The Cybersecurity Investments that Federal Agencies Must Make to Meet New Standards

How Cisco's Cybersecurity Solutions Can Answer the President's Mandate for Improved National Cybersecurity

On May 12, 2021, President Biden issued an Executive Order (EO) entitled Improving the Nation's Cybersecurity[1], identifying ways that critical infrastructure needs to be updated to protect against increasingly sophisticated threats. This included network modernization, cloud adoption, and improved detection, investigation, and response. Federal agencies need to bolster investments in zero trust, multifactor authentication, data encryption, and EDR/XDR to protect against modern threats. This paper maps Cisco Secure products directly to the requirements laid out in the Executive Order.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Table of Contents

Executive Summary

On May 12, 2021, President Biden issued an Executive Order (EO) entitled Improving the Nation's Cybersecurity[2], with nine key sections. This is important that the White House recognizes that modernization, cloud adoption, and improved detection, investigation, and response are lacking across Federal and critical infrastructure networks. Federal agencies will need to bolster investments in zero trust, multifactor authentication, data encryption, and EDR/XDR to protect against modern threats and threat actors.

For Cisco, it is of paramount importance to build partnerships with government CISOs, branch chiefs, and others around cybersecurity initiatives. This is especially true when it comes to securing the customer's infrastructure, keeping systems secure, and protecting sensitive data. This paper maps Cisco Secure products directly to the requirements laid out in the Executive Order. A summary of the Executive Order is found in Table 1.

Executive Order Summary

Section		Executive Order
1	Policy	The prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security.
2	Removing Barriers to Sharing Threat Information	The government will write new contract language so that its contractors and service providers are obligated to share threat and incident information with them.
3	Modernizing Federal Government Cybersecurity	Government agencies will accelerate cloud and zero trust architecture adoption. They will submit reports on progress toward multifactor authentication, and data encryption in transit and at rest.
4	Enhancing Software Supply Chain Security	National Institute of Standards and Technology (NIST) will develop new guidance on software supply chain security because the government lacks visibility into commercial software development practices. They will define what "critical software" means and what security controls will be required for it.
5	Establishing a Cyber Safety Review Board	The [cyber safety review] Board will monitor threat activity, vulnerabilities, incidents, and agency responses for both Federal and non-Federal systems. Membership will include both Federal and private sector organizations.
6	Standardizing Incident Response	The Department of Homeland Security (DHS) will lead an effort to develop a playbook, or standard operational procedures to address vulnerabilities and respond to incidents.
7	Improving Detection of Cybersecurity Vulnerabilities and Incidents	To maximize early detection and improve threat hunting, all agencies will deploy Endpoint Detection and Response (EDR) capabilities. DHS will review options and requirements for a centralized, government-wide program and will ensure that agencies have the resources they need to comply.
8	Improving Investigative and Remediation Capabilities	DHS will investigate and provide guidance on event log collection, retention, and visibility at the highest level of the agency. It will also permit agencies to share log information with other agencies for analysis and incident response.
9	National Security Systems	The Department of Defense and Intelligence Communities will adopt similar requirements for National Security Systems that may not have ordinarily applied. Therefore, this EO extends beyond Federal Civilian Executive Branch (FCEB) Agencies.

Table 1

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

It is impossible to stop all attacks, but it is possible to reduce cost, minimize risk, and reduce time to detection with a properly designed, integrated, and implemented security architecture.

The Cisco Federal Security Team has compiled a series of documents around the cybersecurity architecture solutions that are available to the U.S. Government and fulfill the requirements of the Executive Order. These documents:

- Outline features that are provided by the given technology
- Detail what features are currently being used in the customer environment
- Provide an overall interoperability with other solutions within Cisco's cybersecurity solution portfolio

This document provides a summary of the Cisco approach to cybersecurity and the various capabilities that Cisco can and does provide to protect U.S. Government and critical infrastructure networks.

