# Security Happens at the Edge

## A zero trust approach to security helps agencies manage end points and mitigate risk at the perimeter

**AS THE PERIMETER** becomes more difficult to secure, especially as organizations continue to manage a growing remote workforce, it's more important than ever to apply security policy and controls at the device level.

Traditionally, users, devices and data have been secured within a corporate boundary or an enterprise network, however, corporate networks today have no defined perimeter.

> "We have end point devices scattered throughout all these types of enterprise environments, and we have to secure them."
>
> MATTHEW MARSDEN
> Vice President of Public Sector Technical Account Management, Tanium

The pandemic forced organizations to allow most if not all of their workforce to work from home, and securing devices was often an afterthought to maintaining simple connectivity, said Matthew Marsden, vice president of Public Sector Technical Account Management at Tanium.

"Zero trust helps us to simplify all this by doing real-time authorization and access decisions per user, per device regardless of where you are located both physically and logically within the network," he said.

Zero trust treats every actor, identity, device, and connection on the network as a threat and gives no implicit trust. It is designed to mitigate risk, reduce threats and ultimately increase an organization's security posture.

Agencies today are struggling with how to access applications in the cloud from unmanaged and unsecured devices, manage overloaded virtual private networks, and gain visibility into their incoming network connections, Marsden said.

"We have end point devices scattered throughout all these types of enterprise environments and we have to secure them," he said. "We need to maintain total and complete visibility and control of those devices."

In addition, existing VPNs have been strained by the current demand of a distributed workforce, and in some cases, users have bypassed security protocols "just in the name of getting things done," Marsden said.

Organizations also lack real-time visibility into network connections coming into their enterprise infrastructure to address security issues as they arise.

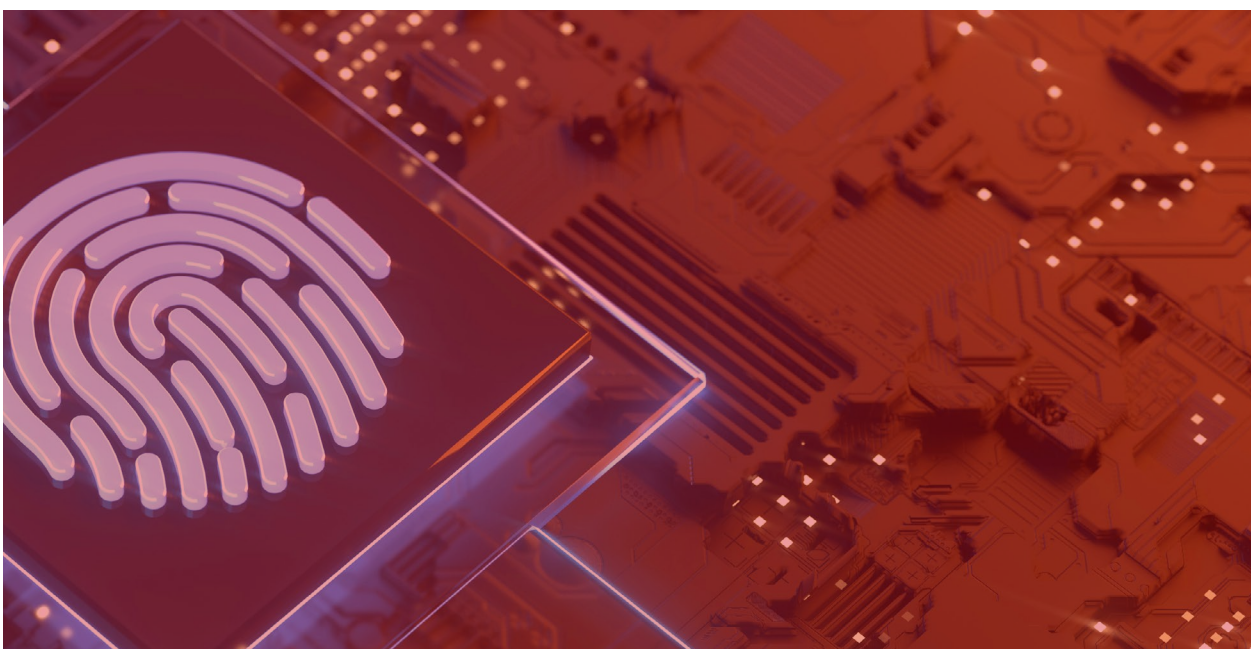
"Security happens at the edge," Marsden said. Everything that touches the network has to be identified and managed so that agencies understand what the threat landscape looks like.

"It's all about the devices that are connected to the network," he said. "What is the attack surface for your environment so you can make informed decisions about how to protect it?"

Security controls must be applied to users and devices, and organizations must understand where sensitive data lives and who has access to it. "Data lives at the point of production and the points of production are generally, if not the workflow servers, the actual end point devices themselves," he said.

"What is the attack surface for your environment so you can make informed decisions about how to protect it?"

MATTHEW MARSDEN
Vice President of Public Sector Technical Account Management, Tanium



A device needs to have its own identity, so that an agency can quickly assess its risk and determine whether it is a high-value asset.

The path to zero trust begins by identifying the actors, assets, and applications that run on the network so agencies can make informed decisions about security and how to implement zero trust. "Security with gaps in visibility is not really security," Marsden said.

Once agencies have identified the actors on the network, they should then choose the communication path for those users to access corporate resources. Then it's time to design, implement and test the technologies and providers they chose.

Zero trust is a journey that takes time, Marsden said. "The secret is to start small and find something you already have that can be tweaked or tuned to apply zero trust practices."

Most importantly, because zero trust will never be done, continuous authorization and assessment must continue, he said.

"We need to continuously monitor the environment and assess our device posture, our security practices so that we can make changes and be proactive in our response, not reactive." ■


Just_Super / iStock