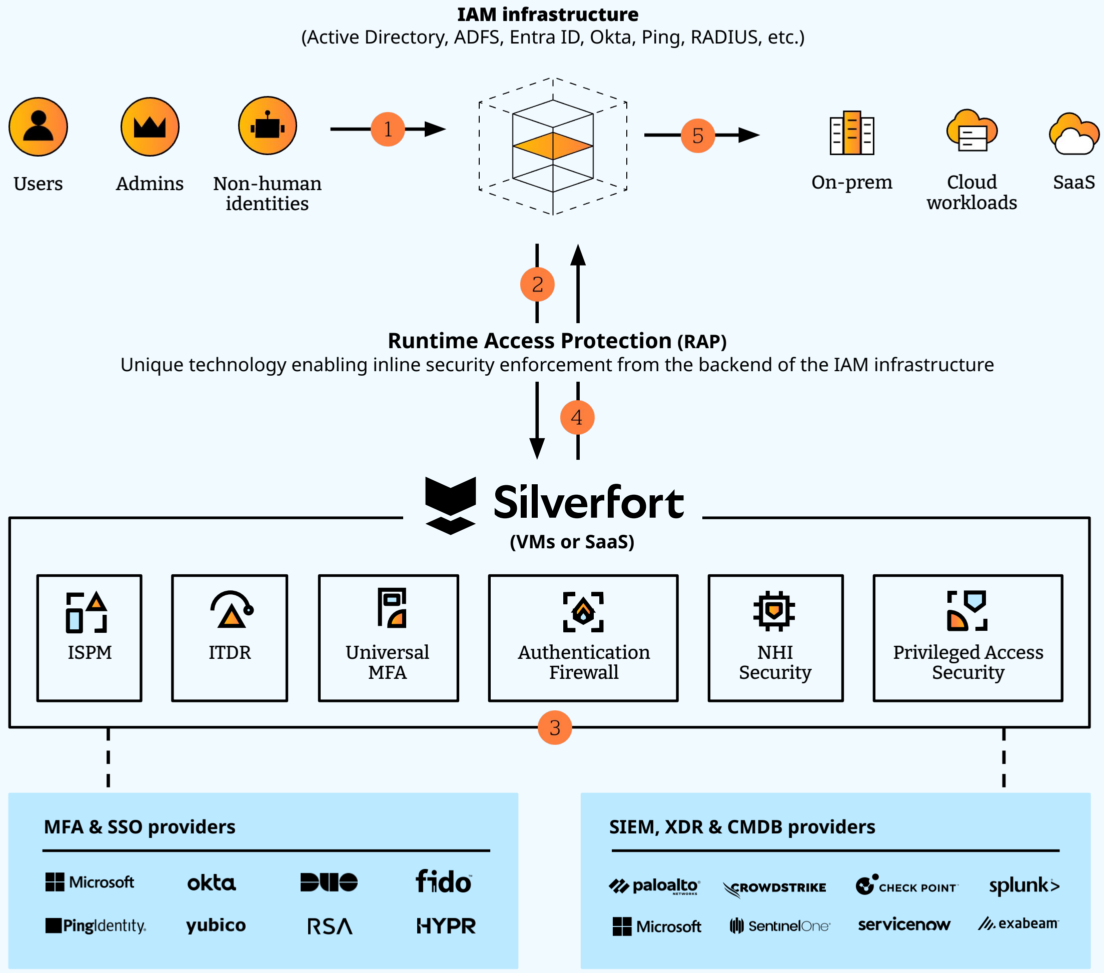
3 Silverfort analyzes risk and triggers inline security controls if needed

4 Silverfort returns security verdict to IAM infrastructure

5 IAM infrastructure grants or denies access

No proxies. No application changes. No change to user workflows.

Silverfort



IAM infrastructure
(Active Directory, ADFS, Entra ID, Okta, Ping, RADIUS, etc.)

Runtime Access Protection (RAP)
Unique technology enabling inline security enforcement from the backend of the IAM infrastructure

Silverfort
(VMs or SaaS)

MFA & SSO providers

SIEM, XDR & CMDB providers

Discover exposures, analyze threats and enforce security controls in real time with Runtime Access Protection (RAP).

ISPM	ITDR	Universal MFA	Authentication Firewall	NHI Security	Privileged Access Security
Uncover, map and analyze identity security exposures	Detect and respond to attacks in real time	Extend Multi-Factor Authentication to any system	Stop unauthorized access with Zero Trust policies	Discover and protect non-human identities	Identify then enforce least privilege & Just-in-Time access