# Zusammen besser: Erweiterter Schutz gegen hochentwickelte Bedrohungen

Vorteile:

- Koordinierte Erkennung und Schutz für das ganze Netzwerk, alle Endpoints, die Cloud, E-Mail und Social-Media-Plattformen
- Vereinte Bedrohungs-informationen für verschiedene Angriffsvektoren
- Einfache Implementierung der gemeinsamen Lösung ohne zusätzliche Kosten

## Kunden von Proofpoint und Palo Alto Networks profitieren nun von einem noch nie dagewesenen Schutz gegen die hochentwickelten Bedrohungen von heute.

Es entstehen ständig neue Formen fortgeschrittener Cyber-Bedrohungen, mit denen Unternehmen auf neuen Wegen und über mehrere Angriffsvektoren gezielt unter Beschuss genommen werden. Aus diesem Grund haben sich Proofpoint und Palo Alto Networks zusammengeschlossen und Ihre Kräfte gebündelt: Gemeinsam liefern wir unseren Kunden einen beispiellosen Schutz und Informationen über die fortgeschrittenen Angriffe, die gegen Personen und Daten gerichtet sind. Ein solches Schutzkaliber ist nur möglich durch die Kombination von Best-of-Breed-Sicherheitslösungen mit einer reichhaltigen Mischung aus Bedrohungs-informationen, die sich über das Netzwerk, Endgeräte, die Cloud, E-Mail und Social-Media-Plattformen erstrecken.


## Komponenten der Lösung

### Palo Alto Networks WildFire

Wenn neue Bedrohungen entstehen, leitet die Next-Generation Security Platform von Palo Alto Networks verdächtige Dateien und URLs automatische an WildFire™ zur eingehenden Analyse. WildFire untersucht wöchentlich Millionen Proben aus seinem globalen Netzwerk von Kunden und Threat-Intelligence-Partnern und ist stets auf der Suche nach neuen Formen bisher unbekannter Malware, Exploits, schadhaften Domains und ausgehenden Command-and-Control-Aktivitäten. WildFire gleicht alle weitergeleiteten Proben mit seiner Datenbank an bekannten Dateien ab. Bislang unbekannte Objekte werden in sicherer Umgebung für weitere Untersuchungen wie statische und dynamische Analysen in verschiedenen Betriebssystem- und Anwendungsversionen ausgeführt. WildFire sucht nach schädlichen Verhaltensweisen und erstellt eine Bewertung sowie einen Verhaltens-bericht. Lautet die Bewertung „schädlich“, so werden automatisch Malware-, URL- und DNS-Signaturen erzeugt und an alle Palo Alto Networks-Plattformen verteilt, auf denen WildFire genutzt wird, und zwar weltweit und innerhalb weniger Minuten. So wird sofort verhindert, dass sich Bedrohungen in den Umgebungen ausbreiten, ohne dass der Benutzer tätig werden muss. Informationen der Indicators-of-Compromise (IoC) aus den WildFire-Analyseberichten werden von der Next-Generation Firewall (NGFW) und Technologiepartnern genutzt, um infizierte Hosts zu erkennen und sekundäre Downloads zu verhindern. Dieser ganzheitlich, automatisierte Prozess gibt Unternehmen die Gewissheit, dass ihre Netzwerke, Endpunkte und Cloud-Umgebungen mit der absolut neuesten Threat Intelligence ausgestattet sind.

### Proofpoint Targeted Attack Protection

Proofpoint Targeted Attack Protection (TAP) hilft Organisationen beim Erkennen, Blockieren und Reagieren auf bekannte und unbekannte Bedrohungen, in schädlichen Anhängen und URLs in E-Mails. E-Mail ist nach wie vor ein starker Bedrohungsvektor, über den Mitarbeiter und Unternehmen angegriffen werden können, da bei der aktuellen Bedrohungslage polymorphe Malware, zu Waffen umfunktionierten Dokumenten und Phishing-Angriffe nach Anmeldedaten zum Einsatz kommen. TAP nutzt ausgereifte Analysemethoden und integriert sich nahtlos in das sichere E-Mail-Gateway von Proofpoint. So liefert es die beste E-Mail-Sicherheit in seiner Klasse, und zwar kosteneffektiv, benutzerfreundlich und cloudbasiert.

### Proofpoint SocialPatrol

Proofpoint SocialPatrol bietet erweiterten Schutz für Unternehmen, Kunden und Marken in allen wichtigen sozialen Netzwerken wie Facebook, Instagram, Twitter, LinkedIn, Google+ und YouTube. Unternehmen wenden erhebliche Summen für ihr Social-Media-Marketing auf, und Hacker folgen dem Geld. Das Durchschnittsunternehmen hat 178 Social-Media-Konten, was die Wahrung der Sicherheit und die Vermeidung kostspieliger Compliance-Verstöße zu einer komplexen Angelegenheit macht.

