Why **success in zero trust** requires a team effort

The expertise of trusted partners can speed agencies' journey to proactive security controls and resilient systems

Meghan Good
Leidos

Government networks are under constant attack by a variety of adversaries. Furthermore, as agencies continue to modernize their IT environments, they are adding complexity in terms of cloud-based and on-premises systems and an ever-changing set of endpoint devices.

Advanced actors often gain access to government systems by compromising the credentials of valid users. Adversaries can spend more than 200 days inside a network before the breach is even identified. That is a significant amount of time to steal information or harm a system in other ways.

Rather than allow users to authenticate once and then have unfettered access to a government network, agencies should move toward continually validating activities in their IT environments on an ongoing basis. Zero trust is the approach that will help agencies do that.

The evolution of least-privilege access

Although it has recently been getting a lot of attention, zero trust is actually the evolution of a security philosophy that has been building for years. It starts by giving users the least amount of privileges to perform their jobs and operating under the assumption that systems have already been breached.

Zero trust focuses on the connection between users and the data, applications, networks and systems they want to access. In zero trust architectures, new administrative tools continually evaluate whether allowing an individual user to have a certain level of access privileges is the right thing to do. The approach gives agencies much more flexibility as they modernize because they can make decisions at a granular level that enable them to secure data and entire IT ecosystems.

President Joe Biden's executive order on cybersecurity mandates the use of zero trust, which puts a lot of weight behind a consistent and coordinated adoption of the approach. However, moving to zero trust can be daunting, which is why we advise agencies to begin by assessing the products, capabilities and policies they've already deployed. In addition, agencies must understand their individual risk appetites and the level of security that is appropriate for their particular missions and critical functions.

Once agencies have that information, they can build a roadmap for achieving a customized zero trust implementation. Leidos has developed Zero Trust Readiness Level (ZTRL™) assessments to aid government agencies in that process.

A big-picture and a granular view of security ecosystems

There are an overwhelming number of options to choose from when building a zero trust architecture. To

Conny Schneider

> **Zero trust focuses on** the connection between users and the data, applications, networks and systems they want to access."

help agencies speed the development of their roadmaps, we bring together the leading products and capabilities developed by members of our Leidos Alliance Partner Network and create different configurations so we can test the technologies in concert with one another.

Leidos assesses those configurations and alternatives to see which works well in a particular situation or when another solution might suit an agency better. If agencies have already chosen a set of products, we can help them select the right complementary components to leverage the investments they've already made.

For example, Zscaler's capabilities provide granular control and visibility when establishing VPN tunnels. As a result, agencies can easily segment networks and make better policy decisions about allowing particular users to access particular resources. That granular level of control is integral to zero trust.

Our experience as a systems integrator and our close partnerships with leading-edge technology companies give us both a big-picture and a granular view of security ecosystems. By applying our knowledge and insights, we can tailor zero trust architectures to individual agencies' needs. ■

Meghan Good is vice president and director of the Cyber Accelerator at Leidos.