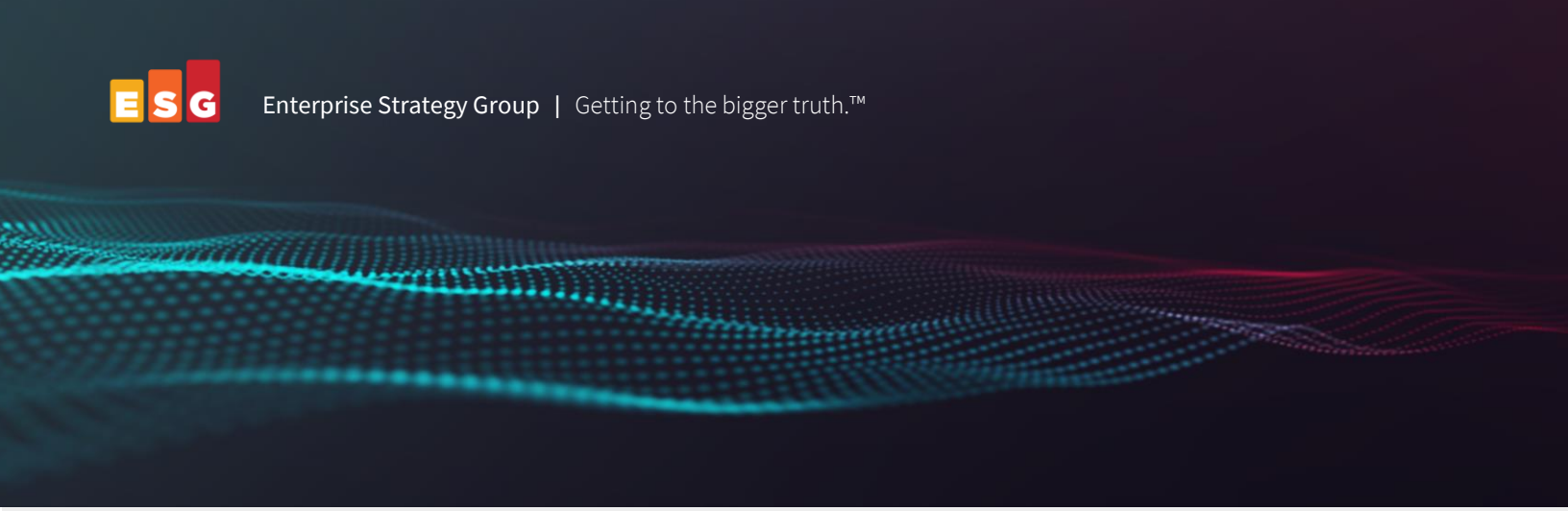


ESG WHITE PAPER

NDR as the Cornerstone for Visibility and Threat Detection to Support the Executive Order on Cybersecurity

By John Grady, ESG Senior Analyst; and Jon Oltsik, ESG Senior Analyst and Fellow

August 2021

This ESG White Paper was commissioned by Cisco and is distributed under license from ESG.

Contents

Executive Summary

Attacks on the United States federal government and critical infrastructure are not new but do seem to be more frequent and disruptive. While the government has implemented different programs over the years with an eye toward improving cybersecurity, their success has been limited to date. While high-level in some regard, the recent Executive Order on Improving the Nation's Cybersecurity certainly feels different from prior initiatives because its issuing is predicated on recent, highly disruptive attacks, and it includes the framework for prescriptive and definitive solutions as opposed to generic guidelines. It covers a variety of topics, but at its core lays out a plan for the government to develop new recommendations and requirements for federal agencies to: modernize their cybersecurity programs, improve the detection of vulnerabilities and incidents, and improve investigative and remediation capabilities for when incidents do occur.

