# **Beyond tools:** A more holistic approach to security

Agencies must improve the way they protect critical assets by embracing an end-to-end mindset that includes zero trust

**Henry Fleischmann**
Director of Government, Education and Healthcare Solutions Architecture, VMware

**WHEN IT COMES TO SECURITY,** agencies face both conventional and evolving challenges. Unlike the commercial sector, they must contend with compliance and transparency demands, complex access controls, and the fact that government data and systems are desirable targets for nation-state actors, black hats and cybercriminals.

To succeed in that environment, agencies need to think more holistically about how they detect, anticipate and respond to threats. Many agencies are reassessing how they secure critical assets. They are finding that more agile IT platforms can help them readily adapt to new kinds of threats, even while they assess the nature of those threats. They do this by focusing on what they're trying to defend — critical assets such as data and applications.

To understand the challenge of a given threat or adversary, agencies need to understand the context in which they will be interacting with it. The security team must partner with the infrastructure, applications, networking, end-user and storage teams to gain those insights. Together, those experts can focus on the interactions between systems and define a view of "normal" activity. Then the agency's IT ecosystem can react to any deviation from that standard.

## Capitalizing on existing security solutions

Fortunately, agencies don't need to start from scratch. Many are adopting an end-to-end security model that leverages security capabilities intrinsic to the systems and solutions that are already in place to create a vision for secure agency operations. This approach allows them to connect context across environments to build a layer of control and intelligence to respond to and remediate threats.

Zero trust is a key component of end-to-end security. Zero trust requires organizations to embrace the notion that their systems are already in a state of compromise. They need resilient programs, capabilities, applications and data that can function even in those circumstances.

Zero trust is a mindset within an agency rather than something it buys or builds. It is an operating model that requires agencies to understand context and what normal activities are so they can react holistically. Similarly, modernization isn't just about upgrading servers, storage networks or applications. It's about adopting modern ways of approaching IT. As agencies prescribe the practices and products for cloud, modern apps and the frameworks that developers use to build those applications, they should also be integrating security into

Shutterstock/FCW Staff

> **Modernization isn't just about upgrading servers, storage networks or applications.** It's about adopting modern ways of approaching IT.

all components of IT, including platforms, application development and operations.

### Extending zero trust out to the edge

With more employees working remotely, agencies are starting to think about the processing that increasingly happens at the edge of their networks. They must craft a security approach that encompasses endpoints the government might not control – for example, remote employees' personal devices. However, in addition to protecting assets, agencies need to ensure that security measures don't interfere with employees' ability to be productive and engaged in their work.

In the past, agencies would buy thousands of laptops, configure and secure them, and distribute them to employees. Now agencies need a flexible and agile model to adapt to endpoints of all kinds, including not only traditional endpoints such as mobile phones, laptops and desktop PCs, but also sensors, 5G and other types of edge workloads.

A zero trust foundation for security has the agility to secure all those different environments, and it doesn't depend on deploying a particular technology. Instead, it depends on adopting a holistic strategy that gives agencies the flexibility to respond to current and future threats. ■

**Henry Fleischmann** is director of Government, Education and Healthcare Solutions Architecture at VMware.