

## KURZVORSTELLUNG

# Microsoft und Proofpoint – Schutz für den modernen Arbeitsplatz

Zwei führende Cybersicherheitsanbieter.  
Eine personen- und KI-zentrierte Lösung.



### Wichtige Highlights

- Reduzierung der Wahrscheinlichkeit von Datenschutzverletzungen
- Schutz der Anwender mit mehrschichtigen Sicherheitsfunktionen
- Vereinheitlichung des Datenschutzes für Microsoft- und Drittanbieter-Anwendungen
- Verbesserung der Compliance und Richtlinienkontrolle

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die sich auf die Behebung der vier wichtigsten personenbezogenen Risiken konzentriert.

### Einleitung

Cyberangriffe nehmen exponentiell zu, da Bedrohungsakteure aufgrund von Fortschritten bei KI nun weitaus umfangreichere Kampagnen ohne zusätzliche Ressourcen durchführen können. Darüber hinaus können diese Angriffe praktisch problemlos im globalen Maßstab gestartet werden.

Microsoft 365 ist als Standardproduktivitätsplattform für Unternehmen jeder Größe zu einem vorrangigen Ziel für diese Angriffe geworden. Obwohl Microsoft starke Schutzmaßnahmen bietet, wäre selbst die leistungsfähigste Cybersicherheit bei dieser überwältigenden Angriffsflut überfordert. Es ist daher wichtig, die Risiken zentraler Schwachstellen in kritischen Kanälen wie E-Mail zu analysieren.

Wenn Sie die Microsoft 365-Sicherheitsfunktionen mit der Proofpoint Nexus™ AI-Plattform kombinieren, erhalten Sie zuverlässigen Schutz vor Bedrohungen, die herkömmliche Lösungen oft übersehen. Zusammen schützen diese Lösungen Ihre Umgebung vor Phishing, Social Engineering, Datenverlust sowie anderen Bedrohungen. Außerdem unterstützen sie Ihre Mitarbeiter und entlasten Ihre Teams, damit sie sich auf Wachstum konzentrieren können.

**„Käufer müssen ergänzende oder zusätzliche E-Mail-Sicherheitslösungen implementieren, um die empfohlenen Vorgehensweisen zur Abwehr moderner E-Mail-Bedrohungen umzusetzen.“**

**GARTNER** | MAGIC QUADRANT FÜR  
E-MAIL-SICHERHEIT,  
4. Quartal 2025

## Sicherheitsherausforderungen des modernen Arbeitsplatzes

E-Mail ist bei heutigen Cyberangriffen nach wie vor der primäre anfängliche Bedrohungsvektor. In den letzten Jahren hat sich die Angriffsfläche allerdings erweitert. Anwender arbeiten heute mit Microsoft Teams, Slack, Cloud-Anwendungen, Social-Media-Plattformen und File-Sharing-Diensten. Daher überrascht es nicht, dass Cyberkriminelle neue Taktiken entwickeln, um diese digitalen Kanäle ausnutzen zu können.

Angreifer umgehen zunehmend herkömmliche E-Mail-Sicherheitskontrollen, indem sie über Collaboration-Tools schädliche Links bereitstellen, Anmeldedaten stehlen und sich unbefugten Zugriff verschaffen. Gleichzeitig nutzen Bedrohungsakteure E-Mails für Exploits wie Phishing und Business Email Compromise (BEC). Diese Taktiken führen weiterhin zu den meisten Kompromittierungen.

Angesichts der Zunahme kanalübergreifender, mehrstufiger Bedrohungen können selbst die fortschrittlichsten Sicherheitstools kaum mithalten – und für Sicherheitsteams wird es immer schwieriger, einen Überblick über Angriffe und die Kontrolle zu behalten.

1. FBI Internet Crime Complaint Center (IC3): *Internet Crime Report* (Bericht zu Internetverbrechen), 2024.

**Personenzentrierte Bedrohungen dominieren die Bedrohungslandschaft. Mehr als 90 Prozent aller erfolgreichen Kompromittierungen beginnen mit einer E-Mail.<sup>1</sup>**

## So schützt Microsoft den Arbeitsplatz

Microsoft 365 bietet durch Defender und Purview eine starke KI-gestützte Sicherheitsgrundlage. Diese beiden Lösungen bilden den Kern der Sicherheitsarchitektur.

