Security Operating Platform

Cybercrime and the types of security threats continue to evolve, challenging organizations to keep up as network boundaries and attack surfaces expand. Security breaches and intellectual property loss can have a huge impact on organizations. Current approaches to security, which focus mainly on detection and remediation, are inadequate to sufficiently address the rise in volume and sophistication of attacks. Cybercriminals leverage automation and big data analytics to execute massively scalable and increasingly effective attacks against their targets. They often share data and techniques with other threat actors to keep their approach ahead of point security products. Cybercriminals are not the only threat: Employees may often unknowingly violate corporate compliance and expose critical data in locations such as the public cloud.

With the rapid evolution of applications moving to the cloud, decentralization of IT infrastructure, and the increased threat landscape, the result has been a loss of visibility and control for organizations. Devices are proliferating and the network perimeter has all but disappeared, leaving enterprise security teams struggling to safely enable and protect their businesses, customers, and users. With new threats growing in number and sophistication, organizations are finding that traditional security products and approaches are less and less capable of protecting their networks against today’s advanced cyberattacks.

At the same time, application development and IT operations teams are accelerating the delivery of new applications to drive business growth by adopting DevOps tools and methodologies, cloud and container technologies, big data analytics, and automation and orchestration. Meanwhile, applications are increasingly accessible. The result is an incredibly complex network that introduces significant business risk. Organizations must minimize this risk without slowing down the business.

A different approach to security is needed. Defenders need to replace siloed point products with security innovations that are tightly integrated. Security requires simplicity. The Palo Alto Networks Security Operating Platform consists of a tightly integrated system of components and services, including a partner ecosystem, that delivers consistent security across the network, endpoints, and cloud. The Security Operating Platform is a fully integrated system that simplifies security by leveraging consolidated threat intelligence information, automation, machine learning, and data analytics.

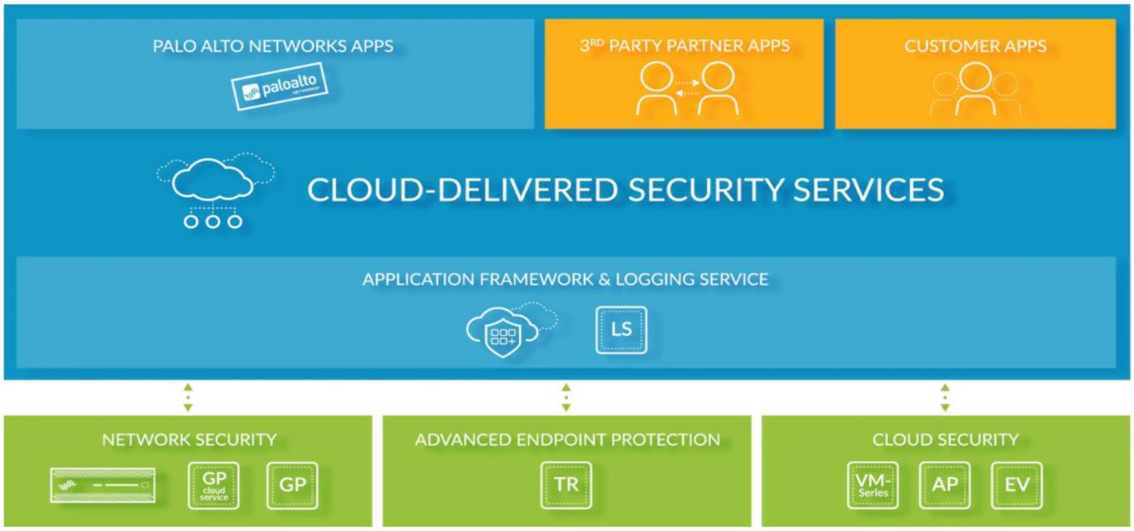

Figure 1-8 *Palo Alto Networks Security Operating Platform*

The Security Operating Platform is designed so that security teams can operate simply and efficiently to protect their organizations. The platform prevents successful attacks and stops attacks in progress while providing consistent protection to secure the enterprise, the cloud, and the future. Rooted in prevention, the Security Operating Platform is designed and purpose-built to counter attacks before they can breach an organization's environment.

The Security Operating Platform's prevention architecture allows organizations to reduce threat exposure by first enabling applications for all users or devices in any location and then preventing threats within application flows, tying application use to user identities across physical, cloud-based, and software-as-a-service (SaaS) environments.

To enable the prevention of successful cyberattacks, the Security Operating Platform delivers four key capabilities:

1. **Provide full visibility.** To understand the full context of an attack, visibility of all users and devices is provided across the organization's network, endpoint, cloud, and SaaS applications.

2. **Reduce the attack surface.** Best-of-breed technologies that are natively integrated provide a prevention architecture that inherently reduces the attack surface. This type of architecture allows organizations to exert positive control based on applications, users, and content, with support for open communication, orchestration, and visibility.

3. **Prevent all known threats, fast.** A coordinated security platform accounts for the full scope of an attack, across the various security controls that compose the security posture, enabling organizations to quickly identify and block known threats.

4. **Detect and prevent new, unknown threats with automation.** Building security that simply detects threats and requires a manual response is too little, too late. Automated creation and delivery of near-real-time protections against new threats to the various security solutions in the organization's environments enable dynamic policy updates. These updates are designed to allow enterprises to scale defenses with technology, rather than people.

Security should not be a barrier to the adoption of new mobility, SaaS, public, or private cloud technologies that enable productivity. With a natively integrated, prevention-first security platform in place, organizations can securely adopt innovative, productivity-enhancing applications and technologies, all while maintaining a comprehensive and consistent prevention-oriented enterprise security posture.

Conclusion

Palo Alto Networks is helping to address the world’s greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, Palo Alto Networks is at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices.

Palo Alto Networks’ broad portfolio of security technologies and solutions address three essential areas of cybersecurity strategy:

Secure the Enterprise (Strata):

Palo Alto Networks’ PA-Series, VM-Series, and K2-Series next-generation firewalls are the cornerstone of enterprise network security. Powered by PAN-OS® software, these next-generation firewalls leverage App-ID, User-ID, and Content-ID to provide complete visibility and control of the applications in use across all users, devices, and locations.

Cloud-based subscription services, including DNS Security, URL Filtering, Threat Prevention, and WildFire® malware prevention, deliver real-time advanced predictive analytics, AI and machine learning, exploit/malware/C2 threat protection, and global threat intelligence to the Palo Alto Networks Security Operating Platform.

Panorama network security management enables centralized control, log collection, and policy workflow automation across all your next-generation firewalls (scalable to tens of thousands of firewalls) from a single pane of glass.

Secure the Cloud (Prisma):

Prisma Cloud is the industry’s most comprehensive threat protection, governance, and compliance offering. It dynamically discovers cloud resources and sensitive data across AWS, GCP, and Azure to detect risky configurations and identify network threats, suspicious user behavior, malware, data leakage, and host vulnerabilities. It eliminates blind spots across your cloud environments and provides continuous protection with a combination of rule-based security policies and class-leading machine learning.

Prisma Access (SASE) helps your organization deliver consistent security to your remote networks and mobile users. It's a generational step forward in cloud security, using a cloud-delivered architecture to connect all users to all applications. All of your users, whether at your headquarters, in branch offices, or on the road, connect to Prisma Access to safely use cloud and data center applications, as well as the internet. Prisma Access consistently inspects all traffic across all ports and provides bidirectional software-defined wide-area networking (SD-WAN) to enable branch-to-branch and branch-to-headquarters traffic.

Prisma SaaS functions as a multimode cloud access security broker (CASB), offering inline and API-based protection working together to minimize the range of cloud risks that can lead to breaches. With a fully cloud-delivered approach to CASB, you can secure your SaaS applications through the use of inline protections to safeguard inline traffic with deep application visibility, segmentation, secure access, and threat prevention, as well as API-based protections to connect directly to SaaS applications for data classification, data loss prevention, and threat detection.

Secure the Future (Cortex):

Cortex XDR breaks the silos of traditional detection and response by natively integrating network, endpoint, and cloud data to stop sophisticated attacks. Taking advantage of machine learning and AI models across all data sources, it identifies unknown and highly evasive threats from managed and unmanaged devices.

Cortex XSOAR is the only security orchestration, automation, and response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle.

Cortex Data Lake enables AI-based innovations for cybersecurity with the industry's only approach to normalizing your enterprise's data. It automatically collects, integrates, and normalizes data across your security infrastructure. The cloud-based service is ready to scale from the start, eliminating the need for local compute or storage, providing assurance in the security and privacy of your data.

AutoFocus contextual threat intelligence service speeds your ability to analyze threats and respond to cyberattacks. Instant access to community-based threat data from WildFire, enhanced with deep context and attribution from the Palo Alto Networks Unit 42 threat research team, saves time. Your security teams get detailed insight into attacks with prebuilt Unit 42 tags that identify malware families, adversaries, campaigns, malicious behaviors, and exploits without the need for a dedicated research team.