At the end of the day, enterprise security systems aim to achieve an optimal security posture. Unfortunately, this threat-response dynamic creates an IT security architecture that itself has become a risk factor. Overloaded IT teams juggle dozens of security tools while patching products and apps against the latest threats. With so many moving parts, it's easy to make mistakes, forget critical steps, or misconfigure tools.

Furthermore, enterprises lose visibility as valuable security data gets spread across the many security tools. It's not that they don't have the information about a lingering threat: they can't act on that information because the signals are hidden across so many tools. Gathering this information and maintaining the discrete tools themselves requires such specialized knowledge and skills that the industry has been left with a well-known shortage of security talent. Only the best-resourced Fortune 500 companies with massive IT teams can (partially) manage this IT security chaos.

This chaos impacts business operations beyond the realm of cybersecurity. Expanding into new regions requires more notice so IT teams can implement their myriad of tools. Unforeseen events — like the COVID-19 pandemic — require tremendous resources and investment to resolve. Even acquisitions are held up by multi-month endeavors to integrate IT infrastructure.

Some of the industry's larger cybersecurity companies attempt to mask the chaos with clever packaging, grouping huge discrete product portfolios from hundreds of acquisitions under a common brand. Such an approach may give procurement departments peace of mind with a single bill of materials, but not the decision makers and operational teams responsible for a company's security posture.

This isn't working. To support the digital transformation of business and the threat landscape, IT security must also transform.

Rather than focusing just on the security features (the "what"), IT security must also consider the operations (the "how"). Enterprises need platforms that deliver the required functional value, and also solve the operational challenges. Yes, enterprises require threat prevention, data protection, and threat management (the "what"), but these cannot compromise on operational experience (the "how").

And what does that operational experience look like? As the operational problems stemmed from too many discrete products, the solution must look at their convergence into a common, global platform that works consistently at scale for all users, devices, and applications anywhere in the world. As the many discrete products left IT unable to cope with unforeseen events, the global platform should not require extensive resources to sustain optimal performance and security posture.

We need an autonomous platform, one that can sustain its own evolution, resiliency, optimal performance, scalability, global reach, and security posture. Ultimately, the platform should let any enterprise achieve an optimal security posture regardless of changing business needs or threat landscape without depending on massive grunt work, hard-to-find skills, and extensive resource investment.

I have been working on such a platform since 2015, four years before Gartner coined the term Secure Access Service Edge (SASE), a cloud architecture model that does exactly what I've described: the convergence of multiple point networking and security capabilities into a single cloud platform. The SASE model defined a way for enterprises to deploy data protection and threat detection capabilities worldwide for all users, sites, and cloud resources almost effortlessly.

In so doing, SASE lets IT focus on its true value — addressing the needs of the business. No vendor or technology can meet and anticipate an enterprise's unique requirements as well as the IT organization. SASE frees IT from much of the "grunt work" to provide true value to the enterprise. With robust AI models, SASE can maintain an optimal security posture on its own. Through convergence, automation, and autonomy, SASE reduces the chance that somebody will make a mistake or forget something, leaving a gap that attackers can come through.

While the "what" of SASE might have started with data protection and threat detection, it will expand in scope into other cybersecurity areas, but never by compromising the "how." Today, SASE has gotten smarter by expanding into threat detection and incident response, on the one hand, and out to the endpoint with end-point protection. But it must only move into these new "what's" without compromising on "the how" by converging them into a common platform.

By rethinking how capabilities are delivered, and creating a new IT security framework, we can extend what capabilities are available without losing control of our security defenses. SASE can become the transformational force IT security needs: the antidote to the chaos I helped create.

Shlomo Kramer, co-founder and CEO, Cato Networks

Shlomo Kramer