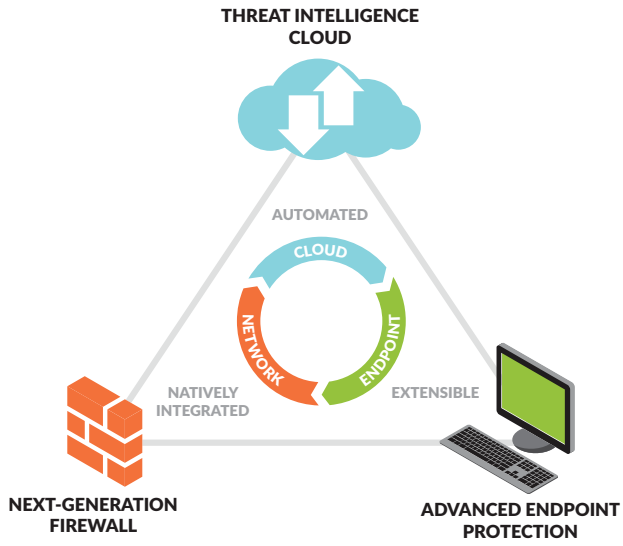
# NEXT-GENERATION SECURITY PLATFORM

## Prevent breaches. Enable productivity. Secure our digital way of life.

Palo Alto Networks® Next-Generation Security Platform enables enterprises, service providers and governments to protect our digital way of life with a prevention-first approach to cybersecurity. Our platform allows organizations to reduce their threat exposure by first enabling the applications for all users or devices, regardless of location, and then preventing threats within application flows, tying application use to user identities across physical and cloud-based networks.

The Palo Alto Networks Next-Generation Security Platform has four key characteristics that enable the prevention of successful cyberattacks:

1. **Natively integrated** technologies that:
   - Leverage a single-pass architecture to exert positive control based on applications, users and content to reduce the organizational attack surface.
   - Support open communication, orchestration and visibility.
   - Enable consistent security posture, providing the same protection on the endpoint, in the data center, on the network, in public and private clouds, and across SaaS environments.
2. **Automation** of protection by creating and reprogramming security postures in real-time across the network, endpoint and cloud environments to counter new threats, allowing teams to scale with technology, not people.
3. **Extensibility and flexibility** that allows for consistent protection as users move off physical networks, and as organizations expand and adopt new technologies and architectures.
4. **Threat intelligence sharing** that enhances prevention and minimizes the spread of attacks by taking advantage of the network effects from the automated sharing of protections across a global community.




### Palo Alto Networks Prevention Platform

- **Next-Generation Firewall**: Our next-generation firewalls make use of a single-pass architecture, enabling security capability that is unique in the industry. This architecture is implemented in a portfolio of both physical and virtualized appliances, designed to cover a range of performance and use case requirements, delivering the power organizations need to stop evasive cyberattacks.

  Features and management are consistent across the portfolio. Integration with GlobalProtect™ network security for endpoints extends policy-based security to mobile devices whether on-premise or remote.

Integration under our Panorama™ network security management enables you to control your distributed network of our firewalls from one central location. View all your firewall traffic, manage all aspects of device configuration, push global policies, and generate reports on traffic patterns or security incidents — all from a single console. In addition, administrators can filter logs based on any log field and forward pertinent logs to the appropriate recipient, enabling cross-functional collaboration between network and security teams to manage different aspects of a deployment. Panorama is also architected to ingest logs from multiple relevant sources beyond the next-generation firewall to provide correlation of indicators of compromise across enforcement points, such as logs from Traps™ advanced endpoint protection, so that evasive threats can be surfaced, as well as the searching of aggregated logs to see evidence of an attack or for historical forensics.

- **Advanced Endpoint Protection:** Compromise isn't inevitable, or at least, it shouldn't be. Traditional endpoint protection simply cannot keep up with the rapidly evolving threat landscape, leaving organizations vulnerable to advanced attacks. A new approach is needed, one that can rebuild confidence in endpoint security. Traps replaces traditional antivirus with multi-method prevention, a proprietary combination of purpose-built malware and exploit prevention methods that protect users and endpoints from known and unknown threats. Traps prevents security breaches, in contrast to breach detection and incident response after critical assets have already been compromised.