Network detection and response (NDR) is critical in supporting many of the recommendations contained in the executive order). The term NDR may be new, but the technology, which is sometimes overlooked in the broad landscape of cybersecurity tools, is not. In fact, NDR should be an essential component of any threat detection and response program. Further, NDR is a core component of XDR strategies and a key aspect of supporting zero trust architectures, all of which are necessary to meet the Biden administration's executive order. Cisco's Secure Network Analytics can support these use cases through its reliance on advanced analytics, coverage for cloud and on-premises environments, and native and integrated approach to facilitate streamlined investigations and response.

Sometimes overlooked in the broad landscape of cybersecurity technologies, NDR should be an essential component of any threat detection and response program, a core component of XDR strategies, and a key aspect of supporting zero trust architectures, all of which are necessary to support the Biden administration's executive order.

The Federal Government Reaches a Cybersecurity Tipping Point

The United States federal government spends an enormous amount of money on cybersecurity products, services, and personnel. Yet despite this significant investment, federal agencies have been subject to a steady stream of successful attacks going back at least to the later part of the last century. Moonlight Maze and Titan Rain were some of the first targeted, successful, and publicized cyberattacks on federal systems in the late 1990s and early 2000s. The 2015 breach of the Office of Personnel Management (OPM) still represents one of the most significant persistent attacks targeting the federal government and resulted in the loss of personally identifiable information of millions of federal employees, contractors, and applicants.

Attacks on the Colonial Pipeline and federal IT suppliers have highlighted the fact that existing federal cybersecurity programs fall short, and an updated approach is needed.

More recently, a multi-year, escalating campaign of ransomware attacks on state and local governments, public sector institutions, small businesses, and large enterprises came to a head with the targeting of the Colonial Pipeline. Despite being privately run, the impact to national security interests of fuel shortages resulting from the pipeline's shutdown was more than enough to warrant federal intervention in the response. More directly, supply chain attacks targeting SolarWinds and Microsoft affected numerous agencies including the Departments of Treasury, Justice, and Energy. While tens of thousands of private sector organizations and other national governments were impacted as well, many believe the US federal government was a priority target of the attack. These attacks on the Colonial Pipeline and federal IT suppliers have highlighted the fact that existing federal cybersecurity programs fall short, and an updated approach is needed.

Where Existing Programs Have Failed to Meet Modern Challenges

The failure to detect and prevent these latest cybersecurity incidents is not due to lack of effort or previous attempts at improving cybersecurity in the federal government. In 2012, the Department of Homeland Security introduced the Continuous Diagnostics and Mitigation (CDM) program to standardize visibility and risk assessment across all federal civilian networks. The program focuses on improving asset inventorying, vulnerability assessment, and patch management; identity and access management; network security management; and data protection management. The goal was to have these broad and diverse disciplines tied together through a single, common dashboard to provide federal agencies a single source of truth for their security posture, streamline Federal Information Security Modernization Act (FISMA) reporting, reduce the threat surface, and improve response capabilities.

While in some ways the CDM program contains the building blocks for zero trust through its focus on identifying everything on the network and continually assessing its security posture, the breadth of the initiative and inconsistency of the dashboard tying the program together have resulted in limited success to date. Further, whereas zero trust requires changing security practices, policies, and strategies toward a default-deny and assume-breach posture, much of the CDM program is focused on aggregating and streamlining visibility across legacy methods to improve time to mitigation, rather than fundamentally altering the security approach.

The Einstein program goes back even further than CDM but similarly failed to detect recent attacks. This should not be surprising given the nature of the program, which was to observe traffic flowing in and out of federal networks and match against a massive database of known signatures. While the scale of Einstein goes beyond an intrusion detection and prevention system, the limitations into visibility of unknown attacks remain the same. Additionally, it remains reactive in nature.

The Executive Order on Improving the Nation's Cybersecurity

To address the shortcomings of existing programs and lay the foundation for modernizing the federal government's approach to cybersecurity, the Biden administration issued an executive order on May 12, 2021.[1] The order acknowledges that it is a first step in a longer but critical process and seeks to more effectively protect federal networks through modernization and improved response capabilities when incidents do occur. Additionally, while the guidance is directed at federal agencies, the order calls out the role of the private sector in managing critical infrastructure and acknowledges that all organizations (both public and private) can benefit from the recommendations the order sets out.

