WHITE PAPER

SILVERFORT

Trust Must Be Earned

SILVERFORT'S RISK-BASED ADAPTIVE AUTHENTICATION

Silverfort delivers adaptive authentication across all corporate networks and cloud environments from a unified platform, without requiring any software agents or inline proxies. By analyzing authentication activity across all users, devices, systems and environments, and leveraging Silverfort's AI-based Risk Engine, it enables holistic risk-based adaptive authentication with unparalleled accuracy. It enables Silverfort to effectively detect threats, stop them and prevent unauthorized access without disrupting the user experience.

This paper reviews the benefits and challenges of adaptive authentication, provides a technical overview of Silverfort's holistic risk engine, and explains the unique advantages of Silverfort's agentless next-generation authentication platform.

TABLE OF CONTENTS

ADAPTIVE AUTHENTICATION: SECURING CORPORATE IDENTITIES AND ASSETS WITHOUT IMPACTING USABILITY

According to Verizon, 81% of all data breaches take advantage of stolen or weak passwords. The risks associated with password authentication have been known for decades, and so is the solution — Multi-Factor Authentication (MFA). But while enforcing MFA is an effective security measure, if users are requested to re-authentication too often, it can be disruptive to the user experience and impact productivity. It is not reasonable to request employees, who access dozens of corporate resources every day, to re-authenticate every time they access a resource — they wouldn't be able to work.

Adaptive authentication minimizes the burden on the user by requiring MFA only when the risk level is high. It leverages real-time risk analysis to determine whether it is safe to allow a user to access a resource, or whether an additional authentication step (MFA) should be required.

The Challenges of Traditional Adaptive Authentication

Over the last few years, the popularity of adaptive authentication has been growing, and many MFA vendors are now offering this capability. However, since current MFA solutions were designed as point-solutions, that protect specific systems, their risk analysis is limited to activities related to those protected systems, covering only a small portion of the user activities. It's incapable of protecting the wide variety of endpoints, applications, servers, infrastructure, data, cloud resources and IoT devices that exist in today's organizations.

For example, a solution that applies adaptive authentication for remote access through a VPN Gateway, can calculate risk only based on connections that are done through that gateway — without considering the larger picture of authentication activity happening within the company's network to a variety of systems, devices and data.

The implementation of MFA as a point solution not only leaves sensitive assets unprotected — it also affects the accuracy of the risk analysis they can perform. After all, how accurate can risk analysis be if it only analyzes user access to a few resources? Or, if it only analyzes remote access? Wouldn't risk analysis be more accurate if it was based on the full scope of user behavior, across all systems and environments? And — if a user demonstrates suspicious behavior on one system — wouldn't you want your risk analysis to take that into account, and require additional authentication when the user attempts to access other systems?

INTRODUCING SILVERFORT'S HOLISTIC ADAPTIVE AUTHENTICATION PLATFORM

Silverfort's next-generation authentication platform monitors user access to all resources across the organization's on-premises and cloud environments, without having to deploy software agents or inline proxies. Its agentless architecture and holistic approach are a big advantage as they enable unparalleled visibility into all user activities, across all systems and environments, continuously analyzing risk for every authentication request with unmatched accuracy.

KEY BENEFITS

- **Apply risk-based adaptive authentication policies across all sensitive assets to block threats and ensure only authorized users are granted access**
- **Improve security and access controls while reducing the frequency of MFA requests and minimizing disruptions**
- **Enable strong authentication for all assets, including assets that were considered "unprotectable" until today: proprietary systems, IoT devices, file shares, critical infrastructure and others**
- **Effectively block threats such as account takeover, lateral movement, ransomware, brute-force attacks and more**
- **Simple installation and maintenance — no need for software agents or inline proxies, no complex integrations or configurations**

Why is Silverfort's Agentless Architecture Such a Big Advantage?

The unique architecture of Silverfort's agentless authentication platform enables it to monitor all authentication activities, across on-premises networks and cloud environments, without the need to deploy a software agent on each protected device or server, without inline proxies and without complex integrations.

Monitoring all authentication activities in one centralized platform allows Silverfort to analyze more data than any other authentication solution — typically hundreds of authentication requests per user per day. This provides a far more accurate risk score and enables adaptive policies that are less disruptive yet more effective. While other adaptive authentication solutions can apply only simple contextual rules based on location, device and time, Silverfort's holistic coverage provides enough data to leverage actual AI.

