SILVERFORT

Silverfort

Unified Identity Protection

Why Are Identity-Based Attacks Still On The Rise?

Identity-based attacks that utilize stolen or compromised credentials to access enterprise resources are increasing in volume, sophistication and impact.
Despite the availability of existing authentication and access solutions, many enterprise assets still rely on weak authentication mechanisms, without sufficient detection and prevention capabilities. This leaves on-prem and cloud environments exposed to account takeovers, malicious VPN compromise and lateral movement attacks.

Silverfort's Unified Identity Protection Platform

Silverfort delivers the first purpose-built solution that prevents identity-based attacks across all network, on-prem and cloud resources. Using innovative agentless and proxyless technology, Silverfort seamlessly integrates with all IAM solutions, consolidating their visibility and security controls. This makes Silverfort the only solution that can monitor, analyze risk, and enforce real-time policies on all user and machine access to all resources, including those that couldn't be protected before.

Key Benefits

- ✓ **Protect the 'Unprotectable'** Extend MFA and Zero Trust policies to any asset including legacy apps, IT infrastructure, command-line tools and more
- ✓ **Non-Intrusive Architecture** No agents, no proxies, no code changes
- ✓ **Covering Both Humans and M2M** Holistic protection for users and service accounts
- ✓ **AI-Driven Risk Engine** Continuously monitoring and analyzing authentication activity across all systems and environments in real time
- ✓ **Minimize Disruptions** Adaptive risk-based policies ensure users' productivity is not disturbed

Silverfort Unified Identity Protection in Action

Continuous visibility across all **network**, **cloud** and **on-prem** access

High-precision AI-based risk analysis based on the full **context of user access activity**

Enforcement of adaptive controls including **MFA, RBA, service account protection and Zero Trust**

What is your Identity Protection Challenge?

Silverfort's Unified Identity Protection Platform Supports a Wide Range Of Use Cases

Extend MFA to Any System

Apply MFA or extend your current MFA to any resource and system, including those that couldn't be protected until today - **Without installing software agents on servers, proxies in the network, or changing apps.** This includes homegrown applications, legacy systems, admin command line access tools, file systems and databases, IT infrastructure and industrial systems.

Service Account and Privileged Access Protection

Protect highly privileged users and service accounts without the need to rotate passwords. Silverfort automates discovery, monitoring and enforcement of adaptive access policies on these accounts, blocking any attempt to leverage them for malicious access.

Identity-Based Zero Trust

Enforce identity-based Zero Trust access policies with a least-privilege approach by continuously analyzing the full context of users' access activity, from initial login through every resource within the hybrid network.

Lateral Movement Protection

Block lateral movement attacks and automated malware propagation in real time, by enforcing MFA and conditional access policies on remote administration and access tools (RDP, SSH, PsExec, PowerShell, WMI, etc.).

Hybrid IAM Consolidation

Consolidate the Identity Protection across your entire network, on-prem and cloud environments on your cloud IAM of choice (Azure AD, Okta, Ping, etc.), to enable unified visibility and security controls from a single console, including for assets that couldn't be migrated into your cloud IAM before.

Unified Risk-Based Authentication

Leverage an AI-based risk engine to analyze access requests of users and service accounts across all network, on-prem and cloud resources to detect identity-based attacks across your hybrid environment, and block them with adaptive access policies, while reducing disruption to the workforce.

Secure Remote Access

Secure all types of remote access by employees, admins and third parties, including VPN, Citrix, VDI, Exchange, SaaS applications, internet-facing servers and on-prem applications, not only at the initial login but also continuously throughout the network.

Visibility and Threat Hunting

Gain a detailed view of every access event to all resources in your on-prem and multi-cloud environments to address security weak spots, detect malicious activity and conduct forensic investigations.

info@silverfort.com

www.Silverfort.com

US
(+1) 646 893 7857
43 Westland Avenue,
Boston, MA, USA

Israel
(+972) 77 202 4900
30 Haarbaa St, 26th Floor,
Tel Aviv, Israel

Gartner COOL VENDOR 2019