

# Proofpoint Targeted Attack Protection URL Isolation for Very Attacked People

## Adaptive Zugangskontrollen für Ihre VAPs

### WICHTIGE VORTEILE

- Isolierung schädlicher URLs bei Firmen-E-Mails durch adaptive, risikobasierte Kontrollen
- Integration in TAP für dynamische, adaptive Kontrollen und Überblick über Ihre VAPs
- Schutz vor Diebstahl und Erfassung von Anmeldedaten
- Nahtloses Surferlebnis für Anwender unter Einhaltung strenger Datenschutzvorschriften
- Anwender können bedenkenlos unbekannte Websites aufrufen, da das Unternehmen zuverlässig geschützt ist

Proofpoint Targeted Attack Protection (TAP) URL Isolation for Very Attacked People (VAP) ermöglicht es besonders häufig angegriffenen Personen, unbesorgt auf unbekannte Websites zuzugreifen. Dadurch schützt die Lösung Unternehmen vor URL- und webbasierten Angriffen. Sie setzt dabei auf eine Cloud-basierte Isolierungstechnologie, um die Angriffsfläche zu verringern, und bietet Schutz vor Phishing- und gezielten Angriffen.

Sie müssen Bedrohungen schon vor der ersten Infektion stoppen, um Angreifer daran zu hindern, die bedeutendste Ressource eines Unternehmens kompromittieren: die Mitarbeiter. Zur effektiven Abwehr von Phishing- und gezielten Angriffen bedarf es einer mehrschichtigen Lösung, die Ihren Anwendern einen ungestörten Ablauf ihrer täglichen Arbeit ermöglicht und Ihr Unternehmen schützt.

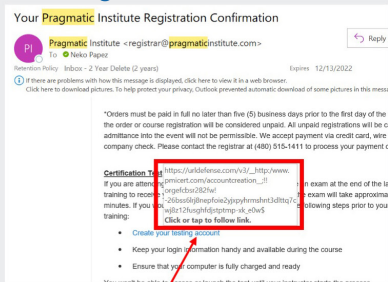
Mit TAP URL Isolation for VAP können Ihre Anwender bedenkenlos unbekannte Websites aufrufen und sind dabei vor URL- und webbasierten Angriffen geschützt. Mit der Integration wird jede URL, auf die Ihre VAPs in geschäftlichen E-Mails klicken, nach konfigurierten Richtlinien analysiert und isoliert. Ihre Mitarbeiter können Websites in geschäftlichen E-Mails bedenkenlos aufrufen, da das Unternehmen zuverlässig geschützt ist.

### Adaptive Isolierungskontrollen für angegriffene Anwender

Durch die Integration mit TAP kann Proofpoint TAP URL Isolation for VAP auch URLs isolieren, die in E-Mails an Ihre besonders gefährdeten Anwender – die VAPs – enthalten sind. Ihre VAP-Liste wird in der Lösung Proofpoint Targeted Attack Protection dynamisch auf Basis der individuellen Bedrohungs- und Risikostufe generiert. Die Integration ermöglicht zudem Phishing-Erkennung und -Scans in Echtzeit.

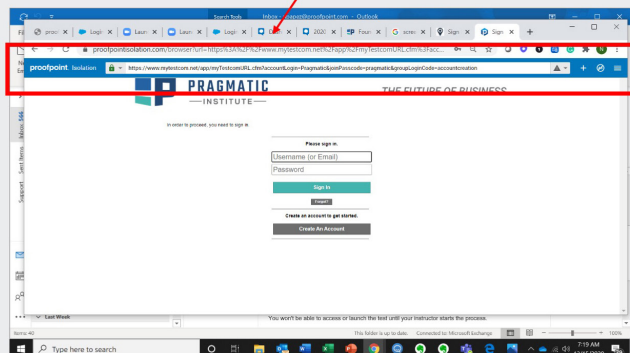
Wenn eine isolierte Browsersitzung gestartet wird, wird dies an das TAP-Dashboard gemeldet, damit Sie neue Bedrohungen aufdecken und das Risiko überwachen können. Die Einbeziehung von adaptiven Kontrollen und TAP ist eine effektive Möglichkeit, das Risiko zu verringern.

