The evolution of **trusted connections**

Zero trust and adaptive security workflows support more robust cloud environments

Habib Hourani
Solutions Engineer, Okta

THE GOVERNMENT IS STARTING TO GO beyond adopting cloud technologies to building policy around them. For example, in response to the sudden explosion in telework during the coronavirus pandemic, the Cybersecurity and Infrastructure Security Agency issued the TIC 3.0 Interim Telework Guidance, which embraces key elements of the latest iteration of the Trusted Internet Connections initiative.

TIC 2.0 basically advocated a straight line from a user to a trusted connection, but TIC 3.0 is a more flexible framework that recognizes the increasingly fluid nature of network boundaries. Rather than running everything through a TIC first, agencies can use policy enforcement points — essentially gatekeepers to digital resources — that are closer to the application or the user. The approach accommodates risk-based tolerances and the ability to add entirely new network zones.

Now agencies can shift workloads closer to end users and take advantage of best-in-breed products while protecting data and enforcing strong authentication.

An omnichannel experience for employees

Under TIC 3.0, agencies can still use network proxies, cloud access security brokers, and security information and event management (SIEM) tools to build a strong security framework, but they don't have to run everything through a TIC. And users don't have to struggle with increased latency and network complexity. Instead, the end-user experience is streamlined because cloud-native tools are handling processes and workloads.

Agencies end up with a clean omnichannel experience for employees because their location no longer matters. Whether they are working on an iPad at home or a desktop computer at a government office, the security level and user experience are the same.

Adaptive, contextual security responses

As security tools and techniques evolve to help agencies better protect their cloud environments, we're seeing a move toward more adaptive responses, and we're starting to see better interoperability between applications.

At Okta, we are building strategic partnerships to help drive that adaptive and contextual response, which connects to the security trend toward zero trust. For example, Okta can track failed login attempts and push that information to a SIEM tool, which can alert the IT service management tool to create a ticket for the security team that points back to the log for root cause analysis.

That automated process can also protect the user's account by putting it in a state where the threat actor can't do any harm and then restore the account to full access once the issue is resolved.

Such a dynamic framework allows agencies to deliver a secure, seamless user experience while keeping up with the latest technology developments. ■

Habib Hourani is a solutions engineer at Okta.