While the order more broadly includes recommendations to facilitate information sharing between the federal government and private sector, enhancements to supply chain security, and the establishment of a cyber safety review board; three sections specify a roadmap for how agencies should begin planning to modernize their cybersecurity, detection, and remediation capabilities.

- Modernizing federal government cybersecurity. Section 3 of the executive order highlights the need for agencies to adopt secure cloud services, implement zero trust architectures, and more broadly employ multi-factor authentication (MFA) and encryption. The call for zero trust architectures is especially noteworthy. While momentum around zero trust has certainly been increasing, the call for agency heads to develop a plan and schedule to implement the initiative within 60 days represents a significant acceleration. The work done by the National Institute

[1] Source: *Executive Order on Improving the Nation's Cybersecurity,* May 2021.

for Standards and Technology (NIST) through Special Publication 800-207 certainly helps and provides agencies a good framework with which to start.[2]

- Improving detection of cybersecurity vulnerabilities and incidents on federal government networks. Section 7 generally calls for the federal government to maximize the early detection of cybersecurity vulnerabilities and incidents by employing "all appropriate resources and authorities." It further identifies the need for centralized visibility into the detection of vulnerabilities and threats across all agency networks to improve the overall cybersecurity of the federal government. Specifically, endpoint detection and response (EDR) is highlighted through guidance that civilian executive branch agencies deploy these solutions and the ordering of the Director of the Office of Management and Budget (OMB) and Secretary of Homeland Security to develop recommendations and requirements for government-wide EDR approaches.

- Improving the federal government's investigative and remediation capabilities. Section 8 identifies the need to standardize and improve logging and retention requirements. In addition to setting a timeframe to assess what types of data should be maintained and for how long, the protection of the data collected is identified as a priority, as is the need for such data to be provided to the Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency (CISA), and the FBI when required.

How NDR Supports the Executive Order

NDR solutions apply a combination of non-signature-based advanced analytical techniques such as behavioral modeling and machine learning to network traffic and flow records to detect anomalous activity other security tools may miss that could be malicious activity. And build upon NTA solutions by providing response capabilities to act upon alerts.

While the executive order calls out some technologies quite specifically (e.g., EDR, MFA, and encryption), much of the guidance focuses on higher-level practices and leaves some room for interpretation. Unmentioned in the executive order specifically, but a critical and common thread across the three sections discussed earlier, is network detection and response. While the term NDR is new, the category is the evolution of the long-standing network traffic analytics (NTA) market. NDR solutions apply a combination of non-signature-based advanced analytical techniques such as behavioral modeling and machine learning to network traffic and flow records to detect anomalous activity other security tools may miss. This model is a baseline of normal network behavior and alerts security teams to suspicious traffic falling outside of that range that could be malicious activity. In some cases, records can be retained to aid in forensic investigations. Finally, these tools build upon NTA solutions by providing response capabilities to act upon alerts through integrations with network access control (NAC) solutions; firewalls; security orchestration, automation, and response (SOAR); or EDR solutions.

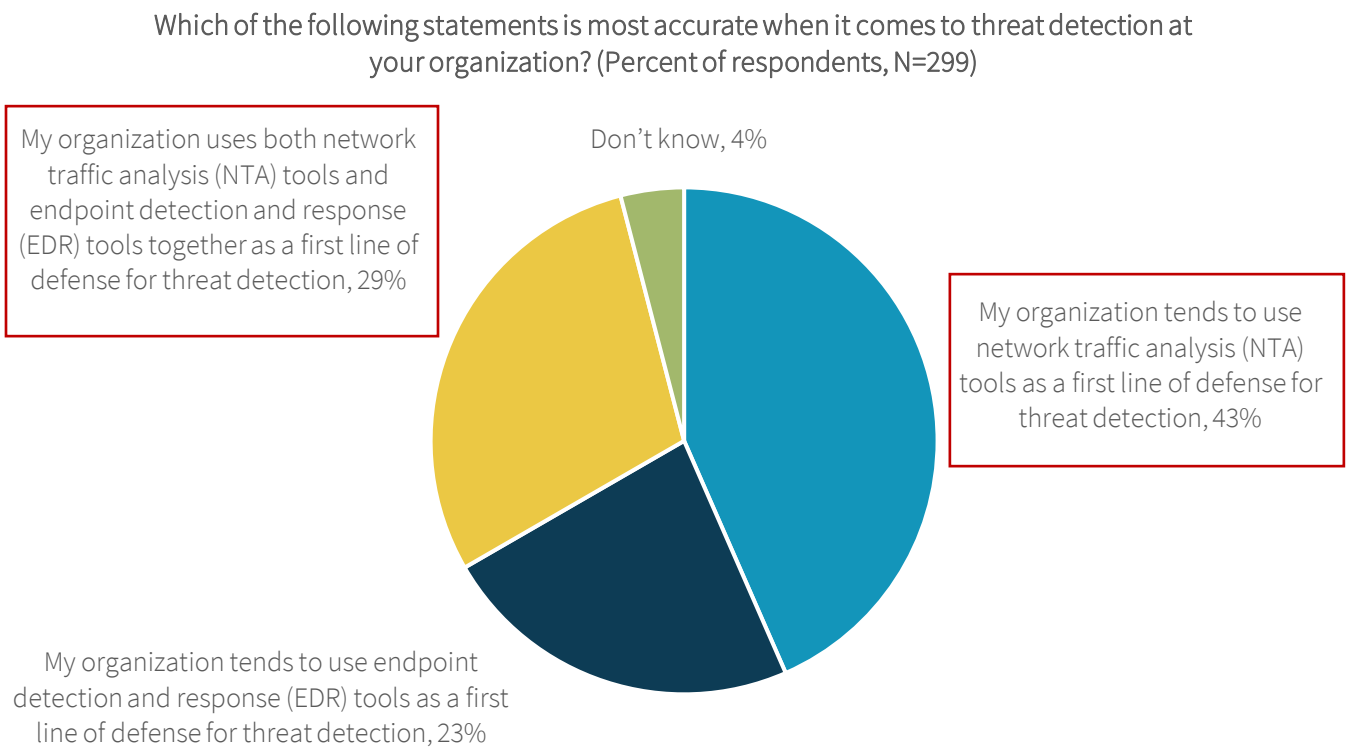
NDR is Critical for Incident Detection

As mentioned, the executive order calls out EDR specifically with regard to improving the detection of cybersecurity incidents on federal networks. However, ESG research has found that the majority of organizations use network-centric detection technologies as a first line of defense (see Figure 1).[3] While EDR can provide a more granular view into the processes running on the endpoint and in some cases more finely tuned response options, NDR is critical for maintaining consistent visibility across the entire network. In fact, 29% of ESG research respondents cite blind spots on the network due

[2] Source: National Institute of Standards and Technology *Special Publication 800-207: Zero Trust Architecture,* August 2020.
[3] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape,* April 2019.

to the inability to deploy agents as one of their biggest threat detection and response challenges.[4] With resources increasingly distributed across the data center, cloud, and branch offices, granular and comprehensive network visibility via NDR is critical to detect threats that have bypassed existing defenses and are attempting to move laterally, escalate privileges, and ultimately exfiltrate data.

Figure 1. How Network and Endpoint Tools Are Used for Threat Detection and Response



Source: Enterprise Strategy Group

NDR is a Key Part of XDR Strategies

In large part because of the importance of both EDR and NDR, and to break down silos between their threat detection and response capabilities, many organizations have begun to show interest in extended detection and response (XDR). ESG defines XDR as an integrated suite of security products spanning hybrid IT architectures, designed to interoperate and coordinate on threat prevention, detection, and response. In other words, XDR unifies control points, security telemetry, analytics, and operations into one enterprise system.