Cybersecurity has historically been a messy array of independent technologies. This approach may have been adequate ten years ago, but today it presents many operational, policy enforcement, and monitoring challenges. Many organizations use dozens of cybersecurity solutions (if not more), from just as many vendors. In many cases, their security teams can investigate only a fraction of the security alerts that are received on a given day. With increasingly distributed workforces, it has become more difficult to at block targeted and sophisticated threats, advanced malware attacks, and zero-day threats.

It is impossible to stop all attacks, but it is possible to reduce cost, minimize risk, and reduce time to detection with a properly designed, integrated, and implemented security architecture. Such an architecture allows the systems itself to learn, adapt, and otherwise better secure a customer's environment. As a cybersecurity partner, Cisco can provide a holistic security architecture to meet the current and future security requirements for the enterprise and missions. Cisco can also provide professional services to assist current investments to meet the Executive Order.

The Cisco Secure Architecture

Cisco's comprehensive and integrated security architecture approach is described in the following section and consists of twelve product families with management, integrated threat intelligence, and the ability to integrate with other vendor security products and solutions using open-industry standards (Figure 1).

Cisco's Integrated Security Product Portfolio Approach

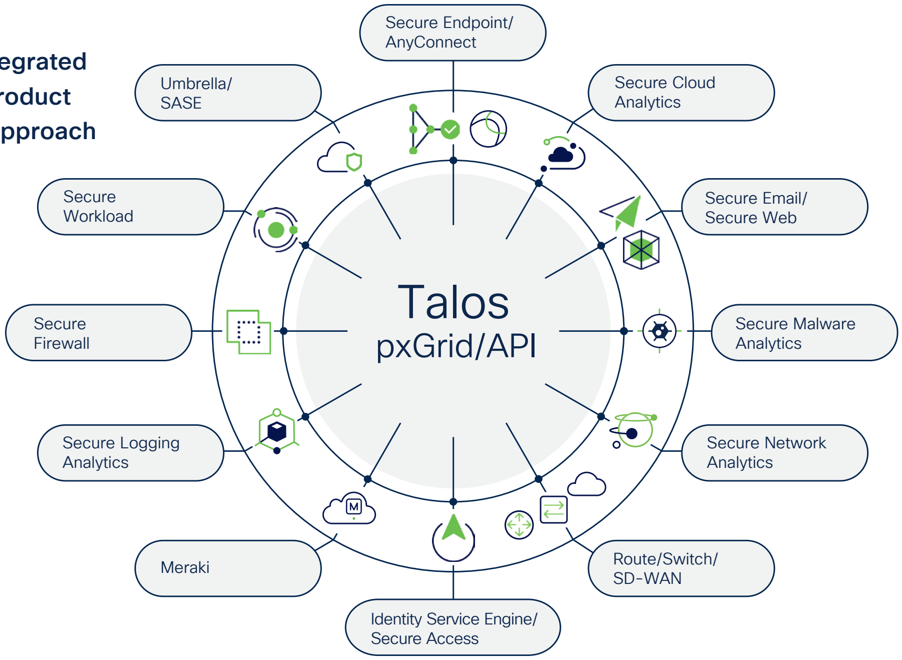

Figure 1

Switches, routing, and WAN solutions are listed in a discussion of comprehensive security products as part of the overall security architecture, because:

- The existing routing and switching environment may very well be your most cost-effective means to gather the data that is needed to assess threats and take proactive steps to protect the network. NetFlow data (from Cisco switches and routers), as well as "flow" from other vendors, is a key security data source to monitor for anomalous behavior and security breach activities. It provides forensic evidence to reconstruct a sequence of events and can be used to help ensure regulatory compliance. It also helps to provide visibility across the entire attack lifecycle.
- Wired and wireless infrastructures provide the groundwork for effective network segmentation. Granular network segmentation (down to the individual interface, person, or device when needed) enables an enterprise to restrict attack and threat vectors, and it is key to network consolidation that can reduce costs and enhance both performance and security.
- It is key to ensuring scalability of networks to handle the dramatic increase in network traffic expected over the coming years.

