

The Palo Alto Networks Portfolio

As a business, you want to secure your users, applications, data, devices, and networks with future-proof solutions in the most cost-efficient way, no matter where they are. As a result, you're likely investing in individual products for each security challenge that your team must deploy, manage, and manually stitch together alerts and insights for actionable intelligence.

Palo Alto Networks was founded to solve this age-old problem. We provide the most comprehensive set of security solutions to secure your entire IT landscape.

With our **CLOUD-DELIVERED SECURITY SERVICES**, our customers get the most advanced range of prevention against exploits, malware, web-based threats, insider threats, data loss, and applications. These services continuously improve via the network effect and are backed by Unit 42's threat research to automatically deliver protection across all threat vectors faster than threats can propagate.

Our **ML-POWERED NGFWs** are industry leading, leveraging machine learning for proactive real-time and inline zero-day protection, and operating as sensors and enforcement points for our security services. We provide flexible consumption choices—hardware, software, containerized, and cloud-delivered—to keep campuses, data centers, uCPE and private, hybrid and public cloud environments covered. All form factors can be managed centrally through a single pane of glass with Panorama™.

PRISMA™ ACCESS, the most comprehensive SASE solution of its kind, secures access, protects users and applications, and controls data for remote users and locations.

Our **SD-WAN** solution provides all the networking services that an enterprise environment needs—from the branch to the edge—by removing the need for locally deployed networking and security point products.

PRISMA™ CLOUD secures any cloud environment and all compute form factors used to build and run cloud native applications, including multi- and hybrid-clouds environments. Prisma Cloud addresses the majority of cloud security use cases a customer might have, such as CSPM, containers, serverless, and identity-based microsegmentation.

For threats that couldn't be stopped in real-time, **CORTEX XDR™** aggregates the data collected from sensors across the infrastructure, applying machine learning behavioral analytics to profile endpoint, network, and user behavior to automatically detect attacks and quickly stop them from spreading.

CORTEX™ XSOAR enables security teams to ingest alerts from multiple sources, including third party sources, and executes standardized, automated playbooks for accelerated incident response. With Cortex XSOAR, security teams can effectively and efficiently carry out incident response, allowing them to focus on more critical actions.

The Palo Alto Networks portfolio secures all users, applications, data, networks, and devices with comprehensive context at all times, across all locations. Our portfolio delivers better prevention and security from a smaller set of products. It deploys, manages and addresses the broadest set of security problems, resulting in improved ROI, maximized operational efficiency, simplified management, centralized policy management, seamless access to applications regardless of location, and support for ever increasing throughput demands.

With the right portfolio, security can be seen as an enabler that grows and innovates alongside the business.