



Authentication Evolved

Agentless | Proxyless | Limitless

“Based on our studies, your account is more than 99.9% less likely to be compromised if you use MFA.”

Alex Weinert, Group Program Manager, Identity Protection





Agentless AI-Driven Authentication Platform

Prevent identity-based attacks with dynamic AI-based policies, including MFA, RBA and Zero Trust, across all sensitive corporate assets - not only at the perimeter, but inside the network too.



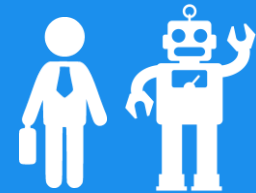
Protecting systems that couldn't be protected before



No agents, no proxies, no code changes!

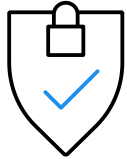


Analyzing 20x-50x more authentication data



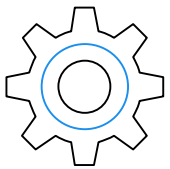
Protecting both human users and service accounts

Common Use cases



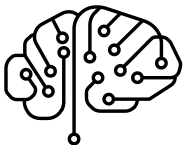
Enable True Coverage – Extend MFA

- Homegrown/Legacy applications (Custom or off the shelf)
- Admin access tools: PowerShell, PSEXEC; Remote Registry, Etc.
- File-shares



Service Accounts

- Discover & Profile
- Monitor
- Protect

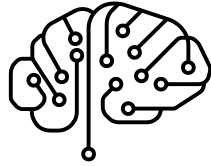


Detect and prevent identity-based attacks

- Unified risk-based authentication
- Zero Trust policies
- User Risk Scoring

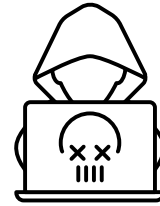
Silverfort's AI-Driven Trust Engine

Thanks to its agentless and proxyless architecture, Silverfort monitors and analyzes more data than any other risk-based authentication solution



1. Anomaly Detection

Continuously analyzing and learning user behavior across all resources and environments, using Machine Learning



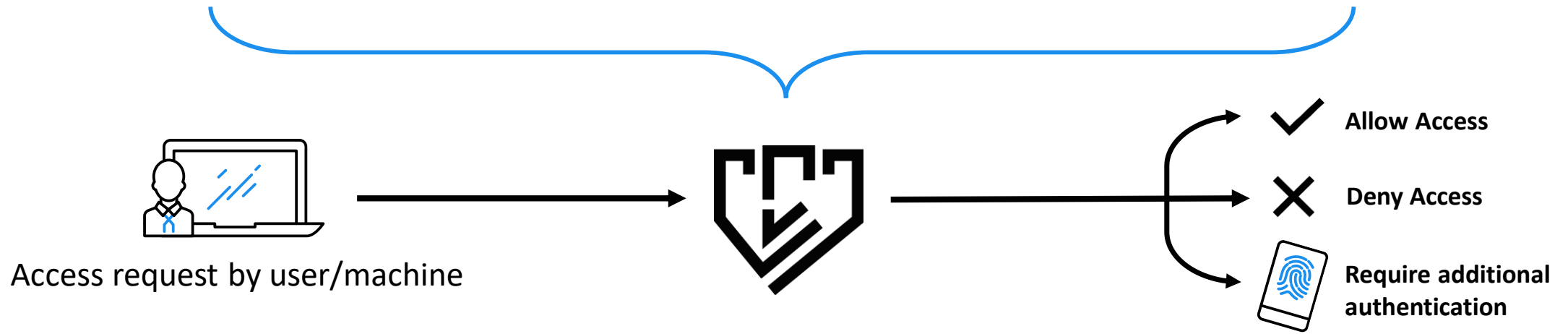
2. Known Threats

Identify known malicious patterns (including lateral movement, ransomware, brute-force and more)



