SILVERFORT

Improving Cybersecurity with Unified Identity Protection

Silverfort's Response to the Executive Order On Improving the Nation's Cybersecurity

Following recent cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident, President Biden signed on May 21st, 2021 an Executive Order (EO) to improve the nation's cybersecurity and protect federal government networks.

The EO states that the United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. Modernization is required for keeping pace with today's dynamic and increasingly sophisticated cyber threat landscape. The prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security.

However, protecting federal networks is not enough. The EO encourages private sector companies to follow the Federal Government's lead and take the required measures to augment and align cybersecurity investments with the goal of minimizing future incidents: "The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace."

Modernizing Federal Government Cybersecurity

The EO states that "The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services… centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals."

Silverfort's Unified Identity Protection platform is uniquely positioned to help agencies and enterprises address three main requirements:

- Establishing multi-factor, risk-based authentication and conditional access across the enterprise
- Prioritizing resources for the adoption and use of cloud technology
- Developing a plan to implement Zero Trust Architecture

Establishing multi-factor, risk-based authentication and conditional access across the enterprise

One of Silverfort's Unified Identity Protection platform core capabilities is the ability to extend multi-factor authentication to any system or resource, including those that couldn't be protected until today, without requiring deployment of software agents on servers, without proxies in the network, and without any application integration or code changes.

Silverfort's patent-pending technology allows enterprises and federal agencies to secure access to any system or resource, across on-premise and cloud environments, including homegrown and legacy applications, IT infrastructure, file shares and databases, and even OT servers in industrial networks.

Silverfort's platform continuously monitors all access – both human-to-machine and machine-to-machine, and leverages a cutting-edge AI-driven risk engine to calculate the risk associated with each request. It can then apply static or risk-based authentication policies to step up the authentication requirements when the risk is high, or block access altogether.

Conditional access policies can be easily created via Silverfort's easy-to-use management console, and enforced in a unified manner across hybrid environments to ensure only authorized access, by validated users, is taking place.

Prioritize resources for the adoption and use of cloud technology

A main barrier to cloud migration is the (lack of) ability to enforce modern security controls, like MFA and Risk-Based Authentication, on migrated assets, and the difficulty of managing complex hybrid networks.

Modern enterprise networks can be highly diverse and include many different assets, from legacy IT infrastructure to modern cloud workloads. This drives the need for multiple IAM products, each covering a different need – access to on-prem resources, access to cloud apps, secure remote access and so on. Today, IAM solutions are not only managed separately, they also provide different protection capabilities, creating both a management and security problem. In terms of Identity Protection, the problem is even more severe. While cloud-native and modern web apps can be protected by MFA, Risk Based Authentication and conditional access policies, which can effectively prevent 99% of identity-based attacks, enforcing these controls on on-prem assets is very difficult, sometimes even impossible. Migrating these on-prem assets to the cloud, requires enforcement of security controls, which often requires some code changes – making the process expensive and difficult, if not impossible.

Silverfort enables enterprises and federal agencies to consolidate their Identity Protection on their Cloud Identity Provider (IdP) of choice, allowing them to simplify and optimize their efforts across on-prem and multi-cloud resources. This unique technology makes Conditional Access, Risk Based Authentication and MFA fully applicable to core enterprise resources – from their cloud IdP. By this, Silverfort enables enterprises to apply best-of-breed Identity Protection across all resources and access attempts. To read more about this see: https://www.silverfort.com/blog/consolidating-your-hybrid-iam-on-microsoft-azure-ad/

Planning and Achieving a Zero Trust Architecture:

The EO explains that the term "Zero Trust Architecture" means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. "Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment."

Silverfort's platform enables enterprises and federal agencies to easily plan and implement an identity-based Zero-Trust security model. Unlike Zero-Trust Network Access (ZTNA) solutions, that focus on the device and the network segment it's attempting to access, an identity-based approach considers the user's identity and behavior profile to determine the risk level and applies dynamic risk-based access controls.

Silverfort's identity-based Zero-Trust security model offers several important advantages:

- **It's quick and easy to implement, no network changes required** – Silverfort's deployment doesn't require any network changes such as deployment of proxies in the network or micro-segmentation. It also doesn't require deployment of software agents or code changes, making both the planning and the deployment smooth and simple.
- **It monitors all access both inside and outside traditional network boundaries** – Silverfort monitors all the authentication activity across the hybrid network, covering any access to on-prem resources and cloud assets. It does not divide the network into micro-segments, assuming that access contained within a segment is trusted. Any access request is monitored and analyzed in real-time to determine if it can be trusted or not.
- **It can apply dynamic risk-based authentication and access policies** – Silverfort continuously monitors all access requests for both on-prem and cloud resources, and leverages a cutting-edge AI-driven risk engine to calculate the risk level associated with each access request – whether it's a human accessing a resource, or machine-to-machine communication executed by service accounts.
- **It provides unified visibility, security and control across all users, devices and resources** - Silverfort offers valuable insights and detailed auditing trail in a centralized dashboard, to support IT forensic investigations. This enables quick detection and response to intrusions, prevents the spread of threats like ransomware, and helps IT determine the extent of an incident after the fact.

To learn more about Silverfort's Unified Identity Protection Platform, its unique agentless and proxy-less technology, and its superior capabilities, visit us at www.Silverfort.com.

About Silverfort

Silverfort is the provider of the first Unified Identity Protection Platform that consolidates security controls across corporate networks and cloud environments to block identity-based attacks. Using innovative agentless and proxyless technology, Silverfort seamlessly integrates with all existing IAM solutions (such as AD, ADFS, RADIUS, Azure AD, Okta, Ping, AWS IAM, etc.), extending their coverage to assets that could not be protected until today, such as homegrown/legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access and more. It continuously monitors all access of users and service accounts across both cloud and on-premise environments, analyzes risk in real time using an AI-based engine, and enforces adaptive authentication and access policies. Silverfort allows organizations to prevent data breaches, achieve compliance, reduce costs and simplify cloud migration. Silverfort is trusted by large enterprises around the world and was named a Gartner 'Cool Vendor'.

To learn more schedule a meeting at:
www.silverfort.com/request-a-demo

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