It also assures that polices are enforced in a holistic manner across all systems and environments: if a user fails the second authentication requirement for accessing a certain resource, Silverfort will elevate the user's risk score and apply appropriate measures (require MFA or block access) across all other corporate resources — whether on-premises or in the cloud.

Silverfort's Advanced Risk Engine Combines 3 Core Components:

- **AI-Based Anomaly Detection:** Silverfort monitors all authentication activity across the organization and builds a rich behavioral profile of each user and device. It continuously uses this data to train and calibrate advanced machine learning algorithms and detects deviations from normal activity.
- **Recognition of Known Malicious Patterns:** Silverfort analyzes monitored activities in search of known malicious attack patterns. It can recognize patterns of brute force attacks, lateral movement and more.
- **Threat indications from 3rd party security solutions:** Silverfort responds to threat alerts received from third party security solutions by instantly stepping up the authentication requirements.

The risk score is used by Silverfort's adaptive policies to determine the level of authentication required for each authentication request — granting access, requiring an additional authentication factor or blocking access as needed. In addition, Silverfort calculates an overall risk score per user, device and resource, to help security teams respond to threats and implement recommended authentication policies.

WHY SILVERFORT?

Silverfort is the only solution that can provide:

- Holistic adaptive authentication platform covering all systems and environments
- The most accurate AI-based adaptive authentication engine, analyzing 10x-50x more data than any other authentication solution
- Non-intrusive adaptive authentication: no software agents, inline proxies or any integration with individual assets
- Threat-Based Adaptive Authentication that responds to 3rd party security alerts with real-time step-up authentication
- Significantly improved user experience that minimizes the frequency of MFA requests and offers user-friendly MFA methods

"Silverfort enabled us to address PCI DSS requirements and easily incorporate MFA to secure privileged access to systems we couldn't previously protect. Other solutions were difficult to implement. Silverfort saved us a lot of resources and time by avoiding any modifications to our systems."

Michael Rubenchuk
VP of IT Operations and Infrastructure at ***BlueSnap***

A DEEP-DIVE INTO SILVERFORT'S ADVANCED RISK ENGINE

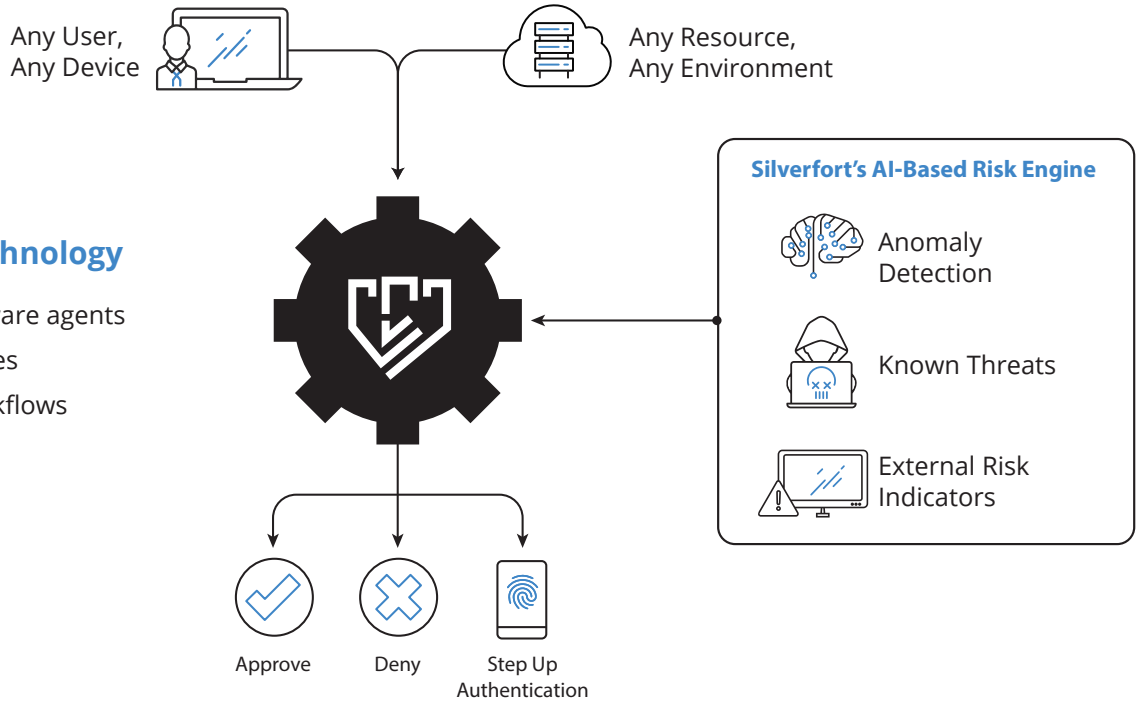
To enable accurate threat detection and effective adaptive authentication, Silverfort leverages an advanced risk engine that continuously calculates the risk of each individual authentication request, as well as the overall risk of each user, device and service in the organization.