  Traps uses an entirely new and unique approach to prevent exploits. Instead of focusing on the millions of individual attacks or their underlying software vulnerabilities, Traps focuses on the core exploits or techniques used by all exploit-based attacks. Traps prevents malicious executables with a unique, multi-method prevention approach that maximizes coverage against malware while simultaneously reducing the attack surface and increasing the accuracy of malware detection. Traps also automates prevention by autonomously reprogramming itself using native integration with threat intelligence gained from WildFire™ cloud-based threat analysis service.

- **Threat Intelligence Cloud:** The sophistication, speed and volume of threats are increasing dramatically. Adversaries are exploiting the commoditization of evasion techniques to hide in plain site without detection. To effectively keep up with automated attackers, protections against threats must be produced at machine scale. We offer advanced, cloud-based protection from known and unknown threats via our Threat Prevention, URL Filtering , and WildFire services. Palo Alto Networks leverages machine learning on threat data to craft researcher-grade protections for command-and-control activity, at scale. WildFire combines an all-new custom-built hypervisor with bare metal execution, allowing the detection and prevention of even the most evasive threat. Through native integration with the Palo Alto Networks Next-Generation Security Platform, as well as the ability to integrate customizable third-party intelligence feeds, these services bring advanced threat detection and prevention at scale throughout network, endpoint and cloud environments, automatically sharing protections with all subscribers globally in as little as five minutes.

  Advanced detection and prevention in the cloud are enhanced with the AutoFocus™ contextual threat intelligence service. As organizations move to a prevention-led approach with our platform, AutoFocus provides security teams with prioritized, actionable security intelligence on the attacks to which they must respond, with the context to take immediate action on critical threats. Through the MineMeld application for AutoFocus, security teams can connect any third-party intelligence source to the Next-Generation Platform for the enforcement of new prevention controls. AutoFocus weaponizes threat intelligence, resulting in quicker and more efficient investigation of targeted and unique attacks.

- **Cloud Security:** The demand for organizations to be more agile is driving a change in the way applications are developed, deployed and adopted. As organizations increasingly take advantage of virtualization by adopting the cloud, their applications and data become more distributed, thereby expanding potential avenues for compromise. Organizations need a consistent approach to securing any of these environments to prevent increased risk, operational complexity and breach. The VM-Series delivers complete next-generation firewall security and advanced threat prevention to private, public and hybrid cloud computing environments. With the VM-Series, organizations gain consistent visibility into any cloud deployments from production to development, combined with the prevention of known and unknown threats. Our native cloud services offer secure, scalable and resilient cloud-centric architectures with easy orchestration and management, and our cloud neutrality provides the freedom to leverage any cloud environment.

- **Aperture:** Every line of business within an organization has already adopted SaaS apps to be more productive and successful. IT and data governance teams are finding it difficult to track the adoption of the growing list of new SaaS applications. The threat surface has increased significantly with apps gaining mainstream adoption and storing terabytes of sensitive data. Aperture extends the Next-Generation Security Platform to protection for SaaS environments by providing visibility into which apps are being used by which users, enforcement of security policy to an expanding universe of supported apps, and automation of risk remediation by offering the capability to quarantine or delete cloud-based assets.

### Focus on Prevention

The downside of the ever-decreasing cost of computing power is the ability for cybercriminals and adversaries to launch automated and sophisticated attacks at lower and lower costs. It is now cheaper than ever to conduct successful cyberattacks, which has led to an onslaught of malicious activity against organizations, threatening the foundations of trust in digital systems critical to business operations and innovative advantage.

The end goal of security is to enable your operations to flourish and keep your organization out of the headlines associated with cyber breaches. This means reducing the likelihood of a successful attack. By focusing on prevention, the Palo Alto Networks Next-Generation Security Platform reduces cybersecurity risk to a manageable degree, allowing organizations to compartmentalize their most serious threats and focus on business operations.

