proofpoint®

E-BOOK

# Intelligenter und schneller E-Mail-Schutz

Fünf Gründe, warum Proofpoint bei der API-basierten Ergänzung der Microsoft 365-E-Mail-Sicherheit die erste Wahl ist

# Einleitung

E-Mail ist schon seit Langem der Bedrohungsvektor Nr. 1. Gleichzeitig nehmen hochentwickelte Angriffe mit Business E-Mail Compromise (BEC), Ransomware und Kontoübernahmen sowie Supply-Chain-Attacken immer weiter zu.

Branchenexperten wie Gartner und Forrester empfehlen daher, die Sicherheitsfunktionen von Microsoft 365 mit weiteren Schutzmaßnahmen zu ergänzen.[1, 2]

Für den umfassenden Schutz von E-Mails, Cloud-Umgebungen und Daten wurden API-basierte, integrierte Cloud- und E-Mail-Sicherheitslösungen entwickelt, die schnelle Bereitstellung sowie effektiven Schutz vor diesen komplexen Angriffen bieten.

Microsoft-Kunden, die ihre Sicherheit kurzfristig ergänzen wollen, entscheiden sich in den meisten Fällen für Proofpoint. 85 % der Fortune 100-Unternehmen und mehr als 1,8 Millionen Kunden weltweit haben uns zu ihrem Sicherheitspartner gewählt. Wir sind ein führender Anbieter im Bereich E-Mail- und Cloud-Schutz.

Proofpoint Core Email Protection API setzt neue Standards für integrierte Cloud-basierte E-Mail-Sicherheitslösungen. Die Lösung bietet nicht nur hervorragende Bedrohungserkennung mit einer Genauigkeit von 99,99 %, sondern stellt dem Sicherheitsteam auch nahtlos integrierte Verwaltungstools bereit. Zudem stützt sich die zukunftssichere Plattform auf die bahnbrechende KI-Technologien von Proofpoint Nexus sowie auf einzigartige globale Bedrohungsdaten. Bei Proofpoint profitieren Sie von folgenden Vorteilen:

- Abwehr der größten Bandbreite an Bedrohungen mit der weltweit führenden KI-gestützten Sicherheitslösung
- Maximale Effizienz für Sicherheitskontrollzentren (SOCs)
- Zukunftssichere Sicherheitsarchitektur, die auch Bedrohungen von morgen abwehren kann

Für Proofpoint Core Email Protection API sprechen jedoch noch weitere Gründe. In diesem E-Book erfahren Sie, warum Proofpoint Core Email Protection API die Sicherheitsfunktionen von Microsoft 365 in Ihrem Unternehmen optimal ergänzen kann.

1. Mark Harris, Peter Firstbrook u. a. (Gartner): *Market Guide for Email Security* (Market Guide für E-Mail-Sicherheit), Oktober 2021.
2. Jess Burn, Joseph Blankenship u. a. (Forrester): *Best Practices: Phishing Prevention* (Bewährte Methoden zum Verhindern von Phishing), November 2021.

# Grund 1

## Schutz vor verschiedensten Bedrohungen

Bedrohungsdaten spielen bei der Erkennung und Abwehr von Bedrohungen eine entscheidende Rolle. Je mehr Daten den Algorithmen zur Verfügung stehen, desto besser können sie Anomalien erkennen.

Proofpoint verwendet eine einzigartige Kombination von Bedrohungsdaten. Unsere mehrschichtige Erkennungstechnologie Proofpoint Nexus AI wurde mit Billionen Datenpunkten trainiert, die wir in über 20 Jahren bei unseren Kunden erfasst haben. Diese Daten kombinieren wir mit den Erkenntnissen unseres Bedrohungsforschungsteams, damit unsere Kunden optimal vor Bedrohungen geschützt sind.

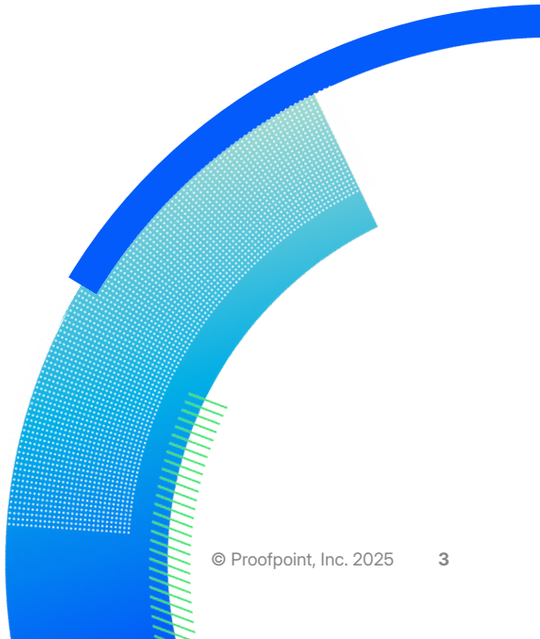
### Höhere Genauigkeit

Die meisten API-basierten Lösungen verwenden nur eine einzige Erkennungstechnik (z. B. Anomalieerkennung). Dadurch werden echte Bedrohungen oft übersehen oder legitime Nachrichten blockiert. Im Gegensatz dazu kombiniert Proofpoint KI- und ML-Methoden (KI/ML) mit Bedrohungsdaten und Sandbox-Analysen, was unseren Erkennungsmodulen eine höhere Genauigkeit verleiht. Außerdem können wir dank unserer umfassenden Datenbestände mehr Bedrohungen erkennen und gleichzeitig die Zahl der False Positives reduzieren.

### Schutz Ihres Unternehmens aus jeder Richtung

Proofpoint Nexus AI verwendet sechs leistungsstarke Module zur Abwehr KI-basierter Bedrohungen.

- **Nexus Language Model (LM)** erkennt mithilfe von subtilen Sprachmustern und Indikatoren für Verhaltensweisen BEC-Angriffe, bevor diese Schaden anrichten können.
- **Nexus Generative AI** erkennt mithilfe von Datenanalysen subtile Muster von Phishing- und Exfiltrationsversuchen in E-Mails, Cloud-Anwendungen und auf Endpunkten.
- **Nexus Threat Intelligence (TI)** bietet Echtzeitinformationen über Taktiken, Techniken und Schwachstellen von Angreifern, mit denen Bedrohungserkennungsmodelle verbessert werden.
- **Nexus Relationship Graph (RG)** überwacht das Anwenderverhalten systemübergreifend und sucht nach ungewöhnlichen Mustern, die auf Insider-Bedrohungen oder Kontenkompromittierung hindeuten. Diese Muster werden in einem Beziehungsdiagramm dargestellt.
- **Nexus Machine Learning (ML)** unterstützt die prädiktive Bedrohungserkennung.
- **Nexus Computer Vision (CV)** identifiziert und neutralisiert Bedrohungen, die in visuellen Elementen verborgen sind, z. B. Phishing-Websites, QR-Codes, schädliche Anhänge und gefälschte E-Mails.