A security architecture that leverages existing Cisco switching, router, and WAN environments offer the most complete and cost-effective network sensor data, as well as the performance and assured scalability built-in to the existing network fabric to handle the rapidly increasing traffic flows. Most significantly, a proper security architecture helps prevent any potential self-inflicted denial (or degradation) of service caused by security solutions that do not factor in network performance considerations or do not integrate well with other solutions, both now and in the future.

Cisco Secure Solutions

This section shows all the Cisco cybersecurity solutions. A summary of each solution is provided along with how the solution aligns with the Executive Order.

Note: Cisco has prepared a more detailed paper for each of these solutions, which provides greater in-depth description of the solution and various platforms the solution can be deployed on.

The Executive Order was summarized earlier in Table 1. Of the nine sections in that document, Sections 1, 2 and 4 do not apply to Industry or any products or solutions that an industry partner would provide to the Federal Government to protect against cybersecurity threats. As a result, when Cisco cybersecurity products are aligned to the Executive Order, Sections 1, 2, and 4 are omitted.

Table 2 shows a summary of the Cisco cybersecurity suite of products and how they align to the improving the nation's cybersecurity Executive Order.

Executive Order Alignment to Cisco Secure Products

	Executive Order Alignment					
Cisco Solution	3	5	6	7	8	9
Talos	●	●	●	●	●	●
Talos Incident Response	●	●	●	●	●	●
Cisco Secure Firewall Malware Defense	●	○	○	●	●	●
Cisco Secure Client	●	○	○	○	●	●
Cisco Secure Application for AppDynamics	●	○	○	●	●	●
Cloudlock	●	○	○	●	●	●
Cisco Cyber Vision	●	○	○	●	●	●
Cisco Defense Orchestrator	●	●	○	●	●	●
DNA Center	●	○	○	○	●	●
Cisco Secure Access by Duo	●	●	○	●	●	●
Cisco Identity Services Engine	●	○	○	●	●	●
Cisco Kenna Security	○	●	●	●	●	○
LiveAction	●	○	○	●	●	●
Meraki	●	○	○	●	●	●
Orbital	●	●	○	●	●	●
SD-WAN	●	○	○	○	●	●
Secure Bot	●	○	○	●	●	●
Secure Cloud Analytics	●	●	○	●	●	●
Secure DDoS	●	○	○	●	●	●
Cisco Secure Email	●	●	○	●	●	●
Cisco Secure Endpoint	●	●	○	●	●	●
Cisco Secure Firewall	●	●	○	●	●	●
Cisco Secure Malware Analytics	●	●	○	●	●	●
Cisco Secure Network Analytics	●	●	○	●	●	●
Secure Platform	●	●	○	●	●	●
Secure SSLI	●	○	○	●	●	●
Secure WAF / KWAF	●	○	○	●	●	●
Cisco Secure Web Appliance	●	●	○	●	●	●
Cisco Secure Workload	●	●	○	●	●	●
Cisco ThousandEyes	●	○	○	●	●	●
Cisco Umbrella	●	●		●	●	●

Table 2

Cisco Secure Product Breakdown

Talos

Executive Order Alignment

3	5	6	7	8	9
◉	◉	◉	◉	◉	◉

Cisco Talos is the threat intelligence organization at the center of the Cisco Secure portfolio. Talos is an elite group of security experts devoted to providing superior protection to customers with our products and services. Every decision point within the security matrix receives common data and can come to a common conclusion about how to deal with any threat. A common operating environment is critical when there is a need to provide security and insight across a large and diverse network.

