FEDERAL NEWS NETWORK

EXPERT EDITION

Tackling the new cyber landscape

Insights by

- Alliance for Digital Innovation
- Centers for Medicare and Medicaid Services
- CISA
- Energy
- GSA
- National Security Council
- U.S. Patent and Trademark Office
- VA

BROUGHT TO YOU BY carahsoft

TABLE OF CONTENTS

Feds push forward on zero trust — by design and by need

The stakes are high in cyber.

"The consequences are no longer just loss of finances, loss of reputation. It's now potentially loss of life and really things playing out in our physical environment, points out Arielle Baine, cybersecurity advisor at the Cybersecurity and Infrastructure Agency.

Agencies across the government are intently focused on cyber initiatives, driven in part by evolving threats and in part by the directives of the White House's executive order on improving cybersecurity.

That said, it's not like one day government's security leaders suddenly began working on zero trust. The evolution to an identity-centric model, where people and devices are continuously vetted, has been underway for several years. But the pandemic sped up the timeline, as did the desire to share more data securely within and across agencies and to make it available wherever feds might need it.

As Kshemendra Paul, chief data officer at the Veterans Affairs Department, puts it: "You can always do more sharing if you build in place better safeguards. And then there's a natural imperative to introduce automation on the safeguarding side to accelerate sharing and to improve safeguarding."

In this ebook, we cover a wide swath of trending security topics:

- Tech leaders at the Centers for Medicare and Medicaid Services, the Energy Department and the White House National Security Council share insights on the current state of cybersecurity.
- CISA details its continued efforts to provide guidance, with the release of the draft TIC 3.0 Cloud Security Use Case.
- The General Services Administration explains why it's working to identify capabilities gaps in federal cyber contracts.
- The U.S. Patent and Trademark Office reveals how it will implement a secure access service edge (SASE) framework as its foundational foray into zero trust.
- Plus, industry experts from AvePoint, Ping Identity, Radiant Logic, SentinelOne and Tanium offer numerous zero trust tips and tactics.

We hope these articles offer valuable takeaway that carry over to the cyber evolution efforts at your organization.

Vanessa Roberts
Editor, Custom Content
Federal News Network

The device pillar in CISA's Zero Trust Model is key to preventing attacks

Matt Marsden
Vice President of Public Sector Technical Account Management, Tanium

The Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model breaks down zero trust architecture into five pillars to make it easier for agencies to digest and focus on where their cybersecurity strategy requires refinement. But only one of those pillars represents the primary attack surface: the device.

"That's where the users are. Users are generally considered the weakest link in enterprise security," said Matt Marsden, vice president of public sector technical account management at Tanium. "So given that you have endpoint devices distributed across many work locations, connected over different networks, and users with differing levels of sophistication and security awareness using those devices; that is really the primary target for attackers."

Phishing and social engineering are common vectors for attackers, and traditional antivirus and endpoint protection products aren't effective against those attacks. The ability to monitor device posture at scale is imperative to finding potential vulnerabilities introduced by these kinds of attacks.

If the device represents the primary attack surface, the data on those devices is what needs protecting. Data is the fifth pillar of CISA's Zero Trust Strategy and protecting the data starts with knowing what exists, where it is located and who has access to it. With the device acting as the point of production for data, knowing your device posture (the second pillar of CISA's strategy) is a critical piece to a successful zero trust implementation.

That means having full visibility into what devices are on the network, how they are configured, if there's been configuration drift and being able to enforce policies at scale. Once organizations have access to key information on a device's posture, then prevention mechanisms should be put in place to block ransomware from taking over, restricting unapproved applications from being downloaded, removing them if they are and limiting process execution on the endpoint.

The challenge of maintaining devices at scale has been made even tougher by the pandemic as IT departments are left trying to figure out how to apply these controls when devices are not in the same building, network or even connected to the domain. To get a real sense of the device posture across all endpoints, IT staff need a solution that allows them to have comprehensive visibility and control at scale. Administrators should be able to manage their assets in real time, whether those devices are directly connected to the agency's network or over an unsecured Wi-Fi in a local coffee shop.

> "That's where the users are; users are generally considered the weakest link in enterprise security. So given that you have distributed endpoint devices at many work locations, connected over different networks, and you have users with differing levels of sophistication, education, and security awareness using those devices; that is really the primary target for attackers,"
>
> **– Tanium's Matt Marsden**

Achieving basic cyber maturity

When it comes to best practices for how to implement a state of full visibility, Marsden emphasized four key components:

1. Agencies need to be able to scan their environment (Windows, Mac or Linux machines and servers) for a comprehensive hardware and software asset inventory ideally using one tool.
2. They need to be able to get back the data they need in minutes, not weeks due to slow scans, or by combining data sets from numerous point tools.
3. They need the ability to remediate any issues found without pivoting to another tool or relying on separate teams.
4. They need the ability to continuously monitor compliance with policies that can be set and enforced.

