Cortex™ is the industry’s only open and integrated AI-based continuous security platform that constantly evolves to stop the most sophisticated threats.
Cortex

AI-Based Continuous Security Platform

Cortex™ delivers radical simplicity and significantly improves security outcomes through automation and unprecedented accuracy. The platform uses rich data from tightly integrated sensors across your enterprise to enable new apps from Palo Alto Networks and third-party Cortex partners. Cortex constantly evolves to deliver disruptive new innovations for security, analytics, and automation. You can recoup time to solve unique and complex problems by automating significant parts of your IT and security operations.

Cortex Data Lake

Cloud-Based Data Collection, Storage, and Analysis Service

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. Cortex Data Lake enables you to effortlessly apply advanced AI and machine learning with cloud-scale data and compute. With trillions of multi-source artifacts for analytics, and by constantly learning from new data sources, Cortex Data Lake significantly improves the accuracy of security outcomes.

Cortex XDR

Cloud-Based Detection and Response

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 XDR speeds alert triage and incident response by providing a complete picture of any threat, revealing the root cause automatically. By stitching together different types of data and simplifying investigations, Cortex XDR reduces the time and experience required at every stage of security operations, from alert triage to threat hunting. Tight integration with enforcement points lets you quickly respond to threats and apply the knowledge gained from investigations to greatly reduce the surface area of risk through continual use.

AutoFocus

Contextual Threat Intelligence

AutoFocus™ is a contextual threat intelligence service that 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 our Unit 42 threat research team, saves time. Your security teams get detailed insight into attacks with pre-built Unit 42 tags that identify malware families, adversaries, campaigns, malicious behaviors, and exploits without the need for a dedicated research team.

AutoFocus improves the speed and precision of attack response by automatically surfacing high-impact threats and indicators to help you prioritize investigations. Automated protection delivered to your Next-Generation Firewalls makes it simple to turn raw intelligence into realtime enforcement across your environment. AutoFocus can organize third-party threat intelligence feeds and share relevant indicators using MineMeld™, a threat intelligence syndication engine hosted in AutoFocus. Security teams can instantly enrich third-party tools and SIEMs with an easy-to-use API for access to collected intelligence. With all in-house and third-party data consolidated in one system, you can quickly investigate, correlate, and pinpoint malware’s root cause without adding dedicated malware researchers or more tools.

Demisto

Security Orchestration, Automation, and Response (SOAR)

Demisto Enterprise 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. Demisto’s orchestration enables security teams to ingest alerts across sources and execute standardized, automated playbooks for accelerated incident response. Demisto’s playbooks are powered by hundreds of integrations and thousands of security actions, striking the right balance between rapid machine execution and nuanced human oversight. These playbooks are further complemented by realtime investigation capabilities so security teams can rapidly iterate to solve emergent threats. Each incident in Demisto has a war room view, which is a shared collaborative workspace where analysts can chat with each other, run commands in realtime, and have their actions documented for future learning. Fully customizable summaries, dashboards, and reports ensure complete visibility across the attack lifecycle. With Demisto, security teams can future-proof security operations to reduce mean time to respond, maintain consistent incident management processes, and increase analyst productivity.