3. External Risk Indications

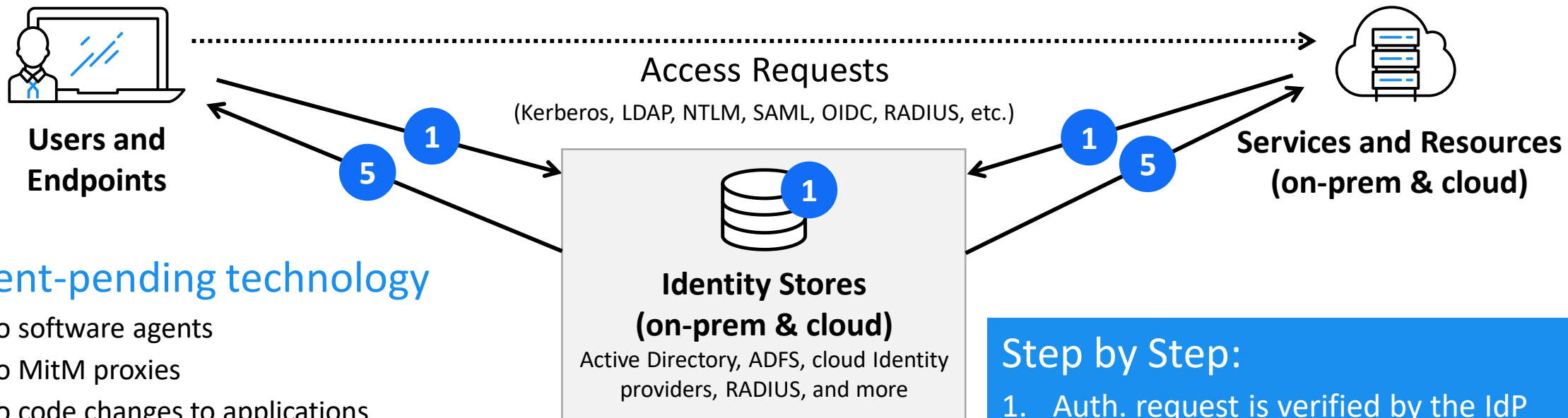
Leverage threat alerts from 3rd party solutions for real-time step-up authentication





Authentication Evolved
Architecture and Demo

How Does It Work?

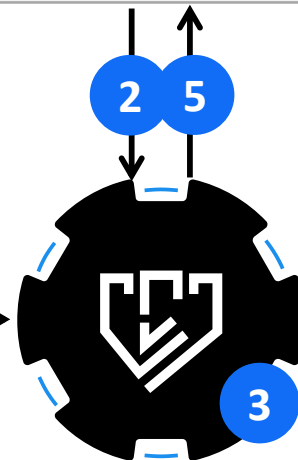


Patent-pending technology

- ✓ No software agents
- ✓ No MitM proxies
- ✓ No code changes to applications
- ✓ No change to user workflows



2nd Authentication Factor
(Silverfort or 3rd party)



Step by Step:

1. Auth. request is verified by the IdP
2. The response is routed as-is to Silverfort for "second opinion" (using native features)
3. Silverfort analyzes the message, calculates risk and applies policy - allow/deny/MFA
4. If needed, user is challenged with MFA
5. If verified, the message is sent back as-is to the unaware client/server



Authentication Evolved
Integrations

Better Together

Silverfort integrates with leading security, IAM and cloud providers, to deliver unified secure authentication across all systems and environments, and prevent threats in real-time

Technology Partners (partial list):





- Silverfort Integrates with Okta's mobile MFA, out of the box, and extends Okta's MFA capabilities to resources that Okta could not protect.
- [Joint press release](#)
- [Joint Datasheet on Okta's website](#)

Okta + Silverfort: Multi-Factor Authentication for Desktops and Systems Across the Enterprise



The explosion of mobile and cloud technologies has dissolved the traditional network perimeter. As a result, organizations can no longer assume trust based on just a username and password or whether or not the user is on the corporate network. In this zero trust world, organizations need better ways of protecting sensitive resources across the corporate network and cloud environments and verifying trust in users and devices before granting access, without adding complexity along the way. Now, Silverfort's agentless authentication platform integrates directly with Okta to extend strong, adaptive multi-factor authentication (MFA) everywhere, to secure access to all enterprise resources, while streamlining operations at the same time.

Protect all your enterprise resources with strong, adaptive MFA

Okta and Silverfort work together to seamlessly extend multi-factor authentication everywhere, across cloud environments and the corporate network, including traditionally hard-to-protect resources and resources for homogenous applications, IoT devices, IP addresses, and more. With Silverfort's agentless authentication platform integrated with Okta, customers can easily extend their strong, adaptive MFA to all sensitive resources, without requiring agents or policies or adding protocol overhead. Enterprise users protect sensitive data breaches, address compliance, and adopt a Zero Trust approach to security while maintaining streamlined usability and control for security and IT teams and a frictionless experience for authorized users.

Together, Okta + Silverfort let you:

- Secure access to sensitive systems across all environments, in an seamlessly enterprise MFA solution

Extend MFA everywhere, including resources like workstation domain logins, homegrown and legacy apps, IP addresses, the cloud, and more

- Enforce security policies, while controlling usability, factor enrollment, and factor enforcement to streamline the deployment

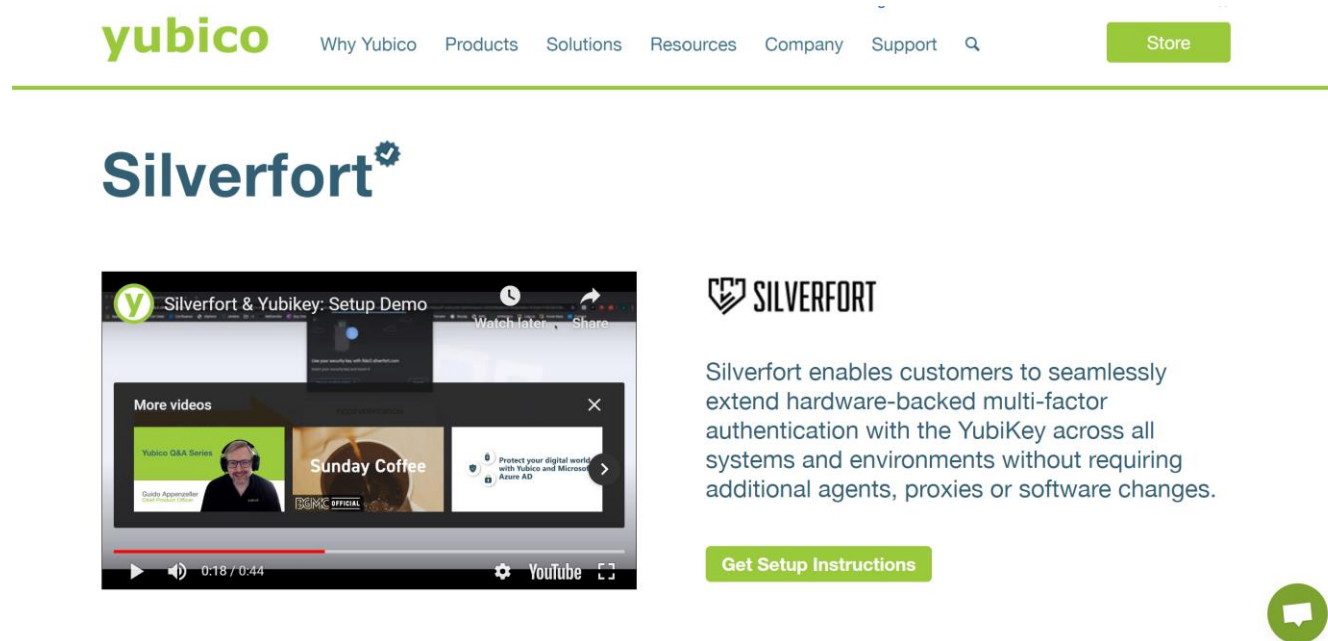
How Okta + Silverfort work together

Silverfort extends authentication protocols and access requests in real-time, across an enterprise's network and cloud, without disrupting them. It then calculates the using an AI-driven risk engine, and applies a policy to either deny, or require MFA. By connecting Silverfort with Okta, customers can use Okta's services and secure MFA experience for enhanced security based on enterprise policy. Silverfort and Okta connect via APIs, enabling Silverfort's platform to trigger Okta's MFA on resource. With Silverfort and Okta working together, enterprises get a secure authentication flow that doesn't affect the client or server, and authorized users get streamlined access to the resources they need.

The explosion of mobile and cloud technologies has dissolved the traditional network perimeter. As a result, organizations can no longer assume trust based on just a username and password or whether or not the user is on the corporate network. In this zero trust world, organizations need better ways of protecting sensitive resources across the corporate network and cloud environments and verifying trust in users and devices before granting access, without adding complexity along the way. Now, Silverfort's agentless authentication platform integrates directly with Okta to extend strong, adaptive multi-factor authentication (MFA) everywhere, to secure access to all enterprise resources, while streamlining operations at the same time.

[Download](#)

- Silverfort enables customers to seamlessly extend the YubiKey FIDO2 hardware-backed Multi-Factor Authentication across all systems and environments, including non-web systems that don't support FIDO2, without requiring additional agents, proxies or software changes.
- [Joint video on Yubico's website](#)



yubico Why Yubico Products Solutions Resources Company Support [Store](#)

Silverfort

SILVERFORT

Silverfort enables customers to seamlessly extend hardware-backed multi-factor authentication with the YubiKey across all systems and environments without requiring additional agents, proxies or software changes.

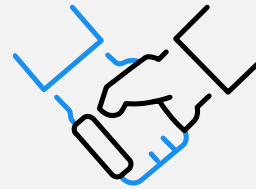
[Get Setup Instructions](#)

ABOUT SILVERFORT



OFFICES

- Tel Aviv, Israel
- Boston, MA
- Dallas, TX
- Antwerp, Belgium
- Singapore



TECHNOLOGY PARTNERSHIPS



CUSTOMERS

- Financial Services
- Healthcare
- Retail
- Media
- Telco
- Energy & Utilities
- Technology
- Legal



INDUSTRY AWARDS

