



Overcome the security barriers to innovation



Enable your business to grow and innovate

As your organization pursues growth and innovation, it's up to you and your team to keep the business secure. In the past, adding new tools to keep up with each new threat may have been enough. But that's when the organization was contained. Today, users work from anywhere, applications are moving to the cloud, and most connected devices are unmanaged and invisible to security teams. Existing infrastructure and internal resources can no longer keep up.

Continuously adding tools leads to the kind of complexity that makes securing the entire organization much more difficult. It's also an invitation for increasingly sophisticated attackers to find new ways in through unforeseen security gaps and errors. In the end, your organization could take on financial and reputational damage, while you and your staff face longer hours, more stress and burnout trying to deal with it all.

Legacy network security can't keep up. 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.

But a few challenges can stand in the way. Let's explore how you can overcome them.



CHALLENGE:

Fragmented data and incomplete visibility

Hybrid work, rapid application development, and other operational shifts are creating new security use cases at an accelerating pace. When it comes time to protect all your devices, applications, users, and locations, the number of different tools involved creates fragmented data and incomplete visibility—compromising security.

You spend too much time simply translating and interpreting the data among different tools. Valuable resources are spent on low-impact activities.

This elevates the risk to your organization's operations and reputation. It's very difficult for your teams to understand the true threat severity across the expanding attack surface and take action to protect the business.

You can't keep your attack surface from expanding. But you become an easy target if you allow this expanded surface to remain exposed.



SECURITY
BREACH



THE SOLUTION:

Consistently secure your whole enterprise

Multiple security measures are no longer sufficient in protecting employees where, when, and how they work; securing applications wherever they run and transact with each other; or safeguarding devices that access your enterprise. On top of that, data center security solutions often don't transition effectively to the cloud and security point solutions expose your network to security gaps.

With Palo Alto Networks, you can:



Verify and control all network activity. You'll apply uniform policies and rules across the entire enterprise and all your assets. Using best-in-class physical or virtual form factors, you can track anomalous user behavior across topographies on your network. And, by consistently protecting all your business applications, you can give users the same seamless experience in any location and protect application-to-application traffic anywhere in your enterprise infrastructure.



Adopt a Zero Trust architecture that limits or blocks everyone except those who require access. Your network security team can fully identify and characterize traffic sources by users, applications, devices, and content. You'll build baseline security policies along with policies to block access programmatically. That will allow you to grant least privileged Zero Trust access while blocking everything else automatically.



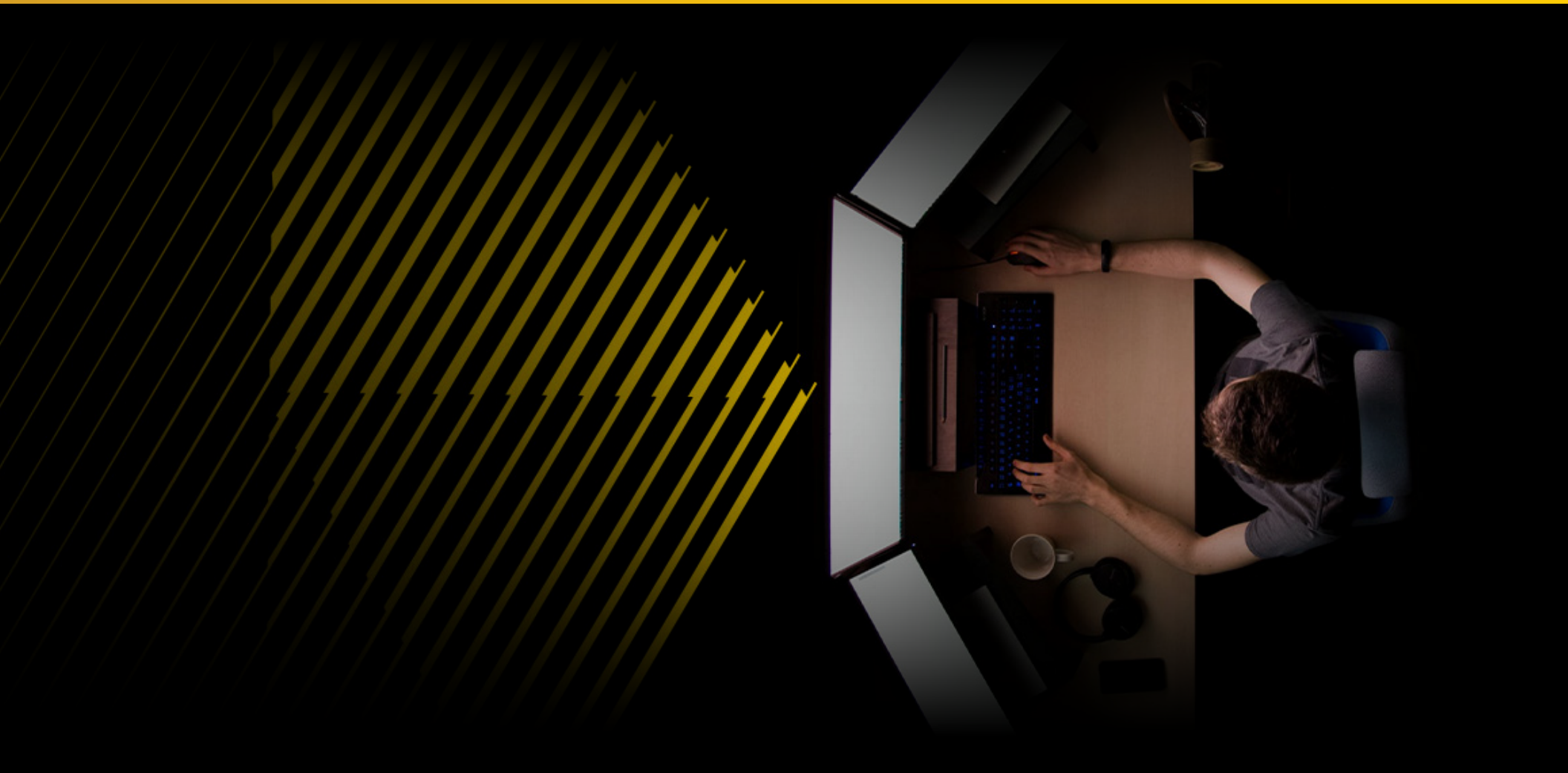
Extend security coverage from edge to edge. You'll secure the network edge uniformly—no matter where the edge location is. And you can extend coverage to every employee everywhere. You'll also secure all traffic across your data center, campus, remote and office-based users, and private and public clouds consistently. Your people can access applications at any time without noticing your security measures.

CHALLENGE:

Evasive threats from an AI-enhanced arsenal

Attackers are moving faster and are more sophisticated. By using AI, bad actors are strengthening their arsenal, creating new attack vectors and complicating the task of defending your organization. Who would have imagined you would have to defend against something like a simulated video call from your CFO asking for a funds transfer?

Allowing these evasive threats to get through when you are patient zero is bad enough. But when a tactic has already been identified—a tactic you should have known about—uncomfortable questions could be raised by the board.



THE SOLUTION:

Apply AI and machine learning to prevent threats

You may have hours—or only minutes—to prepare against novel attacks. Meanwhile, ransomware attacks can quickly penetrate the network, but companies often only learn about the attack several days later. Then, it can take months to repair the damage. In this environment, as your network evolves, your security needs to evolve as well.

With Palo Alto Networks, you can:



Evolve your defenses to outpace the speed of attackers. Backed by 3.5 billion daily events, Palo Alto Networks' inline AI and ML capabilities can help you reduce your risk of being blindsided by a new type of attack. You'll be able to better detect suspicious patterns and behaviors—taking preventative action and forcing attackers to look elsewhere.



Stop invasive threats inline with AI-powered best in class advanced threat prevention. You'll be able to react quickly to threats coming into the firewall and block malicious traffic within seconds, while keeping legitimate traffic flowing. And you can do it all without requiring your people to write code. You'll prevent breaches, reduce the time your team spends on manual interventions, and make your organization safer and stronger.



Bring community intelligence to your defense by leveraging the network effect of security intelligence from Palo Alto Networks' 65,000 global customers. You'll also benefit from network intelligence experts as you automatically apply preventative measures. When a company in the network experiences the first known instance of a new threat, all Palo Alto Networks customers automatically receive protection against the threat within minutes. Meanwhile, your team can easily verify your network's security posture to demonstrate your preparedness for the latest ransomware scheme.

CHALLENGE:

Network security complexity

With each new point solution, your security infrastructure becomes more complex and costly.

What's more concerning, however, is the painful choice you face when you have multiple consoles to manage multiple security products. All too often, the choice is between establishing isolated teams for each product or stretching your security analysts too thin. Either way, you hit the limit on the manual effort your security teams can provide. There is unnecessary duplication of efforts, inconsistent application of policies, and inevitable mistakes. You just can't close the gaps.



THE SOLUTION:

Simplify your network security operations

You must find a way to make things easier for your team. That's easier said than done.

With Palo Alto Networks, you can:



Provide complete visibility—from one place. Palo Alto Networks provides a unified management experience, with AI-powered operations tools, giving your team the intelligence and time needed to take actions in advance. You can also apply policy updates once, removing inconsistencies—reducing the burden and costs of doing so. And, with a full view of how many threats you have blocked across the network, you can demonstrate the value of your efforts and make informed decisions on where to invest next.



Find, fix, and predict security gaps automatically. When outages, configuration, and service issues occur, analysts are not always aware of the impact on their security posture. With Palo Alto Networks, you can identify, anticipate, and address security gaps. Using artificial intelligence for operations technology, you can automate many tasks with ready-made templates and device groups. Equipped with these tools, you can comply with security best practices and sunset outdated or non-compliant tools. You can predict firewall health issues, such as capacity constraints, up to seven days in advance and proactively prevent firewall disruptions.



Consolidate and expand security capabilities. Disparate environments, lack of integration, continual policy updates, and an overtaxed staff may be preventing you from fully realizing the value of the many solutions in your security portfolio. With Palo Alto Networks' integrated best-of-breed security services, you can get consistent security across environments, automatically share intelligence between technologies, and simplify policy creation across intrusion prevention (IPS), malware analysis (sandboxing), web security (SWG), SaaS security, and IoT security.

Securely enable your business for growth and innovation with a platform approach

With Palo Alto Networks' tightly integrated network security platform built on Zero Trust and powered by AI, you'll overcome complex challenges—keeping your organization secure as it innovates with speed.

**SECURE YOUR
WHOLE ENTERPRISE
CONSISTENTLY.**

**PREVENT THREATS
WITH INLINE AI AND
MACHINE LEARNING.**

**SIMPLIFY YOUR
NETWORK SECURITY
OPERATIONS.**

LEARN MORE