paloalto NETWORKS | STRATA

Embrace innovation while securely growing your business

Limited resources and rising threats make innovation challenging

If you think growth and innovation are essential to your organization's success, you're not alone. Seventy-nine percent of organizations ranked innovation among their top three priorities, up from 75 percent in 2022.[1] If security leaders want a seat at the strategic table, they must enable innovation.

But you need to pursue innovation securely and, unfortunately, existing infrastructure and internal resources just can't keep up. In fact, 70 percent of cybersecurity workers feel their organization does not have enough staff.[2]

Meanwhile, future threats are shifting and unknown, which only makes things more difficult.

Simply adding more security tools isn't the answer

Many organizations are investing in numerous security tools to secure their entire network—possibly spanning headquarters, branch offices, mobile workers, data centers, and cloud. For example, they might add a hardware firewall to protect offices and data centers, a SASE solution to protect branch offices and the hybrid workforce, and a software firewall to secure applications in the cloud.

In addition, to block the latest threats, organizations are purchasing specialized solutions. There are different products for intrusion prevention, device security, malware protection, and data loss prevention. And as each new threat emerges, more specialized tools are acquired.

This strategy was viable when the organization was contained—most users worked from offices, most applications were in the data center, and most devices were corporate-managed. But today users work from anywhere, applications are moving to the cloud, and most connected devices are unmanaged and invisible to security teams.

The number of standalone tools and management consoles makes it impossible for your team to consistently secure the entire organization. And trying to create a cohesive view of your network can become a nightmare.

Added complexity can expose you to several risks

Unfortunately, sticking to the current approach can pose significant risks for organizations like yours.

Those include:

Organizational complexity results in new form factors and use cases, creating security gaps and errors. As you attempt to secure each one, you could fall prey to increasingly adept attackers.

Attackers use AI and other sophisticated techniques to create new ways to threaten your organization. The resulting breaches pose a direct financial and reputational risk to you.

You and your staff are working longer and are constantly on edge. That leads to workplace burnout.

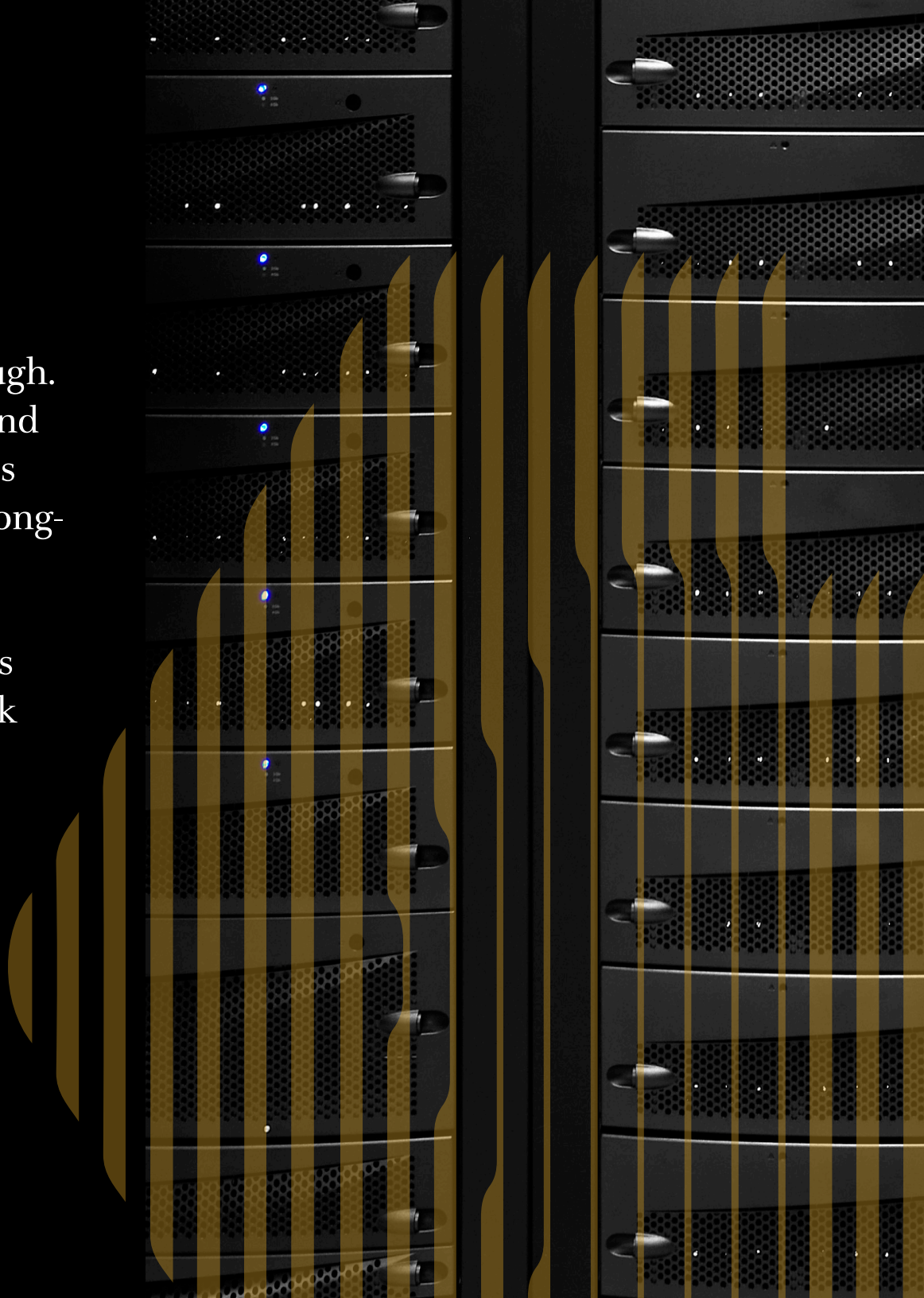
Too often you're forced to accept risk to support innovation—hoping that everything works out.

A new approach for growth and innovation

Providing cybersecurity is no longer enough. You must enable your business to grow and innovate. Responding with point products won't get you there. Instead, you need a long-term strategic security architecture.

You need to securely enable your business for growth and innovation with a network security platform built for Zero Trust, powered by AI.

But how?



Trust Palo Alto Networks

With Palo Alto Networks, you can adopt a tightly integrated network security platform. When you do, you'll have powerful, consistent security, no matter where users, applications, and devices are located. You'll exceed the pace of attackers, today and tomorrow, with AI-powered threat prevention—detecting and stopping attacks in real-time. And you'll ease the burden on your team by automating manual, time-consuming tasks, while reducing operational complexity with unified management and experience.

You'll confidently embrace innovation and move securely forward with speed.

1. Reaching New Heights in Uncertain Times, Boston Consulting Group, May 23, 2023.
2. (ISC)² Cybersecurity Workforce Study, (ISC)², 2022.

paloalto® NETWORKS | STRATA™