### Microsoft Defender

Microsoft Defender verwendet fortschrittliche KI-gestützte Erkennung, um E-Mail-Bedrohungen zu stoppen. Die Lösung analysiert täglich Billionen von Microsoft erfasste Signale (darunter E-Mail-Inhalte, Absenderverhalten und Kontextindikatoren), um böswillige Absichten zu identifizieren. Bei BEC-Bedrohungen führt Microsoft Defender eine Absichtsanalyse durch und erkennt ungewöhnliche Verhaltensweisen. Bildbasierte Bedrohungen (z. B. verborgener Text und QR-Codes) werden mithilfe fortschrittlicher Bildanalysefunktionen erkannt.

### Microsoft Purview

Microsoft Purview bietet unternehmensgerechte Datenverlustprävention (DLP), sodass das Risiko einer Datenschutzverletzung reduziert und die Einhaltung von Vorschriften sichergestellt wird. Durch die Klassifizierung und Kennzeichnung der Unternehmensdaten können Datensicherheitsrichtlinien konsistent für E-Mails, Endpunkte und Cloud-Anwendungen angewendet werden.

## Der Vorteil des personenzentrierten Ansatzes von Proofpoint

Proofpoint bietet eine umfassende, personenzentrierte Plattform, die von unseren Nexus AI-Modulen unterstützt wird. Sie erhalten resiliente Schutzmaßnahmen, die dank einer einfachen Integration mit der Microsoft Graph-API innerhalb weniger Minuten bereitgestellt werden können.

**Die KI-Modelle von Proofpoint werden mit einem der größten und vielfältigsten Datensätze der gesamten Cybersicherheitsbranche trainiert.**

## Proofpoint Collaboration Security Prime

Proofpoint Collaboration Security Prime bietet kanalübergreifenden Bedrohungsschutz, der personen- und agentenzentrierte Angriffe über E-Mail-, Messaging-, Collaboration-Tools, Cloud-Anwendungen und File-Sharing-Dienste in allen Phasen stoppt. Die Lösung erweitert die branchenführende Sicherheit über E-Mails hinaus, um vertrauenswürdige Interaktionen abzusichern und die Resilienz der Mitarbeiter direkt in die Plattform zu integrieren.

Mit automatisierten Workflows und umfassendem Schutz optimiert Proofpoint Prime betriebliche Abläufe und stärkt die Sicherheitsmaßnahmen für alle Collaboration-Umgebungen.

## Proofpoint Data Loss Prevention

Die Proofpoint Data Loss Prevention (DLP)-Lösungen bieten personenzentrierten Omnichannel-Schutz zur Identifizierung und Behebung von Datenverlustrisiken in E-Mails, Cloud und Endpunkten. Proofpoint Enterprise DLP vereinheitlicht Inhalts-, Verhaltens- und Bedrohungs-Telemetriedaten, um das gesamte Spektrum personenzentrierter Datenverlustszenarien abzudecken und nicht autorisierte Übertragungen vertraulicher Informationen zu verhindern. Die Lösung basiert auf einer modernen, skalierbaren Architektur und bietet Transparenz sowie Kontrolle bei Datenexfiltrationsversuchen, ohne die Arbeitsabläufe der Anwender zu stören.

**Mehr als 2 Millionen führende Unternehmen auf der ganzen Welt setzen auf Proofpoint.**

## Gemeinsam sicherer: Proofpoint und Microsoft

Die integrierten Sicherheitstechnologien von Microsoft bieten in Kombination mit Proofpoint Collaboration Security Prime und Proofpoint DLP kanalübergreifenden Bedrohungsschutz für alle Angriffsphasen sowie personenzentrierten Omnichannel-Schutz für Ihre Daten.

Zusammen eingesetzt, vereinheitlichen diese Lösungen die Inhalts-, Verhaltens- und Bedrohungs-Telemetriedaten zu E-Mails, Collaboration-Tools, Cloud-Anwendungen und Endpunkten. Dadurch erhalten Sicherheitsteams Transparenz und Kontrolle über den gesamten modernen Arbeitsplatz, ohne die Arbeitsabläufe der Anwender zu stören.

**Proofpoint Collaboration Security Prime** ergänzt den Microsoft Defender-nativen Schutz vor BEC-, Phishing-, Malware-Angriffen und kompromittierten Lieferantenkonten. Durch unsere Bedrohungsdaten können Sie Angriffe erkennen, die andernfalls übersehen werden könnten. Darüber hinaus bietet Proofpoint einen Überblick über besonders häufig angegriffene Personen, die Very Attacked People™ (VAPs). Dadurch können Sie diesen Anwendern stärkere Sicherheitsmaßnahmen zuweisen. Diese Möglichkeit ist in Microsoft 365 nicht nativ verfügbar.

**Proofpoint DLP** arbeitet mit Microsoft Purview zusammen, um den Datenschutz in allen Bereichen des modernen Arbeitsplatzes zu verbessern. Während Microsoft Purview innerhalb von Microsoft 365 robuste Klassifizierung und Richtlinienkontrollen bereitstellt, bietet Proofpoint einen einheitlichen Überblick über E-Mails, Collaboration-Tools, Cloud-Anwendungen und Endpunkte. Durch die Kombination von Inhaltsanalysen und Anwenderkontext erhalten Unternehmen konsistente Governance für alle Kanäle sowie verbesserten Schutz für vertrauliche Informationen.

Mit den Proofpoint-Lösungen für sichere Zusammenarbeit und Datensicherheit erhalten Sie zusätzlich zwei leistungsstarke, erstklassige Schutzebenen.



Abb. 1: Die personenzentrierten Sicherheitsebenen von Proofpoint zur Verbesserung von Microsoft 365.

## Kundenergebnisse und Umsetzung

Häufig verwenden Unternehmen die Microsoft-Schutzmaßnahmen am Gateway und die Proofpoint-Schutzmaßnahmen für Postfächer.

Unternehmen, die ihre Microsoft 365-Umgebung mit Proofpoint verbessern, erzielen messbare Verbesserungen ihrer Sicherheit.

- Sie können 27 % mehr Bedrohungen abwehren.
- Die Wahrscheinlichkeit einer schwerwiegenden Datenschutzverletzung wird um 75% reduziert.

Diese Ergebnisse haben erhebliche finanzielle Auswirkungen. Sie führen zu Kosteneinsparungen in Millionenhöhe, da ihre Teams weniger Zeit für die Reaktion auf Vorfälle aufwenden, ihre Mitarbeiter produktiv bleiben und ihr Unternehmen kostspielige Geldstrafen vermeidet.

Schöpfen Sie das volle Potenzial der Microsoft 365-Sicherheitsfunktionen aus. Erfahren Sie, wie Proofpoint Ihren Schutz erweitert und verbessert.

[www.proofpoint.com/de/compare/proofpoint-and-microsoft](http://www.proofpoint.com/de/compare/proofpoint-and-microsoft)

# proofpoint®

**Information zu Proofpoint, Inc.** Proofpoint, Inc. ist ein weltweiter Marktführer bei personen- und agentenzentrierter Cybersicherheit und schützt Verbindungen zwischen Anwendern, Daten und KI-Agenten über E-Mail, Cloud und Collaboration-Tools. Proofpoint ist ein vertrauenswürdiger Partner für mehr als 80 Prozent der Fortune 100, über 10.000 große Unternehmen sowie für Millionen kleinerer Firmen und stoppt Bedrohungen, verhindert Datenverlust und sichert die Interaktionen zwischen Anwendern und KI-Workflows ab. Die Collaboration- und Datenschutzplattform von Proofpoint hilft Unternehmen jeder Größe, ihre Mitarbeiter zu schützen und zu unterstützen, damit sie KI sicher und bedenkenlos einsetzen können. Weitere Informationen unter [www.proofpoint.com/de](http://www.proofpoint.com/de).

Verbinden Sie sich mit Proofpoint: [LinkedIn](#)

Proofpoint ist eine eingetragene Marke bzw. ein registrierter Handelsname von Proofpoint, Inc. in den USA und/oder anderen Ländern.

**LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →**