GETTING THE MOST FROM CONTINUOUS DIAGNOSTICS AND MITIGATION

INDUSTRY PERSPECTIVE

EXECUTIVE SUMMARY

The Continuous Diagnostics and Mitigation (CDM) program supports the shift in government cybersecurity to continuous monitoring of information systems and networks. Implementing CDM requires an integrated threat defense strategy that supports automation and simplicity in your security architecture. To understand the keys to successfully implementing a CDM program, GovLoop partnered with experts at Cisco, an industry leader in cybersecurity solutions, for this industry perspective.

Federal networks become increasingly complex as they evolve to support critical internal missions and the delivery of citizen services. At the same time, they face a continuous barrage of probes and attacks from increasingly sophisticated adversaries. To protect complex networks in the face of these threats, federal cybersecurity is evolving beyond periodic assessment of static security controls to continuous monitoring.

To support this shift, the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program provides a suite of commercial off-the-shelf products to help agencies know what is on their networks, who is on their networks, what is happening on their networks and respond to suspicious activity—in as close to real time as possible. The value of continuous monitoring was demonstrated as early as 2009 at the State Department, where then-CISO John Streufert showed that a monitoring program that included accountability and risk-based prioritization reduced vulnerabilities by 90 percent in one year and cut the costs of accrediting IT systems by 62 percent.

The key to implementing a successful continuous monitoring program is an integrated threat defense strategy supporting a holistic security architecture rather than a collection of point solutions. Integration enables automation, which allows faster detection and remediation of problems, and simplicity, which produces actionable information that can be used to make decisions.

THE GOALS OF CDM

Since passage of the original Federal Information Security Management Act (FISMA) in 2002, the National Institute of Standards and Technology (NIST) has produced an impressive collection of guidance for assessing risk and implementing appropriate security controls.

But security of federal information systems was assessed only annually under FISMA, and systems were accredited for operation only once every three years. The result was static IT security that was quickly outdated, while large amounts of time were invested in labor-intensive reviews and reporting. While threats evolved rapidly, cybersecurity defenses were a rigid construct that advanced in fits and starts.

Therefore, government cybersecurity improved little. First established in fiscal 2013, the purpose of CDM was to make available commercial off-the-shelf tools to leverage existing cybersecurity investments, delivering near-real-time visibility into IT systems and networks.

These tools aggregate data from new and existing network sensors, provide dashboard views and reports of current conditions, prioritize problems for remediation and track results. The program was initially implemented with the following three phases, with the possibility that a fourth phase will be added soon.

Phase 1: Endpoint Integrity

Endpoint integrity is about knowing what's on the network, and managing endpoint configurations and vulnerabilities. This phase leverages sensors to enable discovery and management of all network hardware and software.

The configuration of all hardware and software is evaluated, and settings are managed so that they comply with security and mission requirements. Vulnerability management identifies known security vulnerabilities and scores them for prioritization, allowing the most serious issues to be addressed first. Not all vulnerabilities can be eliminated; some are mitigated to present the least risk possible, and some can be accepted if they are minor and the systems they affect are low-impact.

Phase 2: Least Privilege and Infrastructure Integrity

Many agencies are now moving into this phase, which has two purposes: to know who is on the network, and to manage their access privileges and activities.

The goal is to ensure that only trusted users are on the network. Through the effective management of credentials (including passwords and hardware or software tokens) used for accessing network resources, it's possible to then manage individual privileges. Users are provided access only to those assets and activities needed for their jobs.

"While this might seem a simple task, it is no small undertaking in large federated cabinet agencies where employees and contractors change roles frequently; moreover, the ongoing dependence upon legacy systems often presents both a technical and financial challenge," said Cisco Systems' Fellow, and former CIO for the U.S. Department of Health and Human Services, Frank Baitman.

Knowing who is on the network and managing what they are allowed to do not only reduces the opportunities for outsiders to breach defenses, but also reduces insider threats.

Phase 3: Boundary Protection and Event Management

This phase focuses on managing the complete security lifecycle. The goal is to ensure that all network equipment and tools have security built in so that agencies can plan for and respond to events, effectively manage risk, mitigate the impact of incidents, and document security policies and activities. Agencies should be able to not only understand and maintain their current security status, but also to track it and learn from it over time. Ultimately, it will allow administrators to make better-informed decisions and evolve network security.

No one product performs all of these functions, and the best choice of tools for achieving these results will vary for each agency, depending on mission, the existing environment, and other conditions. This puts a premium on the ability to integrate products in an end-to-end solution.

INTEGRATION: THE KEY TO MAKING CDM WORK

Vulnerabilities, threats, and attacks multiply quickly, and the security industry typically responds by producing point solutions to address them as they appear. But this approach increases complexity as each new tool is added to the network, and increases the manpower and training needed to configure and manage them. More importantly, these point solutions need to be woven together so that the insights they produce can be analyzed, and act on their output. The result is an unwieldy security environment in which security gaps are not identified and suspect or malicious activity is not quickly spotted.

Good tools are not enough by themselves to achieve the goals of Continuous Diagnostics and Mitigation. It requires an end-to-end security architecture.

Enabling Automation

Continuously monitoring networks and responding to events at machine speed is too large a task to do by hand. The sheer volume of records generated and the speed at which they are produced (the goal of CDM is for all systems in the enterprise to be scanned every 72 hours) makes manual correlation, analysis and response impossible. This is why the government has put a premium on security automation.

The Security Content Automation Protocol (SCAP) is a suite of interoperable specifications managed by NIST that enable commercial, off-the-shelf security products to share and use information automatically. SCAP is one element of a broader automation agenda addressing the needs of modern cybersecurity. If devices are to remove the burden of human interaction in every security process, they must be able to communicate with and respond to one another. Selecting security products that not only meet a particular need, but also can be integrated with other products is a requisite for automation and for CDM.

In creating an integrated security platform, it is important to distinguish between an end-to-end solution and a collection of independent tools.

"You're striking a long-term partnership with your vendors, so it's important to get a look back in time to see how they've innovated before, and a glimpse into their roadmap to have confidence in their future direction."

Frank Baitman, Cisco Systems' Fellow, and former CIO for the U.S. Department of Health and Human Services

> "Simplicity goes hand-in-hand with integration. Security automation is what it's really about, but with the CDM program and its long list of products, it's easy to get lost in the details."
>
> *Steve Caimi, Industry Solutions Specialist for Cisco's U.S. Public Sector*

The Continuous, Integrated Solution

No one product can do everything, and your solution will not be a single, purpose-built tool. Agencies have invested in a variety of security products to meet different needs, and the multi-vendor environment is here to stay. The key to maximizing the value of the multiple tools in use is to make sure that these products can work together to drive systematic security response. Ease-of-use is a key determinant here: products that are complex, or that don't play well with others, will only obscure the analysis and reporting.

The platform must be able to gather, correlate and analyze data from a variety of sources already deployed on the network—including those networking products that do not have specific security functions—and identify behavior and activity that is suspect or malicious. This provides both the visibility and context for decision-making. The resulting information is available on a centralized console and can be used to generate alerts and reports, and to direct automated responses according to policy.

Automation is not an absolute. The degree of automation in incident response and mitigation will depend on the circumstances of the incident and the requirements of the agency. But an end-to-end solution leveraging an integrated threat defense strategy gives the ability to automate responses as appropriate for each agency, and bring the right people into the loop as needed.

Simplify

Henry David Thoreau famously advised in "Walden," "Our life is frittered away by detail. Simplify, simplify."

That was good advice when he wrote it, and it is still good advice today. "Simplicity goes hand-in-hand with integration," said Steve Caimi, Industry Solutions Specialist for Cisco's U.S. Public Sector. "Security automation is what it's really about, but with the CDM program and its long list of products, it's easy to get lost in the details."

It is important to assess whether an individual point solution adds a capability not already available, and is important enough so as to consume management resources: more than anything else, solutions that must be managed separately add to the complexity of systems. When they cannot be integrated with one another, they are time-consuming, adding to the burden of staff already stretched thin and reducing the time and resources available for training needed to keep up with new technology and emerging threats. The result is that new products introduced into the environment often do not produce a net improvement in performance and security. It actually becomes more difficult for staff to monitor networks, mitigate risks and respond to threats.

