

Adria Forum 2025

Identity security without the hassle? **Yes, with Silverfort**

Shari Daneshjoo
Silverfort VP Sales CEE

Marco Baban
CS Cyber Security Team Lead

14.10.2025



The Identity Security Challenge



- PAM & MFA projects = slow, complex, costly
- Legacy systems and Apps = hard to secure
- Service accounts = too often neglected, yet critical
- Limited visibility into authentication activity
- Hard to limit lateral movement

The Identity Security Challenge

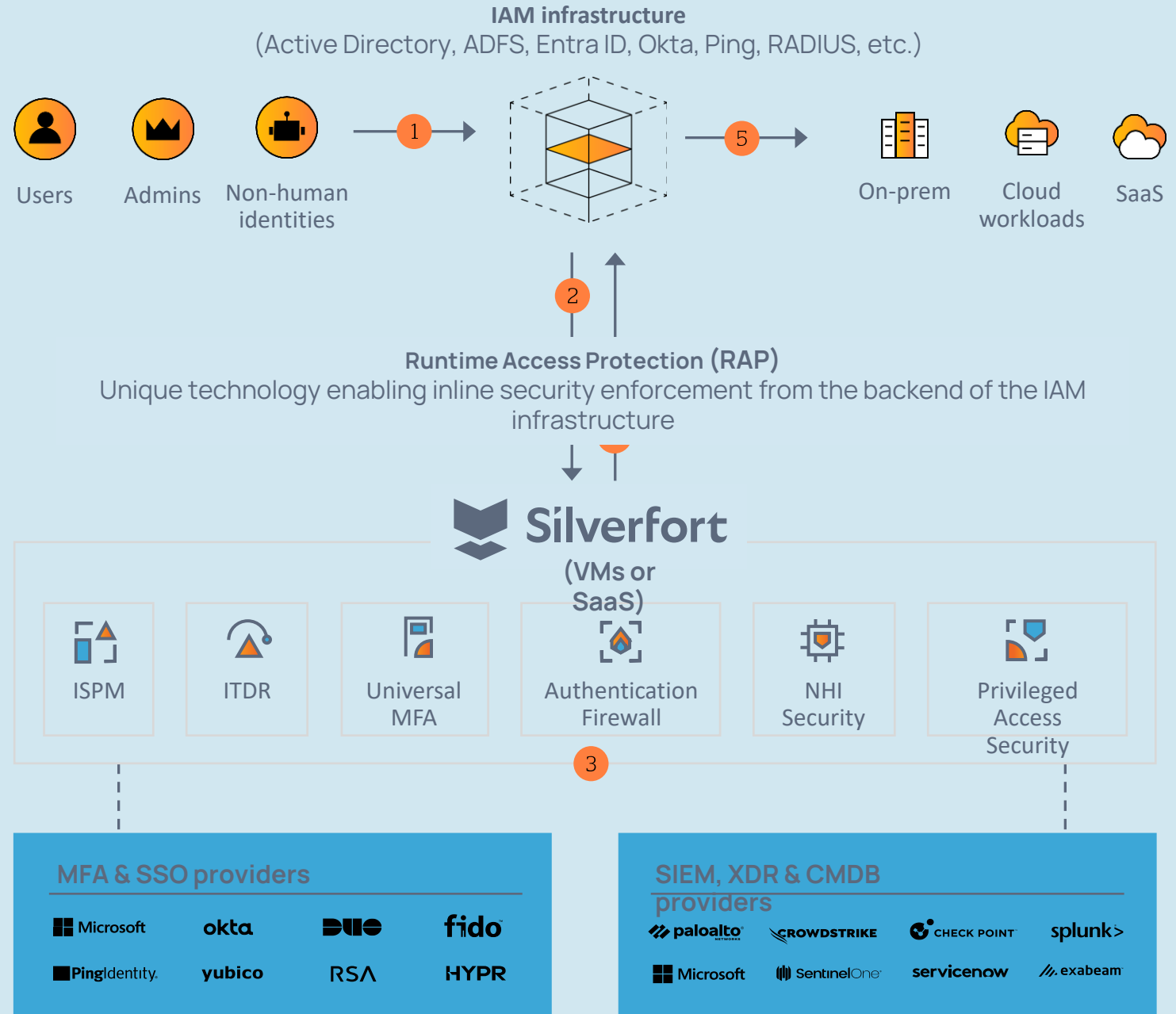


Why is it revolutionary

- 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.