Talos Incident Response

Executive Order Alignment

3	5	6	7	8	9
◉	◉	◉	◉	◉	◉

Cybersecurity teams are overwhelmed with the ever-growing responsibility to respond to threats efficiently and quickly. Many lack the time and expertise they need to develop proactive measures of response which contributes to the complexity and strain of the job. Having proactive security practices in place and utilizing well designed incident response (IR) plans ensures the security team is well prepared for future attacks.

However, IR preparedness does not stop with planning. Without IR playbooks, any team lacks the defined processes and step-by-step guides they need to execute appropriate response workflows. IR playbooks consist of the frameworks, checklists, decision trees and other templatized material to help your team effectively respond to incidents in a timely manner.

The Cisco Talos incident response (CTIR) playbook service helps a security team build effective IR workflows so threats can be effectively mitigated. With CTIR's industry-leading best practices and real-world expertise, any organization is properly prepared for an attack.

The Talos CTIR playbook allows organizations to:

- Develop strong step-by-step guides for the security team so they can better respond to specific incident types and decrease the time to respond
- Gain a comprehensive view into the organization through expert-leading analysis to ensure the customized playbooks address business needs
- Tailored to the threats and business processes of a specific organization, but reliant on the latest threat intelligence and response techniques

Cisco Secure Firewall Malware Defense (AMP for Networks)

Executive Order Alignment

3	5	6	7	8	9
◉			◉	◉	◉

Network-based malware defense must go beyond point-in-time detection to protect across the entire attack continuum. Designed for the Cisco Secure Firewalls (specifically the Next-Generation Intrusion Prevention System (NGIPS) and Next-Generation Firewall), Advanced Malware Protection (AMP) for Networks provides visibility and control to protect against highly sophisticated and targeted advanced malware.

Executive Order Alignment

3	5	6	7	8	9
●				●	●

Cisco Secure Client (AnyConnect)

Cisco Secure Client is a unified security endpoint that delivers multiple security services to protect the enterprise. Cisco Secure Client simplifies highly secure endpoint access and provides the security necessary to help keep organizations safe and protected. Cisco Secure Client modules include:

- Virtual Private Network (VPN)
- Remote Access VPN
- Site to Site VPN
- Network Access Manager
- Web Security
- ISE Posture
- NVM NetFlow

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Cisco Secure Application for AppDynamics

Cisco Secure Application for AppDynamics is an all-in-one monitoring solution for both cloud and terrestrial data center applications. Visibility into applications, whether hosted in a cloud environment or a data center, is often missing or incomplete. For security, the lack of visibility certainly introduces concern.

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Cisco Cloudlock

Cisco Cloudlock is a public-cloud-native cloud access security broker (CASB) that helps customers move to the cloud safely. It protects cloud users, data, and apps. Cloudlock's simple, open, and automated approach uses APIs to manage the risks in the public cloud app ecosystem. With Cloudlock, you can more easily combat data breaches while meeting compliance regulations.

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Cisco Cyber Vision

Industrial control systems (ICS) are ever more connected to corporate IT networks. Deployments of industrial Internet of Things (IoT) technologies are also taking place. This deeper integration between IT, cloud, and industrial networks is creating many security issues that are becoming obstacles to your digitization efforts. Cisco Cyber Vision gives full visibility into your ICS, including dynamic asset inventory, real-time monitoring of control networks and process data, and comprehensive threat intelligence, so you can build secure infrastructures and enforce security policies to control risk.

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

Defense Orchestrator

Cisco Defense Orchestrator (CDO) is a public-cloud-based configuration and orchestration tool for the Cisco Secure Firewall products. CDO helps consistently manage policies across Cisco firewalls and public cloud infrastructure. It cuts through complexity to save you time and keep your organization protected against the latest threats.

DNA Center

Executive Order Alignment

3	5	6	7	8	9
●				●	●

This interconnection of automation and assurance forms a continuous validation-and-verification loop, that alignments network operation with business intent. Through open Application Programming Interfaces (APIs) and Software Development Kits (SDKs), third-party technologies can be run on top of Cisco DNA Center and benefit from its powerful network visibility. Cisco DNA Center is an open, extensible platform that streamlines IT workflows and greater business innovation.

Full automation capabilities for provisioning and change management are enhanced with artificial intelligence/machine learning (AI/ML) enhanced analytics that pull streaming telemetry from everywhere in the network. Applications, services, and users are prioritized based on business goals, within policy parameters and security best-practices. Shortcomings in network, application, or device performance are flagged, and instant remediation guidance saves hours of IT troubleshooting.

Cisco Secure Access by Duo

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

Duo performs Zero Trust by verifying every user (via multi-factor authentication) and every device at every point of authentication, before access is granted.

By turning each application into its own Policy Enforcement Point, Duo can ensure secure connections to cloud, internal, and network connections in real time regardless of user location, and without having to install or configure remote access software on users' devices.

Identity Services Engine (ISE)

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Cisco Identity Services Engine (ISE) simplifies the delivery of consistent, highly secure access control across wired, wireless, and VPN connections. With far-reaching, intelligent sensor and profiling capabilities, ISE can reach deep into the network to deliver superior visibility into who, what, when, where, and how endpoints area accessing resources. It can share vital contextual data using technology partner integrations. Cisco ISE transforms the network from a simple conduit for data into a security enforcer that accelerates the time to detection and mitigates threats.

Cisco ISE also introduces the Cisco Platform Exchange Grid (PxGrid), which is an open, scalable, and IETF standards-driven data-sharing and threat control platform that enables a myriad of third-party security products to integrate with Cisco networking and security products and solutions.

Cisco ISE, along with Cisco DNA-Center, defines Cisco TrustSec. TrustSec is software-defined segmentation that dynamically organizes endpoints into logical groups, called scalable groups. Scalable groups are assigned based on business decisions using a richer context than an IP address.

Cisco Kenna Security

Executive Order Alignment

3	5	6	7	8	9
	●	●	●	●	

Using machine learning and data science, Kenna processes and analyzes 18+ threat and exploit intelligence feeds, 12.7+ billion managed vulnerabilities, as well as your enterprise's security data to give an accurate view of risk. Kenna has risk scoring and remediation intelligence, so information is provided for truly data-driven remediation decisions. Kenna security combines external and internal data into one view of risk.

LiveAction

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

LiveAction allows customers to manage large and complex networks by unifying and simplifying the collection, correlation, and presentation of application and network data to make it actionable for network management teams. The easy-to-use interface allows network management teams to go from a global view and drill down to a location, a single hop, or even an individual packet.

Meraki

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Cisco Meraki is a public-cloud-managed suite of products that provide security solutions to customer environments. The Meraki MX firewalls provide an adaptive security policy, which is critical in any Zero Trust Architecture. The Meraki MX firewalls also integrate with the Cisco Advanced Malware Protection (AMP) for Networks.

Orbital

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

Cisco Orbital is a service that uses Osquery to provide information about your hosts. Osquery exposes an entire operating system as a relational database that can be queried with SQL to gather information about the host. Orbital can be used by both Cisco customers and their applications to query their computers wherever Orbital has been deployed.

SD-WAN (Viptela and Meraki)

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Cisco SD-WAN is a secure architecture that is open, programmable, and scalable. Through the Cisco vManage console, you can quickly establish an SD-WAN overlay fabric to connect data centers, branches, campuses, and colocation facilities to improve network speed, security, and efficiency.

The Meraki MX appliances elegantly create a framework for Cisco SD-WAN powered by Meraki by securely auto-provisioning IPsec VPN tunnels between sites. The Meraki dashboard automatically negotiates VPN routes, authentication and encryption protocols, and key exchange for all Meraki MX appliances in an organization to create hub-and-spoke or mesh VPN topologies. Software defined WAN capabilities in every security appliance reduces operational costs and improves resource usage for multi-site deployments. Network administrators use available bandwidth more efficiently and ensure the highest possible level of performance for critical applications without sacrificing security or data privacy.

