paloalto® NETWORKS

Secure From Every Angle

Achieve Cybersecurity Consolidation to:

- Reduce Complexity
- Automate Security
- Supercharge Risk Posture

Executive Summary

With the emergence of new technologies like artificial intelligence (AI), machine learning (ML), 5G and Industry 4.0, digital transformation continues to change the business landscape and drive more opportunities for growth and innovation. At the same time, these changes are prompting organizations to rethink how to best secure their evolving businesses.

Traditionally, business leaders tackled cybersecurity challenges by bolting on new security solutions on a case-by-case basis. But for many organizations, years of stitching together different security products has led to an awakening: many IT environments today are too complex to manage effectively. Security teams often contend with a maze of nonintegrated products, leading to greater security risks, operational disruptions and financial impacts.

Meanwhile, threat actors have developed new tactics to bypass defenses, and cyber incidents have become more frequent and severe. In fact, our survey of global business leaders, What's Next in Cyber 2022, found that 96 percent of CXOs say their organization has experienced at least one breach in the last year.[1]

Today's business success hinges on establishing a robust framework of digital trust built upon two key pillars: cybersecurity transformation and the ability to attain resilience in crucial areas and at critical moments.

The question, though, is: how? How can you simplify your security landscape while building security into every initiative? How can you reduce complexity, drive automation and supercharge your security posture at today's accelerated rate of change?

96%

OF CXOs EXPERIENCED AT LEAST ONE BREACH

57%

EXPERIENCED THREE OR MORE BREACHES

33%

EXPERIENCED AN OPERATIONAL DISRUPTION AS A RESULT OF A BREACH

1. 2022 Global What's Next in Cyber survey, Palo Alto Networks, September 2022.

Cyber Transformation | 3 Key Trends

Several factors impact your ability to transform your cybersecurity and supercharge risk posture. Let's look at the three most important trends:

1. The Shift to Cloud Has Gone Mainstream

Just a few years ago, moving to the cloud meant shifting applications and workloads to more flexible, scalable infrastructure and making incremental improvements to business operations. Today, it's about leveraging technologies, such as AI, automation, IoT and 5G within the organization and accelerating innovation.

Many organizations are expanding their use of cloud.[2]

33%
ARE MIGRATING ON-PREMISES WORKLOADS TO THE CLOUD

33%
ARE REPLACING LEGACY SOFTWARE WITH CLOUD-BASED TOOLS

41%
ARE INCREASING USE OF CLOUD-BASED SERVICES AND PRODUCTS

The monumental transition to the cloud—and adoption of AI and other emerging technologies—has been a boon to business success, but it's also left security teams scrambling to build the right defenses.

For example, legacy security tools architected for on-premises environments, when extended or retrofitted to the cloud, leave critical security gaps. Threat actors have increasingly powerful ways to target misconfigurations in cloud infrastructure, APIs and software supply chains. These misconfigurations expand the attack surface and leave systems vulnerable to exploits.

2. Google Cloud Brand Pulse Survey, Q4 2022.

2. The Nature of Work Has Changed Fundamentally

Remote and hybrid work have become a way of life. Branch offices are transforming from primary workplaces to collaboration hubs. In many organizations, a large portion of the workforce is now remote or works a hybrid schedule.

Employees access the network from a wide variety of devices using both secured and unsecured wireless networks. In organizations with OT and IoT, employees also interact with connected devices that access the internet and public cloud.

The result is an increasingly complex and interconnected network with a vastly expanded volume of endpoints and applications, requiring an integrated approach to security encompassing users, data, devices, applications and diverse infrastructure.

3. The Threat Landscape Continues to Escalate

Virtually every business sector leverages new technology to drive efficiency and scale—and in the context of cybersecurity, these new technologies are key to protecting against attacks. However, adversaries use the same new technologies to scale operations and launch malicious campaigns.

For example, today's cybercriminals use AI to automate ransomware, phishing and denial-of-service (DoS) attacks. They launch attacks at a scale that overwhelms defenders, leaving human-centered security operations centers (SOCs) unable to keep up. They even leverage generative AI to create malicious code and more human-sounding communications.

