MeriTalk
Improving the Outcomes of Government IT

Underwritten by
DELL Technologies
ViON
Building your enterprise solutions

MISSION FIRST:
WHY AGENCIES ARE EMBRACING MANAGED-RISK SECURITY

Federal cyber leaders are working to keep mission-critical data secure and available to employees working from home, in the office, and in the field at the tactical edge. Despite progress and intense focus, a boom in cybersecurity breaches is commanding national attention and highlighting the need for IT and security modernization throughout the Federal government.

Christopher Wray, director of the Federal Bureau of Investigation, compared the deluge of ransomware attacks to the environment following September 11, 2001. "There are a lot of parallels… and a lot of focus by us on disruption and prevention," Wray said.

Ransomware incidents have tripled in the past year, he explained, "There's a shared responsibility, not just across government agencies but across the private sector and even the average American."

The Biden Administration's Executive Order (EO) on Improving the Nation's Cybersecurity enforces this point with the caveat that "cybersecurity requires more than government action." Agencies must renew their sense of urgency to take bold action to revitalize government security architectures and embrace cybersecurity and risk-management as a springboard for mission innovation.

Time for Definitive Action

"Threats are evolving much faster than the government, and even the private sector, have seen in the past," explained Rob Davies, chief operating officer at ViON Corporation in a recent interview. Agencies are taking a more fluid risk-management posture.

As agencies develop EO-mandated zero trust plans, the private sector is sharing guidance and lessons learned. Cameron Chehreh, federal chief technology officer at Dell Technologies, encourages leaders to use zero trust as an opportunity to shift their paradigm from "security as mission inhibitor" to "security as mission accelerator."

"It's about leveraging existing governance and processes as well as available technology to address needs rapidly and effectively," Davies shares.

Driving Innovation with Managed-Risk

"Accepting risk is healthy," Chehreh says, "It's helping to drive innovation as agencies understand that cybersecurity is not just a 'check-the-box activity' to obtain authority to operate (ATO) on the network." Chehreh says cybersecurity must be a dynamic, daily process that focuses on users and their risk posture throughout the day.

This is particularly important for agencies with remote teams working in unpredictable environments. They are at increased risk for cyber threats. Emergencies direct attention away from standard operations, giving criminals an opportunity to strike.

As an example, the Federal Emergency Management Agency (FEMA) executes missions remotely, under challenging conditions. In this case, a zero trust architecture provides mission agility by securing technologies and applications at the edge that are critical to operations such as disaster relief.

Ted Okada, chief technology officer at FEMA, recently shared the agency is working towards these goals to allow teams to securely store data and compute at the edge, closer to the source.

This approach helps the organization automate compliance and security, and deploy new mobile and remote technologies faster and with greater confidence as they respond to catastrophic events.

> *Often agencies try to protect all parts of their infrastructure equally. Zero trust models align protection with data and application value – and allow teams to continuously assess risks to those critical assets.*

Mission First

When building a strategy for the greatest impact, Davies advises Federal leaders to first consider their agency's unique operations. This will inform changes that are central to the mission.

"Take the time to dig deep and answer core questions that relate to the zero trust pillars, including – Where does my data reside? Where does it move to and how is it used daily – in transport and sessions? Which applications are critical to our mission? Who are our users, and where are they physically located? What devices do they use today? What will they be using in the future?" he said.

"The key to moving fast is understanding your stakeholders – their motivations and what they need to achieve," Chehreh said.

It's all about embracing and executing best practices, Davies adds. Agencies can look to and build upon the pillars of zero trust: device security, workload security, infrastructure security, network security, data security, and process. And ultimately, Chehreh emphasized, "never lose sight of what sits at the very top of these pillars – the mission."

EXECUTIVE Q&A:

VION, DELL TECHNOLOGIES LEADERS CONNECT MANAGED-RISK SECURITY TO FEDERAL MISSION ACCELERATION

The SolarWinds breach, the Colonial Pipeline and JBS meatpacking ransomware attacks, and most recently a ransomware attack on a House of Representative email vendor have Federal cybersecurity and IT leaders wondering what's next.

