

# Partnerschaft von Proofpoint und CrowdStrike



## Schutz für Ihre Mitarbeiter und deren Geräte

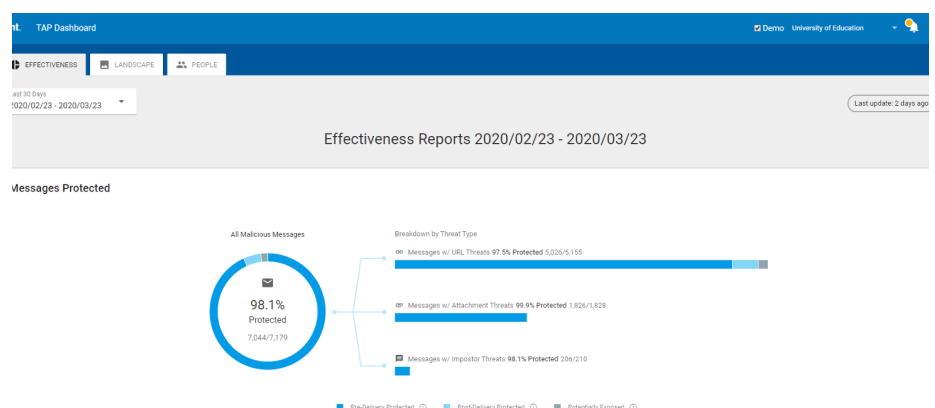
### DIE PARTNERSCHAFT AUF EINEN BLICK

- Austausch erstklassiger Bedrohungsdaten
- Mehrstufiger Schutz vor Bedrohungen
- Schutz von Geräten und Daten vor hochentwickelten Malware-basierten und Malware-losen Angriffen
- Sofortiger Überblick und Kontext zu Angreifern und Angriffsvektoren

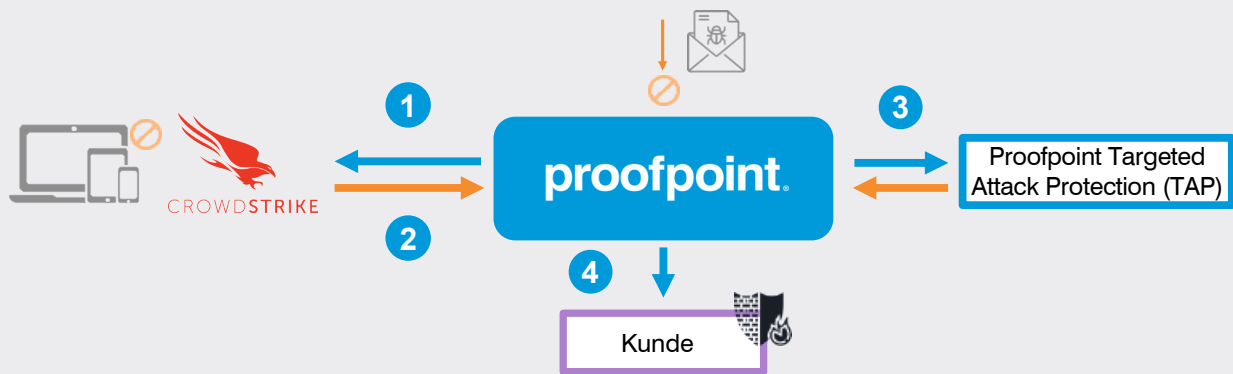
Da Unternehmen weiterhin gezielt mit hochentwickelten Bedrohungen angegriffen werden, sind neue Ansätze zur Minimierung dieser Risiken gefragt. Wir wissen, dass mehr als 90 % aller Cyberangriffe über E-Mails erfolgen. Proofpoint und CrowdStrike arbeiten zusammen, um unseren gemeinsamen Kunden noch mehr Sicherheit zu verhelfen – von E-Mails bis zum eigentlichen Endgerät.

Mit Proofpoint Targeted Attack Protection (TAP) bleiben Sie den Angreifern stets einen Schritt voraus – dank einem innovativen Ansatz, der hochentwickelte Bedrohungen erkennt, analysiert und blockiert, noch bevor sie Ihren Posteingang erreichen. Das umfasst sowohl Ransomware als auch andere hochentwickelte E-Mail-Bedrohungen, die über schädliche Anhänge und URLs übertragen werden. Die Architektur der CrowdStrike Falcon-Plattform setzt auf einen ressourcenschonenden Agenten und Cloud-basierte künstliche Intelligenz (KI) für Echtzeit-Schutz und -Transparenz im gesamten Unternehmen. Mit diesem innovativen Ansatz können Sie solche Bedrohungen zuverlässig abwehren. Sie erhalten einen detaillierten Echtzeit-Überblick über alle Endgeräte-Aktivitäten, sodass Sie Bedrohungen untersuchen und Sicherheitsverletzungen beheben können.