ESG research has found that 69% of organizations indicated it is very important that endpoint and network technologies interoperate, making the combination of NDR and EDR a good starting point for XDR.

There is no commonality across what technologies are included in XDR; rather, the focus is on beginning to bring formerly siloed capabilities together to improve detection and enable more efficient response capabilities. That said, ESG research

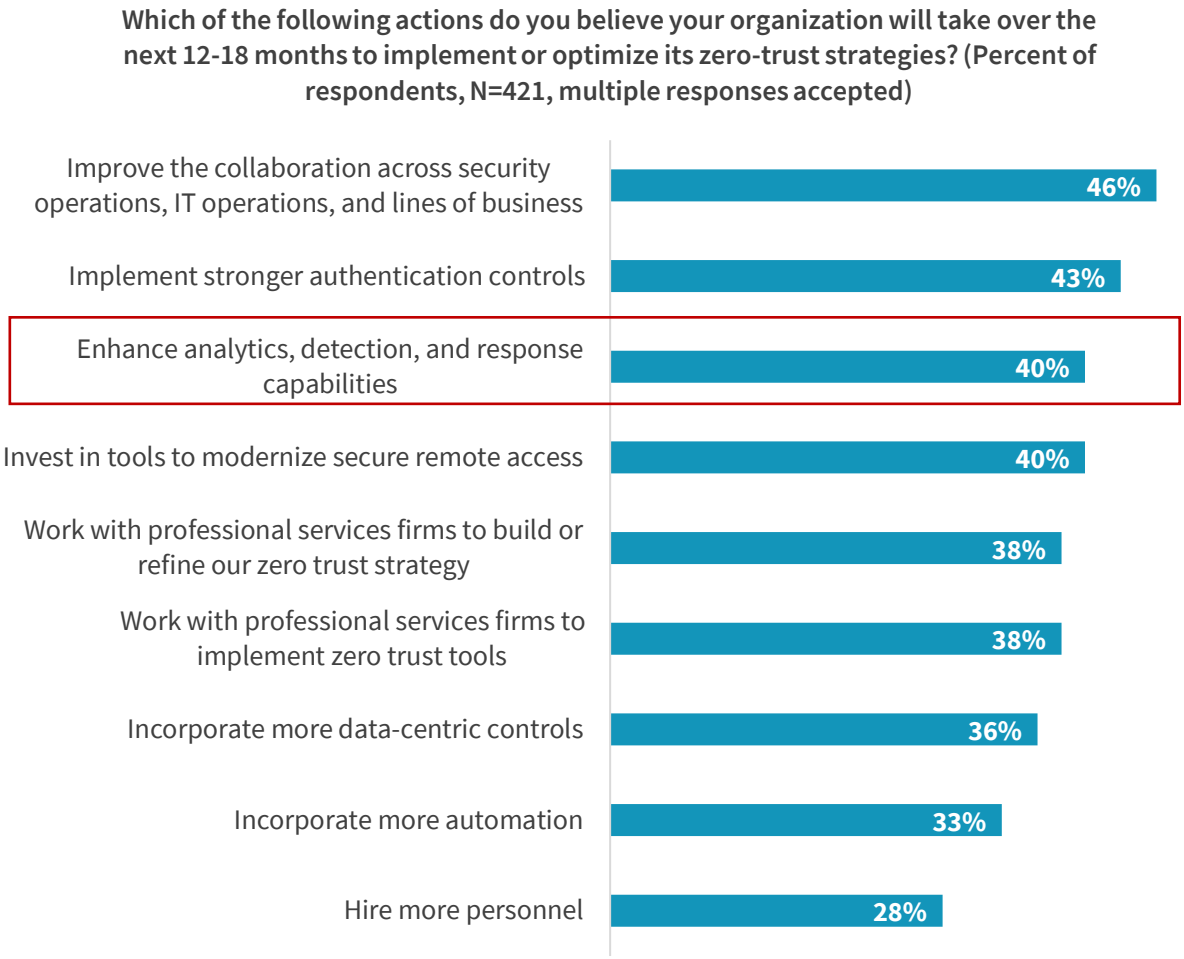
[4] Source: ESG Master Survey Results, *The Impact of XDR in the Modern SOC,* February 2021.

has found that 69% of organizations indicated it is very important that endpoint and network technologies interoperate,[5] making the combination of NDR and EDR a good starting point for XDR.