Mithilfe der zum Patent angemeldeter Technologie stattet SocialPatrol Organisationen mit den nötigen Mitteln aus, um Hacker von der Schädigung ihrer Marken abzuhalten: Unternehmenseigene Social-Media-Accounts lassen sich sperren, Sicherheitsvorfälle werden durch das Blockieren von Malware und Phishing-Angriffen verhindert, Compliance und Nutzungsrichtlinien werden durch das Entfernen unerwünschter Inhalte durchgesetzt und unberechtigte Veröffentlichungen werden durch die Kontrolle verbundener Anwendungen verhindert.

## Palo Alto Networks und Proofpoint

Dieser Zusammenarbeit vereint das Bedrohungswissen  beiden Unternehmen in Echtzeit und bietet gemeinsamen Kunden mehr Transparenz und einen synchronisierten Schutz zur effektiven Bekämpfung der heutigen modernen Bedrohungen. Gemeinsame Kunden können Palo Alto Networks WildFire zügig in Proofpoint Targeted Attack Protection (TAP) und/oder Proofpoint SocialPatrol integrieren – innerhalb von Minuten mit einer einfachen Aktivierung per API-Schlüssel.

Proofpoint TAP und Palo Alto Networks WildFire, eine Schlüsselkomponente der Palo Alto Networks-Sicherheitsplattform, sorgen gemeinsam dafür, dass potenziell gefährliche E-Mail-Anhänge zur Analyse an beide Unternehmen geleitet werden. So entsteht für das Proofpoint E-Mail-Gateway und die Palo Alto Networks Next-Generation Security Platform ein automatisierter Schutz, der Sicherheit für Netzwerke, Cloud und Endgeräte liefert. Wenn TAP einen E-Mail-Anhang mit unbekannter Reputation untersucht, wird die Datei sowohl an die Proofpoint TAP-Sandbox als auch an Palo Alto Networks WildFire zur Analyse gesendet. Beide Lösungen leiten Bedrohungs-informationen ab und werten diese aus. Sollte mindestens eine der Lösungen die Datei als schädlich einstufen, wird TAP die Nachricht entsprechend der konfigurierten Richtlinie blockieren oder nachverfolgen. Es besteht ein sofortiger Schutz. Die Kunden werden benachrichtigt, während WildFire automatisch neue Schutzmaßnahmen erzeugt und diese weltweit an alle Plattformen verteilt, auf denen WildFire genutzt wird. Eine Ausbreitung des Angriffs wird damit verhindert. Die WildFire-Bedrohungsdatenberichte können direkt im TAP-Dashboard aufgerufen werden und geben Sicherheitsteams einen konsolidierten Überblick über den Angriff an mehreren Kontrollpunkten in ihrer Organisation.

Für die Wildfire- und SocialPatrol-Integration können auf Social-Media-Accounts gepostete Links, die mit SocialPatrol überwacht werden, von WildFire in die Sandbox geleitet werden. Schadhafte Links unterliegen dann den Richtlinien der Kunden, die in Proofpoint SocialPatrol konfiguriert wurden. Es besteht die Möglichkeit, schadhaften Content automatisch zu löschen oder einen Administrator zu informieren, der dann weitere Schritte vornimmt. Mit dieser Integration sind Kunden nun vor bekannten und unbekannten URL-Bedrohungen auf Social-Media-Plattformen geschützt – durch die von der WildFire-Cloud bereitgestellten Bedrohungsinformationen.

Mit gemeinsam genutzten Bedrohungsinformationen und einem koordinierten Schutz zwischen Palo Alto Networks und Proofpoint kann dieselbe Bedrohung beim nächsten Auftreten mühelos erkannt und schnell entschärft werden – unabhängig vom Angriffsvektor.

**Über Proofpoint**

Proofpoint Inc. (NASDAQ:PFPT) ist ein führender Security-as –a-Service-Anbieter, mit Schwerpunkt auf cloud basierten Lösungen zum Schutz vor Bedrohungen, Compliance, Archivierung und Governance sowie sichere Kommunikation. Unternehmen weltweit verlassen sich auf die Expertise, die patentierten Technologien und das on-demand Bereitsstellungssystem von Proofpoint, für den Schutz vor Phishing, Malware und Spam, zur Einhaltung von Richtlinien, Verschlüsselung sensibler Informationen und Archivierung und Verwaltung von Nachrichten und kritischen Unternehmensinformationen .

Proofpoint Deutschland
Landsberger Straße 302
80687 München

+49 (0)89 90 405 464
info-germany@proofpoint.com
www.proofpoint.com/de