61%

OF ORGANIZATIONS STRUGGLE TO SECURE THEIR HYBRID WORKFORCE [3]

$2.4M

IS THE AVERAGE COST TO RECOVER FROM A BREACH, NOT INCLUDING DAMAGE TO THE ORGANIZATION'S OPERATIONS AND REPUTATION [4]

The battle for technological superiority is an arms race between your security team and hackers. You have to protect every part of the business—endpoints, applications, data and infrastructure. But it's getting harder to keep up with well-funded, highly motivated threat actors proving to be just as innovative as any security team.

paloalto NETWORKS

3. 2022 Global What's Next in Cyber survey, Palo Alto Networks, September 2022.
4. 2021 State of Enterprise Breaches Report, Forrester Research.

Cybersecurity Has Never Been More Mission-Critical

How can organizations secure their digital footprint, safely enable remote and hybrid work and navigate the escalating threat landscape?

Looking at the security landscape today, we see three areas of opportunity where improvements can help you achieve your business goals faster.

Managing Cyber Risks in Complex, Borderless Environments

Maximizing Security Efficacy and Operational Efficiency

Automating Threat Detection and Response

Managing Cyber Risks in Complex, Borderless Environments

It's nearly impossible for human security teams to identify and manage all the vulnerabilities in today's highly complex and distributed organizations. As your infrastructure becomes more dynamic, you need a security approach that can grow and evolve along with your environment.

The Risk

Employing purpose-built point products for each security area adds complexity and creates security gaps. For example, if your email security tools don't interact with your threat intelligence platforms, or log data in the same way as your anti-malware solution, you can't unify the entire network. You can cobble the pieces together, but you end up with a fragmented, inconsistent view.

Using traditional security products architected for on-premises environments and retrofitted to secure cloud resources similarly provides an incomplete view. Because they weren't originally intended to manage cloud environments, they also leave gaps that threat actors can exploit.

The Solution

To effectively manage risk, you need complete visibility across your entire infrastructure. The products you deploy to secure different areas need to use the same data logging convention mechanisms, context, structure and labeling—and your data needs to be consolidated in one place.

Seamless integration of security tools and applications working together connects security alerts and events to larger data points, drives attack recognition with AI and ensures that issues get resolved in minutes rather than days or weeks.

Maximizing Security Efficacy and Operational Efficiency

Security leaders today face intense pressure to maintain strong security while also reducing costs. Maximizing the efficacy of your products and solutions can significantly improve your security posture and achieve long-term cost savings.

The Risk

On average, large organizations employ 31.5 different security products—many of them from different providers.[5] Each product has to be managed separately, requiring time that could be dedicated to high-value tasks.

At the same time, it takes longer to vet and procure products when they're sourced from different vendors, which makes the security infrastructure less agile in responding to change. And implementing updates and policies consistently across multiple security products takes longer.

Threat actors thrive on security silos. While each product might be effective in its role, the inherent difficulty of integrating them into a unified defense makes it difficult for IT teams to coordinate security across the network. It's like hiring a roster of superstars who can't play together as a team.

The Solution

A consolidated approach to security creates a single, unified view of cyber defense. In a consolidated environment, integrated consoles allow security teams to manage and monitor products from a unified dashboard, removing silos, improving visibility and creating shared intelligence to drive automation.

Automation, in turn, strengthens your security posture by responding to threats more quickly and freeing security analysts to focus on high-value tasks. As a result, you can maximize the efficiency of both your workforce and your security technology.

Security teams spend countless hours exploring products, sourcing vendors and finalizing contracts. Cybersecurity consolidation significantly reduces procurement lead time by providing multiple products and services together.

paloalto NETWORKS

5. 2022 Global What's Next in Cyber survey, Palo Alto Networks, September 2022.

Automate Threat Detection and Response

As threat actors increasingly use AI and automation to exploit vulnerabilities and evade detection, you need the same technologies for your defense. But AI is only as effective as the data it consumes. You need a data structure that allows your entire defense to work together.

