Silverfort for Incident Response

Identity security done right.

Silverfort

Table of contents

Silverfort — The Identity Security Platform Company

2024 Microsoft Partner of the Year Award

Silverfort ranks 4.8 out of 5 stars

Gartner peerinsights

2025 Fast Company Most Innovative Companies List

Silverfort customers **1,000+**

Funding (Series D) **$222m**

Employees around the world **500+**

gm · Costco Wholesale · NVIDIA · Airbus · BHP · Johnson & Johnson · Singtel · TESCO · AAA

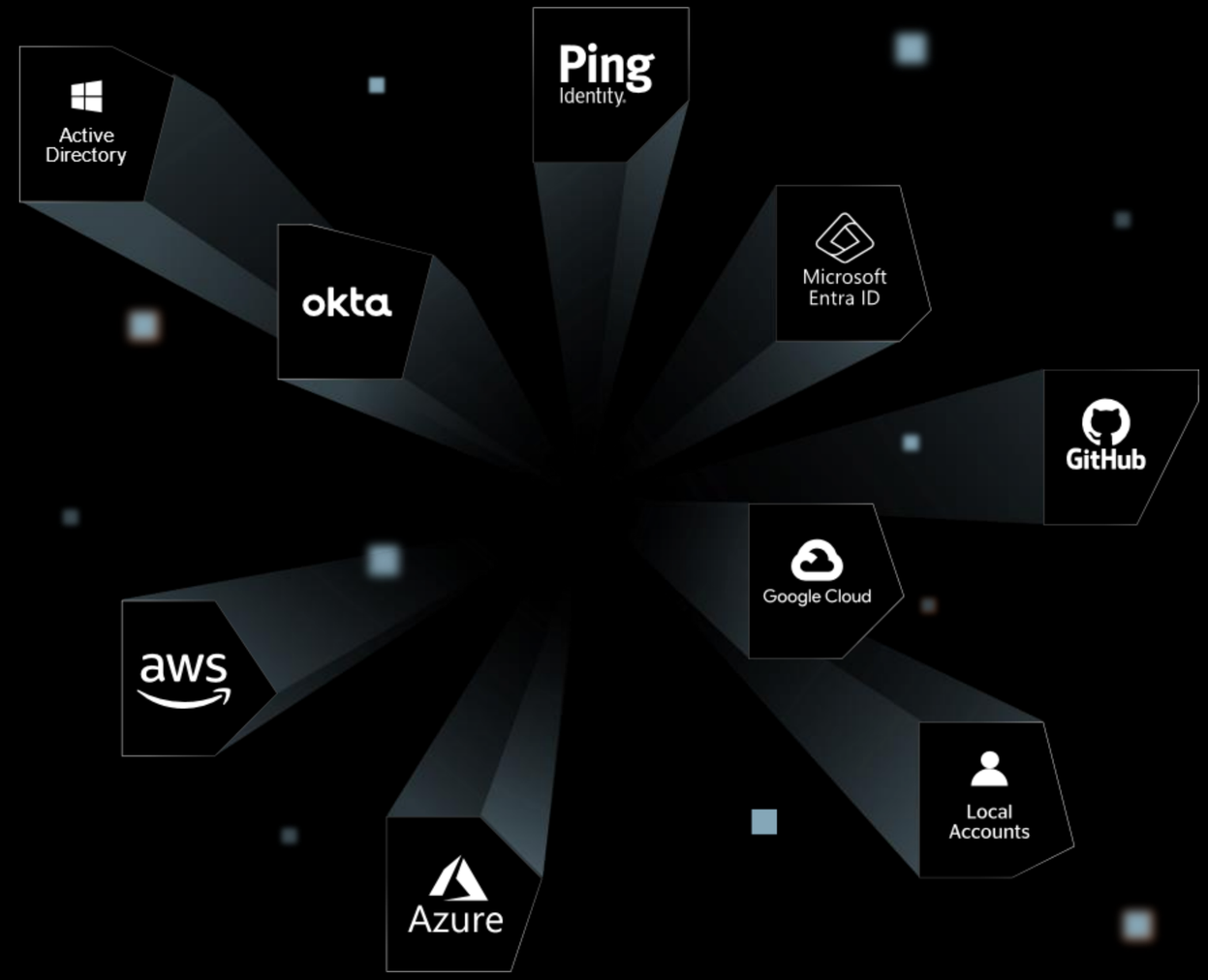
Key Technology Partnerships

Microsoft · okta · Ping Identity · splunk> · cisco · CROWDSTRIKE · yubico · aws · servicenow · Google Cloud · DUO · paloalto NETWORKS · RSA · Check Point Software Technologies Ltd. · SentinelOne

Some of our customers (confidential):