# Grund 2

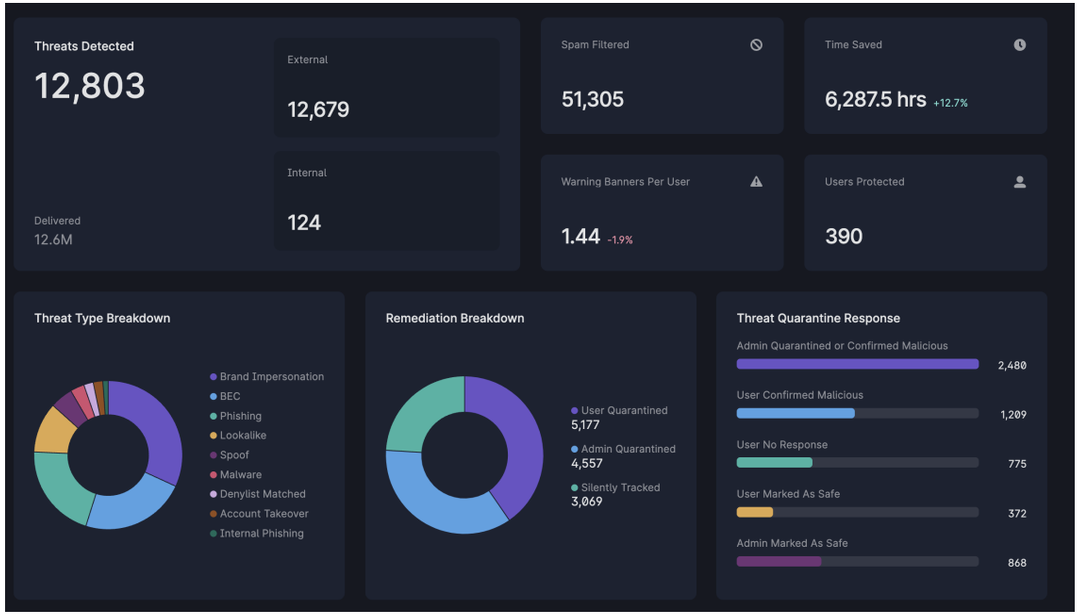
## Äußerst effizienter Betrieb des SOC

Je länger eine Bedrohung in Ihrer Microsoft 365-Umgebung unentdeckt bleibt, desto mehr Schaden kann sie anrichten. Für den Schutz von Microsoft 365 ist eine schnelle und effiziente Reaktion auf Zwischenfälle daher entscheidend.

Proofpoint Core Email Protection API bietet automatisierten E-Mail-Schutz und hocheffiziente Workflows für das SOC-Team, damit es sich auf wirklich wichtige Aufgaben konzentrieren kann.

So unterstützt Proofpoint das SOC:

- **Automatisierte Erkennung, Behebung und Abwehr von E-Mail-Bedrohungen:** Dadurch muss das Team deutlich weniger E-Mail-Bedrohungen untersuchen.
- **Bereitstellung von kontextbezogenen Warnmeldungen und Echtzeit-Beratung:** Dank Warnmeldungen und Echtzeit-Beratung können Administratoren informierte Sicherheitsentscheidungen treffen, sodass sie weniger potenzielle Ereignisse untersuchen und beheben müssen.
- **Kurze Bedrohungszusammenfassungen:** Das Team erhält eine klare und präzise, von einer generativen KI erstellte Beschreibung der wichtigsten Punkte zu jeder Bedrohung.
- **Beschleunigte Bedrohungssuche und Behebung:** Integrierte Suchfunktionen und auf Warnmeldungen basierende Workflows helfen dem Team, echte Bedrohungen schnell zu erkennen und zu beheben, bevor diese Schaden anrichten können.
- **Schnelle Bereitstellung:** Unsere Lösung ist in die Microsoft Graph-API integriert und durchläuft eine automatisierte Lernphase von weniger als 48 Stunden.




**Ihre Vorteile mit Proofpoint**

**99,99 %** der E-Mail-Bedrohungen werden gestoppt, bevor sie Schaden anrichten

**30 %** weniger E-Mail-Bedrohungen müssen vom SOC behoben werden

# Grund 3

## Umfassender Schutz vor aktuellen Bedrohungen

E-Mail-Bedrohungen verändern sich permanent weiter und können kaum abgewehrt werden. Daher fällt es selbst gut ausgestatteten IT-Abteilungen äußerst schwer, die Belegschaft davor zu schützen. Doch Proofpoint kann Ihnen helfen.

Mit Proofpoint Core Email Protection API können Sie bekannte und unbekannte Bedrohungen in Ihrem gesamten Unternehmen identifizieren und stoppen. Das bedeutet, dass raffinierte Bedrohungen wie die folgenden gar nicht erst die Posteingänge Ihrer Mitarbeiter erreichen:

### Phishing, URLs und Malware

Angreifer senden weiterhin unzählige schädliche Links und Anhänge per E-Mail – und diese können nur mit erweitertem E-Mail-Schutz gestoppt werden.

Proofpoint verwendet vorausschauende Sandbox-Analysen, URL-Extraktion, Erkennung von Umgehungsmaßnahmen, Browser-Isolierung und zahlreiche weitere hochentwickelte Technologien, um diese Schaddaten äußerst zuverlässig abwehren zu können.

### BEC-Angriffe

Nachahmerangriffe wie BEC, die ohne Schaddaten erfolgen, gehören zu den am schwersten erkennbaren Angriffstaktiken, da diese E-Mails legitimen Nachrichten häufig sehr ähnlich sind.

Die Proofpoint Nexus AI-Module analysieren die Beziehungen von E-Mail-Absendern und -Empfängern sowie deren Kommunikationsinhalte, um nach potenziellen Hinweisen auf eine Bedrohung zu suchen. Nicht übereinstimmende Header-Attribute, DMARC-Rückkopplungsschleifen und das Absenderverhalten bieten wertvolle Einblicke, die uns helfen, BEC-Angriffe zu stoppen, bevor Schaden entsteht.

### TOAD-Bedrohungen

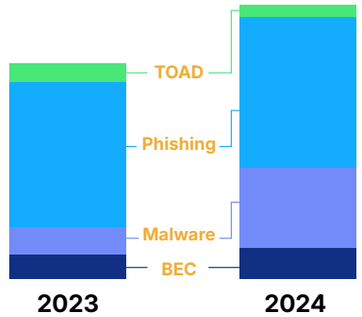
Angriffe per Telefon (Telephone-Oriented Attack Delivery, TOAD) werden auch als Callback Phishing bezeichnet. Bei dieser Taktik senden die Angreifer eine E-Mail, in der sie den Empfänger zum Anruf bei einem (falschen) Callcenter auffordern. TOAD-Bedrohungen sind besonders schwer zu erkennen, weil sie selten Schaddaten enthalten.

Die Proofpoint Nexus AI-Module verwenden Machine Learning und Computer Vision, um per Bilderkennung nach bekannten Bedrohungsindikatoren wie schädlichen Telefonnummern, QR-Codes und bildbasierten Nachahmungen zu suchen und diese Angriffe zu blockieren.

**45,8 %**

Zunahme der an Anwender gesendeten Bedrohungen* im Jahresvergleich

* Schädliche Nachrichten, die von Proofpoint erkannt wurden




**124 Mio.**

Anzahl der BEC-Angriffe, die Proofpoint jeden Monat blockiert

**45 %**

Jährliche Zunahme der an Anwender gesendeten E-Mail-Bedrohungen

**9 Mio.**

Anzahl der TOAD-Angriffe, die Proofpoint jeden Monat blockiert

# Grund 4

## Höchste Anwender-freundlichkeit

Im Bereich E-Mail-Sicherheit gelten „unsichtbare“ Lösungen als besonders anwenderfreundlich. Dank einer Erkennungsrate von 99,99 % können Sie Ihren Anwendern mit unserer Lösung ein optimales Erlebnis bieten. Proofpoint reduziert Störungen für Anwender durch Bedrohungen, Spam und Graymail.

Proofpoint Core Email Protection API bietet Anwendern folgende Vorteile:

- Eine Outlook-native Endnutzererfahrung bei Spam und Graymail
- Weniger Störungen dank branchen-führender Erkennungsgenauigkeit und schneller Behebung
- Kontextbezogene Warnhinweise beraten Anwender in Echtzeit

### Outlook-native Endnutzererfahrung

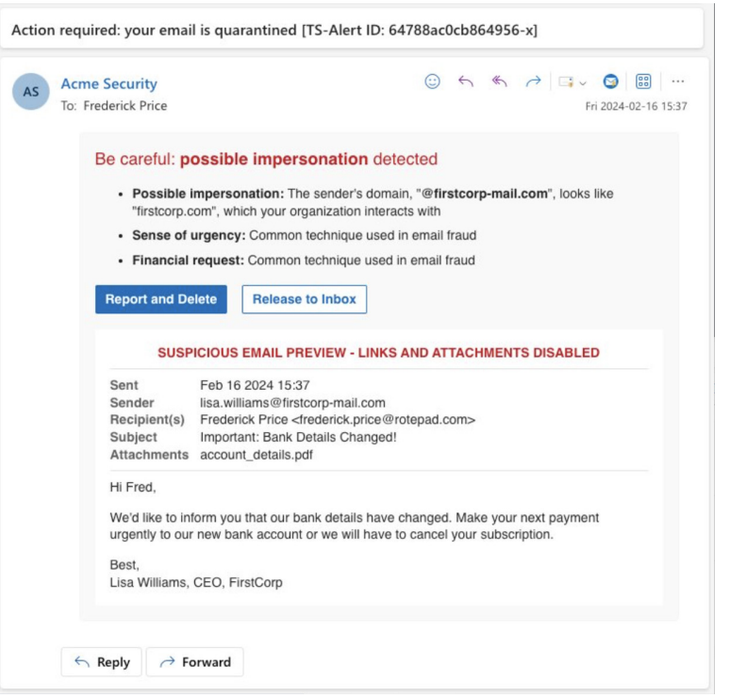
Die wachsende Zahl täglich eingehender E-Mails wird für Anwender immer belastender.

Proofpoint reduziert das E-Mail-Aufkommen, indem Spam und Graymail automatisch aus dem Posteingang in den standardmäßigen Junk-Ordner von Microsoft verschoben werden.

Erwünschte Nachrichten können bei Bedarf per Drag-and-Drop wieder in den Posteingang verschoben werden, sodass E-Mails von diesen Absendern künftig nicht mehr als Spam oder Graymail gekennzeichnet werden.

### Hohe Produktivität für Anwender und Sicherheitsteam

Proofpoint Core Email Protection API gewährleistet hohe Produktivität, da E-Mails mit geringem oder mittlerem Risiko sicher zugestellt werden. Diese Nachrichten werden mit Echtzeit-Hinweisen versehen, damit Anwender informierte Sicherheitsentscheidungen treffen und aus ihren Fehlern lernen können. Dadurch werden die Administratoren entlastet, weil sie weniger potenzielle Ereignisse untersuchen und beheben müssen.




**Echtzeit-Hinweis für Anwender zu verdächtigen E-Mails**

# Grund 5

## Zukunftssichere Sicherheitsarchitektur

Mit Proofpoint kann Ihr Unternehmen bestehende Risiken überall dort reduzieren, wo Ihre Anwender interagieren – heute ebenso wie morgen. Wir schützen Ihr Unternehmen vor Angreifern, die sich als Ihre Mitarbeiter, Partner und Lieferanten ausgeben, und verhindern sowohl versehentlichen als auch vorsätzlichen Datenverlust.

Zudem bieten wir Integrationen für eine Vielzahl von Tools, mit denen Sie Ihre Sicherheitstechnologien automatisieren und konsolidieren können.

Unsere Plattform lässt sich mit Lösungen führender Sicherheitsanbieter wie Palo Alto Networks, Okta, CrowdStrike und vielen anderen integrieren.


## Konsolidierung von Anbietern zur Verbesserung der Rendite

Wenn Sie Proofpoint zur Ergänzung von Microsoft 365 wählen, erhalten Sie auch Zugang zu unseren umfassenden Lösungen, die Ihr Unternehmen nicht nur vor E-Mail-Angriffen schützen, sondern auch modernste Tools zur Optimierung von Arbeitsabläufen zur Verfügung stellen.

Mit Proofpoint erhalten Sie zuverlässigen Schutz für Ihre Mitarbeiter, Ihre Daten und Ihr gesamtes Unternehmen.

