

# PROOFPOINT BROWSER ISOLATION

**SCHUTZ IHRER ANWENDER VOR HOCHENTWICKELTEN BEDROHUNGEN,  
DIE AUF UNTERNEHMENSUMGEBUNGEN UND DAS PRIVATE UMFELD ABZIELEN**

## WICHTIGE VORTEILE

- Isolierung schädlicher URLs in unternehmensbezogenen E-Mails durch risikobasierte Kontrolle
- Isolierung der Browsersitzung bei hochriskanten Websites, z. B. unbekannten oder neuen Domänen
- Schutz vor Diebstahl und Erfassung von Anmeldedaten
- Schnelle und einfache Bereitstellung über die Cloud – keine Hardware oder Endgeräte-Agenten erforderlich
- Nahtloses Surferlebnis für Ihre Mitarbeiter
- Einfache Einhaltung der EU-Datenschutz-Grundverordnung

Der Schutz Ihrer Mitarbeiter vor gezielten Phishing-Angriffen und Anmeldedaten-Diebstahl ist ein endloser Kampf. Die Situation wird dadurch erschwert, dass Angreifer mit schädlichen URLs in groß angelegten Kampagnen schnell die Oberhand gewinnen. Wie können Sie Ihr Unternehmen vor dieser wachsenden Gefahr schützen? Mit Proofpoint Browser Isolation können Ihre Mitarbeiter sicher auf das Internet zugreifen – und werden gleichzeitig vor Malware und Datenverlust geschützt.

## BESCHREIBUNG DES PRODUKTS

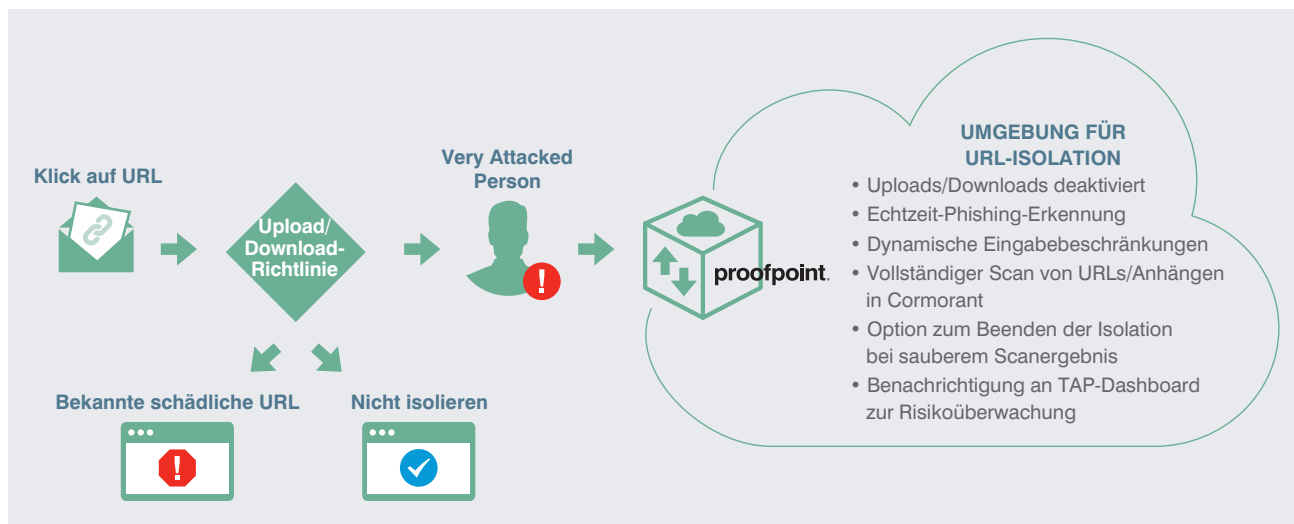
Mit Browser Isolation können Ihre Anwender sicher auf Websites und private sowie unternehmensbezogene E-Mails zugreifen, da die Browsersitzungen in einem sicheren Container isoliert werden. Diese einzigartige Lösung schützt vor Malware und schädlichen Inhalten, indem sie Uploads und Downloads deaktiviert und auf diese Weise den Diebstahl und Verlust vertraulicher Daten verhindert. Browser Isolation behebt die Sicherheits-, Produktivitäts- und Datenschutzprobleme, die durch gezielte Phishing-Angriffe und die Nutzung hochriskanter Websites entstehen. Außerdem profitieren Sie von einfacher Bereitstellung, Verwaltung und Support.

## FUNKTIONEN UND VORTEILE

### **Anpassung der Sicherheit an riskante URLs und angegriffene Anwender**

Angreifer zielen heute mit Phishing-E-Mails auf bestimmte Personen in Ihrem Unternehmen ab. Daher benötigen Sie zusätzliche anpassbare Kontrollen zum Schutz Ihrer am häufigsten angegriffenen Mitarbeiter. Browser Isolation schützt Ihre Mitarbeiter vor schädlichen webbasierten Inhalten in unternehmensbezogenen E-Mails. Mit dieser Lösung werden die Browsersitzungen basierend auf einer Richtlinie isoliert, um Sie und Ihre Mitarbeiter vor hochriskanten URLs zu schützen. Dazu gehören unbekannte URLs, soziale Netzwerke und Online-Cloudanwendungen.

