Modernize Your Network Security With Artificial Intelligence

Key Principles to Adopting a Zero Trust, AI-Powered Approach to Network Security

Challenges of Enterprise Network Security

If you're an IT executive charged with securing the modern enterprise, you face an almost impossible challenge. The onslaught of highly evasive threats, an ever-expanding attack surface, and a new generation of hacker tools based on artificial intelligence (AI) combine to ratchet up the pressure on security groups. System administrators have even less time to patch disclosed security vulnerabilities than previously thought because threat actors scan for vulnerable endpoints within 15 minutes of a new threat being publicly disclosed.[1] In the face of this dynamic and dangerous threat landscape, security professionals can be forgiven for being a little pessimistic.

However, there are good reasons for optimism. Recent advancements in the use of artificial intelligence (AI) for security as well as the ability to process massive amounts of global threat information quickly have leveled the playing field. Now, security teams can block threats instantly and limit the damage done by the very few that do get into the network. Unknown, "zero day" threats that used to take days or weeks to discover can now be detected and neutralized almost immediately, far better than the industry's average time to remediate of six days.[2] In addition to protecting the network, shortening the effective lifespan of these advanced threats disrupts the economics of cybercrime by forcing attackers to invest more time and resources for diminishing returns.

Many security infrastructures have grown piecemeal, creating a complex environment that is prone to security gaps and are difficult to manage. These ad hoc systems limit the effectiveness of security teams by flooding their inboxes with large numbers of alerts—many of which turn out to be false positives—and bogging down highly skilled security professionals with dozens of dashboards from multiple security vendors.

There's good news here as well. Now organizations can invest in an integrated platform that streamlines security management and offers consistent security to relieve some of the pressures on security administrators. The net result is to turn a formerly reactive mindset into a pervasive belief that the organization can protect itself against any threats, anywhere in the sprawling corporate network. Imagine a world where network security professionals can look to the future with confidence, not dread. Such a world is possible, but achieving this highly desirable result requires overcoming three key challenges: evasive threats, fragmentation, and complexity.

AI-Based Evasive Threats Up The Ante

It's hard to believe that, in this day and age, companies need to be wary of fake video calls from their CFO requesting money transfers. If a business falls for a new kind of scam, it's one thing. But if it gets duped by a known tactic, that can lead to some serious questions from corporate leadership.

The rise of AI has been a boon for technology enthusiasts everywhere and cyber attackers are no different. Hackers are now harnessing the power of AI to make threats harder to detect. Just as legitimate users employ tools such as ChatGPT, attackers have their own equivalent malicious alternatives. These rogue AI versions, with names like FraudGPT and WormGPT, assist cybercriminals in crafting highly convincing phishing emails in various languages. In fact, WormGPT has been described as a version of ChatGPT that throws ethics out the window.

1. *Incident Response Report, 2022*, Unit 42, 2022
2. *Unit 42 Cloud Threat Report—Volume 7*, Unit 42, 2023

Mimicking trends in the world of legitimate cloud-based services, some threat actor groups are adopting the "as-a-service' model to monetize their investments in advanced threats with hacking-as-a-service offerings for malware (MaaS), phishing (PHaaS) and even ransomware (RaaS). These XaaS enterprises offer all the benefits of legitimate businesses, including a portfolio of standard products, customization services, and even 24/7 technical support. The impact of the XaaS model is to lower the barrier to entry for wannabe cyberattackers, making it possible for bad actors to launch attacks without coding or technical skills.

One relatively popular variation of RaaS is cryptomalware, which encrypts the victim's data and offers to provide the decryption key upon payment of a ransom, often using bitcoin or other cryptocurrency. Prospective hackers can take advantage of a range of other tools such as infostealers, software agents that collect data on a potential victim and transmit that information to bad actors to help them build effective attacks. Customers can also buy off-the-shelf backdoors to breach perimeter defenses, and to download malicious software onto the victim's system. When it comes to innovation, cyberattackers can be just as creative as their legitimate counterparts.

Fragmentation Reduces Visibility, Drains Productivity

Thanks to recent advances in technology for remote work, more people are working flexibly from various places than ever before. This trend offers benefits such as hiring flexibility, better employee morale and retention, and reduced facilities costs. However, securing all these remote workers and their many devices can be a headache.