## Anwendung adaptiver Isolierungskontrollen auf Ihre VAPs



Jeder Link in Ihren geschäftlichen E-Mails wird automatisch durch Proofpoint URL Defense geändert und in der Isolierungsumgebung geöffnet.

In der Isolierungsumgebung sind Anwender vor Diebstahl von Anmeldedaten und gezielten Angriffen geschützt. Während dieser Zeit sind Upload- und Download-Funktionen gesperrt.



### TAP URL Isolation for VAP

## Überblick über Ihre isolierten Klicks

Für den Schutz Ihres Unternehmens ist es besonders wichtig, dass Sie einen Überblick über Ihre VAPs haben und wissen, auf welche Weise sie angegriffen werden bzw. wann sie mit potenziell schädlichen URLs interagieren. Auf der Bedrohungsdetailseite von Proofpoint TAP sehen Sie jetzt die Zahl der isolierten Klicks. Bei aktiviertem TAP URL Isolation for VAP können Sie nachvollziehen, wie viele Klicks durch die Integration mit der Isolierungstechnologie von Proofpoint TAP geschützt wurden. Sie können außerdem Ihre Richtlinien in der Isolierungskonsole aktualisieren, um noch mehr Klicks vor Kategorien mit hohem Risiko zu schützen.

## Reduzierung der Angriffsfläche mit erweiterten Bedrohungsdaten

Wir isolieren automatisch verdächtige URLs basierend auf zwei prädiktiven Scanmethoden. Bei der ersten Methode handelt es sich um eine Reputationsprüfung, die mit Hilfe des Proofpoint Nexus Threat Graphs feststellt, ob eine bestimmte URL von uns schon als Bedrohung eingestuft wurde. Dabei kommt eine Kombination aus Machine Learning-Funktionen von NexusAI, hochentwickelten Erkennungstechniken und menschlicher Expertise zum Einsatz.

Bei der zweiten Methode wird ein Bedrohungsscans durchgeführt, bei dem der HTML-Code an unser statisches Untersuchungsmodul gesendet wird, um die Seite auf schädliche Inhalte zu prüfen. Zudem werden Dateien oder E-Mail-Anhänge mit Schaddaten oder schädlichen Makros in der isolierten Sitzung gar nicht erst heruntergeladen. Die Eingaben der Anwender werden dynamisch beschränkt, um den Diebstahl von Anmeldedaten über den Browser zu vermeiden. Gleichzeitig werden Downloads blockiert und damit Drive-by-Malware-Angriffe verhindert. Außerdem wird gewährleistet, dass keine schädlichen Webinhalte auf Ihre Endgeräte gelangen. Die Lösung isoliert sogar Inhalte aus vertrauenswürdigen Websites, die kompromittiert wurden.

Unsere Lösung vereinfacht zudem die Einhaltung von Compliance-Vorschriften, weil die isolierten Browsersitzungen vollständig vor Ihrer Umgebung und Ihrem IT-Personal verborgen werden. Dadurch werden jegliche Datenschutzprobleme in Bezug auf die Privatsphäre der Mitarbeiter sowie Compliance-Verletzungen von Anfang an vermieden.

Proofpoint TAP URL Isolation lässt sich einfach implementieren, da es vollständig Cloud-basiert ist. Zudem integriert sich die Lösung problemlos mit Proofpoint Targeted Attack Protection zur Anwendung der adaptiven Isolierungskontrollen auf Ihre VAPs. Dadurch profitieren Sie von geringeren Kosten, höherer Produktivität Ihres IT-Teams und einer gesteigerten Moral unter Ihren Mitarbeitern.

## 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 Unternehmen für Cybersicherheit und Compliance. 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 personenzentrierten 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.