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

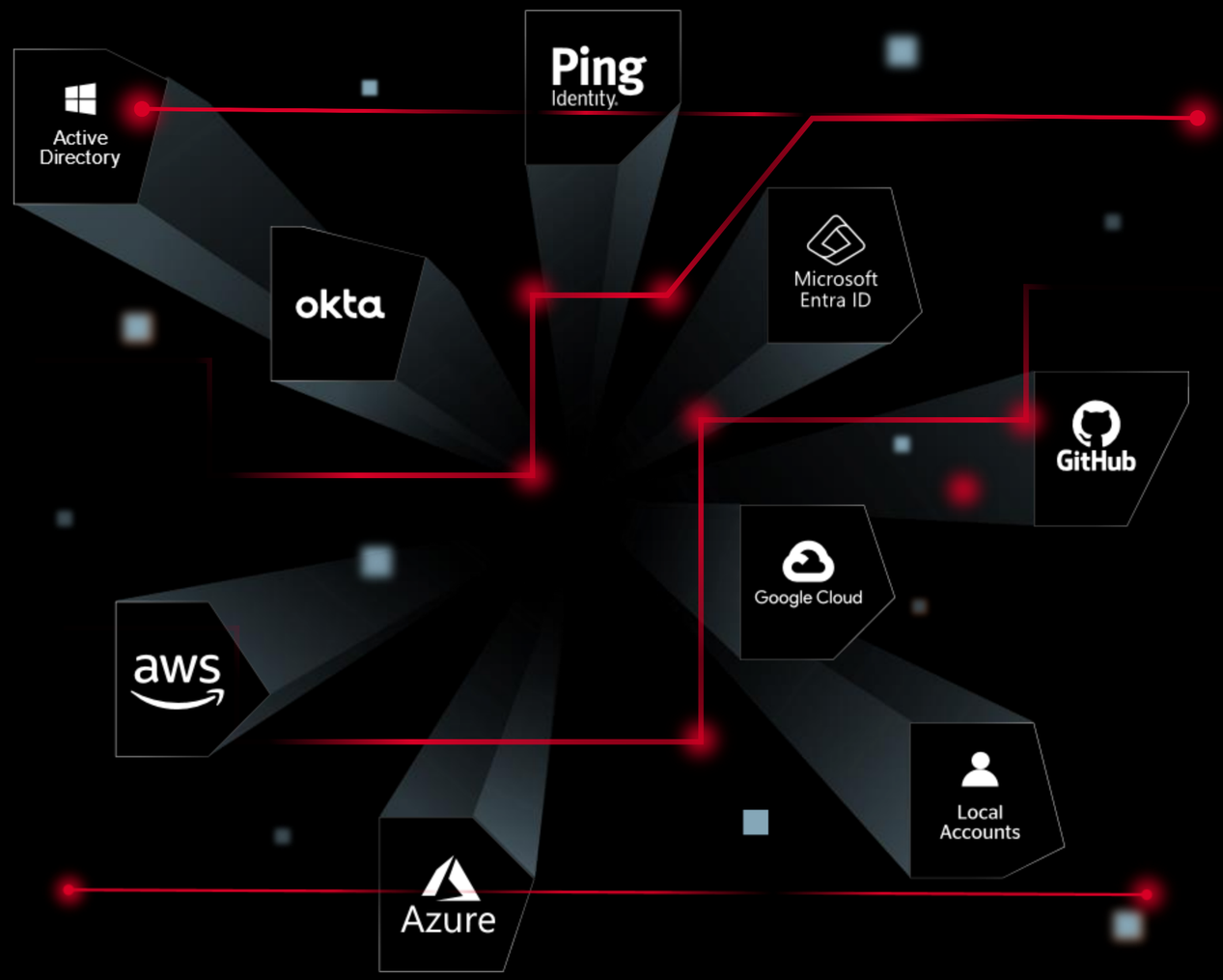
Legacy systems, command-line interfaces (e.g., PsExec), IT/OT infrastructure and more.

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.