Imagine juggling many different balls at once; it's easy to miss catching one. That's how security professionals can feel when they are forced to use multiple tools to protect the organization's technology and critical business data. This fragmentation blurs the full picture, making it more difficult to spot potential threats and manage risk. Network administrators spend valuable time simply translating and interpreting the data between different tools, low-impact activities that drain resources from more strategic initiatives.

Another aspect of fragmentation is the ever-expanding attack surface, that is, the sum of all the possible entry points to the organization's network. You can't keep your attack surface from expanding—this is a given if the business is to grow and innovate. But if you allow this expanded surface to remain exposed, you become an easy target. And if something does go wrong, the company's day-to-day operations, revenue streams, and brand can suffer.

Complexity Compounds the Security Challenge

Organizations often respond to today's more challenging cybersecurity issues by investing in additional point solution tools. While each tool may serve a specific purpose, the lack of integration increases complexity and negates the potential benefits. Managing and maintaining multiple cybersecurity tools can be complex and resource-intensive because each tool requires its own set of configurations, updates, and expertise, leading to increased administrative overhead. When multiple tools work in silos, they may not effectively communicate with each other, leading to a fragmented security posture with blind spots and gaps in coverage. Not all tools may have compatible APIs or interfaces, making seamless integration problematic.

With too many security tools generating alerts and notifications, security teams may suffer from alert fatigue. Teams struggle to correlate information from different tools, slowing down the investigation and containment of threats. Organizations may have difficulties finding qualified personnel with expertise in specific security tools, necessitating expensive and time-consuming training investments.

Zero Trust, AI-Powered Approach to Network Security

Meeting the challenges outlined above requires more than just incremental improvement—nothing short of a complete paradigm shift will do. The need is for a platform that evolves your defenses at a velocity that outpaces the speed of attackers and employs innovative security techniques to block evasive threats, unify security operations, and reduce complexity. This section presents the key principles that must drive the design of a comprehensive, AI-powered security platform.

Principle	Challenge		
	Evasive Threats	Fragmentation	Complexity
Implement Zero Trust	⊙		
Eliminate Gaps	⊙		
Apply Uniform Policies	⊙		
Harness Power of AI		⊙	
Outpace Threats		⊙	
Leverage Threat Intelligence		⊙	
Unify Security Management			⊙
Improve Visibility			⊙
Automate With AIOps			⊙

Implement Zero Trust

Traditional data center security measures often struggle when transitioning to the cloud. Adopting a genuine Zero Trust security approach can change this. By using the Zero Trust policy framework, your network security team can accurately identify traffic based on users, applications, devices, and content. Inspecting interactions using cloud-delivered security services allows your security team to swiftly identify and address new forms of malware and ongoing advanced threats, even decrypting encrypted traffic when needed. This approach simplifies policy management and assures stakeholders that the organization remains safe.

Eliminate Gaps

Relying solely on individual security solutions can leave your network vulnerable to potential threats, as the strength of your network is determined by its most vulnerable point. You need to consistently fortify the entire network perimeter and protect every team member regardless of their location. Your employees, contractors, partners, and vendors must be able to freely use applications without ever being obstructed by security protocols, ensuring that day-to-day operations are never delayed. This holistic security approach not only enhances the overall user experience and efficiency but also leads to cost savings and can position your organization as an industry frontrunner.

Apply Uniform Policies

Crucial requirements for world-class security are to implement policies uniformly across the whole infrastructure and monitor for unusual user activities within the network's different areas. Offering consistent protection to all business applications ensures users enjoy a uniform experience regardless of their location, while also securing interactions between applications throughout your business infrastructure. This approach avoids misconfigurations, reduces unforeseen disruptions, and guarantees uniform performance levels.

Harness the Power of AI

When faced with unexpected security threats, preparation time can be extremely limited. The ideal network security solutions harness the power of AI and machine learning (ML) to process billions of unique daily events, enhancing your defense against emerging attack trends. AI-based solutions can pinpoint anomalous patterns and activities that are difficult or impossible for humans to find. ML allows you to act promptly, deterring adversaries and directing their attention elsewhere. This system also minimizes false alarms, allowing your team to focus on genuine threats that require human intervention.

Outpace Threats

Ransomware attacks can breach firewalls in mere minutes, yet organizations often remain unaware of such intrusions for days, leading to prolonged recovery times. Harnessing top-tier artificial intelligence and machine learning allows your security system to identify and neutralize harmful traffic while ensuring the smooth passage of legitimate communications. This approach not only bolsters immediate defense but paves the way for even faster responses to future threats.