MFA

- Enable system
 - R
 - P
 - F
 - L
- No SA
- Uses A
- Works (Micro

YOU GET MFA, YOU GET MFA

EVERYONE GET MFA

makeameme.org



SaaS



Cloud
Workloads



On Prem

Authentication(Identity) Firewall



- **Full control of authentication and access** with inline enforcement at the authentication protocol level
- **Active prevention of lateral movement and ransomware propagation**
- **Rapid implementation** even during active incident response (IR) events
- **Works alongside network segmentation tools** or as a faster compensating control

Policies

Recently Updated : All Policy Groups : All Users & Groups : All Destination Resources : All ☐ Show inactive policies

Allow (5)

☒ New policy

Policy Name: MFA for Air Gapped Networks

Auth Type: ☒ Active Directory ☐ Azure ☐ Okta ☐ Radius ☐ ADFS ☐ PingFederate ☐ Windows Logon

Protocol: ☒ Kerberos ☒ NTLM ☐ LDAP(s)

Policy Type: ☒ Static ☐ Risk Based

Optimization: ☒ Optimize Policy

Users and Groups: Shopfloor-engineers

Source: Engineering-workstations

Destination: Zone-2/3-workstations

Action: ☐ Allow ☐ Deny ☒ MFA ☐ Notify

MFA Prompt Display Name: \$username, are you trying to access \$destination from \$source?

Tokens: FIDO2 x

[Advance Options](#)

☒ this is another policy 4,572

☐ This is a policy with a really long name that re... 32,622

Identify and protect your privileged accounts



- **Implement and activate rapidly**, unlike any PAM solution
- **Discover and classify** privileged accounts automatically and continuously
- **Enforce Least Privilege** access policies to control where each account can be used
- **Enforce Just-In-Time (JIT) access** at scale to achieve Zero Standing Privileges

Privileged Access Security

Account Status

Accounts directly disabled in Active Directory by JIT policy **194 / 493**

Protected Privileged Accounts

Accounts protected with JIT or Virtual Fencing policies **84 / 493**

Cross Tier

Cross tier accounts protected with JIT or Virtual Fencing policies **0 / 1**

Account Status: All Policy: All Cross Tier: All Sources: All Destinations: All Group / OU: All

Tier 0 (24) Tier 1 (351) Tier 2 0 Unassigned (75)

☐	Name (323)	Status	Sources	Destinations	Cross tier	Policy
>	☐ jordan.beyer Tier 0	Disabled	2	24	None	Unprotected
>	☐ maxkilman2 Tier 0	Enabled 6:34	5	35	None	JIT Fencing
▼	☐ jamie_vardy_adm Tier 0	Disabled	6	12	None	Unprotected

Source	Destination	Cross tier	Authentications	Services	Filter
jvardy-mach	Server1 Tier 2	No	124	scm rpc +10	F
jvardy-mach	Server2 Tier 0	No	56	scm termsrv +10	F
jvardy-mach	Server3 Tier 1	Yes	4	scm mssql +10	J
jvardy-mach	Server4 Tier 0	No	119	scm logon +10	M

>	☐ gordon-anthony Tier 0	Disabled	9	1	2	Fencing
>	☐ epinnock Tier 0	Disabled	2	20	None	JIT Fencing
>	☐ JackHarrison20 Tier 0	Disabled	2	106	None	Unprotected

Protecting the identity security blind spot

- Service Accounts



- Discover and classify all service accounts, keys, tokens and many more
- Map and analyze exactly where these identities are being used
- Enforce 'virtual fencing' for service accounts to restrict sources and destinations
- Automate protection at scale with smart policies