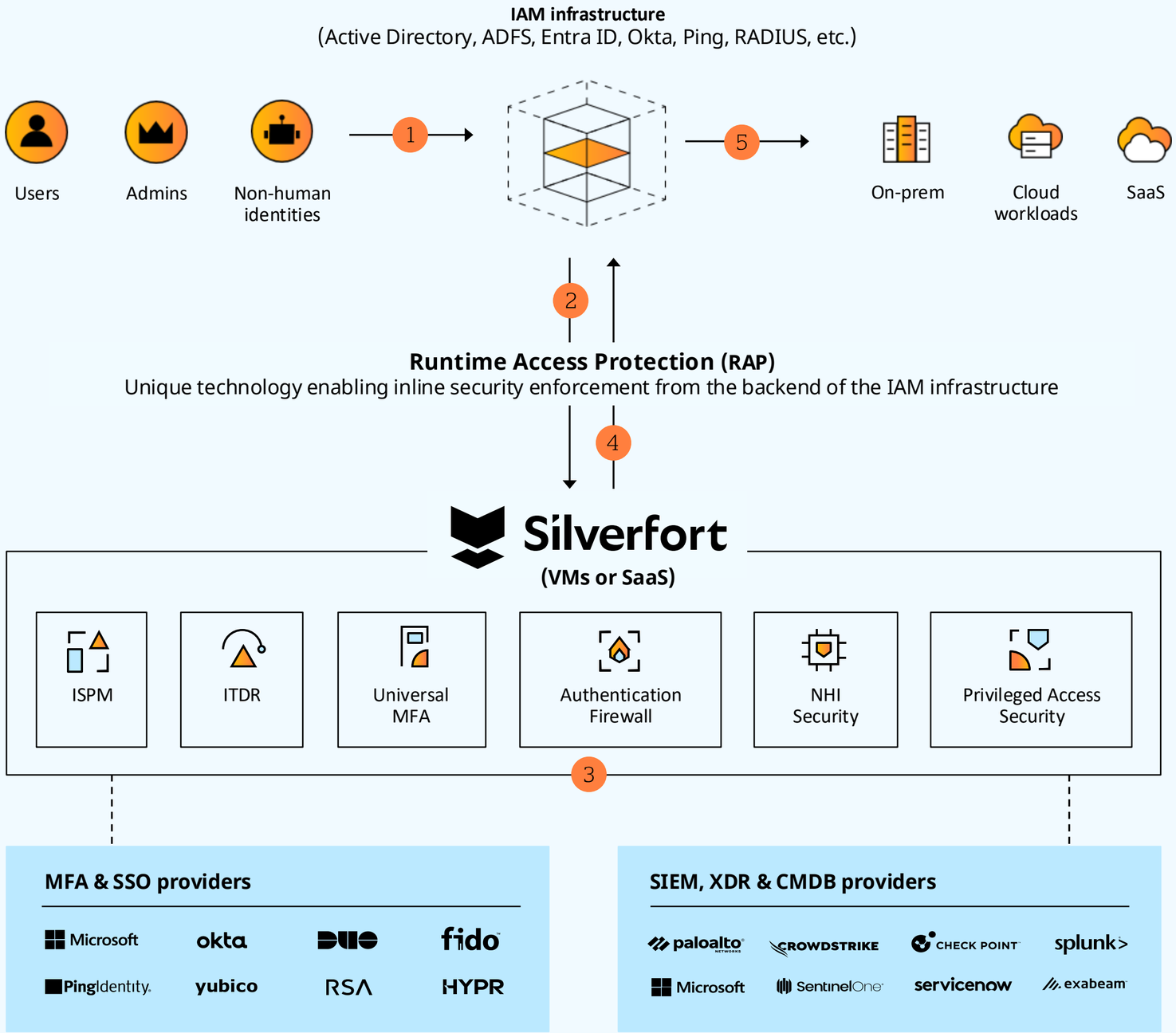
How it works:

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



All environments & resources

Microsoft Active Directory

Other on-prem identities

ADFS PingFederate

RADIUS Local accounts

Cloud IdPs

Microsoft Entra ID okta

onelogin PingIdentity.

IaaS

Azure aws Google Cloud

SaaS

The Silverfort Identity Security Platform

All identities

Workforce users

Privileged users

Third parties

Machine & service accounts

Cloud NHIs

The Silverfort Identity Security Platform

All environments & resources

Microsoft Active Directory

Other on-prem identities

ADFS · PingFederate · RADIUS · Local accounts

Cloud IdPs

Microsoft Entra ID · okta · onelogin · PingIdentity

IaaS

Azure · aws · Google Cloud

SaaS

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

Universal MFA
Extend MFA to every system, including legacy apps

Authentication Firewall
Block unauthorized access and enforce Zero Trust policies

NHI Security
Protect non-human identities from misuse and compromise

Privileged Access Security
Secure privileged identities at scale with unified policies

ISPM
Analyze exposures and prioritize remediation

ITDR
Detect, respond, and contain attacks in real time

Access Intelligence
Understand who can access what, with full risk context

AI Agent Security
Uncover and protect AI agents and model control planes (MCP)

Identity Graph & Inventory : Discover all identities and their relationships across hybrid environments

All identities

Workforce users · Privileged users · Third parties · Machine & service accounts · Cloud NHIs

During an Incident & as Retainer

- Free 60 days Incident License
- 4h SLA
- Instant containment (control every authentication)
- Full authentication visibility
- Optional: Retainer Silverfort Platform License

