proofpoint.

SOLUTION BRIEF

Proofpoint and Palo Alto Networks Partnership Cross-Platform Protection Against Today's Attacks

Products

- Proofpoint Targeted Attack Protection (TAP)
- Palo Alto Networks WildFire

Key Benefits

- Detect and stop advanced email threats containing malicious attachments
- Achieve multi-layered threat protection
- Use best-of-breed threat intelligence sharing

Over 90% of threats originate through the email vector.[1] Companies are struggling to protect against these advanced threats that target their organizations. Companies need a comprehensive solution to mitigate and reduce risk. Proofpoint and Palo Alto Networks have partnered to give shared customers an enhanced security posture—from email to the network and even the cloud.

Proofpoint and Palo Alto Networks

Proofpoint helps you stay ahead of attackers. With an innovative approach it detects, analyzes and blocks advanced threats before it reaches your users. Proofpoint uses both static and dynamic techniques to continually detect and adapt to new attack patterns.

We analyze potential threats using multiple approaches that examine:

- Behavior
- Code
- Protocol

This helps detect threats early in the attack chain. And potentially before they do any damage. We use sandboxing to study a wide variety of attacks. Attacks include the use of malicious attachments and URLs to install malware or trick users into sharing sensitive information. We also use analyst-assisted execution. It maximizes detection and intelligence extraction.

1 Verizon, "Cost of a Data Breach Investigations Report." July 2020.

Palo Alto Networks' 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. It looks for new forms of previously unknown:

- Malware
- Exploits
- Malicious domains
- Outbound command and control activity

WildFire matches any forwarded samples against its database of known files. And it detonates never-before-seen items for further investigation. It covers static and dynamic analysis against multiple OS and application versions. In response to a "malicious" verdict, it automatically generates malware, URL and DNS signatures. And it distributes it to all WildFire subscribed Palo Alto Networks platforms globally within minutes. Plus it immediately halts threats from spreading in their environments without requiring any additional user action.

Palo Alto Networks and Proofpoint have joined forces in a strategic partnership. It provides platform-to-platform intelligence sharing. It protects against today's targeted threats. So you get additional security benefits and expanded visibility at no additional cost.

How the integrations work

Multi-layer protection for email

When an email that contains an unknown attachment is sent to a customer, Proofpoint Targeted Attack Protection (TAP) will begin its sandbox analysis to determine if it is malicious. At the same time, TAP will also send that attachment to Palo Alto Network's WildFire for simultaneous inspection. If either solution condemns the attachment, it will be blocked from ever reaching the user. If WildFire finds the attachment to be malicious, it will take that file hash and add it to Palo Alto Network's Next-Generation Firewall, Advanced Endpoint Protection and Threat Intelligence Cloud. So by using two best-of-breed solutions to prevent malicious attachments arriving to users, you get the protection you need to stay ahead of the threat landscape. This multi-vendor analysis provides joint customers enhanced protection to stay ahead of the threat landscape.

Multi-layer protection for social media

Social media is a great way to promote your products and interact with customers. But as you expand your social media presence, you also increase your exposure to offensive content and security threats. Proofpoint Digital Risk Protection secures your social media accounts with automated, real-time protection against:

- Hacks
- Phishing
- Malicious content

When we identify a social post contains a URL, we use our sandboxing analysis as well as submit it to Palo Alto WildFire for analysis and verdict. From there, malicious posts are deleted by Digital Risk Protection based on policies.

Proofpoint and Palo Alto Networks give you a closed-loop, automated process to assure you that you are armed with the latest threat intelligence. This reduces the risk of data breaches caused by targeted attacks.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.