Adopting a new **defensive strategy**

The playing field is no longer clearly defined, which means agencies need to revise their playbook

Chris Usserman
Principal Security Architect, Infoblox

WE ARE IN THE MIDST OF A PROFOUND CHANGE in the security landscape. Threat actors are shifting their tactics to take advantage of your now decentralized workforce, which means the nature of your enterprise defines your threat landscape.

To use a sports analogy, two teams face off against each other on a football field. The offensive line's actions are executed to make it to the defender's end zone. The line between the two is clearly defined, and each opposing team adjusts its actions to take advantage of the other's potential gaps. Two factors come into play: visibility into how the opposing team is lined up and what plays it usually executes in that situation. In cyber, this requires visibility into where your teammates are, what your gaps are, where the opposing force is and what plays it may execute to take advantage of those gaps.

Before the pandemic, agencies could easily define the playing field. But now threat actors operate almost anywhere the defender's team is — on or off the field. Employees are at home or moving between home and the office on a regular basis. Collectively, they're transporting hundreds or thousands of devices carrying intellectual property and possible malware in and out of the enterprise.

The 'enterprise@home'

Even now, agencies may lack visibility and control to protect these disparate devices operating on vulnerable home networks. While a VPN is a necessary technology, it does not (nor was ever intended to) protect an endpoint or the enterprise from malware exploitation.

Security teams must arm employees with security tools to best protect their remote devices while maintaining visibility and responding to threats in real time.

Just as defensive lines adjust to active plays, security teams need to be able to recognize the play, know where their team is, what their team is doing and then know how to respond to the threat — all in real time.

Everywhere is 'in bounds'

There's no going back to the way things were in the near future. Out of necessity, agencies redefined how they operate. They have invested heavily in their defensive line, but the rules of the game have changed and now even living rooms are "in bounds."

The enterprise infrastructure model for providing frontline defense is no longer enough. These endpoints, wherever they are, are now potential victims to game consoles, televisions and IoT devices in addition to traditional attack methods. To be successful, security teams must know the adversary and its methodologies, and they must know their enterprise and enact real-time detection/containment of threats. ■

Chris Usserman is principal security architect at Infoblox.