Leverage Threat Intelligence

As networks expand, so should their security measures. Threat intelligence gives security managers access to a vast pool of timely and reliable information that can help them effortlessly bolster their defenses. Whenever a new threat is discovered anywhere in the global network, that incident can be immediately disseminated to your security team, making them well-equipped to answer any top-level queries about preparedness. By integrating threat intelligence into their security strategies, businesses can enhance their defense mechanisms, empower teams to tackle challenges more efficiently, ensure continuous operations, and safeguard the organization's reputation and assets.

Unify Security Management

Many large corporations employ a wide range of point solutions, each targeting a distinct threat vector. Yet, the complexity of these environments, the absence of seamless integration, continuous policy modifications, and overwhelmed personnel obstruct these businesses from fully harnessing the potential and value of their security tools. An AI-powered integrated platform can provide unified configuration management aligned with best practices ensure uniform security across all settings, enable automatic intelligence sharing among technologies, and ease the policy-making process for intrusion prevention (IPS), malware analysis (sandboxing), web security (SWG), SaaS security (CASB), and IoT security. Now you can manage your SASE, NGFW, and all security services from a single UI and enforce best practices inline.

Improve Visibility

In response to the fragmentation challenge posed by the deployment of generations of point products, security managers need an integrated platform that can take network visibility to a new level. Solutions based on AI technology can predict potential performance bottlenecks and security loopholes, offering ample time for prevention. With improved visibility comes the ability to streamline policy changes, ensuring consistency while holding down costs.

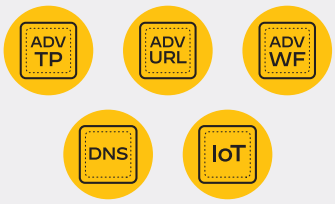
Automate With AIOps

For groups struggling with outages, configuration, and service disruptions, artificial intelligence for operations (AIOps) technologies offer an effective solution. AIOps automates routine tasks using predefined templates and groupings, ensuring adherence to security standards while phasing out obsolete and non-compliant systems. AIOps can in principle predict and preemptively address potential network issues such as firewall capacity limitations days or weeks ahead. Adopting this methodology not only simplifies operations but also diminishes security breaches, bolstering your team's confidence in your protective measures and enabling them to focus on more vital tasks.

Modernize Network Security With Palo Alto Networks

In the high-stakes struggle between cyberattackers and defenders, Palo Alto Networks stands ready to help by offering a fully integrated network security platform with three key attributes: inline AI-powered security, Zero Trust management and operations, and ML-powered NGFWs for every use case.

Inline AI-Powered Security



Security Services

Defend the initial target using a comprehensive suite of inline AI-powered security services to defend against zero-day threats.

Zero-Trust Management and Operations

Cloud-Based Security Management

Reimagine network security with the industry's first AI-powered zero-trust management and operations solution for your entire network security estate.

ML-Powered NGFW for Every Use Case

Wide Range of Form Factors

Benefit from best in-class protection for any location, from the largest data centers to a local retail office, with industry-leading ML-powered NGFWs.

Inline AI-Powered Security

Defend the initial target using a comprehensive suite of inline AI-powered security services to prevent patient zero. Stop zero-day malware in real-time. Safeguard your credentials and sensitive data with industry-first AI-powered detections against advanced and evasive phishing attacks, command-and-control exploits, and DNS threats.

Zero Trust Management And Operations

Reimagine network security with the industry's first AI-powered zero trust management and operations solution for your entire network security infrastructure. Predict and prevent operational disruptions with real-time monitoring. Forecast deployment health and proactively identify capacity bottlenecks to optimize the user experience. Manage your SASE, NGFW, and all security services from a single user interface and enforce best practices inline.

ML-Powered NGFWs For Every Use Case

Benefit from best-in-class protection with the industry's leading machine learning-powered NGFWs. Achieve blazing fast performance up to 1 Tbps in the most demanding environments. Choose from a range of form factors to fit every deployment need, from the largest data center to local retail office and everything in between.

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.

Visit Palo Alto Networks to learn how you can confidently embrace innovation and move securely forward with speed.

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

modernize-your-network-security-with-artificial-intelligence-wp-110623