NDR is a Core Component of Zero Trust

The focus on zero trust as an avenue toward federal cybersecurity modernization certainly aligns with what ESG has found in its research. In fact, 51% of ESG research respondents cite modernizing their cybersecurity program as a top business driver for implementing a zero trust strategy.[6] However, the focus is often on segmentation, secure access, and identity. Analytics generally, and network detection and response specifically, are often overlooked components of zero trust architectures. Even the NIST Special Publication 800-207 fails to specifically call out NDR, even as it does cite the need to understand "the assets active on the network (or those accessing resources remotely) to categorize, configure, and monitor the network's activity." Yet for many organizations investing in zero trust, detection and response are core priorities (see Figure 2).[7] NDR is a key component of this and provides the ability to continually evaluate the trustworthiness of a connection throughout the session by analyzing behavior and serving as a stop gap in case threats are able to bypass authentication.

Figure 2. Actions Taken to Support Zero Trust Strategies



Source: Enterprise Strategy Group

[5] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.
[6] Source: ESG Master Survey Results, *The State of Zero Trust Security Strategies*, May 2021.
[7] Ibid.

Key Requirements for NDR Solutions Supporting the Executive Order

Broadly, it is clear that NDR solutions can help fulfill the guidelines set forth by the Biden administration's executive order. However, as is the case with any cybersecurity tool, capabilities can vary from one solution to the next. Thus, when exploring NDR solutions in the context of the Biden administration's cybersecurity order, there are a few key requirements to consider.

- Detect stealthy and unknown threats with advanced analytics. While many of the threats an organization faces may be of standard sophistication, it is the minority of advanced, zero-day threats that keep security teams up at night. Signature-based tools remain important to block common exploits. However, advanced techniques using machine learning and behavioral modeling are necessary to detect more sophisticated attacks. In order to meet Section 7 of the executive order and maximize the early detection of incidents on federal agency networks, NDR solutions with these advanced analytical capabilities should be prioritized.

- Maintain coverage for cloud and on-premises environments. The executive order prioritizes cloud adoption generally and emphasizes zero trust architectures as a requirement of that migration moving forward. Yet, as is the case in the private sector, many agencies will continue to maintain resources both on-premises and in the public cloud. With threat actors increasingly using this location sprawl to their advantage, maintaining consistent visibility across the entire environment to correlate signals and detect malicious behavior as soon as possible is critical.

- Provide intelligence to enforcement points to support zero trust. To stitch a zero trust architecture together, the network intelligence gathered through analytics should be made actionable through integrations with enforcement points. When the NDR system identifies a malicious event that affects the risk level of an entity, that information should be shared with other parts of the security infrastructure to block user access or isolate an endpoint. Additionally, the network data collected can be used to inform segmentation policies that often form the basis of a zero trust architecture.

- Integrate with SIEM, SOAR, and XDR. To optimize investigation and response capabilities as laid out in the executive order, NDR solutions must integrate with other tools and platforms. This should include XDR, SIEM, and SOAR to give analysts a more complete view of the attack chain and allow them to quickly pivot from one part of the investigation to the next to make the remediation process more efficient and effective. Additionally, with the executive order calling for new requirements with regard to logging, log retention, and log management, NDR solutions that integrate with SIEM products to ensure process automation and data de-duplication can help reduce the complexity and cost of data management.