The Risk

Relying on your security team to investigate and respond to alerts leaves your people inundated with siloed data, manual tasks and innumerable fragmented workflows generated by siloed point products. It takes a human-centered SOC up to 287, days on average, to identify and contain a data breach, and many organizations only discover the attack when they receive a ransom note.[6]

Point products reduce the effectiveness of AI and automation in your cyber defense. The data they generate can't be harmonized effectively, and the automation solutions you put in place won't be able to share intelligence across your network.

The Solution

By consolidating your security, you create a unified data lake to power effective automated threat detection and response. With shared intelligence, your AI- and ML-based solutions will have a complete view of the environment, providing the airtight defense you need against sophisticated, automated attacks.

With effective automation, managing data, unifying workflows and handling low-level tasks, your expert staff can uplevel their performance, dealing only with the events that require human intervention.

6. Cost of a Data Breach Report 2023, IBM, 2023.

Cybersecurity Consolidation
Better Together

Cybersecurity consolidation combines all the strengths of point products with the added benefit of ensuring the products work together through seamless integration.

A unified dashboard simplifies the security team's monitoring of the environment and response to threats. Shared intelligence provides end-to-end visibility and generates the data that unlocks the power of AI and ML.

Through consolidation, you create a united front against attackers by harmonizing reporting, policy creation and other activities across the security infrastructure.

Reduce Complexity

Simplifying management with a single pane of glass reduces staff workloads, increases efficacy and allows the whole security infrastructure to work together.

Drive Automation

Consolidated data, enhanced AI and ML services and end-to-end visibility help the organization stay ahead of today's sophisticated threat actors.

Strengthen Security Posture

Making security a fundamental principle of each new business initiative improves defenses and accelerates digital transformation.

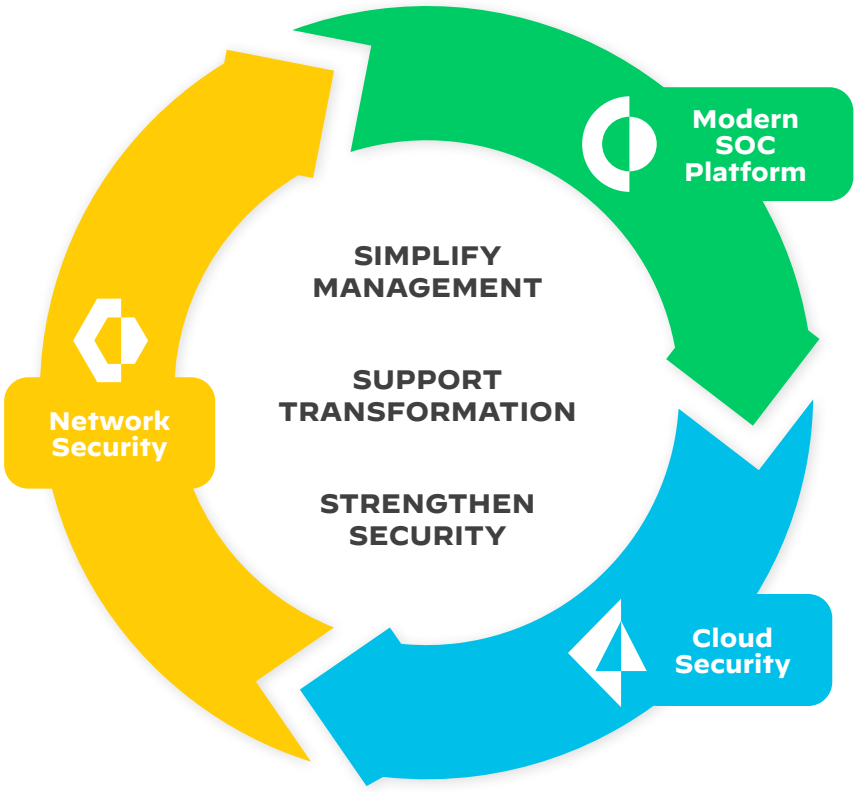
Cybersecurity Consolidation With Palo Alto Networks

Organizations don't have to choose between best-of-breed products from multiple vendors that create operational complexity and security gaps, and a single-vendor solution that may sacrifice security for simplicity. They can have both industry-leading products and the benefits of security consolidation.

