ViON
Building your enterprise solutions

DELL Technologies

Opportunity for Innovation – From Oh No to Let's Go

Rethinking Cybersecurity as an Engine for Mission Innovation

The Federal government and our economy run on data, so it must be available, trusted, and most of all secure. These three requirements are inextricably linked, and a string of high-profile and damaging cybersecurity events in the last year have made this fact crystal clear.

Washington – and the broader public – is hyper-focused on cybersecurity like never before. After a sharp spike in cyberattacks, the Biden Administration released its ambitious Cybersecurity Executive Order (EO). The President also has included cybersecurity investment as an important part of his proposed infrastructure revitalization program.

These initiatives will bring new requirements and complexity, especially in multi-cloud environments, where data is distributed even more widely. They also, however, present a golden opportunity for Federal agencies to rethink cybersecurity as a springboard for mission innovation. **The key is careful planning, a risk-based approach with a Zero Trust Architecture at its core, and collaboration with the larger security ecosystem.**

Opportunity Knocks

The EO and its provisions for expediting Zero Trust Architecture implementation, moving to cloud services, and adopting multifactor authentication and data encryption give Federal IT leaders an opportunity to flip the paradigm from "security as mission inhibitor" to "security as mission accelerator."

Legacy perimeter-focused security models that default to high trust levels on the network are poorly suited for Federal agency missions executed at the edge and a Federal workforce that is now significantly mobile and remote.

Zero Trust changes the narrative because it focuses on securing users, devices, data, and other potential vulnerabilities, instead of network access. It assumes that intruders are already in the network and no connection should be trusted. Therefore, the foundation of Zero Trust is continuous, dynamic authentication and authorization. It's clear to see how this approach opens a world of possibilities for mission acceleration and innovation because it ensures security even at the edge.

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. As early as 2017, more than 90 percent of FEMA's disaster survivor applications came through the internet and the agency's mobile applications, and the agency relies on a host of mobile command centers and applications.

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.

On Your Mark, Get Set, Go

Leaders acknowledge that the Biden EO sets an ambitious timeline for rolling out Zero Trust Architectures and other strategies. Brandon Wales, acting chief of the Cybersecurity and Infrastructure Security Agency, recently said that the EO's many deadlines and condensed timeline will "stretch the system."

Agencies need to get it right the first time, and a three-step strategy creates a solid foundation for success:

1 Focus on the Plan – Then Prepare to Work It

The EO gave agencies 60 days to create a new plan for moving to Zero Trust in line with National Institute of Standards and Technology (NIST) guidance. This presents an opportunity for agencies to identify and define the optimal approach for their organization, answering critical questions, such as:

- Where is our **data**?
- Where does it move daily and how is it used daily – including **transport and sessions**?
- Which **applications** are critical to our mission?
- Who are our **users** and where are they?
- What **devices** do they use today? In the future?

The answers to these questions and more will determine what Zero Trust looks like for each agency. Then, it's time to garner resources and work the plan.

2 Embrace a Risk-Managed Approach to Zero Trust and Cybersecurity

Not all assets, applications, and data are equally important, and agency IT and cybersecurity resources are already stretched to the limit. A risk-managed approach to cybersecurity enables agencies to focus proper resources on their most critical, mission-centric assets. They can then build a Zero Trust policy and architecture that defines appropriate access, authorization, and security controls for their unique situations.

With this model, cybersecurity is not just a check-the-box activity to achieve authorization to operate (ATO). Instead, it is infused throughout the mission and its daily execution. Continually profiling risk throughout the day – based on individual activities, devices, and locations – greatly elevates both visibility and security.

3 Lean in to Partners

Collaboration at every phase will be the key to success when it comes to elevating the Federal government's security posture. First, agencies can look to the private sector, which can provide a roadmap for both best practices and cautionary tales. Industry standards organizations, such as NIST, are also valuable partners, helping agencies remain compliant as they execute.

Further, look to your technology providers for trusted expert advice and solutions. Technology partners, such as Dell Technologies and ViON, can also help Federal IT leaders navigate the complex web of Federal acquisitions, especially when it comes to leveraging new technologies. In many cases, research and development contracts and OPEX models can provide an avenue to rapid procurement – and a low cost of entry – when piloting new solutions.

Dell Technologies and ViON are also equipped to help agencies advance on the EO's new supply chain requirements, ensuring foundational hardware security, software supply chain security documentation and assurance, control audits, and more.

Learn how ViON and Dell Technologies can help your agency innovate with Zero Trust and a risk-managed approach to cybersecurity.

For more information, visit: vion.com/multicloud