Shielding Your IT Operations With a Software-Defined Secure Network

MARKET TRENDS REPORT

govloop

JUNIPER NETWORKS

Introduction

Now that federal IT environments extend to many sites, devices and public clouds, they're more vulnerable than ever to cyberattacks. Depending on multiple standalone security products to protect federal networks, systems and data leads to complexity that could be weakening their defenses. The volume of uncorrelated alerts generated by multiple sources are a top concern for security teams, who must sift through them all to find meaningful, actionable data. Adding to the complexity, many agencies are also adopting a multi-cloud model, which is a hybrid environment containing several public clouds, private clouds or a mix of both.

This fluidity leaves agencies uncertain about the perimeters of their networks. More cybersecurity vulnerabilities emerge, and resources become harder to track as the defined boundaries containing them change. It's a situation that leaves agencies struggling to actively defend against cyberthreats, let alone comply with federal regulations to counter them. Satisfying the requirements of the Continuous Diagnostics and Mitigation (CDM) Program and other federal benchmarks only makes the situation harder. Launched in 2013, CDM aims to fortify cybersecurity for federal networks and systems. Building on the previous phases, which seek to figure out What and Who are on the Network, Phase 3 – What is Happening on the Network – focuses on detecting and mitigating security events across blurred boundaries.

Fortunately, a software-defined secure network (SDSN) can address these challenges. SDSN is an approach that incorporates, unifies and automates security throughout the network to defend against today's sophisticated threat landscape. SDSN enlists platforms from throughout the network to act as security enforcement points and create a comprehensive defense domain, automatically and dynamically detecting and responding to threats as an ecosystem rather than as a collection of individual entities. GovLoop partnered with Juniper Networks, a networking technology provider, on this report about how agencies can secure their networks with SDSN.

The following pages explain how organizations can deploy SDSN to automate and protect their networks. They also contain insights from Greg Fletcher, Director of Business Development and Capture for Civilian Agencies at Juniper Networks.

BY THE NUMBERS

72%

of federal IT leaders see increased vulnerabilities from shared infrastructure as their top cloud security concern.

Source: Thales/451 Research

35,700

federal information security incidents occurred in fiscal year 2017.

Source: Government Accountability Office (GAO)

20%

of federal IT leaders view sensitive information potentially residing anywhere within the environment as their top concern for securing big data.

Source: Thales/451 Research

21%

of federal information security incidents in fiscal year 2017 were attacks executed via an email message or attachment.

Source: GAO

57%

of federal IT leaders reported data breaches and compliance audits in the last year.

Source: Thales/451 Research

THE CHALLENGE

Perimeter Dissipation Leaves You Exposed

The federal government handles huge amounts of data, ranging from financial information to national security secrets. To address the challenge of increasing data and information demands, many agencies are leveraging both public and private cloud services that are designed to meet the sensitivity level of the data stored on each platform.

"As agencies increasingly look to public cloud solutions to augment private cloud capabilities, many are realizing that certain applications work better in certain cloud environments. This creates complexity in managing and securing sensitive government information," Fletcher said. "As time goes on, we're likely going to see an expanding number of different cloud providers. How's an agency going to manage and secure all of that?"

Organizations that have multiple clouds have larger, more complex networks with larger attack surfaces that need defending from cyberthreats. It's a daunting task, as foreign nation-states, terrorists, criminals and hackers constantly threaten federal infrastructure, information and data.

"Every millisecond counts as you're trying to understand the health of your network and have situational awareness about it," Fletcher said. "You have to detect bad actors in various, creative ways, inform the network of their presence, shut down infected areas and keep the network clean."

Unfortunately, perimeter dissipation makes cybersecurity in the multi-cloud model challenging. Perimeter dissipation happens when an agency's information spreads across a growing private and public cloud infrastructure faster than the barriers and techniques used to protect that information. Having more clouds increases the number of potential vulnerabilities needing vigilance.

"You have to detect bad actors in various, creative ways, inform the network of their presence, shut down infected areas and keep the network clean."

—Greg Fletcher, Director, Business Development and Capture for Civilian Agencies, Juniper Networks

THE SOLUTION

Dynamic, Adaptive, Multi-Cloud Security With SDSN

Federal agencies must take a synergistic approach that leverages network and security elements equally in an open, multi-vendor ecosystem with centralized policy, analytics and management to transform their traditional network into a secure network. To proactively defend their networks against evolving cyberthreats, agencies need tools that let them monitor and defend them in real time. Software that is open for integrations and fueled by automation enables this cybersecurity for multi-cloud environments. Using these tools, agencies can reap the benefits of a SDSN to stay ahead of cyberthreats while bringing new levels of efficiency to their security teams.

"With a multi-cloud environment, agencies are increasingly able to move instances wherever there's the fastest, cheapest, most reliable and relevant environment for that workflow. It's whatever the need is at the time. How do you ensure security in such a dynamic environment?" Fletcher said.

SDSN meets this challenge by providing agencies with a platform that integrates, centralizes and automates defense for today's sophisticated threat landscape.

"It's not just network management, it's true network security," Fletcher said. "You're not putting more firewalls and security appliances into your network, you're making your network into a firewall. Instead of your network and security components being siloed, they're all talking to each other and they're all able to be impacted and have policies enforced on them."

It's an approach that additionally helps agencies reach federal cybersecurity standards. SDSN ensures that organizations comply with programs like CDM while simultaneously hardening their cyber defenses.

BEST PRACTICES

Meeting Your CDM Requirements with SDSN

I. Automate your security and compliance

Automation is a necessary component of SDSN. It allows agencies to detect and mitigate cybersecurity risks faster, and it also quickens the rate at which they can comply with federal security standards. Both outcomes free up more energy and time for employees to perform higher-level, more mission-critical functions.

