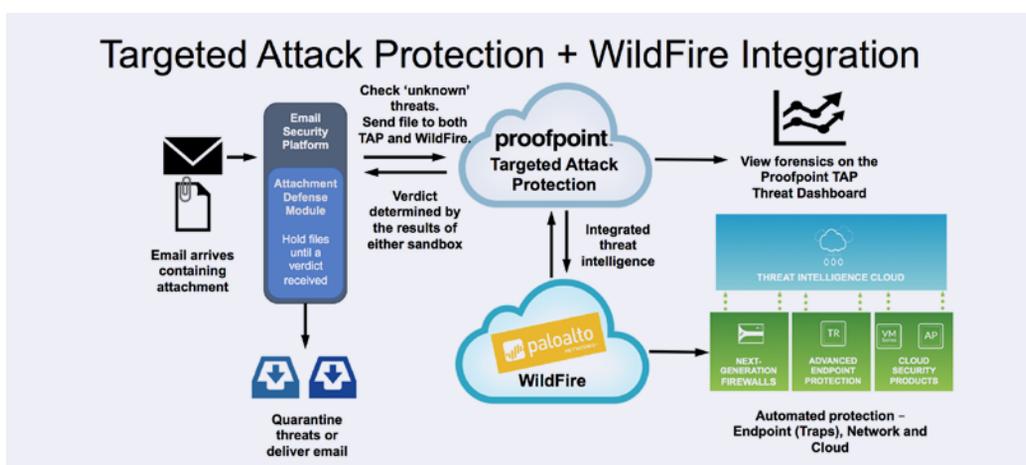


Doppelt genäht hält besser

Die automatisierte Integration der Sicherheitsplattformen von Palo Alto Networks und Proofpoint ermöglicht einen bisher unerreichten Schutz gegen hochentwickelte Cyberbedrohungen – im Firmennetzwerk, beim E-Mail-Verkehr und auf Social Media.



Palo Alto Networks und Proofpoint bieten gemeinsam einen durchgängigen End-to-End-Schutz.

Cyberbedrohungen mit hochentwickelten Angriffsvektoren und unterschiedlichen Wegen sind auf dem Vormarsch. Unternehmen, Mitarbeitende und bestimmte Datenbestände geraten immer gezielter unter Beschuss – vor allem auch via E-Mail und über Social-Media-Plattformen.

Best-of-Breed bietet tiefgehenden Schutz

In der Regel sorgen unterschiedliche Security-Lösungen für die allgemeine Netzwerksicherheit und für den Schutz der E-Mail-Kommunikation sowie von Social-Media-Accounts. Zudem werden typischerweise weitere dedizierte Plattformen – so z. B. zum Schutz der Endgeräte vor Malware – eingesetzt. Die Crux dabei: Unterschiedliche Sicherheitslösungen arbeiten meist nicht optimal zusammen. Sie beinhalten beispielsweise eigene Dashboards und ein proprietäres Reporting. Zudem verbleiben Erkenntnisse über die entdeckten Bedrohungen – die «Indicators of Compromise» – in der Sphäre der jeweiligen Lösung. Ein automatisierter Informationsaustausch ist nicht vorgesehen.

Um diesen Engpass zu beseitigen, haben Palo Alto Networks (PAN) und Proofpoint, zwei auf ihren Gebieten weltmarktführende Security-Anbieter, ihre Kräfte gebündelt. Nun sorgt eine einzigartige, automatisierte Integration der komplementären Best-of-Breed-Lösungen für ein Höchstmass an Sicherheit. Dank des nahtlosen Teilens der jeweiligen Bedrohungsinformationen

entsteht ein durchgängiger End-to-End-Schutz über das Firmennetzwerk, die Endgeräte, die Cloud sowie E-Mail- und Social-Media-Plattformen hinweg.

Grundlage für die enge Integration bildet das Application Framework von Palo Alto Networks. Dieses bietet klar definierte APIs, über die sich andere Lösungen mit der PAN-Plattform verbinden können. Neben Proofpoint umfasst das Ökosystem derzeit über 30 weitere Hersteller.

Nahtlos integriert, clever kombiniert

Bei der Kombination von Palo Alto Networks und Proofpoint stehen vier Komponenten im Vordergrund:

- Die Next-Generation-Firewall von PAN sorgt für einen umfassenden Perimeterschutz.
- Unterstützung leistet dabei die cloudbasierte Malware-Analyseplattform WildFire.
- Targeted Attack Protection (TAP) von Proofpoint deckt Bedrohungen durch schädliche Anhänge und Links in E-Mails ab. Dabei integriert sich TAP nahtlos in den Secure E-Mail Gateway Proofpoint Protection Server (PPS), lässt sich jedoch auch als Stand-alone-Lösung nutzen.
- Bei Bedarf unterstützt eine weitere Proofpoint-Lösung namens SocialPatrol den Schutz von Unternehmen auf Social-Media-Plattformen – dies u. a. durch das Blockieren von Malware- und Phishing-Angriffen sowie durch das Entfernen unerwünschter Inhalte.

So funktioniert's

Das folgende Beispiel veranschaulicht die Funktionsweise der integrierten Sicherheitsumgebung:

Eine E-Mail-Nachricht trifft am PPS ein. TAP leitet eine Kopie der Anhänge und mögliche Links sowohl an die TAP-Sandbox als auch an WildFire weiter. Sobald beide Plattformen ihre Beurteilung abgegeben haben, wird die Nachricht entweder in Quarantäne gestellt, gelöscht oder zum Empfänger geschickt. Neu erkannte Bedrohungen legt WildFire in seiner Cloud-Datenbank ab, wo sie allen weltweit angeschlossenen Kunden zur Verfügung stehen. Die kombinierten Bedrohungsinformationen von TAP und WildFire sind darüber hinaus auf dem TAP-Dashboard ersichtlich und werden ans Threat-Response-Netzwerk von Proofpoint übermittelt. Dies alles geschieht vollautomatisch und in Echtzeit.

Proofpoint und Palo Alto Networks: die Highlights

- Umfassender Cyberschutz durch Best-of-Breed-Ansatz
- Automatisierte Integration von Netzwerk- und E-Mail-Sicherheit
- Schutz vor fortgeschrittenen E-Mail-Bedrohungen
- Brand Protection für Facebook, Instagram, LinkedIn, Twitter etc.
- Mehr Sicherheit durch zweifache Prüfung
- Kombinierte End-to-End-Sichtbarkeit aller Bedrohungen
- Einheitliches Reporting für beide Plattformen
- Integration einfach einzurichten
- Keine Zusatzkosten für Kunden beider Anbieter

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch