Every Network Is Now an OT Network. Can Your Security Keep Up?



Every network today is now an OT network. Or it will be soon. Of course, part of this transformation is due to the ongoing convergence of OT and IT networks. As many of us have experienced, previously isolated OT networks, like manufacturing, processing, distribution, and inventory management, have now been woven into our larger IT networks. This integration enables better controls, more responsiveness, broad interconnectivity for better communication, and seamless resource expansion, distribution, and redistribution. It also introduces new security risks.

But that’s just half the story. Modern enterprise IT networks must now include smart, energy-efficient physical resources. Fortinet’s new carbon-neutral campus, for example, includes

integrated OT smart building elements like automated lighting, windows, shades, HVAC systems, and a wide variety of headless IoT devices—and we have had to integrate all of them into our IT network fully. As a result, our network, like many of yours, now faces many of the same challenges that industrial environments have experienced for years. These issues are compounded further in extended environments like smart cities or organizations with multiple smart campus environments.

And as more and more of your business operations are digitized, securing such complex, hybrid network environments will only become increasingly challenging. Add things like mobile workers, cloud-based services and resources, edge computing, and essential business applications like streaming video, and the legacy security solutions and strategies you have in place will inevitably begin to create bottlenecks and gaps in your protection—if they haven't already.

If you're like most companies, you have likely tried to address this expanding challenge piecemeal by adding even more point security solutions to your already overflowing security portfolio. But adding complexity will not only further overwhelm your IT staff but also decrease the security of your digital and connected physical environments. Numerous management consoles, isolated security tools, and incompatible or inconsistent policies reduce visibility and control, making it difficult to accurately detect and respond to threats in a comprehensive manner and impossible to implement the kind of automation needed to stay ahead of today's rapid cyberattacks.

Securing today's expanding hybrid networks requires a holistic approach, beginning with rethinking how and where security is implemented. Here are five things your organization needs to consider before you spend another dollar on expanding your legacy security toolset.

1. **Start with a universal, integrated security platform.** Most organizations have dozens of point security

solutions deployed across their distributed network that struggle to share real-time threat information and coordinate an effective response. Visibility and control are essential to effective security, but as networks expand, they struggle to keep up. Building your security architecture around platforms that can operate in any environment and form factor is a critical first step in ensuring that you can identify and address security weaknesses, detect brewing and active events, and launch a coordinated response across every segment of your network. Hybrid mesh firewalls are an excellent example of this critical cross-network interoperability.

- **Use security tools designed to operate as a single system.** Your security platform must include a portfolio of security technologies designed to serve as a single, integrated solution. A centralized, single-pane-of-glass management system, consistent policy deployment and enforcement, the sharing of real-time threat intelligence, and the ability to operate natively in any cloud environment should be table stakes for designing and implementing a modern network security system. This includes solutions designed specifically for OT environments, including ruggedized systems, OT-specific modules, and deep interoperability with OT systems.

- **Converge your network and security.** Many legacy systems treat networking and security as siloed functions, but it’s critical to build infrastructure and leverage solutions that bring security and networking together, meaning they have critical security functionality woven directly into their operations or, better yet, have been built on a security platform. Networking equipment that can implement security elements natively and in concert with the larger security posture ensures that IoT and OT devices connect to the network with the appropriate security context. For example, Secure SD-WAN converges

security and networking functions to ensure optimal user experience without sacrificing security. Additionally, organizations can route traffic from IoT and OT devices for security checks in the cloud via SSE or SASE points of presence. This seamless convergence of networking and security means all devices, even those without an agent, connect securely.

- **Implement zero trust everywhere.** One of the biggest risks of legacy network environments is that they were often built around an implicit trust model. Automatically trusting traffic that has passed through a demarcation point is a recipe for disaster, especially with highly mobile users and devices and widely deployed applications and other resources. Zero trust takes the opposite approach where every user, device, and application must be authenticated per session, are only granted access to the resources needed to do their job, and are monitored end to end to detect any deviations from their sanctioned behavior. Going a step further, universal zero trust network access, which applies the same principles to remote and on-premises users and devices, is the best way to ensure the same access controls are applied to any connection, regardless of location.

- **Use AI. But you need to understand it before you buy it.** AI is the new buzzword in security and networking. It can potentially detect complex threats before they launch, fix misconfigurations, take on manual tasks to free up IT staff to work on higher-order issues, reduce the time to detect and respond to breaches, and much more. But there is remarkably little consistency in what vendors mean when they slap an AI label on their product. Beyond how the AI algorithm was trained and whether it is an assisted or autonomous system, there are some fundamental issues you need to understand. For

example, which of your security and networking tools does it work with? AI operating across multiple systems is often far better than one that only works with a siloed solution. What threat feeds does it use? Remember that the adage, “garbage in, garbage out,” also applies to AI. And critically, does it recognize and work with OT systems and environments? The best advice here is, “Do your homework.”

Networks are undergoing the most rapid transformation in their history. And for a long time, we’ve been advising IT leaders that their security must keep up. And now, as nearly every IT network becomes an IT-OT network, the stakes are even higher. This means that if you’ve been putting off redesigning your security systems, now is the time to make it a priority.

Every Network Is Now an OT Network. Can Your Security Keep Up?