2. Reach CDM cybersecurity benchmarks

CDM assists agencies by finding and ranking the biggest security risks to their infrastructures. It relies on automated, agency-installed sensors to continuously monitor known cyber flaws. An organizational dashboard then informs network and security managers about their most serious problems. This assists them with better allocating their resources and responding to problems more efficiently.

SDSN boosts the speed at which agencies can reach CDM standards using automation for continuous monitoring and mitigation of cyberthreats. Meeting these requirements improves the cyberdefense posture of both your agency and the overall federal government.

3. Understand and adhere to CDM phases

The Department of Homeland Security (DHS) announced in November 2018 that the CDM program has recently shifted focus to capabilities, rather than a phased approach. Despite this, each phase offers important cybersecurity insights to agencies.

SDSN is especially relevant to CDM's Phase 3, as it concerns what's happening on a network. This is because CDM's capabilities include data at rest and in transit, user activities and behavior and device, host, network and perimeter components. Given every section of SDSN constantly finds and stops cyberthreats, it's the perfect model for Phase 3.

Phase 3 is crucial for moving beyond asset management to more dynamic, extensive monitoring of security controls. Agencies that deploy CDM tools are more capable of recognizing dangers on their networks and halting them from causing additional damage elsewhere.

4. Partner with a knowledgeable vendor

CDM sets high security standards for the federal government, and implementing SDSN with its many capabilities is a complex process. Having private sector partners with expertise on the program is a valuable resource for agencies. These companies can save energy, money and time for their public sector counterparts by helping them more quickly implement SDSN at CDM levels.

How Juniper Networks Helps

Juniper Networks provides agencies with a synergistic approach to networking and security with its SDSN solution. SDSN can transform organizational networks from infrastructures that need defending to secure infrastructures that can defend themselves.

Automation is the force driving this change. Juniper Networks' SDSN automates cyberthreat detection and remediation. This ensures that agencies can defend any part of their networks in real time without losing any continuity in their operations. The burden on employees is also reduced, letting them focus on more complex concerns.

SDSN also elevates agencywide security. Organizations gain visibility into their networks end to end, ensuring that vulnerabilities don't go undetected. This is because SDSN uses on-premise and cloud capabilities for constant vigilance and threat mitigation across every physical and virtual component organizations have.

Juniper Networks' SDSN platforms, meanwhile, automate and centralize cybersecurity for agencies using software. This hub unifies detection, enforcement and policy for organizations, helping them achieve their desired defense posture more quickly and easily.

Compliance is an additional concern for agencies, but Juniper Networks' SDSN platform is aligned with the federal government's latest security standards. These tools meet not only CDM benchmarks, but other guidelines too. For example, SDSN satisfies the National Institute of Standards and Technology's (NIST) cybersecurity standards.

"We've built government standards deliberately into the solutions we've created," Fletcher said. "Juniper is committed to ensuring that agencies are getting properly vetted security products from us to secure their networks."

The following table demonstrates Juniper's compliance with the CDM requirements as part of its acceptance in 2017 to the CDM Approved Product List and GSA CDM SIN.

Learn more here: https://www.juniper.net/us/en/products-services/what-is/sdsn/

	CDM Phase	Phase 1 What is on the Network?				Phase 2 Who is on the Network?				Phase 3 How is the Network protected?	Phase 3 What is happening on the Network?		
	Juniper Network Products	Hardware Asset Management	Software Asset Management	Configuration Settings Management	Vulnerability Management	Manage Trust	Manage Behavior	Manage Credentials	Manage Privileges	Boundary Protection	Manage Events	Operate, Monitor and Improve	Design and Build-in Security
Network Security Products	MX/vMX Routers				✓	✓	✓	✓	✓	✓			✓
	EX Switches				✓	✓	✓	✓	✓	✓			✓
	QFX Switches				✓	✓	✓	✓	✓	✓			✓
	NFX	✓	✓		✓	✓	✓	✓	✓	✓			✓
	SRX/vSRX Firewalls	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
	Contrail Services Orchestrator*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security Products and Features	AppSecure	✓	✓							✓			
	Juniper Identity Management Service					✓	✓	✓	✓	✓			
	SSL Proxy		✓	✓	✓	✓	✓	✓	✓	✓		✓	
	Intrusion Prevention Service					✓	✓			✓			
	Unified Threat Management				✓	✓				✓			
	SDSN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Contrail Security*		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Advanced Threat Detection	SkyATP				✓						✓	✓	✓
	JATP				✓		✓				✓	✓	✓
Policy and Analytics	Junos Space Security Director	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
	JSA	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	
	Policy Enforcer				✓						✓	✓	

*Onboarding for CDM in early 2019

Shaded boxes represent capabilities met with partner collaboration

Conclusion

Agencies must constantly juggle complying with federal standards, protecting their cybersecurity and serving citizens. It's a complicated performance that only becomes harder as extra clouds are added to the routine.

SDSN ensures that organizations effectively manage their multi-cloud environment without interrupting their business. SDSN gives agencies a secure network across both their public and private clouds. It's a tool that actively finds and stops perils while meeting federal security standards.

Cybersecurity incidents are a question of when, not if. SDSN, however, uses automation to watch every part of your network in real time. Regardless of how your organization's perimeter evolves, SDSN keeps shining a light on your vulnerabilities and what's endangering your network. Leveraging an SDSN strategy allows agencies to keep citizen data safe, reduce cyber operational challenges, and increase resources and focus on serving the U.S. citizen.

ABOUT JUNIPER NETWORKS

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value.

Additional information can be found at Juniper Networks, or connect with Juniper on Twitter and LinkedIn.

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 300,000 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

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

www.govloop.com
@GovLoop