### Stoppen personenzentrierter Angriffe

- Schutz vor Malware-, Phishing- und BEC-Angriffen per E-Mail
- Verhinderung von Nachahmer-Angriffen und Kompromittierung von Lieferanten
- Schutz von Collaboration-Tools vor Anmeldedatendiebstahl und Malware-Angriffen

### Schutz für Daten und digitale Kommunikation

- Verhinderung der versehentlichen Gefährdung von Daten durch Anwender
- Erkennung böswilliger Insider-Aktivitäten und Unterstützung durch Echtzeit-Warnmeldungen
- Kanalübergreifende Verwaltung der digitalen Kommunikation

### Bessere Sicherheitsentscheidungen durch Schulungen

- Bereitstellung maßgeschneiderter, risikobasierter Schulungen
- Simulierte Angriffe zur Bewertung der Anwenderresilienz
- Förderung von Verhaltensänderungen durch Echtzeit-Warnhinweise in E-Mails und Web

### Eindämmung von SaaS-Identitätswildwuchs

- Erkennung und Abwehr von Kontoübernahmen
- Proaktive Nachverfolgung von Angriffspfaden in Active Directory
- Erkennung von SaaS-Konten (Software-as-a-Service) und Wiederherstellung von Sicherheitsstandards

# Zusammenarbeit mit einem Branchenführer

Bei Proofpoint müssen Sie sich nicht zwischen erstklassiger Technologie und einer vollständig integrierten Lösung entscheiden. Wir sind ein ausgewiesener Branchenführer in den Bereichen Cybersicherheit, Datenverlustprävention (DLP) und Compliance.

## Anerkennung in der Branche für Proofpoint Core Email Protection

**Gartner**

**Ein Leader**
Magic Quadrant 2024 für E-Mail-Sicherheitsplattformen

**Nr. 1 bei 4 von 5 Use Cases**
Im Magic Quadrant 2024 für E-Mail-Sicherheitsplattformen:
– Grundlegender E-Mail-Schutz
– Sicherheitsplattformen
– Schutz ausgehender Nachrichten
– Poweruser

**FORRESTER®**

**Forrester Wave™:**
E-Mail-Sicherheit für Unternehmen, 2. Quartal 2023 | Leader

**FROST & SULLIVAN**

**Frost Radar™ 2023:**
E-Mail-Sicherheit, 2023:
Seit neun Jahren in Folge marktführendes Unternehmen für E-Mail-Sicherheit in den Kategorien Marktanteil und Wachstum

**Frost & Sullivan 2024**
Unternehmen des Jahres | Weltweit führender Anbieter für E-Mail-Sicherheit und hervorragende Best Practices

**Frost & Sullivan 2025**
Unternehmen des Jahres | Führender Anbieter für E-Mail-Sicherheit in Australien und hervorragende Best Practices

**GIGAOM**

**GigaOm Radar für Phishing-Schutz 2023:**
Als Leader und Fast Mover positioniert

**GigaOm Radar für Erkennung und Abwehr identitätsbezogener Bedrohungen 2024:**
Als Leader und Fast Mover positioniert

**GigaOm Radar für Täuschungstechnologie 2024:**
Als Leader und Fast Mover positioniert

**kuppingercole ANALYSTS**

**Leadership Compass für E-Mail-Sicherheit 2023:**
Leader in allen vier Kategorien: Gesamt, Produkt, Innovation und Markt

**OMDIA**

**Omdia Universe für E-Mail-Sicherheit 2024:**
Leader

**Radicati Market Quadrant für E-Mail-Sicherheit 2024:**
Top Player

proofpoint.



# Nächste Schritte

Die beste Cyberabwehr stoppt Bedrohungen bereits in ihren Anfängen. Deshalb haben uns mehr als 1,8 Millionen Kunden weltweit zu ihrem Sicherheitspartner gewählt.

Proofpoint Core Email Protection API stoppt 99,99 % aller E-Mail-Bedrohungen, Spam- und Graymail-Nachrichten. Unsere mehrschichtige Erkennungstechnologie Proofpoint Nexus kombiniert Beziehungsdiagramme, Machine Learning, Bilderkennung sowie semantische Analysen und stützt sich dabei auf Bedrohungsdaten aus mehr als 3 Billionen jährlich analysierten E-Mails. Dadurch kann die Lösung besonders raffinierte aktuelle Bedrohungen verhindern.

