AT A GLANCE
THREAT PREVENTION

Organizations face a frequent barrage of attacks by threat actors around the world who are looking to make a profit. Attackers' tactics continue to evolve, and security products must keep pace to effectively protect organizations. Palo Alto Networks® has built an entirely new way to detect advanced threats and automatically stop them in their tracks.

Prevention at Every Stage of the Attack Lifecycle

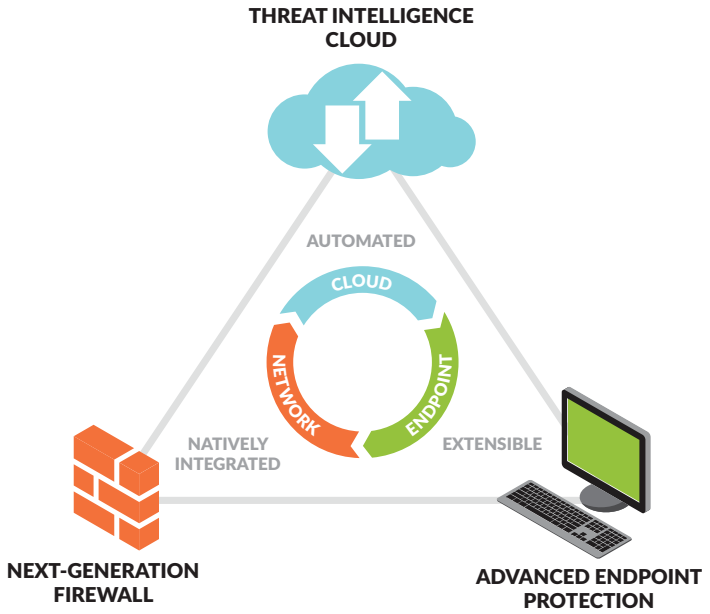
In order to prevent an attack at each stage of its lifecycle and shut down advanced threats, we built threat prevention services into the Next-Generation Firewall component of our Next-Generation Security Platform, which are central to our proactive, prevention-oriented approach. Our natively integrated security platform brings network, cloud and endpoint security into a common architecture, with complete visibility and control, ensuring your organization can detect and prevent attacks.

Threat Prevention is integrated into the single-pass architecture of our NGFW and provides coordinated protection against intrusion, malware and command-and-control activities by whittling down the number of attack vectors into an organization. We've also re-engineered the way threat intelligence is leveraged. In addition to informing customers of new threats, WildFire™ cloud-based malware analysis takes it a step further by automatically creating protections and distributing them to all security products in your organization within minutes, protecting your network against the latest attacks. Our platform streamlines day-to-day operations and boosts security efficacy; and the one-of-a-kind, multilayered defense model prevents threats at each stage of the attack lifecyle.

For effective and coordinated protection, we recommend deploying Threat Prevention with WildFire and URL Filtering.

Threat Prevention Highlights

- Prevents a wide variety of threats, including vulnerability exploits, malware and botnets
  - Detects and prevents threats hidden within SSL-encrypted traffic
  - Outsmarts polymorphic malware by focusing on payload, instead of hash or filename
- Protections are automatically updated every five minutes, making sure your defenses keep pace with the latest attacks (when deployed with WildFire)
- Actionable, correlated forensics and reporting for fast remediation



AT A GLANCE
THREAT PREVENTION

YOU NEED	WE OFFER
Total visibility and assurance that your organization is protected	Because our NGFW provides visibility into and context for all traffic on all ports and protocols, including SSL encryption with App-ID™ and User-ID™, it's able to not only reduce the attack surface in terms of access to applications, data and websites but also scan all traffic into and out of your network for threats. Our proactive approach to security focuses on stopping attacks at every single stage in the attack lifecycle by automatically enforcing security policies.
Defense against targeted attacks	The collective global threat intelligence shared by our community of customers significantly reduces the success rate of advanced attacks by stopping them in as little as five minutes of first being seen. Attacks that use never-before-seen exploits, malware, malicious URLs or CnC channels are analyzed by WildFire. Protections are then created and made available with the threat prevention features on all Palo Alto Networks devices within your network around the globe in as little as five minutes, quickly and automatically keeping your network defenses up to date.*
Comprehensive security for all data, applications and users	We offer flexible deployment options that extend protection against advanced threats to the entire organization, inside and outside the corporate network and at each point of segmentation. We provide comprehensive detection, quick prevention, and customized mitigation consistently across the network, including within the data center via virtualized NGFWs and beyond the confines of the office to mobile and remote users via GlobalProtect™ mobile security, ensuring that your data, applications, and users are protected from threats.
Automated security with less manual work	Once a new threat is detected, protections are automatically created, delivered to the NGFW and Threat Prevention service, and implemented, which reduces the time between detection and prevention to as little as five minutes. In addition, threats and indicators of compromise (IOCs) are easily correlated and reported on, so you know exactly who was compromised and how, without having to dig through multiple logs.*

*Active WildFire and URL Filtering subscriptions are needed.

"PALO ALTO [NETWORKS] HELPS US WITH THE LONG-TERM ABILITIES OF BEING ABLE TO DETECT AND RESPOND TO CURRENT AND FUTURE CYBER THREATS, AS WELL AS MOVING US TO THE LEFT OF THE KILL CHAIN MORE TOWARDS THAT ULTIMATE GOAL OF PREVENTION."

— Paul Carugati

Sr. Manager of Information Security Solutions, Motorola Solutions, Inc.