How the cloud is **redefining security**

TIC 3.0 is allowing agencies to extend security to users beyond the network's perimeter

Stephen Kovac
Vice President of Global Government, Zscaler

THE TRUSTED INTERNET CONNECTIONS initiative was created in 2007 after the Office of Management and Budget conducted a study that found thousands of unprotected internet connections at agencies. Back then, we were using the internet mainly for email and web browsing, so when the government mandated that all internet traffic must go through a trusted connection, it made sense.

But over the years, agencies have moved workloads to the cloud, and now employees' activities rarely travel through an agency's data center. As a result, TIC became a barrier to cloud adoption.

The TIC 3.0 draft guidance, however, is a crucial step toward removing those obstacles.

Policy enforcement at the edge

Under TIC 3.0, industry partners can perform security services for agencies as long as they comply with government standards. Furthermore, the telework guidance issued during the COVID-19 crisis allowed agencies to provide remote access for employees via a zero trust architecture that meets the requirements of TIC 3.0.

The latest advancement in cloud technology is Gartner's secure access service edge (SASE) model, which decentralizes security services for greater performance, reliability and scalability. The FedRAMP-authorized Zscaler Cloud Security Platform is a SASE service that's delivered across data centers throughout the U.S. and globally on U.S. sovereign ground, ensuring secure, fast and local connections for users everywhere. Zscaler also provides zero trust access to private applications in the data center or cloud without ever putting user traffic on the agency network.

Embracing the opportunity to change

At Zscaler, we have cloud nodes all over the globe, which allows users to have the same experience and protections on any device, anywhere. If a user logs into our cloud from anywhere in the world, we can immediately log the user and detect for suspicious activity. And if we identify a vulnerability, we block, we notify, and then we update all our global cloud nodes within seconds. This is called the cloud effect – the ability to protect all our users globally within seconds of detecting a vulnerability.

TIC 3.0 is helping agencies redefine cloud security now that there is no longer a network perimeter, and many agencies have embraced the opportunity to change. However, it's still a transformation that will likely take a year or longer as agencies start small and then tackle more complex activities. Ultimately, those activities will be more secure in the cloud, and the user experience will be superior. TIC 3.0 is the catalyst for change, and the time is now. ■

Stephen Kovac is vice president of global government and head of corporate compliance at Zscaler.