SILVERFORT

INDUSTRY BRIEF

ENABLING SECURE AUTHENTICATION ACROSS IT AND OT NETWORKS WITHOUT AGENTS OR PROXIES

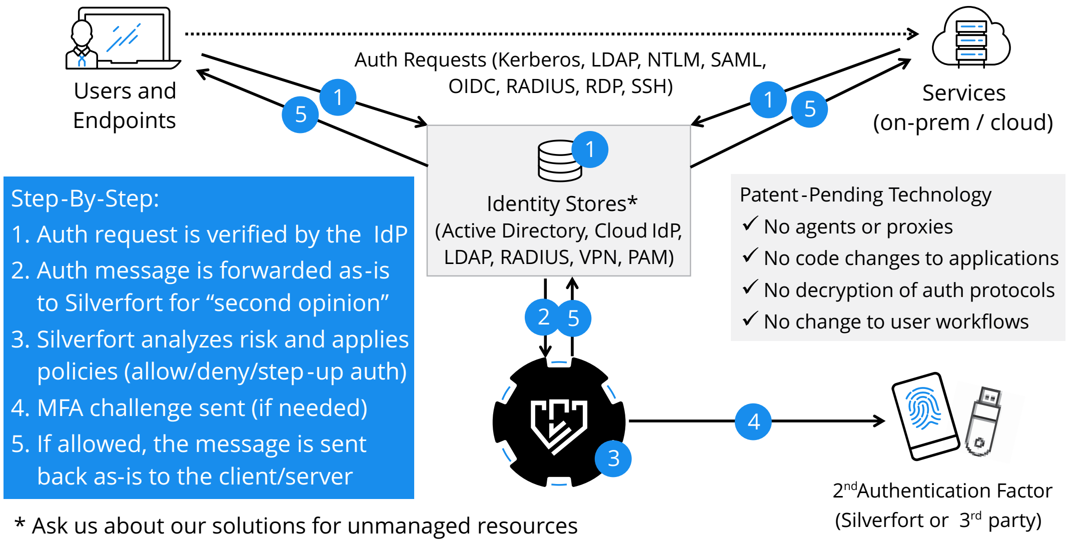
Silverfort enforces secure authentication and access policies across corporate networks, industrial networks and cloud environments, including sensitive IT and OT systems that were considered 'unprotectable' until today, enabled by an innovative agentless and proxyless architecture.

Corporate and industrial networks are more connected than ever – both to each other and to the external world. Enforcing secure authentication on access to sensitive assets in both environments is a critical security measure for preventing data breach and unauthorized access. However, many of these sensitive assets cannot be integrated with any standard Multi-Factor Authentication (MFA) solution, because such solutions require software agents, proxies and/or code changes, that are often not applicable in these environments. This leaves many sensitive systems exposed.

Silverfort Next-Generation Authentication Platform

Silverfort applies an innovative architecture and a powerful AI-driven risk engine to monitor, analyze and secure all authentication and access across the enterprise, including both IT and OT networks. It enables Multi-Factor Authentication (MFA), Risk-Based Authentication (RBA), Zero Trust policies and holistic visibility across all sensitive systems, including systems that were considered 'unprotectable' until today, without requiring any agents, proxies or code changes. This includes homegrown and legacy systems, remote admin tools (such as Remote PowerShell), file systems (often targeted by ransomware), IT infrastructure, SCADA and other operational servers, engineering workstations, HMIs, IIoT devices, machine-to-machine access and more.

How Does It Work?


Users and Endpoints
Auth Requests (Kerberos, LDAP, NTLM, SAML, OIDC, RADIUS, RDP, SSH)
Services (on-prem / cloud)
1
5
1
5
1
Identity Stores* (Active Directory, Cloud IdP, LDAP, RADIUS, VPN, PAM)
2
5
3
4
2nd Authentication Factor (Silverfort or 3rd party)

Step-By-Step:

1. Auth request is verified by the IdP
2. Auth message is forwarded as-is to Silverfort for "second opinion"
3. Silverfort analyzes risk and applies policies (allow/deny/step-up auth)
4. MFA challenge sent (if needed)
5. If allowed, the message is sent back as-is to the client/server

Patent-Pending Technology

- ✓ No agents or proxies
- ✓ No code changes to applications
- ✓ No decryption of auth protocols
- ✓ No change to user workflows

* Ask us about our solutions for unmanaged resources

Unique Benefits

→ Enables secure authentication and Zero Trust policies for any sensitive asset, including systems that could not be protected until today

→ Provides a unified platform for monitoring and securing authentication across the enterprise, from legacy systems, HMIs and IIoT devices to cloud resources

→ The first non-intrusive authentication solution – no agents, proxies or code change!

→ Delivers unparalleled AI-driven risk and trust engine, detecting threats across the network and automatically responding with step-up authentication and real-time prevention

→ Enhances security while minimizing disruptions to the workforce

We Enable Enterprises to Protect Authentication and Access to Their Most Sensitive Systems

Agentless MFA for 'Unprotectable' Assets

- Homegrown and legacy applications
- IT infrastructure (hypervisors, DCs, etc.)
- SCADA servers, HMIs and IIoT
- File shares and databases (including ransomware protection)
- Workstations, VDI, Win/Unix servers (including remote admin tools that cannot be protected today, like Remote PowerShell)

Machine-to-Machine Access

- Automatically discover service accounts based on their behavior
- Detect deviations from intended use
- Provide automatic AI-driven policy recommendations
- Prevent unauthorized use in real-time, or require admin approval

Secure Privileged Access

- Automatic discovery and monitoring of privileged accounts (including stealthy admins)
- MFA for PAM solutions (including the PSM RDP/SSH Proxy)
- Seamless user-experience - no portal/proxy, no need to re-enter OTP for each session (which could make MFA unusable)
- MFA for admin access, including remote admin tools that cannot be protected by standard MFA products, such as Remote PowerShell, WinRM and more

Compliance and Red Team Assessments

- Achieve compliance with PCI DSS, NY-DFS, SWIFT CSP, NIST and more
- Improve red team assessments and security audits
- Address findings of these audits and effectively prevent such attacks from compromising the network

Proxyless Zero Trust Architecture

- Monitor and control all user and machine access throughout the network and cloud, and not only at the gateway
- Enable Zero Trust even in large and complex environments, by avoiding any proxies, agents or certificates
- Leverage an unparalleled AI-Based Risk and Trust Engine for intelligent access policies

Secure 'Lift-and-Shift' Cloud Migration

- Enable secure authentication and access for homegrown/legacy systems, and allow migration without security barriers
- Avoid the need to implement modern authentication for each application/server individually

AI-Driven Risk-Based Authentication

- Continuous risk and trust assessment across all users, devices and services, both on-premise and in the cloud
- Leverage AI for behavior analytics, community clustering, human/machine fingerprinting and more
- Prevent lateral movement (e.g. Mimikatz), brute-force, ransomware, reconnaissance
- Automatically respond to detected threats (including 3rd party alerts) with real-time step-up authentication
- Minimize false-positive alerts for the SOC

Unified Visibility and Auditing

- Consolidated auditing of all access activity across the organization
- Identify authentication vulnerabilities, high-risk accounts and unutilized privileges
- Actionable insights, reports and logs

SILVERFORT

US: (+1) 646.893.7857
43 Westland Avenue, Boston, MA, USA

Israel: (+972) 77.202.4900
30 Ha'arbaa St, Floor 26, Tel Aviv, Israel

Email: info@silverfort.com
www.silverfort.com

Gartner
COOL VENDOR
2019