ACCOUNT LIST

Filters: Baseline Change: All | Name: All | Protection status: All | Risk: All | Protected Accounts Actions: All | Domain: All | + More

Machine to machine (94) | Hybrid (8) | Scanners (0) | Dormant (146) | Removed (1)

PROTECTION	SERVICE ACCOUNT	SOURCE	DESTINATION	AUTH	RISK
☐	ciscomail@intranet.cs.hr*	0 Sources	2 Destinations	9.1 M	Low
☐	opamgr@intranet.cs.hr*	2 Sources	3 Destinations	4.0 M	Low

ACCOUNT OWNER: N/A | COMMENT: N/A

Allow authentications that meet the following conditions:

SOURCE

☐ All sources

☒ Selected sources:

Device	Hits	Action
cs-srv-opm01	4.0 M	Allow
192.168.0.88	3.0 M	Allow

Add...

DESTINATION

☐ All destinations

☒ Selected destinations:

Device	Hits	Action
CS-SRV-EXCH03 (intranet.cs.hr)	2.6 M	Allow
krbtgt (INTRANET.CS.HR)	1.4 M	Allow
192.168.0.141	824.4 K	Allow

Add...

PROTOCOL

☒ Kerberos	Last seen 10/06/2025
☒ NTLM	Last seen 10/06/2025
☐ LDAP/S	Not seen

WHEN

☒ Always

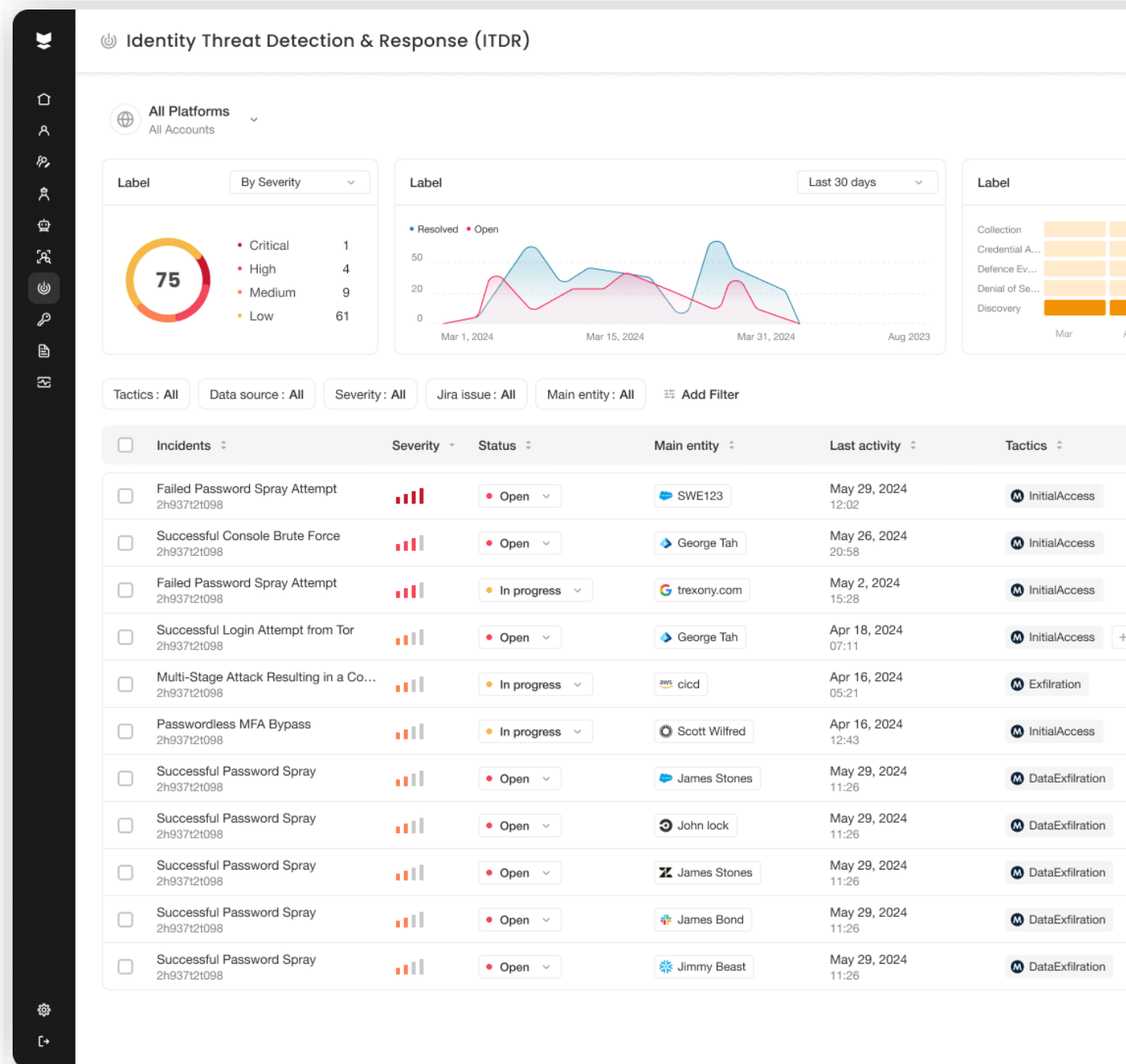
☐ Risk level is Medium or lower.

