How and Why to Consolidate Your Cybersecurity Platforms: Tips & Takeaways

Organizations have spent generously on cloud-based IT investments and expansions in recent years to bolster business agility and flexibility while accommodating remote and hybrid work — and that's dramatically increased attack surfaces, making agency networks more vulnerable to cyberthreats.

Now faced with economic uncertainties — forced to do more with fewer resources — how can organizations protect their networks, clouds, data and endpoints from increasingly severe cyber assaults? Through consolidation.

Benefits of Cybersecurity Consolidation

Consolidation of cybersecurity combines traditionally separate — often disparate — tools (intrusion prevention, anti-malware, DNS security, URL filtering, etc.) into a single platform that provides all those protections together. The benefits of consolidation include:

- Eliminates security gaps
- Less complexity and fewer vendors
- Seamless data-sharing across the platform (eliminates silos)
- Dramatically reduces the number of manual tasks for security operation centers (SOCs), allowing analysts to focus on higher-priority tasks
- Much faster identification and responses to cyberthreats, thanks to artificial intelligence (AI)

287 days

Today's human-centered SOC is inundated with siloed data — with teams taking 287 days on average to ID and contain a data breach.

"We're starting to see more and more connected systems inside of the federal space. ... This idea of zero trust is not just a policy decision or buzzword."

— Drew Epperson, Senior Director of Federal Engineering, Palo Alto Networks

Zero Trust With Zero Exceptions

Zero trust is a simple concept — rooted in the principle of "never trust, always verify" — that applies wholistically to an organization's network and devices. By default, a zero-trust framework denies users access to enterprise data and utilizes multifactor authentication, encryption, continuous monitoring and verification, and other tools to grant limited access as appropriate. No person or device is trusted implicitly.

Agencies today need a zero-trust architecture for maximum cyber protection.

govloop carahsoft paloalto NETWORKS PRESIDIO FEDERAL Think Mission.

3 Pillars of Palo Alto Networks' Zero-Trust Framework

	Identity	Device/Workload	Access	Transaction
Zero Trust for Users	Validate users with strong authentication	Verify user device integrity	Enforce least-privilege access for workloads accessing other workloads	Scan all content for malicious activity and data theft
Zero Trust for Applications	Validate developers, DevOps, and admins with strong authentication	Verify workload integrity	Enforce least-privilege user access to data and applications	Scan all content within the infrastructure for malicious activity and data theft
Zero Trust for Infrastructure	Validate all users with access to the infrastructure	Identify all devices including IoT	Least-privilege access segmentation for native and third-party infrastructure	Scan all content for malicious acitivty and data theft

How Palo Alto Networks, Presidio Federal, and Carahsoft Can Help

"We deliver the entire package, both the AI-based processing ... as well as all the different point products — network security, endpoint, cloud and so on — to generate the data that's required for the AI-based security operations center. I don't know of any other vendor that's delivering this complete package."

— Nir Zuk, Founder and CTO, Palo Alto Networks

Palo Alto Networks' Cybersecurity Platforms

Network Security
STRATA | PRISMA SASE
Best-in-class security delivered across hardware, software and SASE

Cloud Security
PRISMA CLOUD
Comprehensive platform to secure everything that runs in the cloud

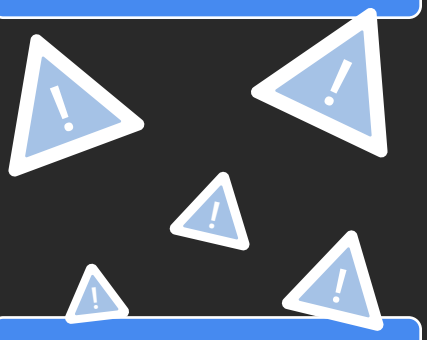
Security Operations
CORTEX
A new approach to SOC with fully integrated data, analytics and automation

Threat Intelligence and Advisory Services
World-renowned threat intelligence, cyber risk management and advisory services

"In five years, those who've gone through a consolidation are going to have a cybersecurity infrastructure that is being run by machines, by AI. They're going to be able to detect and stop attacks as they happen, with a very, very small mean time to detect and to respond. And they're going to be safe.

"And those that haven't gone through a consolidation, those that keep buying point products that don't talk to each other and are running their security operations with a SIEM [security information and event management] approach... I'm just not sure how you're going to be able to secure yourself."

— Nir Zuk, Founder and CTO, Palo Alto Networks



For more information, **visit https://presidiofederal.com/partners/paloalto/.**

govloop carahsoft paloalto NETWORKS PRESIDIO FEDERAL Think Mission.