Secure Bot

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Cisco Bot management defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Cisco bot management solutions – powered by Radware – leverage proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent behind an API request and block malicious activity.

Secure Cloud Analytics

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

The Cisco Secure Cloud Analytics is a SaaS-based network and cloud security solution. Cisco Secure Cloud Analytics detects early indicators of compromise in the cloud or on-premises, including insider threat activity and malware, as well as policy violations, misconfigured cloud assets, and user misuse. And like other Cisco security tools, it receives a wide variety of network telemetry and logs. Abnormal behavior or signs of malicious activity generate an alert so you can quickly investigate it.

Secure DDoS

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Cisco Secure DDoS Protection defends organizations and ensures network availability using behavior-based and machine-learning algorithms to rapidly detect and mitigate sophisticated DDoS attacks targeting both the network- (L3/4) and application-layer (L7). Cisco DDoS mitigation solutions protect against SSL-based DDoS attacks without adding latency and use automatic, adaptive real-time protection to defend against zero-day attacks.

Cisco Secure Email

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Cisco Secure Email enables users to communicate securely. It helps organizations combat business email compromise, ransomware, advanced malware, phishing, spam, and data loss prevention (DLP) with a multilayered approach to security.

Cisco Secure Endpoint (formerly AMP for Endpoints)

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

Powered by Cisco Talos, Cisco Secure Endpoint blocks more threats than any other security provider. Once a threat is seen by Secure Endpoint, it can be immediately blocked. And, since the threat is now known, it will be blocked it everywhere it tries to spread. It is even possible to automate the threat response with one-click isolation of an infected host.

Cisco Secure Firewall (ASA and FTD)

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

The Adaptive Security Appliance (ASA) provides intelligent threat defense that stops attacks before they penetrate the network perimeter, controls network access, and delivers secure remote access and site-to-site connectivity. The result is a powerful, multifunction network security appliance family that provides security breadth, precision, and depth for protecting business networks of all sizes, while reducing the overall deployment and operations costs associated with implementing comprehensive multilayer security.

The Cisco Firepower Threat Defense (FTD) includes the industry's most widely deployed stateful firewall and provides granular control over more than 4,000 commercial applications. Its single management interface delivers unified visibility from the network to the endpoint. Firepower NGFW enables comprehensive policy management that controls access, stops attacks, defends against malware, and provides integrated tools to track, contain and recover from attacks that do get through.

The Cisco Secure Firewall FTD are centrally managed by the Cisco Firepower Management Center (FMC). The FMC provides a consistent licensing, configuration, and operating system experience for all firewalls in the network.

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

Secure Malware Analytics (formerly Threat Grid)

Secure Malware Analytics allows customers to understand and prioritize threats faster. It combines advanced sandboxing with Talos threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, it is easy to understand what malware does, or attempts to do, how large a threat it poses, and how to defend against it.

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

Secure Network Analytics (formerly Stealthwatch Enterprise)

With the Secure Network Analytics system, the customer can baseline, inventory, and label network assets, uncover and remediate security deficiencies, and continuously monitor and report on issues to maintain a strong security posture. Stealthwatch can transform the network into a virtual sensor grid that helps facilitate compliance and ensure the ongoing visibility and control needed to minimize risks. Encrypted Traffic Analysis (ETA) is also possible as security without traffic decryption.

Secure Network Analytics also provides access to Cisco Cognitive Threat Analytics (CTA), which automatically analyzes more than 10 billion web requests daily. It zeroes in on malicious activity that has bypassed security controls and is using web-based communications. This includes standard, encrypted, and anonymous channels that can be used to attack your organization.

CTA introduces Cisco Encrypted Traffic Analytics (ETA), which identifies malware communications in encrypted traffic through passive monitoring and the extraction of relevant data elements and supervised machine learning with cloud-based global visibility.