Silverfort Use Cases

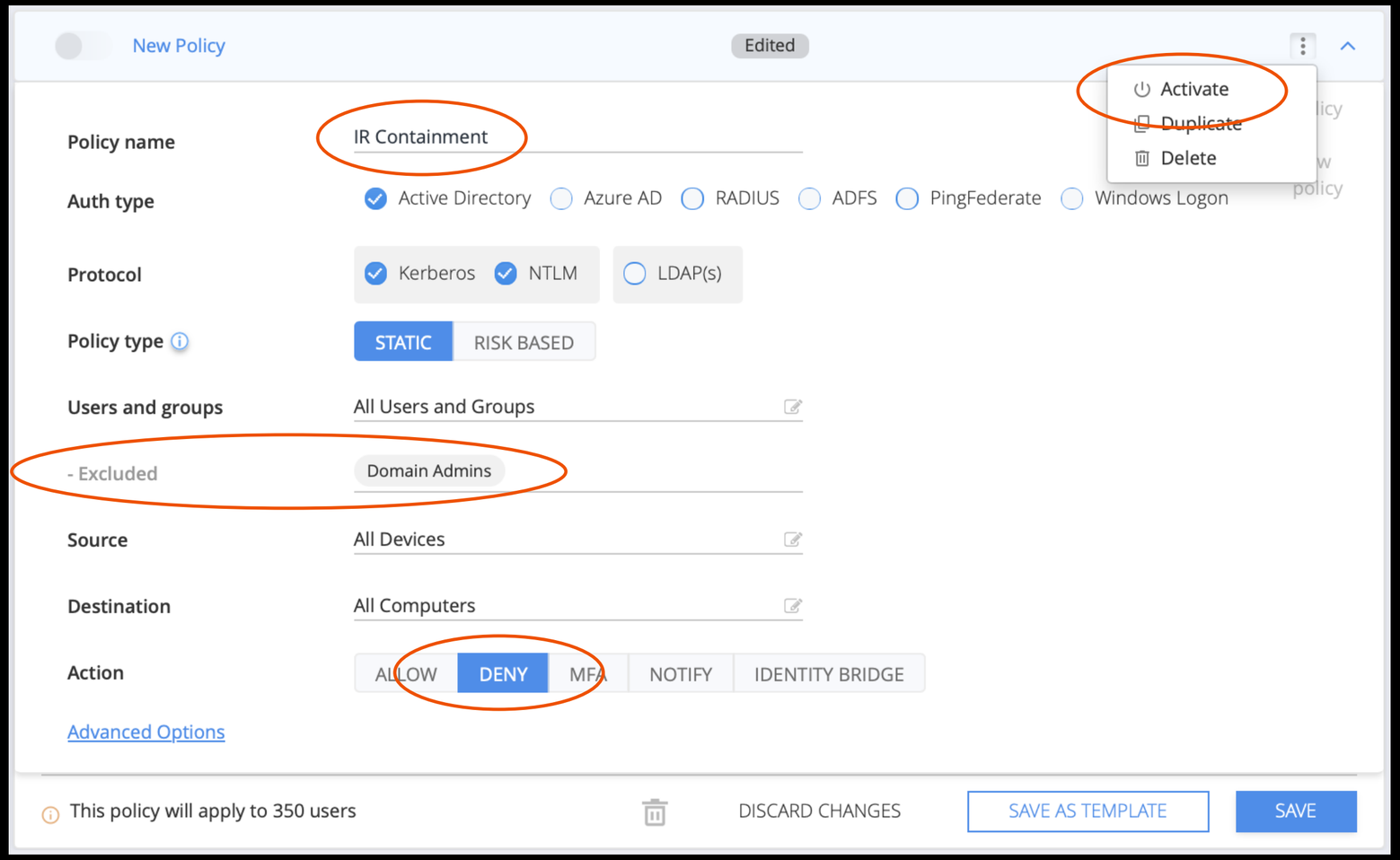
For Assessments, Table Tops & Trainings

- **Free 30 days consultancy license**
- **Full Authentication Monitoring**
- **Silverfort Identity Risk Report**