These best practices help lay the groundwork for having good cyber hygiene, and therefore the foundation of a solid zero trust strategy, and will bring agencies to the most basic level of cyber maturity according to CISA's model. From there, to improve to the advanced maturity level, they need to ensure device access is properly managed.

Continuous monitoring

"Ultimately, the optimal level of maturity in a zero-trust implementation is having consistent and real-time continual security and device monitoring, as well as policy enforcement and validation," Marsden said. "Continual monitoring and accurate analytics are only feasible after comprehensive visibility and control are achieved."

Marsden said Tanium has helped several federal agencies through the continuous diagnostics and mitigation program from CISA to measure and enhance their cyber hygiene by giving them a more complete view of their hardware and software asset inventories, as well as their vulnerability management. Those agencies are now providing much better data to their CDM dashboards.

"Many of our customers have consolidated disparate point solutions used for managing, securing, patching and configuring devices. Tanium's platform brings together the activities related to IT operations, security, risk management and all-around cyber hygiene," he said. "Tanium can tear down those silos, enabling these different teams to work from the same singular data set and console, which helps them save time in tedious processes, money in paying for numerous tools, and results in a safer federal government."

It can be difficult for the federal government to find the right tools to support their zero-trust journey. As long as agencies focus on

three main components -- device posture, network security and identity management -- all in concert together, they can address the main attack vectors to their organization. And, with a special emphasis on device posture and compliance monitoring, if an adversary does get in, security teams need to be able to identify them quickly, take action to shut them down, and implement prevention tactics moving forward. According to Marsden very few tools can do all of these things, but ensuring that these tools have the extensibility to integrate with each other helps future-proof an agency's zero trust approach.

"Ultimately, the optimal level of maturity in a zero-trust implementation is having consistent and real-time continual security and device monitoring, as well as policy enforcement and validation. Continual monitoring and accurate analytics are only feasible after comprehensive visibility and control are achieved,"

– Tanium's Matt Marsden

Count on Carahsoft® and Our Partners for Cybersecurity Products and Services

Carahsoft has established strategic, long-term relationships with the industry's leading cybersecurity manufacturers and resellers to offer government entities proven, cost-effective protection for infrastructures, networks and assets with solutions from the following vendor partners.

Akamai	f5	Forcepoint	FORESCOUT	Gigamon	Infoblox	Micro Focus Government Solutions
okta	paloalto NETWORKS	RSA	splunk>	Symantec A Division of Broadcom	Trellix	zscaler
AGARI	ALTR	anchore	ANOMALI	aqua	Aquera	ARMIS
Attivo NETWORKS	AvePoint Public Sector	Bastille	BAYSHORE NETWORKS INDUSTRIAL AND IT NETWORK SECURITY	BeyondTrust	BlackBerry	blancco
Blinkly	Cellebrite	CertiPath	COFENSE	CONCEAL Detect. Defend. Isolate.	Contrast SECURITY	CYBERARK
BlackBerry CYLANCE	DATAGUISE	DATALOCKER SIMPLY SECURE	DIGITAL GUARDIAN	druva	DTEX WORKFORCE CYBER INTELLIGENCE & SECURITY	eclypsium
ENTRUST	exabeam	exterro	Fidelis Cybersecurity	FLASHPOINT	ForgeRock	FORNETIX
FORTINET	FORWARD NETWORKS	globalscape by HelpSystems	HashiCorp	HID	iboss	IDENTITY AUTOMATION
imperva	Information Security CORPORATION	Inspired eLearning	IronNet	KEEPER	Kion	Kiteworks
Lookout	MEDIGATE	netskope	NETWITNESS An RSA Business	neustar	NIGHTDRAGON	Nlyte Software
OSIsoft. is now part of AVEVA	Ping Identity	proofpoint.	Qualys.	RACKTOP	RADIANT LOGIC	RANGEFORCE
RAPID7	Recorded Future	RISKSENSE	SailPoint	SANS	SAVIYNT	Secureworks
securonix	SentinelOne	SKYBOX SECURITY	solarwinds government	sonatype	STEALTHbits TECHNOLOGIES	TANIUM
TEMPERED NETWORKS	tenable	THALES	ThreatConnect	THREATLOCKER	THREATQUOTIENT	TREND MICRO
Trustwave Government Solutions	tufin	Venafi	VERACODE	WATERFALL Stronger Than Firewalls	WHITE CANYON SOFTWARE	zeva

Carahsoft's cybersecurity solutions are available through its reseller partners on a variety of contracts including GSA MSA, 2GIT, SEWP V, ITES-SW2, and numerous state and local contracts. To learn more about available solutions, contact the Carahsoft Cybersecurity Team at (888) 662-2724; cybersecurity@carahsoft.com; or visit carahsoft.com/solve/cybersecurity.

carahsoft. The Trusted Government IT Solutions Provider®