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

Cisco SecureX

Cisco SecureX is a public-cloud-native, built-in platform that connects the Cisco Secure portfolio and the network infrastructure. It allows any customer to radically reduce dwell time and human-powered tasks. Secure Platform is available to any customer who has any Cisco Secure product and is connected to the public internet.

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Secure SSLi

Cisco SSLi Bundles combine Radware Alteon SSL acceleration with Cisco Secure Firewall and/or Web Security Appliance (WSA) to offer a highly scalable solution for SSL traffic inspection. The solution provides visibility into encrypted outbound traffic with minimal latency and reduces overall security costs by offloading SSLi functions to purpose-built devices. Each bundle uses a front and a backend Alteon in a “sandwich” configuration for high availability (HA) and scaling of SSL inspection beyond current limits.

Secure WAF / KWAF

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Cisco Advanced Web Application Firewall (WAF) ensures fast, reliable, and secure delivery of mission-critical web applications for corporate networks and the cloud. Through the combination of advanced positive and negative security models, the Cisco Secure WAF solutions provide complete protection against the full spectrum of web-based attacks.

The web application security solutions can be deployed as a stand-alone WAF appliance or integrated with Cisco Secure Application Detection and Control (ADC) and can be deployed on-premises or in the cloud, inline or out-of-band. There's also a Kubernetes edition.

The Kubernetes WAF enables secure, rapid delivery of applications without compromising agility. It is designed to fit the Kubernetes orchestration system in service mesh architectures, providing market-leading application security as well as the advanced automation, autoscaling and elasticity required by today's DevOps and security teams.

Cisco Web Security Appliance

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

Cisco Web Security Appliance provides protection before, during, and after an attack. The Web Security Appliance provides automated monitoring and analysis across the network. When compromise occurs, it can quickly determine the scope of the damage, remediate it, and bring operations back to normal.

Cisco Secure Workload (formerly Tetration)

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

Cisco Secure Workload platform uses comprehensive traffic telemetry data collected from both servers and Cisco Nexus switches. The platform performs advanced analytics using an algorithmic approach and provides comprehensive workload protection for a multi-cloud data center. The single software package, configures all the foundational big data components, generates signed certificates for the customer environments, and installs all necessary algorithms.

Cisco ThousandEyes

Executive Order Alignment

3	5	6	7	8	9
●			●	●	●

Cisco ThousandEyes combines a variety of active and passive monitoring techniques to provide deep insight into user experience across the applications and services that are offered and consumed. It also leverages an expansive internet monitoring data set to provide real-time outage detection powered by collective intelligence. It allows for a cross-correlated visibility view to isolate problems and resolve issues faster.

Cisco Umbrella

Executive Order Alignment

3	5	6	7	8	9
●	●		●	●	●

Cisco Umbrella delivers a fast, secure, and reliable Internet experience to thousands of organizations. Umbrella uses the Internet's infrastructure and the power of Cisco Talos to block malicious and unwanted domains, IP addresses, and cloud applications before a connection is ever established.

Cisco Umbrella Investigate provides the most complete view of an attacker's infrastructure and enables security teams to discover malicious domains, IPs, and file hashes, and even predict emergent threats. The web-based console provides real-time access to Talos intelligence and the ability to interactively pivot on different data points during investigations.

Conclusion

Cisco's comprehensive, integrated security architecture approach consists of all Cisco Secure offerings with management, integrated threat intelligence, and the ability to integrate with other vendor security products and solutions using open-industry standards. Furthermore, existing routing and switching environments may very well be the most cost-effective means to gather an organization's data needed to assess threats and take proactive steps to protect the organization's network.

Cybersecurity products experts can help assess the current capabilities of any organization and create bespoke recommendations that will help them with current compliance needs and future goals.

For more information on how to partner with Cisco and enable security transformation in your organization, check out the following:

- Federal Government Digital Transformation
- Modernizing Government Cybersecurity
- Meeting the Needs of Our Federal Customers