Forcepoint

Solution Brief

Executive Order on Improving the Nation's Cybersecurity

Important steps our Federal Government must take to strengthen our Federal Cybersecurity

Challenge

- There has been a 63% increase in Federal cybersecurity incidents
- 65% of agencies report the severity of incidents is getting worse

Solution

Biden's latest Executive Order attempts to lay out a framework to improve Federal Cybersecurity by:

- Adopt security best practices to move left of breach
- Improving security for cloud services
- Requiring agencies to adopt Zero Trust architectures

Outcome

- Meaningful visibility: Understanding user behaviors with real-time risk calculations
- Expanding your data protection to the cloud to secure inter-agency data sharing and prevent data leakage
- Leveraging behavioral attributes for continuous, adaptive Zero Trust

Challenge

In the wake of recent attacks on U.S. agencies like Sunburst, newer Critical Infrastructure attacks like Colonial Pipeline attack, and recent data showing that similar attacks are growing in frequency, learning from these incidents and setting a new course for national cybersecurity is critically important.

In May of 2021, President Biden signed an Executive Order that outlines steps the US Federal Government must take to improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. It also outlines steps to partner with the public sector to improve collaboration.

Improving our Nation's Cybersecurity and Moving Left of Breach

The Biden EO states that agencies must work with the private sector to adapt to a continuously changing threat environment, ensure products are built and operate securely, and partner to foster a more secure cyberspace.

Moving "left of breach" is the modern cybersecurity path forward that every agency should be striving for. That means focusing cybersecurity resources on detecting and preventing potential breaches rather than cleaning up after a breach has already occurred. The private sector is also important to any plan the Federal Government makes to move "left of breach ," as the software supply chain vulnerabilities are being actively attacked as we saw recently in the SolarWinds attack

Getting to a more proactive cybersecurity posture requires agencies and the private sector to work to achieve meaningful visibility. Navigating a rapidly changing borderless security environment is challenging. Basic visibility isn't good enough. Getting to meaningful visibility will require a re-examination of your data and user protection strategies.

Core elements of a robust strategy includes:

→ Visibility to how users interact with an organization's data and intellectual property (IP)

→ Continuous evaluation of user interaction with data and devices/ applications.

→ Leveraging behavioral intelligence with meaningful data to identify and mitigate risks.

"When balanced with existing cybersecurity policies and guidance, identity and access management, continuous monitoring, and best practices, a ZTA [Zero-Trust Architecture] can protect against common threats and improve an organization's security posture by using a managed-risk approach." **NIST SPECIAL PUBLICATION 800-207**

These core elements enable agencies and industry partners to gain deep visibility on the interaction between users, data, and applications to improve their data protection and compliance strategies. Most organizations have a certain degree of network visibility. Even so, this can improve.

Expanding data protection coverage to the Cloud

Agencies are challenged with complicated environments, where data is everywhere and require the protection of data in places that are not managed or owned by the agency. For this reason, agencies require a comprehensive data security policy that extends protections to the cloud and protects federal data, wherever it resides. The Biden Executive Order calls for the Federal Government to maniacally focus resources on protecting and securing its computer systems, whether they are cloud-based, on-premises, or hybrid. In this environment, agencies must focus response team to identify and protect data across cloud applications, network stores, databases, and managed endpoints.

- → Identify and automatically prevent sharing of sensitive data to external users and unauthorized internal users.
- → Protect data in real-time for upload into and downloads from critical cloud applications including Office 365, Box, Dropbox, Google Apps, Amazon AWS, Zoom, Slack, and many more.
- → Unify policy enforcement with a single, consolidated policy that defines and applies protection for data in motion and discovery for data across all channels—cloud, network, and endpoints.
- → Extend DLP policy features including fingerprinting and machine learning to cloud applications, while having the option to maintain incidents and forensics data within your secure environment.

Improving the effectiveness of data loss prevention

Understanding behaviors, especially in terms of how users interact with data across networks and devices is starting to emerge as a piece of the puzzle. That's a big reason why more agency leaders and CISOs are beginning to see behavior-based technologies as the future of cybersecurity.

Leverage behavioral attributes for continuous adaptive Zero Trust

The EO also stresses the importance of Zero Trust and calls for federal agencies to develop plans to adopt Zero Trust architectures within 60 days following the issuance of the order.

Previously there were quite a few models and definitions for Zero Trust for agencies to implement. However, the EO suggests that agencies should "incorporate, as appropriate, migration steps that the National Institute of Standards and Technology (NIST)...has outlined in standards and guidance." This may help to provide a provides a standard definition and framework upon which agencies can and should build their Zero Trust security posture.

An effective Zero Trust architecture drives agencies towards a more data and user-centric approach while moving away from being perimeter-centric. Integrating DLP with behavioral analytics enables your Zero Trust architecture to have:

- → Individualized adaptive data policies
- → Behavioral analytics driven insights
- → Data discovery and classification
- → Maximizing security analyst efficiency and reducing fatigue

Using behavior-based cybersecurity, your security adapts to changing levels of risk. This includes enterprise-wide visibility (network, endpoints, and cloud) and enables detection when people are exhibiting risky behavior: their risk score changes depending how they behave at any time, allowing security to tighten targeted policies and block actions if required. This helps security teams decide what is innocent or suspicious based on behavior in context, reducing false positives by leveraging intelligent data security to revisit decisions as you and your machines learn.

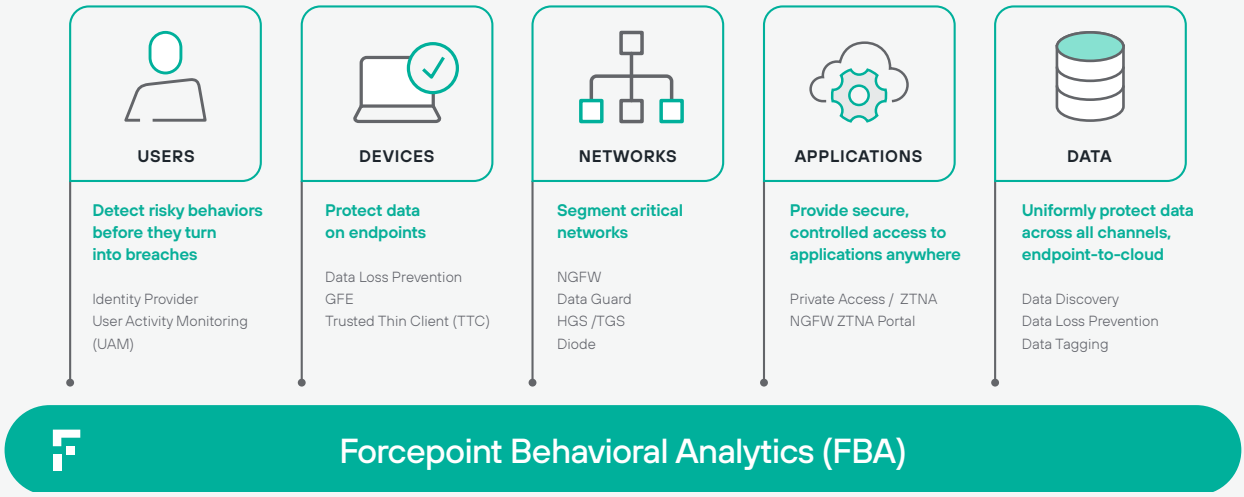
Partnering with Forcepoint for Zero Trust Continuous Risk-Adaptive Protection

By partnering with Forcepoint, agencies can move toward Zero Trust continuous risk-adaptive data protection. Only Forcepoint can provide this level of comprehensive protection for the agencies and has the building blocks to grow with them as they look toward Zero Trust in the future.

Forcepoint brings together best-in-class capabilities, including Data Loss Prevention (DLP), Cloud Access Security Broker (CASB), Web/Email Security and Network Security that can stand alone or integrate within an existing environment. These solutions, when deployed together, enable agencies to extend comprehensive data leakage protection across common vectors of data loss.

Zero Trust Continuous Risk-Adaptive Data Protection

Forcepoint converged cybersecurity solutions audit for threats across your environment and enable you to automate remediation.



forcepoint.com/contact