An integrated solution creates a simpler environment and eliminates many of the details with which administrators would otherwise fritter away their working lives. It allows monitoring, analysis, detection and mitigation to be automated, so that humans are free to do what they do best—make critical decisions based on actionable intelligence. "To depend upon an integrated solution, however, means that you're also depending upon the vendor's ability to innovate and to rapidly respond to emerging threats," explained Baitman. "You're striking a long-term partnership with your vendors, so it's important to get a look back in time to see how they've innovated before, and a glimpse into their roadmap to have confidence in their future direction."

SUPPORTING THE GOALS OF CDM THROUGH TECHNOLOGY SOLUTIONS

Cisco offers a complete set of solutions supporting the goals of the CDM program, including policy and access controls, next-generation network security and advanced threat solutions.

Agencies do not have to have an all-Cisco environment to take advantage of these capabilities. We believe that the multi-vendor environment is here to stay and agencies must be able to leverage their existing investments. What is important is that tools can be integrated effectively to support swift, automated action. Cisco provides this ability in its comprehensive cybersecurity portfolio.

Policy and Access

Solutions in this arena need to provide next-generation network access security, with awareness of everything on the network to ensure access and controls are consistently applied. They profile devices so that unauthorized or vulnerable devices can be prohibited from accessing government networks. They tie user identity and role information to the device, and thus enforce the appropriate access policy from the appropriate device. For example, the Policy and Access solution might allow a user's personal device on the network for basic internet access and other low-risk tasks, but it can block the BYOD device from accessing sensitive or classified information.

Next-Generation Network Security

In network security, solutions need to block more threats and quickly mitigate those that do breach defenses, combining the firewall appliance with effective next-gen IPS.

Solutions should integrate real-time contextual awareness, intelligent security automation and superior performance to provide visibility, automation, flexibility and scalability. Next-generation network security solutions provide application visibility and control, not just packet filtering or stateful inspection. They must have deep application awareness to mitigate against today's advanced threats.

Advanced Malware Protection

Technology needs to provide global threat intelligence, advanced sandboxing and real-time malware blocking, as well as continuously analyze file activity to quickly detect, contain and remove all malicious code.

Solutions should be holistic, combining static and dynamic malware analysis with threat intelligence in one unified solution to help agencies understand what malware is doing, the threat it poses and how to defend against it. They must understand that today's advanced malware is designed to evade detection, so all files must be tracked throughout the network. If one or more files are allowed onto the network but begin acting maliciously, Advanced Malware Protection solutions must be able to identify and stop them no matter where they traveled.

Cisco provides tools that do all of the above. It offers CDM solutions for policy and access, next-generation network security, advanced threat protection and more. Cisco's CDM solutions can help federal agencies fulfill their mandate, stay on the forefront of cybersecurity technology and provide the best protection for their critical information.

CONCLUSION

No one security product can do everything, but a holistic security architecture will integrate your network and security point solutions to achieve a comprehensive cybersecurity portfolio and chart a path to compliance with programs such as CDM.

Using an integrated threat defense strategy when selecting CDM solutions is vital. With automated analytics and response capabilities, security professionals benefit from a firm understanding of where security is working, where investment is needed and where their greatest risks of attack lie. Just picking point products from the CDM product catalog won't get you there.

With the right vendor partner, agencies can take full advantage of the tools in their environment to produce the integrated security platform needed to enable continuous and automated monitoring and response.

About Cisco

Cisco fully enables the government's digital transformation with technologies and services that transform citizen experiences, agency processes and business models. Our innovative solutions in cloud computing, cybersecurity and collaboration are helping government integrate the Internet of Things (IoT) to connect employees and citizens anywhere, anytime to better protect, serve and educate our nation.

Cisco solutions provide integrated and validated architectures, an extensive partner ecosystem and decades of expertise in best practices for government. Working together with government, we are delivering strategies for digitization to meet the 24/7 demands of today's world while keeping networks secure.

For more information visit: cisco.com/go/federal.

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW, Suite 800
Washington, DC 20005

(202) 407-7421
F: (202) 407-7501

www.govloop.com
@govloop