Palo Alto Networks industry-leading solutions work harmoniously to deliver end-to-end security and minimize gaps.

NETWORK SECURITY PLATFORM

- Firewall
- Intrusion Detection and Prevention
- URL Filtering
- Sandbox Detection
- DNS Security
- IoT Security
- Data Loss Prevention
- Cloud Access Security Broker
- Posture and Health Management
- Remote Access for Users
- SWG
- SD-WAN



MODERN SOC PLATFORM

- XDR
- SIEM
- Endpoint + EDR
- NTA/UEBA
- SOAR
- Attack Surface Management

CLOUD SECURITY PLATFORM

- Cloud Security Posture Management
- Cloud Workload Protection
- Cloud Infrastructure Entitlement Management
- Code Security
- Web Application / API Security

Network Security

Secure users, apps and data anywhere—on-premises, in the cloud or hybrid. Get complete Zero Trust network security to see and secure everything from your headquarters to branch offices and data centers, as well as your mobile workforce.

Palo Alto Networks offers a consistent, integrated and effective network security platform delivered in hardware, software and cloud-based form factors.

Our ML-Powered NGFWs and Cloud-Delivered Security Services leverage inline deep learning to stop unknown zero-day attacks so you can go beyond signature-based detection to block even the most evasive threats.

Learn More About Network Security

Cloud Security

The move to the cloud has changed all aspects of the application development lifecycle—security being foremost among them. Security and DevOps teams face a growing number of entities to secure as the organization adopts cloud-native approaches. Ever-changing environments challenge developers to build and deploy at a frantic pace while security teams remain responsible for the protection and compliance of the entire lifecycle.

Palo Alto Networks secures your infrastructure, workloads, and applications from code to cloud. With our comprehensive cloud security platform, Prisma® Cloud, our integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively, and accelerate application development and deployment securely.

Learn More About Cloud Security

Endpoint Security and Security Operations

Palo Alto Networks offers the industry's most comprehensive product portfolio for security operations, empowering enterprises with best-in-class detection, investigation, automation and response capabilities. We secure the future by providing SecOps teams with Cortex®, an integrated platform that addresses all key challenges in a more efficient way so they can focus on delivering higher security outcomes.

We can help you reduce the number of security alerts, automate end-to-end security operations and gain holistic visibility across your enterprise. With native integration and interoperability, SOC teams can close the loop on threats with continual synergies across the Cortex ecosystem. These products work in concert to monitor the threat landscape and provide the most robust detection, response and investigation capabilities in the industry.

