Rethinking security **in the cloud**

Now that the network perimeter has dissolved, agencies must focus on protecting the user

Stephen Kovac
Vice President of Global Government and Compliance, Zscaler

AS CLOUD COMPUTING has evolved, so have efforts to make the technology more secure and efficient. When users and applications first moved beyond the network's boundaries, many organizations continued to route security through their data centers. Though users were working remotely in new and profound ways, cybersecurity remained centralized, becoming a choke point for traffic and the source of slow performance and user frustration.

The subsequent shift to virtual environments simply added another layer of management, with virtual machines that didn't always run as well as the bare-metal systems they were replacing.

zscaler™
Looking to enable digital government with zero trust networking?
Watch our video
zscaler.com/ztna

Now with many, if not most, applications residing in public and private clouds and users increasingly mobile, agencies need to focus on securing every connection between users and their applications, no matter where or how they connect.

Secure, seamless connections

A paradigm shift is happening today that involves providing users with a consistent experience, the same performance and identical security regardless of where they are. Several tools and techniques hold great promise for helping agencies do just that.

For example, zero-trust networking connects a trusted user to a trusted application using new techniques like microsegmentation and encrypted microtunnels. It eliminates the need for virtual private networks because the user is no longer being routed back onto the agency's network. Secure cloud gateways and proxies can also give users the experience of being directly connected to their applications without agencies having to invest in expensive networks or security devices.

In addition, the cloud streamlines agencies' ability to take advantage of threat intelligence. In the past, organizations would collect and analyze threat feeds then write a patch package that would have to be manually installed on all devices. But now, if an agency's systems are running on a secure, multi-tenant cloud platform, the provider can identify a problem and push out a patch to all its customers across the globe instantly.

Removing barriers to innovation

Fortunately, the government recognizes that the security landscape is changing quickly, and leaders are taking steps to change with it. Agencies are turning to industry for insight into best practices and learning to understand their risk factors and risk tolerance so they can make better decisions about security investments.

In more good news, directives such as the Federal Data Strategy, the "cloud smart" initiative and Trusted Internet Connections 3.0 are removing barriers that have made it difficult for agencies to try new technologies. As long as an innovative product or service meets the intent of security policies, the government should have the opportunity to pursue it. ■

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