Silverfort's risk engine combines 3 core components to analyze authentication activities in real-time and detect a wide range of malicious behaviors and threats. The combination of these components results in the most accurate risk score, and enables adaptive policies that are less disruptive yet more effective.

Patent-Pending Technology

- No need to deploy software agents
- No need for inline proxies
- No changes to user workflows

Silverfort's risk engine combines 3 core components



AI-Based Anomaly Detection

By monitoring all authentication activity across the organization, Silverfort builds a rich behavioral profile of each user and device. These profiles are used for training advanced machine learning algorithms which look for deviations from normal activities. While Silverfort is protecting the network, it continuously learns and updates these behavioral profiles.

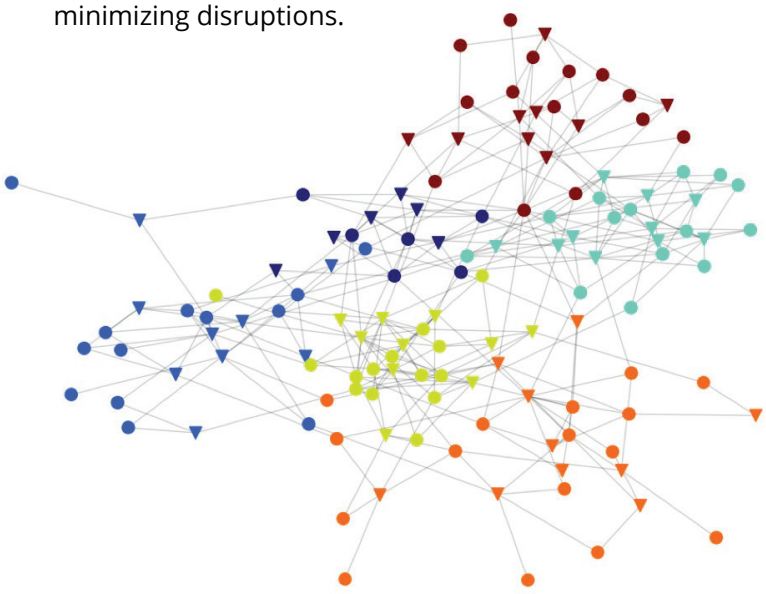
Silverfort's AI-based behavior analysis engine takes into consideration a number of important parameters, including:

- Authentication data: user name, client device, requested server and service name, authentication protocol, IP addresses, time, etc.
- Data from corporate directories: last logon, last password change, client OS, country code, group affiliation, user attributes, etc.
- Access patterns: resources typically accessed, endpoints typically used, work days, activity hours, frequency and velocity of access, etc.
- User & resource criticality: the level of criticality of the relevant user and the requested resource, as pre-determined by the organization
- MFA responses: approved, denied, timed out — this is also used for reinforcement learning (continuous training of Silverfort's machine learning algorithms using the MFA response as automatic feedback).
- Community clustering and peer analysis: automatic clustering of organizational groups and roles based on their access activity, and analysis of individual user behavior compared to others in the same group.

While other adaptive authentication products may offer AI-based risk engines, these risk engines can only provide a partial analysis as they are limited to monitoring the authentication activity related to the specific systems on which they are deployed. This does not provide enough data for an effective behavior analysis.

"AI is only as good as the data you give it"
— Dr. Nicola Millard

Silverfort's agentless technology and holistic approach provide a significant advantage over any other adaptive authentication solution. The ability to learn user behavior across all systems and environments enables Silverfort to better analyze user activities, detect more threats more accurately, and apply effective adaptive authentication policies that improve security while minimizing disruptions.



Example of community clustering (Δ = servers; O = users; the algorithm automatically classifies groups and paints them with different colors. In this case, the yellow group is likely to be the company's IT department. Authentication between communities that rarely interact is of higher risk)

Recognition of Known Malicious Patterns

Silverfort's risk engine includes a unique component for detecting known threats, based on known malicious patterns. These patterns are a result of attack simulations, analysis of real threat logs that were shared by key Silverfort customers, and expert knowledge of Silverfort's top security researchers.