### Consistent Security Architecture from the Network, to the Cloud, to the Endpoint

Security should not be an impediment to the adoption of new mobility, SaaS, and public or private cloud technologies that enable productivity. Your organization should enjoy the protection against cyberattacks that can automatically adjust to the risk based on how or where your applications and data reside and are being used. Only a natively integrated security platform, with components across these rapidly evolving technology environments, can keep pace with modern attackers, who leverage new attack vectors and security gaps to their target. The Palo Alto Networks Next-Generation Security Platform is composed of natively engineered technologies that leverage a single-pass prevention architecture to exert positive control based on applications, users and content. The result is a reduced attack surface, increased visibility, and consistent security posture from the network, to the cloud, and the endpoint.

### Agility and Security: Why Choose?

Inflexible and complex security postures can pose major hurdles to the adoption of new technologies, such as cloud computing and SaaS applications, necessary for organizational agility. In this context, security and agility become tradeoffs, which can lead to either lost opportunities to raise productivity, or increased organizational risk as users circumvent rigid security controls.

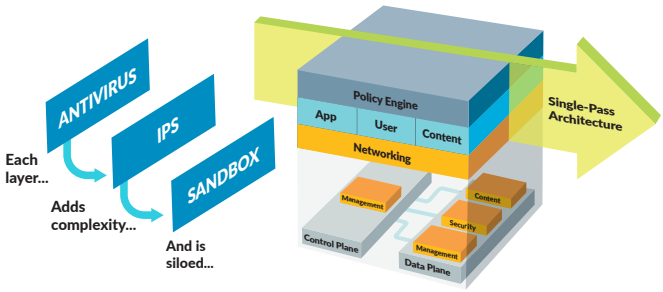
Our platform allows for the consistent enforcement of security policy, including threat detection and advanced intelligence analytics in both physical and virtual environments, by classifying all traffic by application, user and content, regardless of where it lives. With these measures in place, the platform enables the secure adoption of new productivity-enhancing technologies, such as public and private cloud and SaaS applications.

### Improved Security

Defenses made up of multiple point products that do not integrate protections leave gaps that expose organizations to attack. Modern attacks go through multiple steps to achieve their objectives, the prevention of which requires information from multiple sources to be shared automatically and then acted upon. Siloed tools do not communicate with one another well, and changes of one tool to adapt to a new threat almost invariably require manual tuning of all other tools to reflect this change.

The natively integrated Palo Alto Networks Next-Generation Security Platform provides full visibility into all traffic, classifying it by application, user and content levels, and provides the context necessary to enforce security policy and correlate all logs with other security-related events, providing detailed threat intelligence and analysis. The detection of an unknown attack triggers the creation of a protection mechanism and automatic reprogramming of the security infrastructure, allowing defense to scale with machines, not people.

### Legacy vs. Next-Gen Security




### Increased Efficiency – Decreased Cost and Complexity

Security postures built on a wide array of point products from multiple vendors create complex and expensive environments in the level of investment in equipment, the multiple subscriptions and service costs, and the level of effort required to operate and maintain them. With the proliferation of deployed point products, the security architecture for the enterprise became exponentially more complicated, and the more complex environments are, the easier it is for security teams to make a mistake in the deployment. Managing a disparate portfolio of point security products also leads to inefficient utilization of security staff, who increasingly find themselves overwhelmed with alert volumes and bogged down in manual processes.

By classifying and judging all traffic based on application, user and content, our security platform provides the ability to isolate unique and targeted attacks with context and analysis to help security staff prioritize efforts and operate more efficiently. The integrated platform also reprograms itself automatically upon the detection of an unknown attack, creating and disseminating protection mechanisms, a process that does not rely on manual intervention. Palo Alto Networks Next-Generation Security Platform can reduce complexity by consolidating investments in multiple products, which can lead to higher usability while lowering capital and operational expenses.

paloalto NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054

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

www.paloaltonetworks.com