Strategic Zero Trust Compliance

Defense Agency Deploys an Autonomous SOC

PUBLIC SECTOR

The release of Presidential Executive Order 14028, "Executive Order on Improving the Nation's Cybersecurity", requires all federal agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year 2024.

Given the tight timeline to convert from a perimeter-focused cybersecurity structure to a fully compliant Zero Trust Architecture (ZTA) strategy, many agencies are evaluating a wide variety of alternative solutions that could be quickly integrated into their existing cybersecurity portfolios.

But in a rush to meet ZTA compliance requirements, many of these agencies will miss out on the opportunity to make major improvements in their approach to cybersecurity.

Implementing Zero Trust is an opportunity to streamline, simplify, and save on their entire cybersecurity ecosystem. To implement an effective and reliable approach to ZTA, organizations must take a holistic view of the entire IT and security architecture instead of trying to bolt on a zero-trust front-end tool.

A HOLISTIC APPROACH TO ZERO TRUST

An effective Zero Trust Architecture is like a four-legged stool. It leverages MDR, Authentication, SASE, and SIEM to create a solid foundation for ZTA, where every element optimizes the value of the other elements.

MDR

MDR stands for Managed Detection and Response. It is an end-to-end solution that encompasses people, process, and technology to deliver security outcomes. The aim is to identify and respond to active cyber threats and exposures, conducting in-depth investigations to enable rapid elimination and/or containment.

AUTHENTICATION

Authentication is the process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

SASE

Secure access service edge, or SASE (pronounced "sassy"), is an emerging cybersecurity concept that Gartner first described in the August 2019 report "The Future of Network Security in the Cloud" and expanded on in their 2021 Strategic Roadmap for SASE Convergence.

SIEM

Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources.

To optimize their zero-trust effectiveness, organizations should seek to have an autonomous SOC that leverages AI and machine learning to not only collect endpoint data, but to monitor network activity and correlate it to identify threats, vulnerabilities, attacks, and provide incident response.

THE AUTONOMOUS SOC AND ZERO TRUST COMPLIANCE

As its new global SIEM, a Defense agency is deploying the Devo Platform, the first cloud-native security operations solution to combine critical security capabilities together with auto enrichment, threat intelligence community collaboration, a central evidence locker, and a more efficient analyst workflow. This powerful combination will enable the agency to transform its security operations centers (SOC) and scale security operator effectiveness. Devo will serve as the central security hub for protection, detection, and response across the agency worldwide for enterprise defense.

Devo, the only cloud-native logging and security analytics platform, recently acquired LogicHub, a security orchestration, automation, and response (SOAR) innovator.

Bringing SOAR technology to the Devo Platform realizes the complete stack of capabilities needed to deliver the autonomous SOC, a vision Devo unveiled earlier this year that aims to reinvent how security professionals work by providing complete visibility, automation, analytics, and access to the latest community expertise and content.

RAPID DEPLOYMENT, SCALABILITY, AND SPEED

Devo is cloud native, which enables massive scalability and takes less time to deploy than other solutions. This will allow agencies to develop a fully realized autonomous SOC well in advance of the deadline for zero trust compliance.

Since it is estimated that it takes a bad actor approximately 19 minutes to be fully embedded in an organization's infrastructure, Devo's ability to alert the SOC well under this threshold enables the agency to respond before damage can be done.

Unlike Splunk, Devo does not index data at the time of ingest. Devo can alert on suspect data immediately.

OPERATIONAL AND FINANCIAL BENEFITS

Organizations that migrate from Splunk to Devo can achieve significant direct cost savings, cost reductions, cost eliminations, and future cost avoidance.

Because Devo is deployed in the cloud, the organization doesn't have to pay to manage the infrastructure or pay for additional storage or servers.

Staffing is simpler and less expensive with the Devo Platform than with other solutions.

A key reason for the defense agency award was that the initial implementation showed the Devo Platform reduced more than 20,000 human hours of time currently spent by the agency's cyber operators on threat isolation, triage, and investigation processes, freeing analysts to focus on critical threat-hunting and resolution efforts.

STRATEGIC ZERO TRUST COMPLIANCE

Devo enables agencies to streamline, simplify, and save on their entire cybersecurity ecosystem while achieving zero trust compliance.

For more information, contact the Devo Public Sector team at public-sector@devo.com

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.