These events have catapulted cybersecurity to the forefront of the national agenda – with the White House, U.S. Congress, and Federal agencies focused on prevention through modernization and education. The Biden Administration's Cybersecurity Executive Order is setting the pace. Zero Trust Architecture is a pillar of the new strategy, along with moving to secure cloud services, adopting multifactor authentication and data encryption, and boosting supply chain security.

MeriTalk recently connected with Rob Davies, chief operations officer at ViON Corporation, and Cameron Chehreh, federal chief technology officer at Dell Technologies, to discuss the steps agencies can take to protect critical infrastructure and data from the influence of cybercriminals. Davies and Chehreh also provide insight on challenges unique to multi-cloud environments and how Federal leaders can accelerate mission value with a managed-risk approach to cybersecurity.

MeriTalk: The Federal government's reliance on data is growing, and so is the cyber threat. How are recent attacks changing how teams approach data security in cloud environments?

Cameron Chehreh: We're seeing changes at every level — from the White House and Congress to Federal agencies. Recent events, including the Colonial Pipeline and JBS meatpacking ransomware attacks, are making cybersecurity a mainstream conversation. The Biden Administration Cybersecurity Executive Order sets the course. Congress is supporting broader cybersecurity initiatives and committing funds for them. At the agency level, leaders are beginning to embrace cybersecurity as a mission accelerator.

Rob Davies: Agencies are looking to their partners to help them make good decisions about priorities. Threats are evolving much faster than the government and even the private sector are used to moving. We're seeing important discussions around critical questions, such as "How should I prioritize issues? How can I best use my contract vehicles to get what I need quickly?"

Agencies want to understand how they can garner resources at their disposal to get the results they need. It's about leveraging existing governance and processes as well as available technology to address needs rapidly and effectively.

MeriTalk: How can agencies execute on mission in a risk-managed way, balancing the need to leverage data for innovation and the need to protect it?

Chehreh: When the Federal government pivoted to telework, agencies realized they didn't have the luxury of absolute cybersecurity assurance. Instead, they had to move toward a more fluid, risk-management posture. That's a good thing.

The move to Zero Trust further underscores that accepting risk is healthy. It's helping to drive innovation as agencies understand that cybersecurity is not just a "check-the-box activity" to obtain authority to operate (ATO) on the network. Instead, it must be a dynamic, daily process that focuses on users and their risk posture throughout the day.

For example, an agency can assess the risk associated with a user's smartphone or laptop based on where they are and what applications they're using. The ability to actively monitor and create a risk profile throughout the day can significantly improve overall security.

MeriTalk: What unique security challenges do multi-cloud environments present?

Davies: A multi-cloud world presents new opportunities and challenges, especially when a large part of the workforce is working remotely. Agencies are moving data that used to be solely in their data centers to one or more public or private clouds. The job of knowing where data is located, and who is using it and how, becomes much more complex, as does the process of assuring that data is not compromised at any point.

MeriTalk: How can teams minimize the complexity of these challenges to accelerate mission value and reduce risk?

Chehreh: The Federal government needs to raise awareness of how to operate safely and have the right safeguards in place for the mission.

> *Zero Trust presents a golden opportunity to accelerate mission value and reduce risk. It gives leaders the chance to flip the paradigm from "security as mission inhibitor" to "security as mission accelerator."*

Zero Trust also changes the narrative because it focuses on securing users, devices, data, and more, instead of network access. The model assumes that intruders are already in the network and no connection should be trusted. Zero Trust, therefore, focuses on continuous, dynamic authentication and authorization. It opens a world of possibilities for mission acceleration and innovation because it ensures security even at the edge, where so many Federal agencies execute daily.

