Expanded Attack Surface Brings Security Challenges

While digitization and the cloud have brought great convenience to your users and employees, the attack surface is expanding, and new threats are emerging. According to the 2020 CISO Benchmark Study, 44 percent of organizations experience 10,000 daily security alerts but only respond to half of them. Additionally, 82 percent of CISO's said managing alerts from multiple vendor products was challenging[1]. In the past, your organization may have addressed those threats with individual, one-point solutions. However, as network threats become more sophisticated, securing your digital infrastructure will require more time and money. For IT, this approach to network security is causing more confusion and resources are being stretched too far to keep up.

Adding solutions and updating your security infrastructure may position your organization to stay ahead of the increasingly volatile threat landscape for a time. But a multi-vendor patchwork of disparate security solutions can be chaotic. Often, these components don't communicate well with each other. And trying to manage this hodgepodge of solutions brings unnecessary complexity. Your organization can try to organize this type of security infrastructure but incompatible interfaces, steep learning curves, and siloed communication limit operability. Security solutions should work as a team, learning from each other, listening and responding as a coordinated unit. What you really need is an effective way to gain enhanced visibility, access to key metrics and actionable insights, and a clear understanding of your network vulnerabilities. Success in this security environment requires:

- **Reducing complexity** by integrating security products together with out-of-the-box interoperability.
- **Automating security workflows** to increase the efficiency and precision of existing resources and to stay ahead of an ever-changing threat landscape.
- **Integrating third-party products** in an open platform approach and unifying them in a virtuous cycle of increased value from a central location.

Reduce Complexity and Increase Security Automation

Cisco SecureX™ connects the Cisco® integrated security portfolio and your entire security infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoint, cloud, and applications. By connecting technology in an integrated platform, Cisco SecureX delivers measurable insights, desirable outcomes, and cross-team collaboration while reducing complexity and overhead.

Organizations can reduce complexity and cost by connecting disjointed technology to an integrated platform built for the security needs of today and tomorrow. Cisco SecureX also turns security from a blocker to an enabler, expanding the benefits of your security investments. This platform experience is built into the existing Cisco Security portfolio and it works with your entire security infrastructure to speed time to value and reduce cost.

---

[1] 2020 CISO Benchmark Study