Durch die Integration mit Proofpoint Targeted Attack Prevention (TAP) erhalten aktuelle TAP-Kunden mit Browser Isolation zusätzlich Schutz für unternehmensbezogene E-Mails. Die personenorientierten Kontrollen sind in Kombination mit TAP eine effektive Möglichkeit, das Risiko zu verringern. Basierend auf Risikofaktoren in Ihren unternehmensbezogenen E-Mails können Sie festlegen, welche Anwender für die Isolationsumgebung in Frage kommen. Die Integration mit TAP ermöglicht Echtzeit-Phishing-Erkennung und -Scans. Die Daten zu isolierten Browsersitzungen werden an das TAP-Dashboard gesendet, damit Sie einen vollständigen Überblick erhalten und das Risiko überwachen können.



### Reduzierung Ihrer Angriffsfläche

Wie viele andere Unternehmen erlauben Sie Ihren Mitarbeitern am Arbeitsplatz, private Webmails zu nutzen oder im Internet zu surfen. Angreifer wissen das und nutzen diese Tatsache für raffinierte Angriffe. Laut Untersuchungen resultieren sogar bis zu 60 % aller Angriffe daraus, dass auf Unternehmensgeräten Webmails oder private E-Mails verwendet werden. Wie reduzieren Sie also das Risiko, ohne Ihren Mitarbeitern die Möglichkeit zu nehmen, im Internet zu surfen und private E-Mails zu nutzen?

Mit Browser Isolation können Sie festlegen, dass bestimmte Websites oder Cloudanwendungen isoliert werden. Dadurch können Ihre Mitarbeiter sicher surfen und auf private Webmails zugreifen, während die Sicherheitslage Ihres Unternehmens verbessert wird – ohne jedes Risiko für Ihre Unternehmensressourcen. Es ist nicht notwendig, Dateien zu untersuchen und das Verhalten Ihrer Anwender zu überwachen. Zudem werden Dateien oder E-Mail-Anhänge mit Schadstoffen oder schädlichen Makros gar nicht erst heruntergeladen. Die Lösung isoliert sogar Inhalte aus vertrauenswürdigen Websites, die kompromittiert wurden. Dadurch werden Sie vor Watering-Hole-Angriffen und E-Mail-Links zu manipulierten Cloudanwendungen wie Microsoft SharePoint oder Dropbox geschützt. Dank dynamischer Eingabebeschränkungen wird auch die Gefahr durch browserbasierten Diebstahl von Anmeldedaten verringert. Browser Isolation verhindert außerdem Drive-by-Downloads und gewährleistet, dass keine schädlichen Webinhalte auf Ihre Endgeräte gelangen.

### Reduzierung der Belastung für das IT-Team

Wenn Sie Ihren Mitarbeitern den Zugriff auf nicht kategorisierte URLs und private Webmails erlauben, gehen Sie ein großes Risiko ein. Doch Ihre Mitarbeiter haben häufig gute Gründe, diese Websites aufzurufen. Bei den meisten Lösungen müssen die IT-Teams entscheiden, ob sie diese Websites zulassen oder blockieren. Wenn alle diese Domänen blockiert werden, erhält Ihr IT-Team unzählige Anfragen zu einmaligen Zugriffsausnahmen.

Browser Isolation bietet eine bessere Alternative, da die Sicherheits-, Produktivitäts- und Datenschutzprobleme behoben werden, die durch die Webnutzung Ihrer Mitarbeiter entstehen. Und da die Surfsitzungen in einem sicheren Container isoliert werden, können Ihre Mitarbeiter frei auf private Webmails und andere Websites zugreifen. Davon profitiert auch Ihr IT-Team, da es seine Zeit nicht mehr mit fallbasierten Ausnahmen verbringen muss und die Lösung einfach bereitstellen, verwalten und unterstützen kann. Ein Vorteil für Ihr Unternehmen sind die sofortigen Kosteneinsparungen durch die höhere Produktivität Ihres IT-Teams und die gesteigerte Moral unter Ihren Mitarbeitern, weil Sie ihnen vertrauen. Außerdem vermeiden Sie Compliance-Verstöße, da die Webmails Ihrer Anwender privat bleiben. Als vollständig cloudbasierte Lösung lässt sich Browser Isolation leicht implementieren. Zudem können Sie sie in Ihre vorhandenen Lösungen für Webfilter, Proxy, Gateway und Firewall integrieren.

Weitere Informationen finden Sie unter [www.proofpoint.com/de](http://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 zugleich das größte Kapital aber auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Cybersecurity-Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und IT-Anwender in den Unternehmen für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, verlassen sich auf Proofpoint, um ihre wichtigsten Sicherheits- und Compliance-Risiken bei der Nutzung von E-Mails, der Cloud, Social Media und dem Internet zu minimieren. [www.proofpoint.com/de](http://www.proofpoint.com/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.