Proofpoint Core Email Protection API stoppt jedoch nicht nur Bedrohungen, sondern unterstützt auch Sicherheitsteams mit vereinfachten, auf Warnmeldungen basierenden Workflows und integrierten Suchfunktionen. Zudem werden von Anwendern gemeldete E-Mails automatisch behoben, während die Anwender beim Melden einer verdächtigen E-Mail einen kontextbezogenen Hinweis erhalten.

Erfahren Sie mehr darüber, wie Proofpoint Ihnen bei der Ergänzung der E-Mail- und Cloud-Sicherheitsfunktionen von Microsoft 365 helfen kann.

proofpoint.com/de/products/threat-defense

## Informationen zu Proofpoint

### Personenzentrierter Schutz

**3,4 Bill.**
E-Mails pro Jahr gescannt

**>1,4 Bill.**
SMS/MMS pro Jahr gescannt

**124 Mio.**
BEC-Angriffe pro Monat abgewehrt

**>183 Mio.**
Phishing-Simulationen pro Jahr gesendet

**0,8 Bill.**
Anhänge pro Jahr gescannt

**21 Bill.**
URLs pro Jahr gescannt

**177 Mio.**
TOAD-Angriffe pro Jahr abgewehrt

## Marktdurchdringung

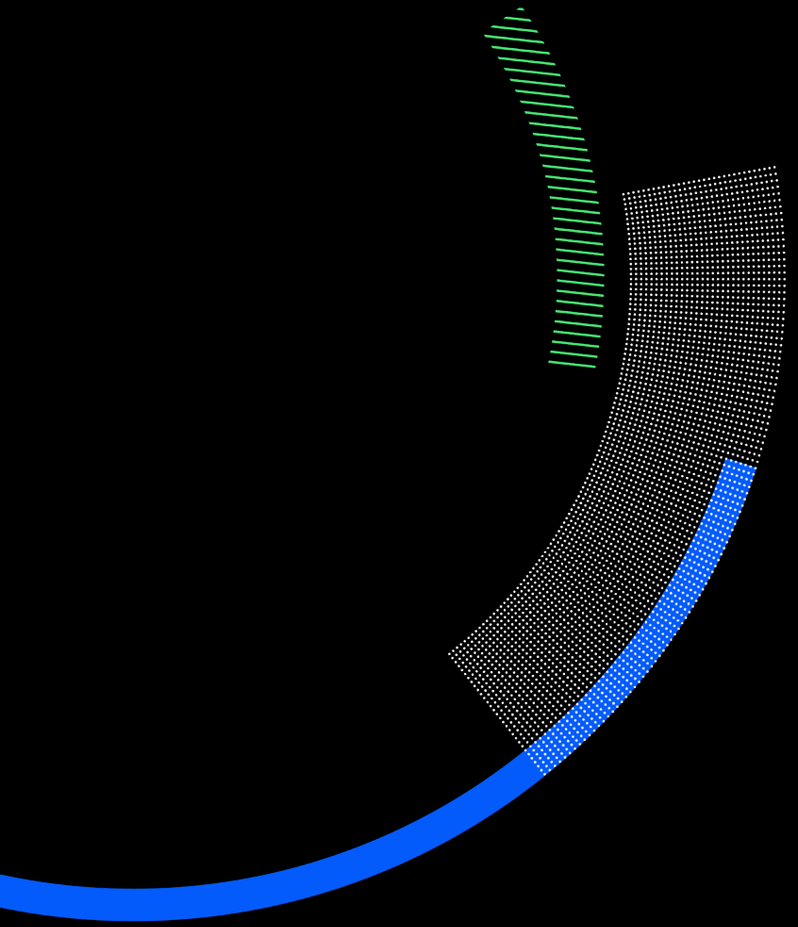
**>1,88 Mio.**
Kunden

**>150**
Weltweite ISPs und Mobilfunkbetreiber

**85 %**
der Fortune 100 von Proofpoint geschützt

**50 %**
der Fortune 100 nutzen Proofpoint DLP

**>60 %**
der Fortune 1000 von Proofpoint geschützt



proofpoint.

Proofpoint, Inc. 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 85 Prozent der Fortune 100-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.

**Verbinden Sie sich mit Proofpoint:** LinkedIn



LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →