Stronger Cybersecurity Starts With a Data Operating System

Modern

In an ambitious effort to reduce the threat of cyber attacks on critical infrastructure in the United States, President Biden signed an executive order to improve cyber threat information sharing between the government and the private sector. Signed in May, the order aims to fill gaps in the public and private sector approach.

This move highlights how critical advanced cybersecurity is to US infrastructure. The community talks a lot about how digital transformation is a crucial part of creating a disruption-proof supply chain. However, one downside is that with increased connectivity comes more responsibility to stay ahead of threats. The executive order can guide companies on how to protect their supply chain and what a next-gen cybersecurity approach can look like.

The Government Is Making Cybersecurity Policy a Top Priority

The government's approach to cybersecurity has been patchy and with little guidance for the private sector. However, an increase in cybersecurity threats to the private sector from government sources of other nations has changed the game.

Biden plans to increase support for new cybersecurity measures and approaches and to explore bold changes to the government's entire infrastructure to protect assets. If the government plans to follow through with these actions, the private sector can't help but follow.

The supply chain can expect more guidance from governmental sources in the coming months and years as the executive order takes effect. However, reciprocal communication will be a priority, so companies will need to structure the data ecosystem to account for this information sharing.

Cyber Threat Information Sharing Is a Key Priority

Section two of the new order requires that IT service providers — including cloud providers — share data breach information liberally with government departments and agencies tasked with fighting cyber threats. Until this point, providers could choose to withhold information from certain departments.

Service providers will be supplying more information about breaches and potential threats, making it easier for the government to adjust responses. This could be very good for private sector companies looking to move their own cyber threat responses to a more proactive approach.

Federal Cybersecurity Standards Are Modernizing — Everyone Else's Should Too

Other sections in the executive order aim to fully modernize the government's approaches and tools in the realm of cybersecurity. The executive order outlines:

- Pursuit of Zero Trust Architecture (ZTA)
- The transition to more secure cloud services
- Centralized, streamlined access to cybersecurity data
- A focus on endpoint detection and response (EDR)
- Making system log information available from internal and third-party networks

Again, this is a coordinated, proactive approach to cybersecurity. The government wants to monitor and respond early to nation-state attacks on both public and private sector assets and is willing to make big investments for the tools to make that possible.

Protecting the Supply Chain From Cyber Threats Requires Something New

Supply chain companies will need a new approach to cybersecurity to remain in compliance with the executive order and to prevent another SolarWinds-style attack. Threat actors tend to attack the following when trying to breach a supply chain:

- Login Credentials: JBS and the Colonial Pipeline hacks were due to login credential weaknesses.
- Software loopholes: Unprotected remote desktop protocols, VPNs, and untested open-source software have all been vulnerabilities in the past.
- Unaddressed digital risks: More tools, more data copies, and more vendors leave plenty of weaknesses in a cybersecurity management plan.

Companies can better address these threats by unifying their data ecosystem under a single roof. This doesn't have to be a rip-and-replace approach. Companies can create an operational layer that allows them to take the following steps towards protecting the supply chain.

Improve Observability Throughout the Entire Organization

Companies need to understand the five Ws of their data: who, what, when, where, and why. Therefore, implementing a single data ecosystem with central, native governance and full visibility is essential. A data operating system can tell decision makers where their data comes from, who has access, when data was used, and for what task. It also could provide context for all dependencies. This observability helps companies quickly sort out their data parameters.

Implement Zero trust Architecture
There are many moving parts: companies sharing data, workers performing tasks remotely, partners reporting, audits. It's a long list. Zero trust assumes all network activity is malicious by default, which reduces common cyber attack weak points — emails, logins, and other access points. In addition, threat actors know that third-party vendors are a potential weakness because they often have access to a company's sensitive data but may not have the same security protocols.

Eliminate Shadow IT
Shadow IT, or IT products and tools deployed without the knowledge of major decision makers within the IT department, can be another serious weakness in security. These products have access to the network, but IT may not know it, leaving them outside the range of normal observability. Instead, implementing integration products that connect legacy systems with modern tools without patchwork solutions can reduce the risk that shadow IT will provide a loophole.

Leverage Attribute-based Access Controls
Data should be available to all stakeholders for decision-making. This is the primary goal of digital transformation within any organization. However, freeing data may improve predictive analytics and operational automation, but it opens the supply chain up to greater risk. Native ABAC governance controls enable the organization to make data available appropriately for stakeholders without creating many different data copies or introducing inconsistencies in the security policy.

A Data Operating System Can Help Protect the Supply Chain

The government's executive order is clear: it's time to take better care of cybersecurity policies and treat threats more efficiently. With a data operating system, companies can still leverage the full power of their data and its ecosystem while building secure frameworks like ZTA. It can automate reporting to share with public entities and create a layer of observability into the data ecosystem and all its dependencies. The executive order may start another cybersecurity transformation, but the data operating system will bring it all together.

Learn more about security and governance with DataOS.

Learn more →

BY E. WALLACE

TheModern DataCompany

Stronger Cybersecurity Starts With a Data Operating System

The Modern Data Company
306 Cambridge Ave
Palo Alto, CA 94306
TheModernDataCompany.com
info@TMDC.io