The Federal Emergency Management Agency (FEMA), which conducts its mission remotely and under some of the most challenging conditions, demonstrates Zero Trust's potential to power greater mission agility. Criminals see opportunities to strike during emergencies when processes are fluid, and FEMA is particularly vulnerable. Zero Trust Architecture will enable the agency to deploy new mobile and remote technologies faster and with greater confidence to expedite assistance and resources when and where they're needed most.

MeriTalk: The White House Cybersecurity Executive Order directs agencies to deliver Zero Trust implementation plans in 60 days. What should Federal teams consider when developing these plans?

Davies: Focus on building on the right plan for your agency. Take the time to dig deep and answer core questions that relate to the Zero Trust pillars, including: Where does my data reside? Where does it move to and how is it used daily – both in transport and sessions? Which applications are most important and critical to our mission? Who are our users, and where are they physically located? What devices do they use today and will they be using in the near future?

Chehreh: The key to moving fast is understanding your stakeholders – their motivations and what they need to achieve. This plan is not about the business case. Instead, it focuses squarely on what agencies need to get the job done when it comes to implementing Zero Trust.

The planning process is also an important opportunity to rationalize the application portfolio. Agencies need to know what applications people are using and how they help to advance the mission. Keep it simple. Which applications should we retire? Which can we quickly modernize? Where do we need new applications? This approach enables a surround-and-suffocate strategy that gets agencies to Zero Trust quickly and effectively.

MeriTalk: Where should leaders focus as they implement Zero Trust across disparate cloud and hybrid environments?

Chehreh: Agencies should focus first on the Zero Trust pillars – device security, workload security, infrastructure security, network security, data security, and process security – because it will help them collect their thoughts in a logical way. But never lose sight of what sits at the very top of these pillars – the mission. Before implementing Zero Trust, agencies must look at their specific mission scenarios and how they connect and play out across various clouds.

MeriTalk: What types of resources are available and most important?

Davies: There are many resources available to help at every phase. Agencies should look to the private sector, which can provide a roadmap for best practices and cautionary tales. Industry standards organizations, such as NIST, can help agencies focus on the intersection of best practices and standards.

I expect to see many discussions between agency leaders and their technology partners. The focus should be on getting information to Federal agencies and having an open dialog because it can get complicated quickly. For example, technology partners, such as ViON and Dell Technologies, can help agencies navigate the complex Federal acquisitions process, especially when it comes to leveraging new technologies. Research and development contracts and OpEx models, for instance, can expedite procurement – and ensure a low cost of entry – when piloting new solutions.

MeriTalk: The human element is the most critical link in cybersecurity? What do agencies need to do to educate users about Zero Trust and its role in elevating cybersecurity?

Chehreh: It's about creating a culture of awareness. Do you know the system you're working in? What about your location? Focusing on the basics of cybersecurity hygiene will go a long way toward instilling a culture of safety.

Davies: I think back to some of the great public education campaigns, such as Smokey the Bear, seat belt awareness, and anti-littering campaigns. We need a similar approach to instilling a culture of safety throughout the user community. Agencies must continually educate and reinforce the importance of good cybersecurity hygiene.

MeriTalk: How do ViON and Dell Technologies deliver secure solutions to help teams optimize and secure workloads to maximize investments in cloud?

Chehreh: This is where the power of the partnership between ViON and Dell Technologies is extraordinary for our customers. To maximize the security posture in cloud and multi-cloud environments, we start from the supply chain and move up. This includes establishing hardware root of trust, software integrity, shipment security documentation and assurance, control audits, and much more.

Davies: ViON has stringent requirements for supply chain risk management, and it's critical that we understand what our OEMs are doing in this regard. We need to understand where the technology we sell or sponsor has been and how our partners assure supply chain integrity.

Business models continue to change, and so must we in terms of ensuring supply chain security. There are a set of technology products and tools that we can leverage from Dell Technologies and other partners to make the environment more secure. At the core, it's all about embracing and executing best practices.