REPORT REPRINT

Silverfort looks to fill the white space in the highly fragmented authentication market

GARRETT BEKKER

25 AUG 2017

The startup has introduced an authentication platform that it claims can deliver strong authentication to any user, device, resource or system without making any changes to client devices or applications or installing an agent or in-line gateway.

We have written often about the growing cries for eliminating passwords, and with many studies pointing to compromised credentials as the main culprit in most data breaches, there has been a surge of interest in new technologies intended to get rid of passwords once and for all. Yet one of the common shortfalls of most authentication offerings – both legacy and 'next-gen' – is that they are typically designed for specific user populations and sets of resources.

For example, traditional hardware tokens are most often used for remote employees accessing internal applications via a VPN, privileged account management (PAM) tools focus on controlling access by high-risk insiders to critical resources, and many 'newer' authentication offerings are largely focused on controlling access to web-based applications that support standards like SAML or OAuth.

Israel-based startup Silverfort offers an authentication platform that can deliver strong authentication to any user, device, resource or system, across on-premises, cloud and hybrid environments. More importantly, the company claims it can accomplish this without making any changes to client devices or applications or requiring any modifications to user behavior, and also without installing an agent or in-line gateway.

THE 451 TAKE

By targeting resources that are currently difficult to support with strong authentication, Silverfort is trying to find white space in the market that is either not touched by or is underserved by existing authentication vendors. 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. Although Silverfort's technology could logically make a claim as a primary authentication choice, it may prove difficult to unseat incumbent authentication vendors. The challenge will be to convince organizations they need a secondary or tertiary authentication vendor to cover additional resources and use cases, and that a startup can serve as a consolidating force. Silverfort's best chance of near-term success will likely be as a complement to existing authentication offerings, and thus developing strategic partners will be key.

CONTEXT

Silverfort was founded in 2016 by CEO Hed Kovetz, president Matan Fattal and CTO Yaron Kassner, each of whom previously served in the highly regarded 8200 cybersecurity unit of the Israeli Defense Forces. Leonid Shtilman, co-founder and CEO of Viewfinity (acquired by CyberArk in 2015 for $30.5m in cash), serves as executive chairman and VP of business development. Silverfort maintains its current headquarters in Tel Aviv and plans to open a US office soon. The vendor recently emerged from stealth and claims it has several customers in production mode, and employs 12 full-time staff. Silverfort has raised $2.5m in seed capital from StageOne Ventures, SingTel Innov8 (SingTel's VC arm) and private investors, and plans to raise a series A round later in the year.

PRODUCTS

Silverfort bills itself as an authentication platform, which essentially serves as an overlay on top of an organization's existing directory services. In terms of architecture, Silverfort started out as an in-line gateway device, but found that performance challenges and the need to deal with encrypted traffic warranted a different approach. The current architecture involves a virtual appliance that sits either on the customer's premises or, more likely, is hosted in a cloud service such as AWS or Microsoft Azure and communicates with the organization's directory servers.

The directory server is configured to forward authentication requests to Silverfort's virtual appliance (over a VPN), which inspects each authentication request and compares it to an access policy to determine whether additional protection should be enforced (for example, requiring a second authentication factor or denying access). In cases where additional authentication is needed, Silverfort's appliance performs an out-of-band authentication to a mobile phone or other authenticator (from either Silverfort or other MFA vendors). If the authentication is approved, Silverfort's appliance releases the original message back to the directory server.

Because Silverfort does not interfere with or alter the actual authentication messages, both the client and the service remain unaware of the additional authentication layer. Silverfort has a patent pending that allows the product to analyze authentication messages in real time without decrypting them, and thus does not require any keys or permissions. Since Silverfort leverages the built-in features of existing directory services, the directory server can also handle failover if something goes wrong.