As Leave Behind / Managed Service

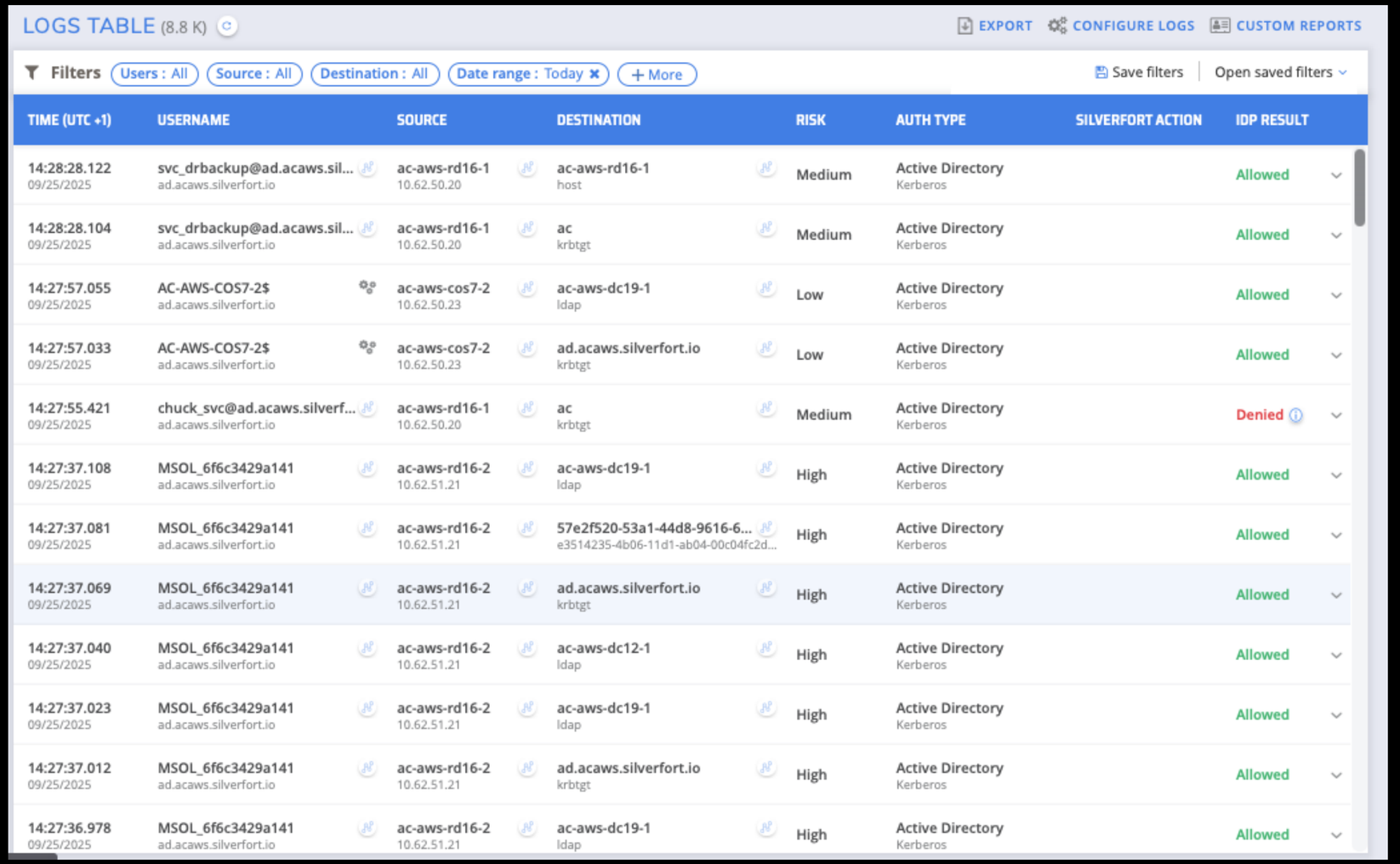
- **SaaS or On-Prem**
- **SOC connectivity**
- **Silverfort ISPM & ITDR & Alerting**

During an Incident: Instant Containment / Identity Lockdown



One rule to deny all authentications except for trusted accounts

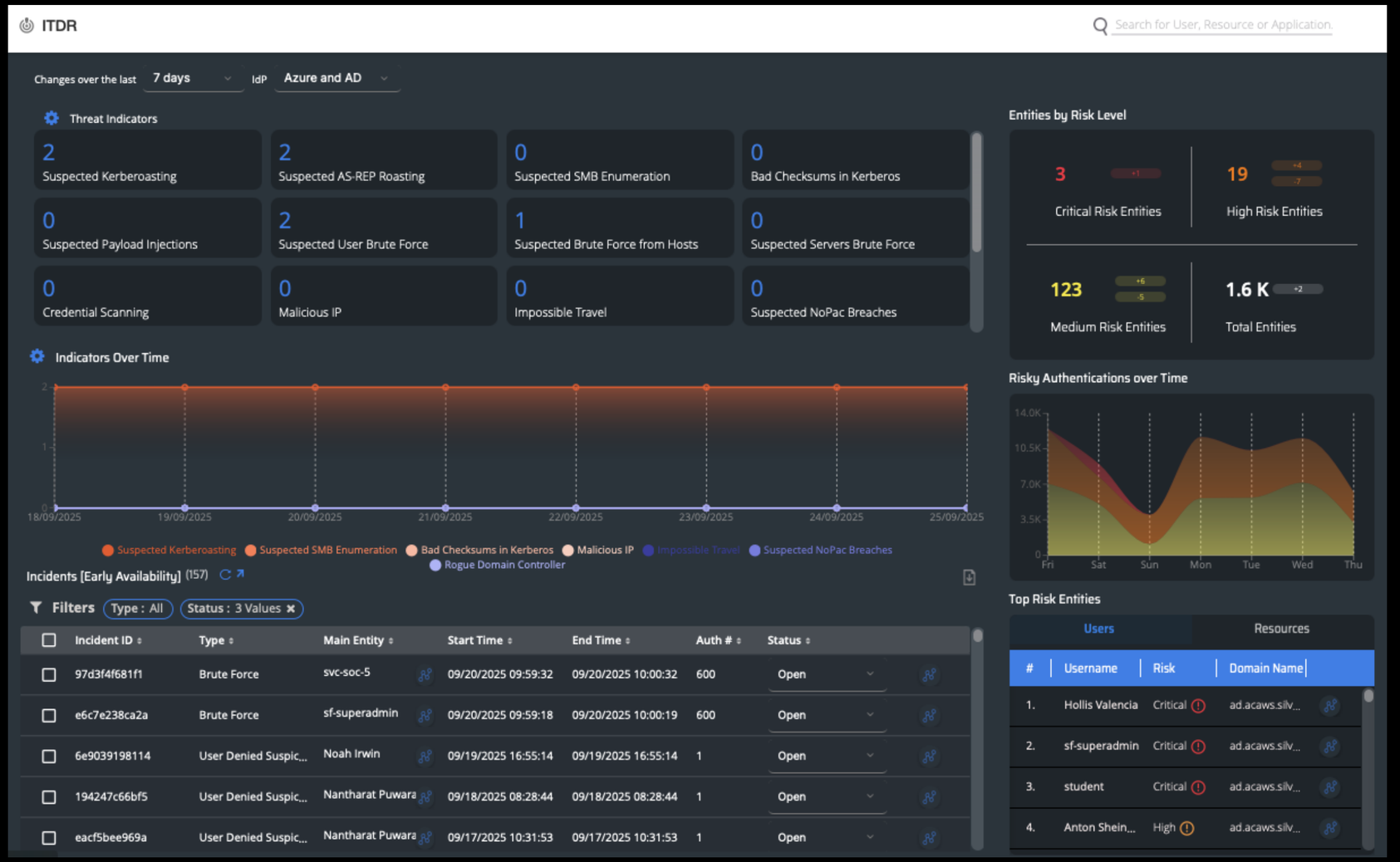
During an Incident: Complete Authentication Visibility