Silverfort's known malicious pattern detection engine considers all the data and parameters that are analyzed by the AI-based anomaly detection engine (see above) and applies an additional layer of analytics, searching for any indications of known attack patterns. This includes brute force attacks, lateral movement (such as Pass the Hash and Pass the Ticket), ransomware attacks and more.

To keep up with evolving threats, Silverfort continuously updates its algorithms, improving existing attack profiles and adding new ones as part of its software updates.

Unlike other adaptive authentication solutions which apply simple rules based on location, device and time, Silverfort uses real time threat detection to determine the risk score. Silverfort's unparalleled coverage and combination of AI-based anomaly detection with recognition of known malicious patterns enables Silverfort's risk engine to significantly improve adaptive authentication intelligence

"... by covering a broader set of use cases and resource types, Silverfort will have access to a greater swath of authentication telemetry and thus be able to make more informed contextual access decisions than more narrowly focused adaptive authentication offerings... We like Silverfort's approach, and see a clear need to eliminate functional silos in one of the most fragmented corners of the highly-fragmented cyber security market."

Garrett Bekker
Principal Security Analyst, ***451 Research***

Threat Indications from Third Party Security Solutions

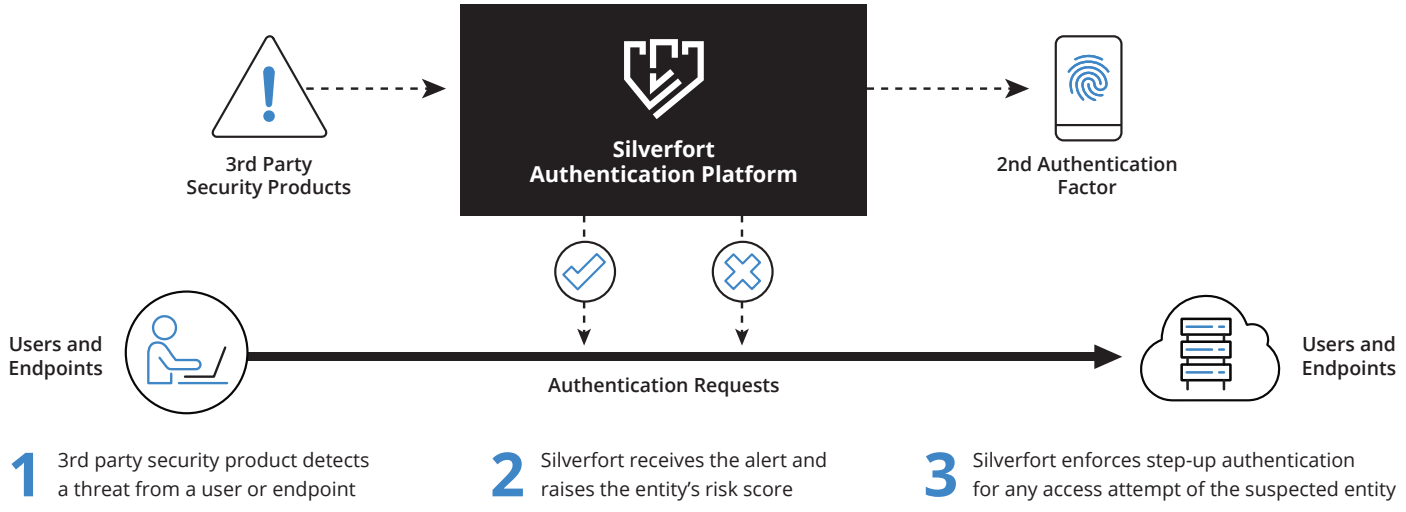
While other adaptive authentication solutions rely only on authentication activity as context for risk analysis, Silverfort looks at the larger picture. To further enrich Silverfort's behavior analysis, the platform can also leverage 3rd party risk indications and security alerts as triggers for step-up authentication. Silverfort can seamlessly integrate with third party security products, including firewalls, endpoint protection solutions, UEBA solutions, SIEMs and more. Silverfort's technology partnerships with leading vendors such as Microsoft, Check Point, Palo Alto Networks, CyberArk and others ensure joint customers can leverage best-of-breed solutions for effective real-time threat response.

