Practical Steps for Turning Zero Trust Strategy Into Mission Progress

As federal agencies advance zero trust modernization, some of the hardest work happens where architecture, deployment, operations, and acquisition intersect. Progress depends on clear visibility across applications, data, users, infrastructure, and mission risk – across enterprise, tactical, and operational environments.

MeriTalk recently sat down with Chris "CT" Thomas, technical director in Dell Technologies' Global Office of the Chief Technology Officer, to discuss practical considerations for SD-WAN, secure access service edge (SASE), security service edge (SSE), and related capabilities that can help agencies make measurable zero trust progress. The conversation explores deployment models, infrastructure readiness, AI-enabled automation, Thunderdome lessons, procurement considerations, and near-term steps agencies can take to move from strategy to measurable progress.

MeriTalk: What are the most common barriers agencies face when trying to move from zero trust strategy to implementation across enterprise, tactical, and operational environments?

Thomas: The biggest challenge is gaining a full understanding of what zero trust truly looks like across the enterprise. Each agency will judge mission success differently.

Agencies have to rationalize each application – how it is consumed, how many users consume it, what the user experience looks like, and the associated risk around data. Data is now the product. You have to focus on that, understand who the data owners and stewards are, and understand how that data is stored, processed, and disseminated across the network.

MeriTalk: How should agencies assess whether their current network architecture is ready to support SD-WAN, SASE, SSE, and other capabilities that support zero trust modernization?

Thomas: Organizations need a documented baseline. They need to understand where they are having challenges – whether that is at edge sites, branch offices, geographically dispersed sites, or in denied, disrupted/degraded, intermittent, and limited (DDIL) environments.

Once you understand that baseline, SD-WAN or software-defined router capabilities become very useful because they can reduce manual complexity for field technicians or engineers. Simplifying that experience and managing more at the software layer provides tremendous value.

MeriTalk: What does a practical deployment path look like for agencies with complex legacy environments?

Thomas: I would start regionally. Go to the places where you know you have great documentation, where you know you have the resources and skill sets, and where you understand exactly what success looks like from a key performance indicator (KPI) perspective.

Then get that regional deployment optimized. Take those successes and replicate them across the rest of the environment at scale. That removes a lot of complexity in the rollout, and it gives the organization confidence as it moves forward.

For KPIs, look at end-user experience, latency, jitter, authentication, authorization, and the cybersecurity profile of the endpoint. If a device has a host-based or next-generation firewall running on it, that consumes CPU resources too. Those factors all matter when you are building enterprise architecture at scale.

MeriTalk: How do tactical requirements, such as satellite connectivity, comms-on-the-move, DDIL conditions, and autonomous systems change the way agencies should think about secure network architecture?

Thomas: We are seeing convergence in the backhaul and transport for the wide area network. Agencies want that to be seamless. They do not want hits or loss of connectivity as users transition from one transport path to another, especially in mobile or disrupted environments.

The number of units being deployed matters, and so does understanding which applications are most critical. That is where organizations often struggle, because every team believes its applications are the most important. Agencies have to understand what is required for that team or unit to achieve mission success – based on the commander's requirements – and then prioritize those applications.

MeriTalk: What are some security and operational considerations for IoT and OT environments, especially when those systems support facilities, physical security, critical infrastructure, or field operations?

Thomas: Agencies need to understand and enforce compliance before a device is authorized to connect to the network. That means establishing a baseline. Is the device running the right firmware? The right BIOS? Is it configured correctly?

If the device is a sensor without the intelligence in its operating system to support higher-level functions, agencies can mitigate risk by enabling a proxy or gate. That forces the device through an inspection point before it communicates with anything on the network.

MeriTalk: What infrastructure considerations are most important when agencies are trying to reduce deployment risk, improve performance, and support secure operations across on-premises, cloud, and edge environments?

Thomas: The ability to automate is key. AI can support automation by doing checks that a technician might otherwise spend hours or weeks verifying before moving forward.

That could include coordination across Microsoft, Linux, DNS, and other services. If we automate some of those processes, we remove potential for conflict.

MeriTalk: DISA's Thunderdome initiative is often discussed as a proof point for zero trust modernization. What lessons from that effort are most relevant across defense, civilian, and intelligence agencies?

Thomas: The biggest lesson is getting started. Set a charter. Define the end state. Then put the resources behind it to achieve the goal at scale.

That means working with industry partners, end customers, and mission partners to understand their requirements and then taking action. Don't let obstacles become a reason to deviate from the goal.

MeriTalk: How should agencies think about AI in the context of zero trust and network modernization – as a mission capability to secure and as a tool that can support visibility, automation, and response?

Thomas: To achieve more advanced zero trust functions at scale, AI will increasingly be essential. The system has to become dynamic because of the amount of data agencies are seeing today. There is no way for a human analyst to sift through every log and event manually.

AI can help structure that information so analysts can focus on critical things. It can also help identify anomalies and correlate hundreds of events over time in a way that a human cannot do continuously.

Some tools are already trained to look at network traffic. Others are optimized for Windows logs, Linux logs, or other data sets. But agencies may still need fine-tuning based on their enterprise traffic. Department of Defense traffic,

Treasury traffic, or Commerce traffic may all look different, so monitoring cannot be one-size-fits-all.

MeriTalk: What procurement or acquisition considerations should agencies keep in mind as they look for practical ways to accelerate zero trust modernization?

Thomas: Most importantly, adhere to modular open systems architecture. Agencies want to avoid vendor lock-in. They should look for solutions and partners that have done the validation work already – how a solution scales, what the licensing model looks like, and how it moves from a few users to thousands or tens of thousands. That removes guesswork for the agency.

It also helps with the analysis of alternatives. What works for one agency may be the best thing for them, but it may not be the best fit for the way your organization operates today.

Agencies should also consider how today's infrastructure decisions will support post-quantum cryptography. Adversaries are harvesting encrypted data today with the intent to decrypt it later, once they can do so at scale. That makes post-quantum readiness part of a long-term zero trust strategy. Agencies should look for equipment vendors that support backwards compatibility, so they can move toward post-quantum implementations without creating a rip-and-replace situation with existing infrastructure.

MeriTalk: What's one simple step that agencies can take to make measurable progress in the next six to 12 months?

Thomas: Do a workshop. Bring the right stakeholders together and go through the rationalization of applications. Dell and its channel partners use that session to work directly with agency teams, map the organization's concept of operations, and outline priority areas for follow-on work. Understand the organization's specific concept of operations and identify the highest-impact, highest-risk issue to solve first.

I compare it to securing a home. If the windows are not installed, the door locks still matter, but you have a bigger issue to solve first. Agencies need to identify that bigger issue and start there.