TIME (UTC +1)	USERNAME	SOURCE	DESTINATION	RISK	AUTH TYPE	SILVERFORT ACTION	IDP RESULT
14:28:28.122 09/25/2025	svc_drbackup@ad.acaws.sil... ad.acaws.silverfort.io	ac-aws-rd16-1 10.62.50.20	ac-aws-rd16-1 host	Medium	Active Directory Kerberos		Allowed
14:28:28.104 09/25/2025	svc_drbackup@ad.acaws.sil... ad.acaws.silverfort.io	ac-aws-rd16-1 10.62.50.20	ac krbtgt	Medium	Active Directory Kerberos		Allowed
14:27:57.055 09/25/2025	AC-AWS-COS7-2$ ad.acaws.silverfort.io	ac-aws-cos7-2 10.62.50.23	ac-aws-dc19-1 ldap	Low	Active Directory Kerberos		Allowed
14:27:57.033 09/25/2025	AC-AWS-COS7-2$ ad.acaws.silverfort.io	ac-aws-cos7-2 10.62.50.23	ad.acaws.silverfort.io krbtgt	Low	Active Directory Kerberos		Allowed
14:27:55.421 09/25/2025	chuck_svc@ad.acaws.silverf... ad.acaws.silverfort.io	ac-aws-rd16-1 10.62.50.20	ac krbtgt	Medium	Active Directory Kerberos		Denied
14:27:37.108 09/25/2025	MSOL_6f6c3429a141 ad.acaws.silverfort.io	ac-aws-rd16-2 10.62.51.21	ac-aws-dc19-1 ldap	High	Active Directory Kerberos		Allowed
14:27:37.081 09/25/2025	MSOL_6f6c3429a141 ad.acaws.silverfort.io	ac-aws-rd16-2 10.62.51.21	57e2f520-53a1-44d8-9616-6... e3514235-4b06-11d1-ab04-00c04fc2d...	High	Active Directory Kerberos		Allowed
14:27:37.069 09/25/2025	MSOL_6f6c3429a141 ad.acaws.silverfort.io	ac-aws-rd16-2 10.62.51.21	ad.acaws.silverfort.io krbtgt	High	Active Directory Kerberos		Allowed
14:27:37.040 09/25/2025	MSOL_6f6c3429a141 ad.acaws.silverfort.io	ac-aws-rd16-2 10.62.51.21	ac-aws-dc12-1 ldap	High	Active Directory Kerberos		Allowed
14:27:37.023 09/25/2025	MSOL_6f6c3429a141 ad.acaws.silverfort.io	ac-aws-rd16-2 10.62.51.21	ac-aws-dc19-1 ldap	High	Active Directory Kerberos		Allowed
14:27:37.012 09/25/2025	MSOL_6f6c3429a141 ad.acaws.silverfort.io	ac-aws-rd16-2 10.62.51.21	ad.acaws.silverfort.io krbtgt	High	Active Directory Kerberos		Allowed
14:27:36.978 09/25/2025	MSOL_6f6c3429a141 ad.acaws.silverfort.io	ac-aws-rd16-2 10.62.51.21	ac-aws-dc19-1 ldap	High	Active Directory Kerberos		Allowed

See every authentication attempt

During an Incident: ITDR



And every potential identity threat

- Discovering excessive activity
- Monitoring newly created/enabled accounts
- Separating human from automated activity
- Monitoring denied authentication
- Detecting compromised endpoints
- Chasing the threat – users to computers to
- users to computers…

For Assessments: Risk Report

Executive Summary

Above 80% of ransomware attacks involve Identity theft and Lateral Movement techniques.

