A GOVERNMENT TECHNOLOGY Q&A | FORTINET

MANAGING CYBER RISK

Why State and Local Governments Must Work Together for Cyber Defense

*Federated security brings multiple government agencies together in a common cyber defense effort. **Jim Richberg**, public sector field CISO and vice president of information security with Fortinet, explains why more agencies are adopting a federated security posture. Before joining Fortinet, a Silicon Valley security technology firm, Richberg spent more than three decades in cybersecurity and intelligence roles for the U.S. government.*

Why is today's threat landscape making federated security more important?

State and local governments worry about being targeted or being caught in the crossfire of malicious cyber activity associated with the Russia-Ukraine War. Also, because ransomware has been so lucrative compared to the boom or bust nature of other criminal schemes, we're seeing the rise of advanced persistent criminal activity. Criminal groups that might have disbanded as their activities became less profitable are staying together. And they have the funds to invest in developing new online exploits that are more stealthy and sophisticated. In response to this dual threat from nation-states and criminal groups, we're seeing U.S. states and larger cities and counties looking to band together for collective security.

What does a federated security operations framework look like for state or local government IT organizations?

It starts with building shared situational awareness or a common operating picture of threats and figuring out what to do about them. Building a single integrated view of network health and threats across organizations is difficult. So, many organizations opt to pool or share their separate views, relying on analysts to integrate them manually. Even if a collation can use automation to ease the burden, building this situational awareness takes most of every hour of a security operations center's time and attention. The remaining minutes that can be spent on actually doing something about threats should be as efficient and automated as possible.

There are three approaches to this. First, you can build tools from scratch, working from common data formats and standards. This is expensive and doesn't scale well. Second, you can leverage tools for security information and event management (SIEM) or security orchestration, automation and response (SOAR). These products are good at dealing with varied inputs, and with generating outputs that can support multiple controls and solutions from multiple companies. This has the advantage of putting much of the work onto manufacturers and vendors rather than the government customer organizations.

The third approach is to consolidate around a small number of mesh architectures or ecosystems of interoperable capability.

Why is a mesh architecture essential to federated security success?

A mesh architecture unloads even more of the work onto the vendors, which enables an even greater degree of burden-sharing with the vendor community than under a product-focused approach. Today, there are only a handful of mesh architectures, which gives government organizations a relatively straightforward set of choices. The more work government can offload to a mesh architecture, the less work the federated group will have to orchestrate or do itself.

FORTINET

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network — today and into the future. **www.fortinet.com**