Don't miss the endpoint

When it comes to federal network security, agencies must keep an eye on the proliferation of endpoints

Katherine Gronberg
Vice President of Government Affairs, Forescout Technologies Inc.

THE ADAGE, "KNOWING you have a problem is the first step toward recovery," is applicable to the challenge presented by a diverse and growing array of endpoints connecting to government information systems. What are these endpoints? Why are agencies connecting them to their IT networks? And perhaps most important: What cybersecurity threats do these endpoints pose?

An endpoint is any physical or virtual device that transmits data that connects to an IT network. An endpoint can be a traditional IT device — such as a computer, server, smartphone or tablet — or a peripheral device, such as a printer. Increasingly, however, endpoints consist of consumer internet of things (IoT) devices or networked mission-supporting devices such as building automation systems, industrial control systems, engines and even weapon systems.

Such nontraditional devices process data, can be easily deployed and typically have limited functionality. In 2018, U.S. Cyber Command defined six categories of endpoints: mobile devices; workstations and servers; networked user support devices; network infrastructure; IoT; and platform information technology (PIT). Much like in the consumer sector, government agencies are connecting these devices because they increase efficiency and safety and enhance mission effectiveness and delivery of services.

davooda/Shutterstock/FCW Staff

Detecting nontraditional network devices

Most organizations struggle to detect nontraditional endpoints. IoT devices, PIT systems and many user support devices cannot run management software, as computers do, that allows them to be detected on the network and assessed for their security. Because IoT and PIT endpoints cannot support the installation of software (in industry speak, an "agent") on them, most security products such as antivirus or patching tools miss them completely. This is analogous to a class chaperone who stands on the bus and asks: "Is everyone here?" To secure nontraditional endpoints, another approach is required — one that is not dependent on software being deployed on an endpoint.

This was the approach taken by the Department of Homeland Security when it created the Continuous Diagnostics and Mitigation program. CDM's purpose is to enable agencies to identify cybersecurity risks on an ongoing basis, prioritize these risks and mitigate the most significant problems first. The Defense Department is currently implementing a similar program called Comply to Connect (C2C). Both programs depend on agentless asset detection technology to achieve full visibility of the enterprise.

When the federal civilian agencies deployed the CDM toolset using the Forescout platform as the hardware detection tool, they discovered an average of 75 percent more devices on their networks than they previously knew existed, according to CDM Program Manager Kevin Cox. In Forescout's experience, this visibility

> To secure nontraditional endpoints, another approach is required — **one that is not dependent on software** being deployed on an endpoint.

gap — the devices agencies can't detect — is predominantly attributable to nontraditional endpoints, which are simply proliferating faster in agencies' environments.

Closing the visibility gap

Being blind to so many endpoints in your network environment creates serious risk. You cannot secure the endpoints you cannot detect. Further, because these devices frequently support physical missions, failure to secure them can have operational consequences, including disruption of the mission. All organizations must have the right tools to expose and close the visibility gap created by unknown, nontraditional endpoints.

In securing federal systems, we must transition from old ways of thinking. We must resist the urge to be that wishful class-trip chaperone. With programs like CDM and C2C, the U.S. government has made a strong statement that the future of federal network security hinges on continuous and automated detection and assessment of all endpoints. To do otherwise would be missing the point. ■

Katherine Gronberg is vice president of government affairs at Forescout Technologies Inc.