Silverfort's appliance can provide strong authentication to proprietary applications and IT infrastructure such as domain controllers and hypervisors, Windows and Linux servers and file servers, and also for machine-to-machine use cases without requiring an agent or SDK as many existing authentication offerings do. The product is also architected to protect resources in on-premises, cloud and hybrid environments. Silverfort is working on a SaaS-based version of its authentication server for those who are willing to open a VPN tunnel from their directory to the cloud.

Silverfort is also working on developing a risk engine for adaptive authentication, and plans to give customers the option to use either Silverfort's own risk engine or integrate with customers' existing UBA systems to alert on potential anomalies and send requests for step-up authentication. The intent is that 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.

Silverfort also has a discovery component that can scan an entire organization's network (both on-premises and cloud), including users, groups, devices and resources, to create an 'access map' that can be used to configure authentication policies. It also looks for potentially vulnerable or risky authentication processes. An administrator dashboard provides trending analysis for visibility, auditing and reporting.

STRATEGY

Silverfort will focus initially on midsized to large enterprises in the usual cyber security target verticals, including financial services, health care and technology. The initial go-to-market plan is to focus on providing adaptive authentication for resources that other vendors can't support (mainly, non-web systems), and possibly integrate or partner with web-focused vendors to achieve more holistic coverage.

Silverfort will make its products available as either an on-premises or cloud-hosted virtual appliance, while a forthcoming SaaS version will likely attract SMB customers. Pricing is via an annual subscription, with fees both for the number of users (list price at roughly $15 per user) and for directories supported (roughly $1,000 per directory instance).

Other features on the company's development roadmap include user behavior analytics (UBA) and a risk engine that will support adaptive or risk-based authentication and also consume data feeds from other UBA or adaptive authentication vendors.

Silverfort also plans to pursue technology integrations with network security vendors to inject identity into network access controls. An example use case would be if a firewall or IPS sees a bot or something suspicious, it could send an alert to Silverfort and require that those endpoints or end users provide MFA before accessing a potentially affected resource.

COMPETITION

Although Silverfort does offer its own authenticator for firms that don't already have their own, the company is clear that it is not looking to compete directly and views itself as more complementary to pure authentication offerings such as Duo Security, Google Authenticator, RSA Security (Dell), Entrust Datacard, Gemalto SafeNet or Yubico. By targeting resources that are currently difficult to support with MFA, Silverfort is trying to find white space in the market either not touched by or underserved by existing MFA vendors. As an example, Silverfort could provide authentication for proprietary apps or resources that don't support SAML or other standards without needing an agent, alongside authentication vendors that mainly provide strong authentication to web- or cloud-based apps. Silverfort does provide its own proprietary authenticator for customers that currently lack MFA, but the vendor plans to compete mainly on the value of its platform and can easily consume authenticators including the above-mentioned Duo Security, Google Authenticator, RSA Security (Dell), Entrust Datacard, Gemalto SafeNet or Yubico.

As its adaptive authentication capabilities are built out, Silverfort could overlap with vendors such as Duo Security, SecureAuth, RSA Security (Dell), Entrust Datacard and Gemalto SafeNet, as well as IDaaS vendors with adaptive authentication capabilities such as Okta and OneLogin – particularly following the former's acquisition of Stormpath. Other new vendors such as Auth0 and Transmit Security are looking to provide authentication platforms for application developers to easily integrate strong authentication into custom apps, with Transmit focusing more on anti-fraud use cases.

SWOT ANALYSIS

STRENGTHS

Silverfort has the ability to support MFA for a wide variety of resources and architectures with limited configuration work and without installing agents or relying on SDKs.

WEAKNESSES

Silverfort is in an early stage, and thus many planned features are still in development, such as a risk engine for adaptive authentication and support for directories other than Active Directory.

OPPORTUNITIES

Silverfort will likely gain initial traction with midsized to large enterprises that have heterogeneous environments spanning on-premises and cloud architectures.

THREATS

The primary threat to Silverfort will likely come from existing MFA vendors that may look to extend their support for a wider variety of non-standards-based resources.