paloalto NETWORKS®

CLOSING THE LOOP: BENEFITS OF COMBINING NETWORK AND ENDPOINT SECURITY

Integrated network and endpoint security results in seamless coordination, communication and enforcement. Together, they can:

- Detect and prevent known and unknown exploits and malware
- Share threat intelligence across the endpoint, network and cloud
- Coordinate enforcement across the network, endpoint and cloud

Learn more

An integral part of the Palo Alto Networks® Security Operating Platform, WildFire® cloud-based threat analysis service is a keystone to integrating endpoint, network and cloud security, serving as the central prevention orchestration point. With WildFire, you have:

300M newly identified malware samples every month

45% of new malware samples detected by WildFire that are unknown in VirusTotal®

5 minutes to generate automated protections against known threats

When Traps™ – Palo Alto Networks advanced endpoint protection offering – is integrated with next-generation firewalls in conjunction with WildFire, the results are:

100% block rate against exploits, malware and offline attacks*

0% false positives*

$1.7M in breach avoidance costs**

1.52 fewer hours per incident spent on incident response**

$4.7M in security management savings**

Learn more

Traps, deployed in concert with next-generation firewalls, converts endpoints into sensors and enforcement points with a prevention-first approach that minimizes the impact of attacks.

To learn more about combining network and endpoint security for your organization, read "Network and Endpoint Security: Working together to deliver greater visibility, protection, and enforcement."

*Results from the December 2017 Breach Prevention Systems Test Report by NSS Labs®

**Data based on a three-year Total Economic Impact™ (TEI) study of the Security Operating Platform conducted by Forrester® Consulting