Bei dieser technischen Partnerschaft konzentrieren wir uns auf das gemeinsame Ziel, Menschen und ihre Geräte vor aktuellen raffinierten Bedrohungen zu schützen. Sie profitieren also – ohne Zusatzkosten – von zusätzlicher Sicherheit und erweiterter Transparenz. Außerdem können Sie die Vorteile nutzen, die die Integration dieser erstklassigen Lösungen mit sich bringt.



Proofpoint TAP-Dashboard



- 1 Proofpoint TAP Attachment Defense untersucht die Datei und sendet eine Abfrage an die CrowdStrike Intelligence-API.
- 2 Wenn eine Datei bei CrowdStrike als schädlich bekannt ist, wird sie von Proofpoint TAP in die Quarantäne verschoben und nicht an den Endnutzer übertragen.
- 3 Wenn die Datei bei CrowdStrike unbekannt, bei Proofpoint TAP jedoch als schädlich bekannt ist, wird sie in die Quarantäne verschoben und nicht an den Endnutzer übertragen.
- 4 Durch den Austausch von Bedrohungsdaten wird der Schutz für den Kunden verbessert.

## FUNKTIONSWEISE DER INTEGRATION

### Austausch von Bedrohungsdaten

Durch die Integration ist es möglich, Bedrohungsdaten zwischen Proofpoint TAP und der CrowdStrike Falcon-Plattform auszutauschen. Wenn eine E-Mail mit Anhang an einen gemeinsamen Kunden beider Unternehmen gesendet wird, überprüft Proofpoint TAP mit einer Sandbox-Analyse, ob sie schädlich ist. Gleichzeitig fragt Proofpoint TAP die Reputation der Datei bei CrowdStrike Falcon X ab. Wenn CrowdStrike die Datei als schädlich kennt, wird Proofpoint TAP darüber informiert. Anschließend werden die Nachricht und die Datei in die Quarantäne verschoben und so verhindert, dass sie den Endnutzer überhaupt erreichen. Dieser Austausch der Bedrohungsdaten von zwei erstklassigen Lösungen ermöglicht zuverlässigen Schutz vor hochentwickelten gezielten Angriffen.

### Mehrstufiger Schutz

Um mehrstufigen Schutz zu gewährleisten, tauscht Proofpoint TAP Bedrohungsdaten mit der CrowdStrike Falcon-Plattform aus. Dadurch erhalten Sie und Ihre Mitarbeiter Schutz vor Angriffen über E-Mails und über das eigentliche Endgerät. Wenn TAP eine schädliche Datei erkennt, die per E-Mail übertragen wurde, können wir eine Anfrage an das Bedrohungsdaten-Modul von CrowdStrike Falcon X senden, um festzustellen, ob sie bereits bekannt ist. Wenn der schädliche Inhalt bekannt ist, ist keine Aktion erforderlich, weil das Gerät bereits geschützt wird. Wenn sie noch unbekannt ist, werden die entsprechenden Hash-Informationen zur CrowdStrike-Liste der benutzerdefinierten Kompromittierungsindikatoren (IOCs) hinzugefügt. Gleichzeitig wird eine Warnmeldung generiert, sobald der schädliche Inhalt versucht, sich auf dem Gerät auszuführen. Diese kundenspezifischen Daten werden zu CrowdStrike Falcon X hinzugefügt, damit ähnliche Angriffe auf Endgeräte in Ihrem Unternehmen in Zukunft proaktiv abgewehrt werden können.

Die Integration von Proofpoint und CrowdStrike vereinfacht die Erkennung, Untersuchung und Behebung von E-Mail-Bedrohungen – und schafft eine zusätzliche Schutzebene für Ihr Unternehmen und Ihre Mitarbeiter.

## WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter [proofpoint.com/de](https://www.proofpoint.com/de).

### INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenorientierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter [www.proofpoint.de](https://www.proofpoint.de).

© Proofpoint, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.