Silverfort's report reveals where your biggest Identity security vulnerabilities and threats are:

125

2

46

54.1 K

How do I Compare to Industry Benchmarks?

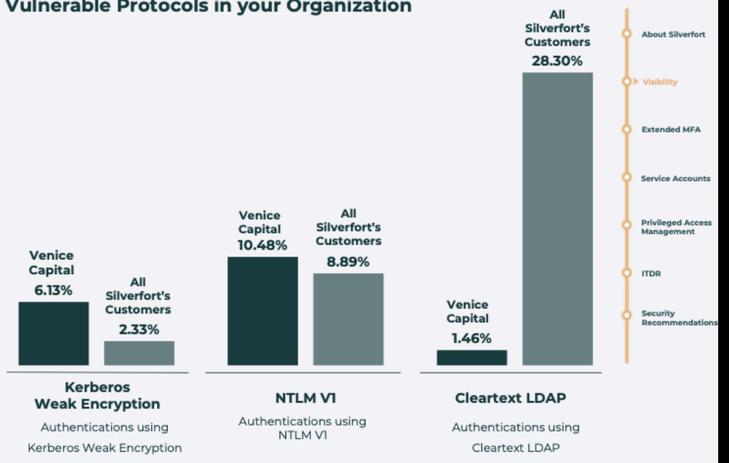
Authentications Health Meter

82.93% Non-Risky Authentications

18.07% Risky Authentications

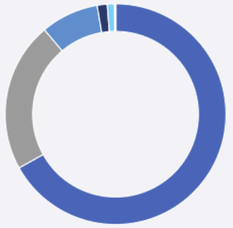
In the meantime, Silverfort encourages configuring MFA policies on risky protocols to better secure your environment.

Vulnerable Protocols in your Organization



How your Users and Servers Authenticate?

Authentications by Protocol



66.92% Kerberos

0.05% RADIUS

Weaknesses in Protocols

Kerberos - While Kerberos is considered a secured protocol, if weak encryption for tickets is being used, then it makes it easier to obtain password value using cryptographic-based attacks.

NTLM - NTLM is a legacy protocol required in cases where the client is unable to validate the server's identity in front of the DC. It is considered a weak protocol with new security issues regularly found for it.

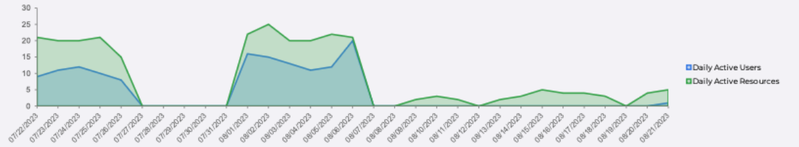
NTLM V1 - NTLM V1 uses a weak encryption algorithm and has no client challenge, making it more vulnerable to brute-forcing.

Cleartext LDAP - Unsecure traffic such as LDAP simple-bind is highly susceptible to interception by man-in-the-middle attacks. These types of

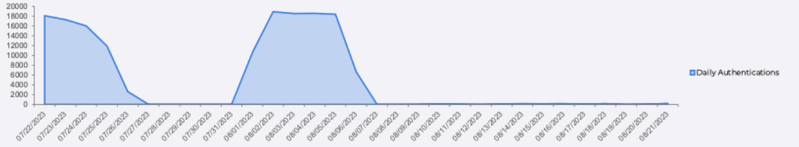
Active Directory

54.2 K Users | 3 Domains | 158.0 K Servers & Workstations | 549 Cloud Applications

Daily Active Users and Resources over Time



Daily Authentications over Time



For Assessments: Risk Report

Extended MFA

119 / 123
Unprotected Admin Users / Admin Users

33 / 42
Unprotected Privileged Users / Privileged Users

54.1 K / 54.2 K
Unprotected Users / Total Users

4
MFA Policies

12
Denied authentications by MFA policies

2
Configured IDPs

About Silverfort
Visibility
Extended MFA
Service Accounts
Privileged Access Management
ITDR

Service Accounts

Discovery

Service accounts have predictable behavior patterns which enable Silverfort to identify them automatically. This is based on a variety of parameters including naming conventions, AD attributes, and actual behavioral analysis that detects non-human access patterns.

46.7 / 158.7 K
Authentication Requests made by Service Accounts / Total Authentication Requests

4.3 K
Machine to Machine Accounts
Accounts that are used by machines to interact with other machines or services

533
Hybrid Accounts
Accounts used by both humans and automated processes in parallel

22
Scanners
Accounts that are used by a few devices to communicate with many devices inside a network

33.56 K
Total Service Accounts

Monitoring

Silverfort monitors service accounts' activity to create a baseline of their standard behavior and detect anomalous access attempts

About Silverfort
Visibility
Extended MFA
Service Accounts
Privileged Access Management
ITDR

Privileged Access Management

Silverfort protects your privileged accounts by bringing MFA, conditional access and visibility on all access attempts to on-prem and cloud resources.

123
Domain Admins
Domain Admins in the directories protected by Silverfort

42
Privileged Accounts
Part of known privileged groups like schema admins, enterprise admins and more

125
Highly Privileged Service Accounts
Suspected Service Accounts with privileged permissions

33
Users with SPN
These privileged users are susceptible to the "Kerberoasting" attack

266
Azure Shadow Admins
Azure Shadow Admins are user accounts in the Azure environment that have hidden privileges

54.0 K
AD Shadow Admins
Shadow Admins are user accounts in your network that have hidden privileges

2
Privileged Stale Users
Users with privileged permissions who have not been seen active in the past year

3
Privileged Users with Password Never Expires or Old Passwords
The number of privileged users with passwords that are set to "never expire" or passwords that have not been changed in the last year

About Silverfort
Visibility
Extended MFA
Service Accounts
Privileged Access Management
ITDR
Security Recommendations

SILVERFORT

Identity Threat Detection & Response (ITDR)

Risk Based Authentications

Users by Risk Level

1	Critical Risk Users
54.0 K	High Risk Users
27	Medium Risk Users
27.1 K	Low Risk Users

Authentications by Risk Level

7.8%	Critical Risk Authentications
39.07%	High Risk Authentications
44.67%	Medium Risk Authentications
8.43%	Low Risk Authentications

Top Risk Users

	USER NAME	Risk
1	jane.smith	critical
2	michael.johnson	high
3	emily.wilson	high
4	david.anderson	high
5	sarah.jackson	high

Top Risk Resources

	RESOURCE NAME	Risk
1	17.2.62.222	medium
2	_Ser22	medium
3	233.2.63.195	medium
4	Nexus	medium
5	28.2.31.3	medium

About Silverfort
Visibility
Extended MFA
Service Accounts
Privileged Access Management
ITDR
Security Recommendations

SILVERFORT

Exposures Covered by Silverfort Risk Assessment

Privileged Accounts

- Domain Admin
- Privilege Account
- Global Admin
- Privileged Stale User
- Privileged User with Old Password or Password never expires

Privilege Escalation

- Shadow Admin
- Entra ID Shadow Admins
- Hosts with Privilege Escalation Path
- Privilege Accounts - Used on Tier 1 & Tier 2 Asset
- Unprivileged DNS Admins
- ADCS Domain Escalation 4

Credential Access

- Accounts with SPN
- Admins with SPN
- Human Operated Accounts with SPN
- Kerberos Pre-Auth Not Required
- Leaked Credentials
- NTLMv1 Authentication (Servers)
- Unconstrained Delegation (Users)
- Weak Encryption (Servers)
- Weak Encryption (Users)
- Clear Text LDAP
- LDAP(s) over Obsolete TLS

Insecure Configuration

- Password Not Required
- Password Never Expires
- Users with Old Password
- Shared Accounts
- Locked Accounts
- Account lockout post password reset
- Stale Accounts
- Old Operating Systems
- Shared Devices
- Stale Devices
- Print Nightmare

Service Accounts

- Privilege Service Accounts
- Machine to Machine
- Scanner Accounts
- Hybrid Accounts
- Dormant Accounts
- Service Accounts with Interactive Logins
- Visibility on Source + Destination + Protocol Used
- Privilege Service Accounts - Used on Tier 1 & Tier 2 Asset

How Silverfort can help in IR?

- **Visibility into Authentication Traffic:** Gain complete visibility into authentication activity across on-prem Active Directory, federation servers (ADFS, PingFederate), cloud identity providers (Entra ID, Okta, etc.), SaaS applications, and cloud infrastructure (AWS, Azure, GCP).

- **Immediate Control Over Lateral Movement:** Enforce authentication firewalls and MFA across all access attempts, effectively shutting down attackers' ability to pivot between systems within minutes.

- **MFA for Legacy Systems and Protocols:** Extend MFA protection to legacy systems and protocols such as RDP, PowerShell, PSExec, SMB, and others—without requiring native support or endpoint modifications. Regain control of critical infrastructure frequently targeted by attackers, including identity infrastructure and virtualization platforms (e.g., ESXi, Hyper-V).

- **Enhanced Visibility into Service Accounts:** Automatically identify all service accounts within the environment and provide tools to secure them. This visibility is essential to defend against compromise and lateral movement, especially in environments with a high volume of non-human identities.

- **Safe and Swift Recovery:** Enable a gradual and secure return to normal operations once accounts and network segments have been remediated and verified as clean.

Silverfort IR Program

IR Service

- Used for incidents
- Free 30 days license
- SLA w. IR Firm
- Domain-independent, victim unknown

Pre-Breach Service

- Used for consultancy
- Identity Risk Report
- Free 30 days license

One agreement / amendment to cover all use cases
4 hour SLA for IR license delivery & assistance

Discussion and next steps