Better Together: Deliver Extended Protection Against Advanced Threats

Key Benefits

- Deliver coordinated detection and protection throughout network, endpoint, cloud, email, and social media platforms.
- Provide unified threat intelligence across different attack vectors
- Implement the joint solution easily, at no additional cost.

Proofpoint and Palo Alto Networks customers can now capitalize on unprecedented protection against today's sophisticated attacks

New forms of sophisticated cybersecurity threats continually emerge to target enterprises in new ways, utilizing multiple attack vectors. That is why Proofpoint and Palo Alto Networks are uniting forces in a partnership to help customers deliver unprecedented protection from and intelligence into the sophisticated attacks targeting their people and data. This caliber of protection is only possible by combining best-of-breed security solutions with an enriched blend of threat intelligence spanning network, endpoint, cloud, email, and social media platforms.

Solution Components

Palo Alto Networks WildFire

As new threats emerge, Palo Alto Networks next-generation security platform automatically routes suspicious files and URLs to WildFire™ for deep analysis. WildFire inspects millions of samples per week from its global network of customers and threat intelligence partners, looking for new forms of previously unknown malware, exploits, malicious domains, and outbound command and control activity.

WildFire matches any forwarded samples against its database of known files and detonates never-before- seen items for further investigation, which covers static and dynamic analysis against multiple OS and application versions. WildFire looks for malicious behaviors and populates a verdict and behavioral report. In response to a "malicious" verdict, it also automatically generates malware, URL, and DNS signatures and distributes them to all WildFire-subscribed Palo Alto Networks platforms globally within minutes to immediately halt threats from spreading in their environments, without requiring any additional user action. Indicators of compromise (IoC) information from WildFire analysis reports are used by the NGFW and technology partners to identify infected hosts and prevent secondary download.

This closed-loop, automated process gives organizations the assurance that their networks, endpoint and cloud are armed with the absolute latest threat intelligence

Proofpoint Targeted Attack Protection

Proofpoint Targeted Attack Protection (TAP) helps organizations detect, block, and respond to known and unknown advanced threats that target people through malicious attachments and URLs in email. Email continues to be a powerful threat vector for attackers to reach people and the companies they represent, as today's threat landscape is plagued with polymorphic malware, weaponized documents, and credential phishing attacks. TAP uses sophisticated analysis techniques and seamlessly integrates with the Proofpoint secure email gateway to deliver best-in-class email security in a way that is cost-effective, easy-to-use, and cloud-based.

Proofpoint SocialPatrol

Proofpoint SocialPatrol provides advanced protection for companies, customers, and brands across all major social networks, including Facebook, Instagram, Twitter, LinkedIn, Google+, and YouTube. Companies devote significant resources to social media marketing, and hackers follow the money. The average enterprise has 178 social media accounts, making it very complex to manage security and avoid costly compliance violations.

Using patent-pending technology, SocialPatrol empowers organizations to stop hackers from defacing their brands by locking corporate-owned social media accounts, prevent security incidents by blocking malware and phishing attacks, manage compliance and acceptable use requirements by removing inappropriate content, and prevent unauthorized publishing by controlling connected applications.

Palo Alto Networks + Proofpoint

This integration aligns threat knowledge between the two companies in real-time, providing joint customers with increased visibility and synchronized protection to effectively combat today's advanced threats. Joint customers can rapidly integrate Palo Alto Networks WildFire with either or both Proofpoint Targeted Attack Protection (TAP) and Proofpoint SocialPatrol in a matter of minutes with a simple API key-based activation.

The integration of Proofpoint TAP and Palo Alto Networks WildFire, a key component of the Palo Alto Networks security platform, ensures that potentially malicious email attachments are delivered to both companiesfor analysis, enabling automated protection across the Proofpoint secure email gateway and Palo Alto Networks Next-Generation Security Platform that delivers network, cloud and endpoint security. When TAP inspects an email attachment with unknown reputation, the file will be sent to both the Proofpoint TAP sandbox as well as Palo Alto Networks WildFire for analysis. Both solutions will derive threat intelligence and return a verdict. If either solution condemns the file then TAP will block or track the message based on the configured policy, providing immediate protection and notification to customers while WildFire automatically generates new protections and distribute them to all WildFire subscribed platforms globally preventing the spread of the attack. WildFire threat intelligence reports can be seen directly from the TAP dashboard providing security teams consolidated visibility into the attack across multiple control point in their organization.

For the Wildfire and SocialPatrol integration, links posted on social media accounts monitored by SocialPatrol can be sandboxed by WildFire. Malicious links can then be enforced by the customer's policies configured in Proofpoint SocialPatrol, including the ability to automatically delete malicious content or notifying an administrator to take action. With this integration customers are now protected from both known and unknown URL threats on social media platforms from the threat intelligence provided by the WildFire cloud.

With shared threat intelligence and coordinated protection between Palo Alto Networks and Proofpoint, the next time the same threat appears anywhere – regardless of the attack vector – it will be easily detected and quickly prevented.

892 Ross Drive
Sunnyvale, CA 94089

1.408.517.4710
www.proofpoint.com