SILVERFORT

SOLUTION BRIEF

PROTECTING THE UNPROTECTABLE

With Agentless Multi-Factor Authentication

Silverfort's holistic authentication platform monitors user access across all systems and environments and enforces adaptive AI-driven MFA, without agents, proxies or local configurations. It enables organizations to mitigate threats in real-time and achieve compliance with various regulations and industry standards including PCI DSS, GDPR, HIPAA, SOX, NIST and more.

Compromised and weak credentials are currently leveraged in four out of five data breaches. Mainstream MFA solutions can no longer handle the complexity and dynamic nature of today's networks. In many companies, the use of homegrown and proprietary systems that are not supported by current MFA solutions creates significant security and compliance challenges.

Agentless MFA for Any Sensitive Asset, including "Unprotectable" Systems

Silverfort's agentless MFA technology can seamlessly enforce MFA on access to any sensitive system or device, across all corporate networks and cloud environments. It enables MFA for sensitive resources without deploying software agents or inline proxies and without integrations with individual systems - an impossible task in large and dynamic networks. This enables Silverfort to extend protection to systems that were considered "unprotectable" until today, including: Homegrown and critical business applications, regulated systems and data (financial, healthcare, etc.), production servers, IT infrastructure (e.g. hypervisors, DCs and network equipment), administrative access (e.g. PAM, RDP, SSH), file shares, databases, SCADA, IoT devices and more.

AI-Driven Adaptive Authentication Across All Systems and Environments

Silverfort's Authentication Platform analyzes user behavior across all devices, resources and environments, on-premises and in the cloud, to enable continuous risk and trust analysis and adaptive authentication policies with unparalleled coverage and accuracy. Silverfort's advanced AI-based risk engine detects identity-related threats, including account takeover, lateral movement, ransomware and brute-force attacks, enabling real-time threat mitigation without disrupting the user experience.

> ***"Silverfort enabled us to address PCI DSS requirements and easily incorporate MFA to systems we couldn't previously protect. Silverfort saved us a lot of time and resources by avoiding any modifications to our systems."***
>
> **Michael Rubenchuk,**
> VP of IT Operations and Infrastructure at ***BlueSnap***
>
> BlueSnap®

Holistic Visibility, Continuous Risk and Trust Assessment

Silverfort's agentless architecture and holistic approach provide a big advantage as they enable unparalleled visibility into all user and machine activities across all systems and environments, continuously assessing risk and trust for every access request with unmatched accuracy. Silverfort provides a consolidated audit trail of all user activity and assists organizations in achieving least privileges as part of periodic entitlement reviews, by clearly showing which entitlements are being used and which are redundant. Silverfort automatically maps vulnerabilities and risks, including use of weak authentication protocols, stale accounts and devices, old or expired passwords, shared accounts and more.

Addressing Compliance Requirements with Silverfort

Silverfort helps organizations achieve compliance with the following regulations:

Regulation	Silverfort addresses the following requirements
PCI DSS	**Req 7:** Control all access to the CDE
	Req 8.3: Enable MFA across the CDE
	Req 10: Audit user access to all CDE assets
GDPR	Apply MFA for any access to applications, databases and file shares that contain personal information.
HIPAA and HITECH	Enable strict control over access to electronic health records (EHR) including data stored in file shares, databases and applications that process it.
	Secure communications with medical devices (including IoT devices) to ensure only authorized personnel can access them and alter their configurations.
SWIFT CSP	**Req 4.2:** Enable MFA across all SWIFT servers
	Req 5.1: Restrict unauthorized access and achieve least privileges
SOX (Sarbanes-Oxley Act)	Ensure secure access and least privileges by monitoring all activity and mapping redundant entitlements.
NIST SP 800-171	**Req 3.5.3 and 3.7.5:** Enable MFA for local and network access to privileged accounts, network access to non-privileged accounts and for maintenance access.

Silverfort's Unique Advantages

- Agentless MFA enablement for homegrown, proprietary and critical infrastructure systems
- The most accurate AI-based adaptive authentication engine, leveraging 10x-50x more data than any other authentication solution
- Non-intrusive MFA: no software agents, inline proxies or any integration with individual assets
- Enhances security while improving user experience, by minimizing MFA requests to high-risk situations
- Holistic authentication policies across all systems and environments

SILVERFORT

Contact us

US: (+1) 646.893.7857
43 Westland Avenue,
Boston, MA 02115

Israel: (+972) 54.660.0161
30 Ha'arbaa St, Floor 26,
Tel Aviv, Israel

info@silverfort.io

WWW.SILVERFORT.IO