Silverfort's ability to enforce step-up authentication in response to external threat indications is valuable not only for improving authentication policies, but also for achieving real-time threat-prevention across the organization without affecting legitimate users.

When an alert is received from a third-party solution indicating suspicious user activity, Silverfort enforces MFA on any following user activities, providing the suspected users a chance to prove their identity.
If the user authenticates successfully, access is granted, and the user can continue to work without disruptions. However, if it's a malicious entity that fails to authenticate, access will be denied. For example, if a third-party firewall detects bot activity from a specific host, Silverfort automatically requires additional authentication for any subsequent access attempt performed from this host to any resource. This prevents attackers from accessing sensitive systems and data, on-premises or in the cloud, and from moving laterally in the network.

Silverfort's authentication results can also be used as automated feedback, allowing security teams to focus on actual threats and reduce the amount of false positive alerts.

Illustration of Silverfort's Threat-Based Step-Up Authentication



COMPARATIVE ANALYSIS: SILVERFORT AND OTHER ADAPTIVE AUTHENTICATION SOLUTIONS

1. Coverage

	Other Authentication Solutions	Silverfort
Cloud applications	Yes	Yes
Modern on-prem applications	Yes	Yes
VPN gateways	Yes	Yes
RDP (remote desktop)	Yes, but requires an agent/proxy	Yes
SSH	Yes, but requires an agent/proxy	Yes
Windows logon	Yes, but requires an agent	Yes
Hypervisors and other IT infrastructure	Specific integrations only	Yes
3rd party appliances	Specific integrations only	Yes
File shares (ransomware protection)	No	Yes
IoT devices / OT systems	No	Yes
Critical financial systems (e.g. SWIFT)	No	Yes
Proprietary/legacy applications	No	Yes

2. Risk Engine

	Regular Authentication Solutions	Silverfort
Scope of risk analysis	Based on users' access to the specific servers/applications that are integrated with the solution (usually a small portion of corporate assets)	Based on continuous learning of all user activity across the entire organization, including access to all devices, servers and applications both on-prem and in the cloud. This results in detailed behavior profiles
Amount of data analyzed	Typically, less than 10 authentications per user per day	Typically, 200-300 authentications per user per day (including all user activity within the AD SSO)
Advanced AI-based policies	Simple static rules only — based on location, device, time, etc. No real AI.	Enables the creation of custom policies, provides advanced AI-based policies and includes out-of-the-box policies based on knowledge of known malicious patterns
External risk sources	No external real-time feeds	Capable of receiving real-time security alerts from 3rd party security products and use them to enrich the adaptive policy engine and trigger step-up authentication as immediate response

3. Deployment and Maintenance

	Regular Authentication Solutions	Silverfort
Deployment process	1. Deploy appliances/VMs 2. Integrate with each protected asset individually (typically using software agents/SDKs) 3. If hard tokens are used — manage distribution 4. If cloud-based MFA is used — export all corporate identities to the vendor's cloud service	1. Deploy VMs 2. Apply a simple configuration on the company's directory (Group Policy in the case of AD) • No modifications to endpoints and servers, no software agents, no inline proxies, no requirement to export identities to the cloud
Deployment Time	Depending on amount of assets. Typically, weeks (in SMBs) to months (in enterprises)	Hours to deploy a POC in the customer's network depending on network size
Maintenance	1. Additional integration required whenever a new server/application requires protection 2. Hard tokens need to be distributed, can be lost, and last 2-3 years	1. New assets are protected without any additional efforts 2. Automated self-service user enrollment mechanism

ABOUT SILVERFORT

Silverfort delivers strong authentication across entire corporate networks and cloud environments, without any modifications to endpoints and servers. Using patent-pending technology, Silverfort enables adaptive multi-factor authentication for all sensitive users, devices and resources, including systems that don't support it today, such as IoT devices, critical infrastructure, file systems and more. Silverfort allows organizations to prevent data breaches and achieve compliance instantly, by preventing identity-based attacks even across complex, dynamic networks, including hybrid and multi-cloud environments.

The company has received world-wide recognition and several industry awards, including the InfoSecurity 2018 Global Excellence Awards for Best Authentication Product and Best User and Entity Behavior Analytics Product, the Frost & Sullivan 2017 New Product Innovation Award, and is a gold winner of the Cybersecurity Excellence Awards in the Multi Factor Authentication category. To learn more visit: **www.silverfort.io**

CONTACT US

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

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