UNDERSTANDING AND CONTROLLING THE CONNECTED DEVICE LANDSCAPE

Shawn Taylor, senior systems engineer with Forescout, explains how continuous device visibility and automated controls enable organizations to take fuller advantage of emerging technologies.

How are network attacks against government organizations changing, and what are the implications for cybersecurity?

One of the biggest changes is the regularity of attacks. Ransomware and malware are for hire today, so adversaries don't need to be particularly skilled to execute an attack. In addition, state and local government entities are typically understaffed, underfunded and consequently underprepared from a tools and automation perspective. That puts a big bullseye on their organizations.

What unique challenges do smart cities, smart transportation and other enterprise-wide initiatives pose?

IoT devices, operational technology devices and other non-traditional computing devices are not inherently designed with security in mind, so security is often an afterthought in these initiatives. Organizations bolt these devices onto infrastructure that's providing PII, HIPAA, IRS 1075 and many other sensitive data feeds that traverse the enterprise. Organizations must ensure they're continuously aware of all these devices throughout their life cycle on the network, that they protect them and more importantly, that they protect the institutional data.

With high-value and PII data spread throughout the enterprise, how can organizations improve their security posture without impeding services or the free flow of information?

Two key aspects are dynamic segmentation and role-based access control that ties into the underlying infrastructure of hardware and software asset management. When I log in to a resource, you need to understand who I am, my user role and what data I'm authorized to see. At the same time, you must understand the device I'm using to log into the network and its context. For example, does the device have inherent authorization to see PII data? If not, there should be an automated segmentation process to deny that access, even if my credentials or group memberships would otherwise allow me to access PII data. So it's understanding the device itself as well as the user, and then using that information to automatically execute a permit/deny access decision.

What is device visibility and control, and why is it important to government security efforts?

It's a concept that says you must be able to understand the entire connected device landscape at any given point in time — what types of devices are on my network; who is logged in to them; are they a risk and so on. Then, along with that visibility you need an automated mechanism to execute control actions such as restricting, allowing or segmenting devices throughout the network after they connect.

What advice do you have for organizations as they consider emerging technologies such as AI and machine learning to improve their cybersecurity stance?

First, it's important to have continuous situational awareness of the device landscape and add that information into the overall picture. You need to understand the devices that are sending data to AI and machine learning technologies for analysis. Second, when your AI or machine learning detects an event, you need to know what action to take and how you can do that in an automated, orchestrated fashion without human intervention.

<) FORESCOUT®

The Leader in Device Visibility and Control
for State and Local Goverments

100% Device Visibility and Control

Across Your Extended Enterprise

<) Gain Continuous Security Awareness

<) Mitigate Threats with Policy-based Controls

> “With the Forescout solution, we expect to save millions from exponentially faster audits that produce fewer findings and require less remediation effort.”

– Phil Bates, Chief Information Security Officer, State of Utah

www.Forescout.com