Learn More About Security Operations

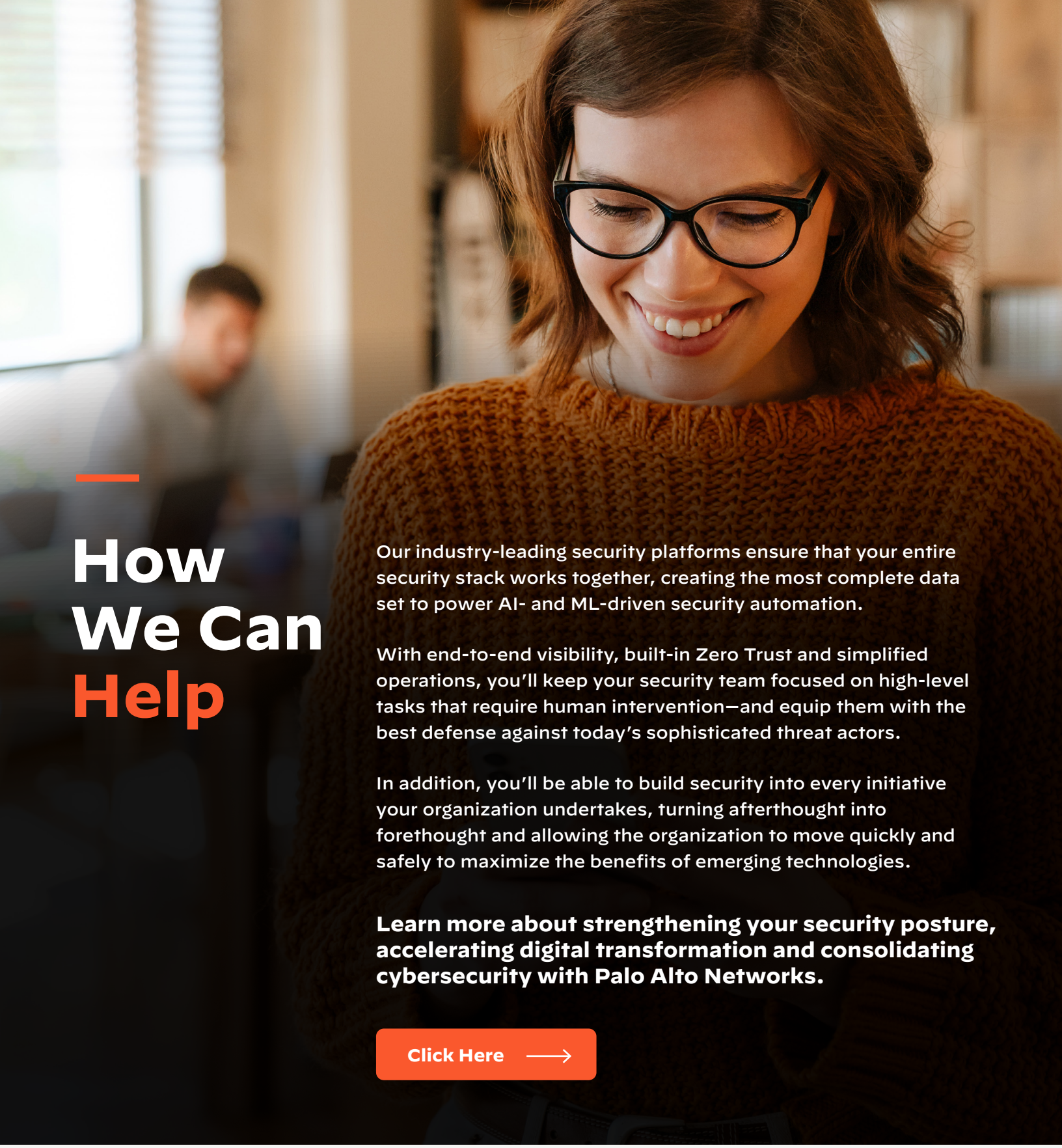
Threat Intelligence and Incident Response Services

Palo Alto Networks Unit 42® brings together world-renowned threat researchers, elite incident responders and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against real-world threats, transform your security strategy with a threat-informed approach and respond to incidents in record time so that you get back to business faster.

When you team up with Unit 42, you partner with an elite team of security experts who use best-in-class tools to help you stop the attack and prevent the next one. Unit 42 is on the approved vendor panel of more than 70 major cybersecurity insurance carriers and 150+ law firms.

Learn More About Unit 42

paloalto® NETWORKS



How We Can Help

Our industry-leading security platforms ensure that your entire security stack works together, creating the most complete data set to power AI- and ML-driven security automation.

With end-to-end visibility, built-in Zero Trust and simplified operations, you'll keep your security team focused on high-level tasks that require human intervention—and equip them with the best defense against today's sophisticated threat actors.

In addition, you'll be able to build security into every initiative your organization undertakes, turning afterthought into forethought and allowing the organization to move quickly and safely to maximize the benefits of emerging technologies.

Learn more about strengthening your security posture, accelerating digital transformation and consolidating cybersecurity with Palo Alto Networks.

Click Here →

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com