- Analyze encrypted traffic. The executive order calls for agencies to implement encryption for data both at rest and in transit. While this will increase the amount of SSL/TLS traffic on the network, the reality is that the vast majority of user traffic is already encrypted. In fact, the percentage of encrypted webpages users load in Chrome is now well over 90% across Windows, Mac, and Android devices.[8] Attackers know this and use it to their advantage to obfuscate attacks, hide command and control traffic, and stealthily exfiltrate data. Decrypting and inspecting the traffic is one option to overcome this obstacle. Yet this is not always possible due to performance impacts, privacy concerns, or regulatory mandates. Solutions that can inspect the metadata of the traffic to look for signs of malicious activity, without decrypting the traffic itself can improve the security team's visibility into traffic that cannot otherwise be terminated and inspected.

[8] Source: Google Transparency Report, *HTTPS Encryption by Chrome Platform,* July 2021.

Cisco's Approach to Network Detection and Response

Cisco provides network detection and response through its Secure Network Analytics solution. Secure Network Analytics provides network-wide and context-rich visibility, paired with advanced analytics to deliver high-fidelity behavioral-based threat detection capabilities. Customers use Secure Network Analytics to attain comprehensive visibility into their network environments and support real-time threat detection of unknown, encrypted, and insider threats; incident response and forensics; and network segmentation initiatives. The solution offers different deployment models - on-premises as a hardware appliance or as a virtual machine, or cloud delivered as a SaaS solution (Secure Cloud Analytics) to provide visibility across private networks and public cloud environments.

Secure Network Analytics ingests telemetry from NetFlow, Internet Protocol Information Export (IPFIX), and infrastructure devices, including routers, switches, and firewalls, to provide a complete picture of network activity. Logs across internal, perimeter, and public cloud firewalls are collected through Cisco's Security Analytics and Logging capability to extend visibility to the network perimeter. Additionally, Secure Network Analytics can ingest telemetry data from the AnyConnect Network Visibility Module to capture endpoint-specific user and device context to extend zero trust to any device globally and support remote worker monitoring by delivering complete and continuous visibility that expands outside the corporate network. The solution continuously analyzes telemetry from these sources over time to develop a baseline of normal network behavior. It then uses this baseline along with a combination of non-signature-based advanced analytics, including behavioral modeling, machine learning algorithms, and global threat intelligence from Cisco Talos, to identify anomalous network traffic patterns and detect and respond to threats in real-time. A cloud-based, multilayered machine learning engine correlates threat behaviors seen in the enterprise with those seen globally, providing an additional layer of detection. Malicious activity hiding in encrypted traffic can be detected without having to decrypt it through Encrypted Traffic Analytics, which uses network metadata from Cisco routers and switches.

From a management perspective, customers can retain data for months or more, depending on licensing, to support extended investigation and forensics activities. In addition to a variety of integrations with SIEM and SOAR providers, Secure Network Analytics comes with the Cisco SecureX platform built-in. This simplifies and automates threat response by providing streamlined detection, investigation, and orchestration capabilities. Also, SecureX and Secure Network Analytics further support zero trust implementations through the unified visibility, intelligence sharing, and automation across multiple threat vectors and enforcement points that they offer.

The Bigger Truth

Cybersecurity is hard and becoming more difficult due to ever-evolving adversaries. There are no silver bullet approaches to improve security, protect critical assets, and prevent attacks. The executive order does seem to recognize this through its focus on everything from information sharing to supply chain security to the establishment of a cybersecurity safety review board. However, the focus on modernization and detection and response improvement represents an attempt to enhance some of the foundational elements of the federal government's security posture.

While it is good to see a more dedicated focus to cybersecurity from this administration, much remains to be determined and the slow pace of change often prevalent in the government sector may ultimately delay any positive impacts. More specific guidance will undoubtedly be provided to agencies in the coming months, but it is not too early to begin considering how current security programs are aligned to (or deviate from) the tenets of the order; where the most critical needs for attention reside; and where the order may have the correct goals in mind, if not the specific solutions needed to achieve them. Network detection and response should fall into the latter category for many agencies and be considered as a key technology in supporting the Executive Order on Improving the Nation's Cybersecurity.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.


www.esg-global.com


contact@esg-global.com


508.482.0188