Actions:

☒ Deny Access ☒ Send to SIEM ☒ Notify

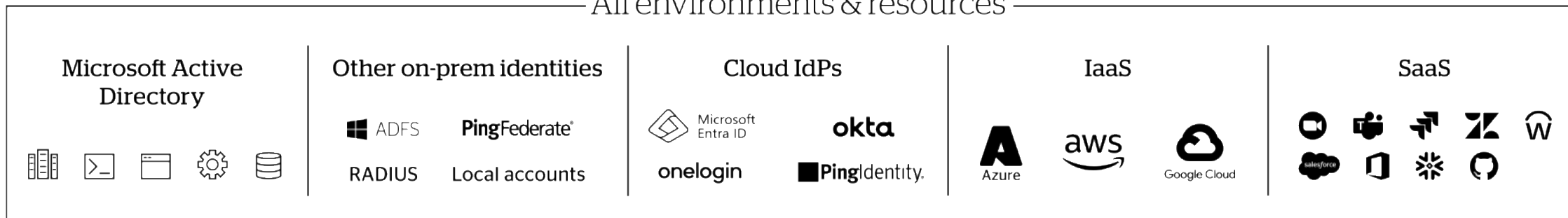
Do you know what your accounts are doing?

- **Advanced threat detection engine** that analyzes every access attempt
- **Move beyond passive detection to active inline response**
- **Stop attackers without stopping your users**
- **Integrations with XDR, SIEM and SOAR products**



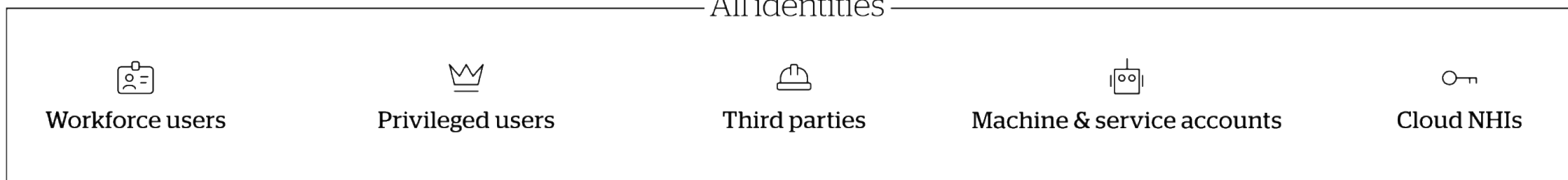


All environments & resources



The Silverfort Identity Security Platform

All identities



The Silverfort Identity Security Platform



— All environments & resources —



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



— All identities —





Adria Forum 2025

Thank You