E-BOOK

Das Potenzial von Proofpoint

10 Gründe, warum Unternehmen ihre Microsoft 365-Investition mit personenzentrierter Cybersicherheit schützen

proofpoint.

Einführung

In der modernen Geschäftswelt sind nur wenige Tools so wichtig wie Microsoft 365. Für viele Unternehmen ist die Plattform die Grundlage für Remote-Arbeit, die weltweite Zusammenarbeit und die Cloud (und steht meist als Synonym für diese neuen Arbeitsweisen).

Leider ist diese Plattform aufgrund ihrer Reichweite und zentralen Rolle bei der Arbeit auch ein bevorzugtes Ziel für Cyberangreifer – und häufig der wichtigste Vektor zur Kompromittierung von Opfern. Gleichzeitig hat der Wechsel zu Remote- und Hybrid-Arbeit auch die Sicherheit erschwert und zu Datenverlust durch Insider geführt.

Microsoft 365 ist zwar ein unverzichtbares Produktivitätstool, allerdings empfehlen Experten wie Gartner und Forrester den Einsatz einer umfassenden Lösung für E-Mail-, Cloud- und Datensicherheit statt der plattformeigenen Angebote.[1, 2]

In Anbetracht der aktuellen komplexen und dynamischen Bedrohungs- und Compliance-Landschaft ist ein neuer Ansatz für den Schutz vor Bedrohungen sowie Datenverlust und zur Gewährleistung von Compliance erforderlich. Deshalb bietet Ihnen Proofpoint eine einzigartige personenzentrierte Lösung mit folgenden Vorteilen:

- Der branchenweit effektivste Schutz vor Bedrohungen und Datenverlust
- Verwertbare Einblicke und Kontextinformationen für interne und externe Bedrohungen
- Ein moderner, integrierter Ansatz zur Verhinderung von Bedrohungen, Datenverlust und Compliance-Verstößen
- Ein erstklassiges Erlebnis für Ihr Team und Ihre Endnutzer

Genauso wie Microsoft als Ihr Partner für Produktivität gilt, will Proofpoint Ihr Partner für Cybersicherheit sein. Mehr als 200.000 Microsoft 365-Kunden vertrauen beim Schutz ihrer Cloud-Investition bereits auf uns.

Nachfolgend erfahren Sie, wie wir Ihnen helfen können, die Sicherheit von Microsoft 365 zu erweitern.

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

Erweiterter Schutz vor Phishing, BEC-Angriffen und anderen Bedrohungen

Die beste Cyberabwehr stoppt Bedrohungen bereits in ihren Anfängen. Deshalb helfen wir mehr als 200.000 Microsoft 365-Kunden dabei, mehr Bedrohungen und unerwünschte E-Mails aufzuhalten – noch bevor sie in die Posteingänge der Anwender gelangen.

Mit einer mehrstufigen Sandbox-Analyse, die auf statische sowie dynamische Techniken zurückgreift, gehen uns mehr Bedrohungen ins Netz. Unsere Untersuchungen werden zudem von Proofpoint-Analysten überwacht, um damit die Erkennung weiter zu verbessern und wertvolle Bedrohungsdaten zu erhalten. Unser KI- und ML-gestütztes Erkennungsmodul nutzt moderne Verhaltensanalysen, um sowohl schädlichen Code als auch Websites mit Anmeldedaten-Phishing zu erkennen. Es kann zudem Angriffe mit Sandbox-Umgehungstechniken erkennen, die andere VM-Tools (virtuelle Maschine) übersehen.

Außerdem erhalten Sie Einblicke in folgende Bereiche:

Welche Anwender mit BEC ins Visier genommen werden

Die am häufigsten gegen Ihre Anwender eingesetzten BEC-Taktiken

Welchen BEC-Bedrohungen Ihre Umgebung im Laufe der Zeit ausgesetzt ist

Eine prädiktive URL-Analyse scannt und neutralisiert verdächtige URLs, bevor sie zugestellt werden und wenn Anwender darauf klicken. Sie können Anhänge mit dubiosen URLs blockieren und verdächtige URLs umschreiben – unabhängig davon, ob diese in Textdateien (TXT), Rich-Text-Dateien (RTF) oder als HTML auftreten.

Wir stoppen eine Vielzahl anderer Bedrohungen, darunter BEC-Betrug (Business Email Compromise), Lieferantenbetrug und andere Social-Engineering-Formen, die nicht immer auf unsicheren Anhängen oder URLs basieren.

Unsere Machine Learning- (ML) und Verhaltensanalysen, die mit Billionen Datenpunkten trainiert wurden, erkennen und blockieren jeden Monat 2,2 Millionen BEC-Bedrohungen. Wir bieten Ihnen detaillierte Forensikanalysen, damit Sie nachvollziehen können, warum eine Nachricht als unsicher eingestuft und blockiert wurde.

Unsere integrierte Lösung bietet Ihnen umfangreiche Einblicke in böswillige Aktivitäten und Anwender-verhaltensweisen und kann somit die meisten Bedrohungen stoppen. Für den Fall, dass etwas schief geht, automatisiert die Lösung wichtige Teile der Reaktion auf Zwischenfälle, sodass Sie Ihre Anwender umfassend schützen können.

Dank einer durchschnittlichen Analysedauer von weniger als drei Minuten blockieren wir unsichere Anhänge schon bevor Anwender die Gelegenheit haben, damit zu interagieren – und ohne die Produktivität der Anwender zu beeinträchtigen. Wir unterstützen eine große Auswahl an Dateitypen jenseits von Microsoft Office-Dokumenten, darunter PDF- und HTML-Dateien.

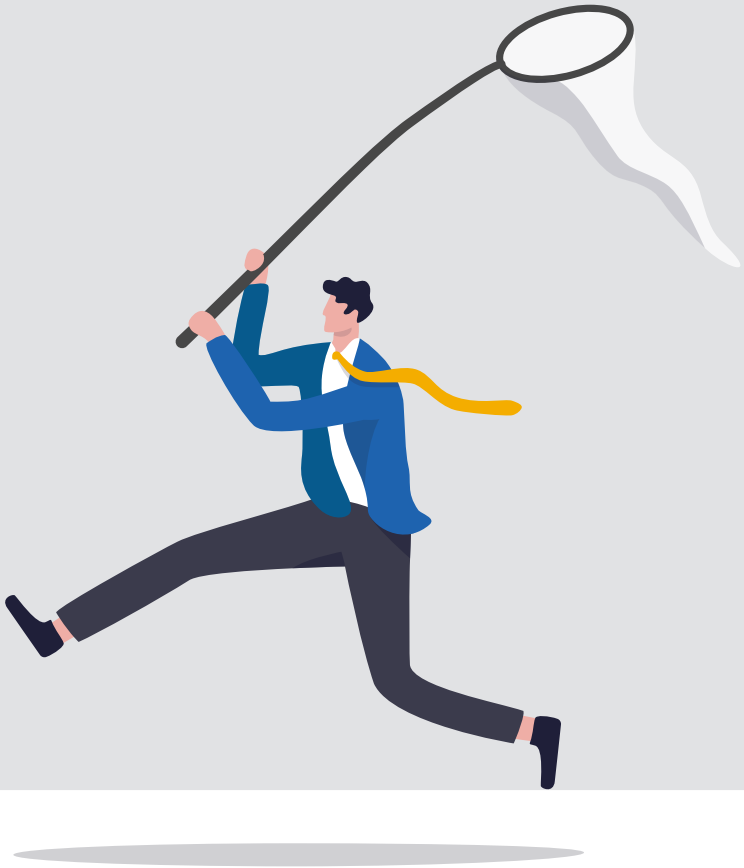
Für besonders gefährdete Anwender und riskante Websites öffnet unsere URL-Isolierungslösung unbekannte Links aus E-Mails in einer sicheren, abgeschlossenen Umgebung. Die E-Mails werden dadurch von potenziell schädlichen Inhalten befreit und sind dennoch für die Anwender vollständig lesbar.

Zudem mahnen konfigurierbare E-Mail-Warnhinweise für Ein-Klick-Meldungen die Anwender zu besonderer Vorsicht und erleichtern ihnen die Meldung unsicherer Nachrichten.

GRUND 2

Moderne personenzentrierte Datenverlustprävention

Die bisherigen Netzwerkgrenzen wurden defacto bereits durch den „Mitarbeiter als Perimeter“ ersetzt. Im Zeitalter von Remote- und Hybrid-Arbeit müssen Ihre Mitarbeiter personenbezogene Informationen und andere vertrauliche Daten in E-Mails, der Cloud, dem Web und auf Endpunkten verwalten. Diese Trends erschweren die Datenverlustprävention (Data Loss Prevention, DLP) und die Abwehr von Insider-Bedrohungen (Insider Threat Management, ITM).



Mit Proofpoint ...

können Sie mühelos individuelle Datenrichtlinien für Ihr Unternehmen einrichten und pflegen. Unsere Plattform verfügt über folgende Funktionen, die das Auffinden, Verwalten und Melden von Verstößen erleichtern:

- Native algorithmische Analysen
- Ein intelligentes Identifikatormodul
- Vorkonfigurierte Wörterbücher
- Standardmäßige DLP-Workflows

Wir helfen Ihnen, Ihre Daten durch bessere Einblicke und optimierte Abläufe vor externen und internen Bedrohungen zu schützen. Sie erhalten personenzentrierten Kontext, um die Ereignisse hinter jeder DLP-Warnung zu einem Gesamtbild zusammenfügen zu können. Dank unserer einzigartigen Zeitleistenansicht sind Sie in der Lage, schnell einen Zusammenhang zwischen Inhalten, Verhalten und Bedrohungen herzustellen. Dies ermöglicht eine schnelle Einschätzung der Absichten des Anwenders und eine problemlose Zusammenarbeit mit der Rechts- und Personalabteilung zwecks einer angemessenen Reaktion.

Wir vereinfachen die Erstellung, Anwendung und Durchsetzung einheitlicher Richtlinien für E-Mail, Web, Cloud und Endpunkte, sodass Sie Ihre Daten schützen und geltende Vorschriften einhalten können.

Unser KI-gestütztes Datenklassifizierungsmodul erkennt, klassifiziert und kennzeichnet geschäftskritische Daten, um Ihr DLP-Programm zu verbessern und zu beschleunigen. Sie können aus hunderten vortrainierten Klassifizierern auswählen oder von unserem KI-Modul generierte Klassifizierer aus Beispieldokumenten erstellen lassen. In beiden Fällen lernt das Modul dynamisch aus den Daten in der Cloud und in lokalen Repositories und schlägt Wörterbücher vor, die sich mit einem Klick auf alle Kanäle anwenden lassen.

Nicht alle DLP-Zwischenfälle sind gleich. Unsere Information Protection-Plattform stellt Zusammenhänge zwischen Inhalten, Verhaltensweisen und externen Bedrohungen her. Dadurch können Sie leichter erkennen, ob Datenverlust durch fahrlässige, böswillige oder kompromittierte Anwender verursacht wurde. Wenn Sie wissen, aus welchem Motiv ein Anwender gehandelt hat, können Sie entsprechend reagieren.

Ihr Team spart Zeit und Kosten mit einer einzigen integrierten, Cloud-nativen Konsole. Der Datenschutz ist standardmäßig integriert, sodass DLP nicht auf Kosten des Anwender-Datenschutzes geht.

Wir bieten Schutz für Anwender, vertrauliche Daten und Cloud-Anwendungen und erweitern so die integrierten Microsoft 365-Sicherheitsfunktionen erheblich. Durch die Identifizierung besonders gefährdeter Anwender können Sie risikobasierte Kontrollen anwenden, um deren Konten zu schützen.

GRUND 3

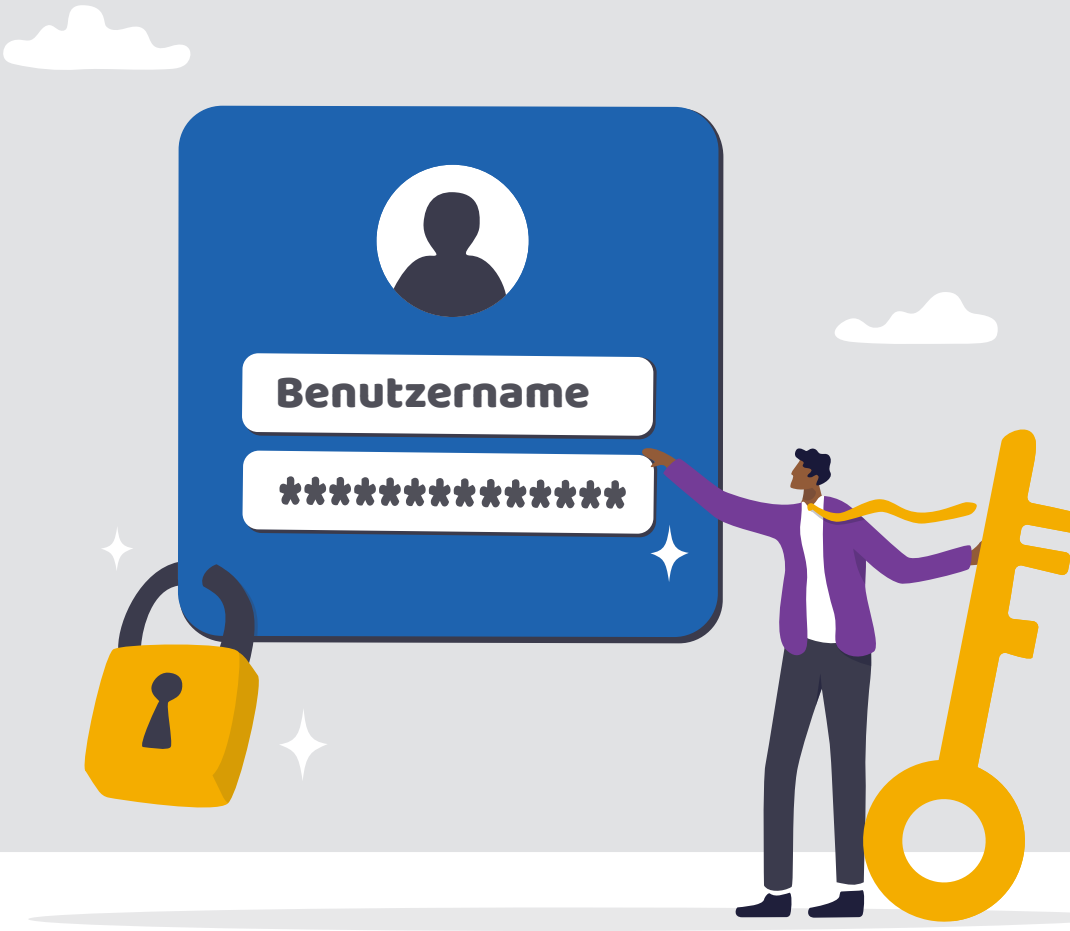
Schutz vor Kontoübernahmen

Wenn Ihr Cloud-Konto in die falschen Hände gerät, kann es als Waffe missbraucht werden.

Cyberangreifer, die ein Konto übernehmen können, erhalten ungehinderten Zugang zu den vertraulichen Daten, auf die normalerweise der Kontoinhaber Zugriff hat. Und jeder, der ein E-Mail-Konto kontrolliert, kann Menschen ausnutzen, die diesem Konto vertrauen – innerhalb ebenso wie außerhalb Ihrer Umgebung.

Mit unserem mehrstufigen Ansatz helfen wir Ihnen, Ihr Microsoft 365-Konto bei verdächtigen Aktivitäten mit Echtzeitwarnungen, automatischer Behebung und risikobasierten Zugriffsberechtigungen zu schützen.

Zuverlässige Richtlinien weisen in Echtzeit auf Probleme hin, sodass Sie Warnmeldungen – und alle vorher erfolgten Aktivitäten – mithilfe eines intuitiven Dashboards schnell untersuchen können. Von dort können Sie kompromittierte Konten beheben, unsichere Dateien unter Quarantäne stellen und dafür sorgen, dass die erforderliche Authentifizierung auf dem aktuellen Risiko basiert.



Die Integration in Okta erlaubt die Identifizierung einer Vielzahl von ungewöhnlichen und unsicheren Aktivitäten:

Erfolgreiche, aber verdächtige Anmeldungen bei Microsoft 365

Fehlgeschlagene Anmeldungen

Unerwartete Zugriffe auf Geschäftsanwendungen

Rechteerweiterungen, die Zugriff auf wichtige Cloud-Ressourcen ermöglichen

Rechteerweiterungen, die Anwender von den üblichen Authentifizierungsfaktoren befreien

GRUND 4

Transparenz und Schutz für die Cloud

Proofpoint CASB erweitert unsere personenzentrierte Sicherheit auf die Cloud. Wir unterstützen Sie bei der Erkennung, Untersuchung und Abwehr von Cyberkriminellen, die sich Zugriff auf Ihre Daten in Microsoft 365- und Cloud-Anwendungen verschaffen wollen.

Es gibt Drittanbieter-Anwendungen, die den Funktionsumfang von Microsoft 365 erweitern. Einige von ihnen sind jedoch schlecht programmiert oder direkt schädlich. Angreifer können die Anwender mithilfe von Drittanbieter-Add-ons und Social Engineering dazu verleiten, ihnen Zugriff auf Ihre SaaS-Anwendungen und Daten zu gewähren.

Wir unterstützen Sie bei der Erkennung, Bewertung und Kontrolle unsicherer Anwendungen und Add-ons. Dank unserer leistungsstarken Analyse können Sie die Zugangsberechtigungen zuweisen, die den für Sie relevanten Risikofaktoren entsprechen. Anwenderspezifische Risikoindikatoren in Kombination mit Bedrohungsdaten aus E-Mails, SaaS- und anderen Anwendungen erkennen Anomalien in Cloud-Anwendungen, einschließlich Kontoübernahmen und verdächtige Dateiaktivitäten.

Mit der IaaS- und SaaS-Sicherheitsverwaltung lassen sich riskante Administrationsaktivitäten mühelos überwachen. Zudem helfen wir Ihnen bei der Suche nach Konfigurationsfehlern und Compliance-Problemen, um selbstverschuldete Probleme zu vermeiden.

GRUND 5

Blitzschnelle und umfassende Reaktion auf Zwischenfälle

Je länger eine Bedrohung in Ihrer Microsoft 365-Umgebung unentdeckt bleibt, desto mehr Schaden kann sie anrichten. Deshalb ist eine schnelle, effiziente Reaktion auf Zwischenfälle für den Schutz von Microsoft 365 so wichtig.

Proofpoint Threat Response Auto-Pull (TRAP)

Automatische Entfernung schädlicher E-Mails aus Posteingängen durch verbesserte Sicherheitswarnmeldungen und verwertbare forensische Informationen

Proofpoint Closed-Loop Email Analysis and Response (CLEAR)

Anwender können verdächtige Nachrichten problemlos melden und erhalten positive Rückmeldungen, die die Sicherheitskultur verstärken

Unsere Lösung Proofpoint Threat Response Auto-Pull (TRAP) entfernt schädliche E-Mails automatisch aus Posteingängen. Dies umfasst auch E-Mails, die von Anwendern gemeldet wurden, sowie solche, die erst nach der Zustellung „scharf geschaltet“ werden – selbst wenn sie bereits an andere Anwender weitergeleitet wurden.

Die Proofpoint CLEAR-Funktion (Closed-Loop Email Analysis and Response) erleichtert Ihren Anwendern die Meldung verdächtiger Nachrichten. Die gemeldeten Nachrichten werden schnell analysiert, damit tatsächliche Bedrohungen verifiziert und blockiert werden. Zudem erhalten die Benutzer nach der Meldung eine positive Rückmeldung, die zur Stärkung Ihrer Sicherheitskultur beiträgt. HTML-basierte E-Mail-Warnhinweise machen Anwender auf potenziell unsichere E-Mails aufmerksam. Gemeinsam verringern diese Funktionen den Zeitaufwand für die Untersuchung und Behebung von E-Mail-Bedrohungen erheblich.

Proofpoint TRAP ergänzt Sicherheitswarnmeldungen zudem mit verwertbaren forensischen Informationen, sodass Ihr Sicherheitsteam Zwischenfälle schneller und effizienter überprüfen und beheben kann. Proofpoint TRAP baut auf einem riesigen Schatz an Bedrohungsdaten auf. Unser Nexus Threat Graph, der auf Billionen von Datenpunkten basiert, berücksichtigt Echtzeitdaten aus Millionen Posteingängen weltweit sowie Erkenntnisse aus Proofpoint Emerging Threats und Drittanbieterquellen.

Proofpoint ermöglicht Ihnen zudem, Übernahmen von Microsoft 365-Konten zu beheben, bevor es zu nachhaltigen Schäden kommt. Außerdem bieten wir Integrationen mit bereits von Ihnen eingesetzten Sicherheitstools, darunter Okta und CyberArk.

GRUND 6

Intelligente Compliance und Archivierung

Ein Archiv, aus dem Sie benötigte Daten nicht schnell abrufen können, hat seinen Zweck verfehlt.

Wir garantieren Ihnen, dass Ihre Suchvorgänge mit Proofpoint unabhängig von der Größe Ihres Archivs maximal 20 Sekunden dauern – nicht Minuten oder Stunden.

Unser Cloud-basiertes Archiv unterstützt mehr als 500 Dateitypen in der Cloud und lokal, nicht nur E-Mails.

Wir unterstützen eine unbegrenzte Anzahl an einbeziehbaren E-Discovery-Fällen, rechtlichen Sperrfristen und Datenexporten – ganz gleich, ob es sich um 10.000 oder 100.000 (oder auch mehr) Postfächer handelt.

GRUND 7

Security-Awareness-Programme, die Anwenderverhalten verändern

Das Hauptziel der Angreifer sind Ihre Anwender – und diese stellen damit das größte Risiko Ihres Unternehmens dar. Machen Sie sie mit erstklassigen Security-Awareness-Schulungen zur starken letzten Verteidigungslinie.

Mittels bewährter wissenschaftlicher Lerntechniken lernen Ihre Mitarbeiter, schädliche E-Mails zu erkennen, abzuwehren und zu melden, sodass unsere Schulungen dazu beitragen, das Anwenderverhalten nachhaltig zu verändern.

Wir bieten eine umfangreiche Auswahl an ansprechenden Inhalten auf Grundlage tatsächlich eingesetzter Angriffstechniken. Die Schulungsmaterialien basieren auf unseren eigenen Bedrohungsdaten und den Wissenslücken Ihrer Anwender. Zudem lassen sie sich auf die speziellen Sicherheitsanforderungen in Ihrem Unternehmen und mit den Zeitplänen Ihrer Mitarbeiter abstimmen.

Mit Phishing-Simulationen, die auf echten Bedrohungen und Techniken basieren und testen, wie zuverlässig Ihre Anwender die neuesten Angriffsformen erkennen, gehen wir noch einen Schritt weiter. Für Anwender, die auf die Angriffe hereinfallen, bieten wir punktuelles Feedback und nachträgliche Schulungen, damit Fehler zu lehrreichen Erfahrungen werden. Lernfortschritte lassen sich unkompliziert nachverfolgen und in Berichten zusammenfassen, sodass Sie Verbesserungspotenzial erkennen und eine Kultur des Sicherheitsbewusstseins aufbauen können.

GRUND 8

Lückenlose, vollständig integrierte Sicherheit, die Abläufe optimiert

Unsere umfassende Sicherheitsplattform kombiniert leistungsfähigen, effektiven E-Mail-, Cloud- und Datenschutz zur Bewältigung der drängendsten Sicherheits- und Compliance-Probleme unserer Zeit. Wir integrieren zudem erstklassige Sicherheitsanbieter wie Palo Alto Networks, Okta und CrowdStrike, sodass Sie Ihren Workflow optimieren können und Ihr Sicherheitsteam schneller und besser arbeiten kann.

Das Ergebnis ist eine integrierte, personenzentrierte Sicherheitslösung, die Ihre Microsoft 365-Investition schützt.

Durch unseren bewährten Sicherheits- und Compliance-Ansatz für Microsoft 365 erhalten Sie folgende Vorteile:

Minimierung von Risiken

Entlastung wichtiger Sicherheits- und IT-Ressourcen

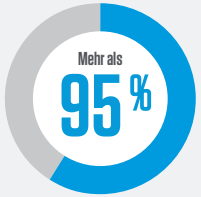
Geringere Kosten

Höhere Effektivität und Effizienz Ihrer Sicherheitsabläufe

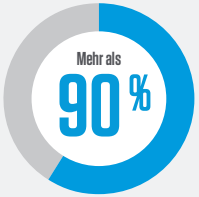
GRUND 9

Erstklassiger Support

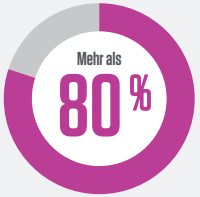
Wir kümmern uns um die vollständige Installation und Anpassung Ihrer Bereitstellung und nutzen dabei die neuesten Branchenentwicklungen sowie empfohlene Vorgehensweisen. Nach der Bereitstellung erhalten Sie Support rund um die Uhr an 365 Tagen im Jahr – ganz ohne komplizierte Service-Add-ons.



zufriedene Kunden



jährliche Verlängerungsrate



der Fortune 100-Unternehmen gehören zu unseren Kunden

Unser Unternehmen erreicht dauerhaft eine Kundenzufriedenheit von mehr als 95 % und eine jährliche Verlängerungsrate von mehr als 90 %. Daher ist es nicht überraschend, dass über 80 % der Fortune 100-Unternehmen zu unseren Kunden zählen. Wir bedienen folgende Unternehmen:

Die weltweit größten Banken

Die weltweit größten Einzelhändler

Die weltweit größten Pharmaunternehmen

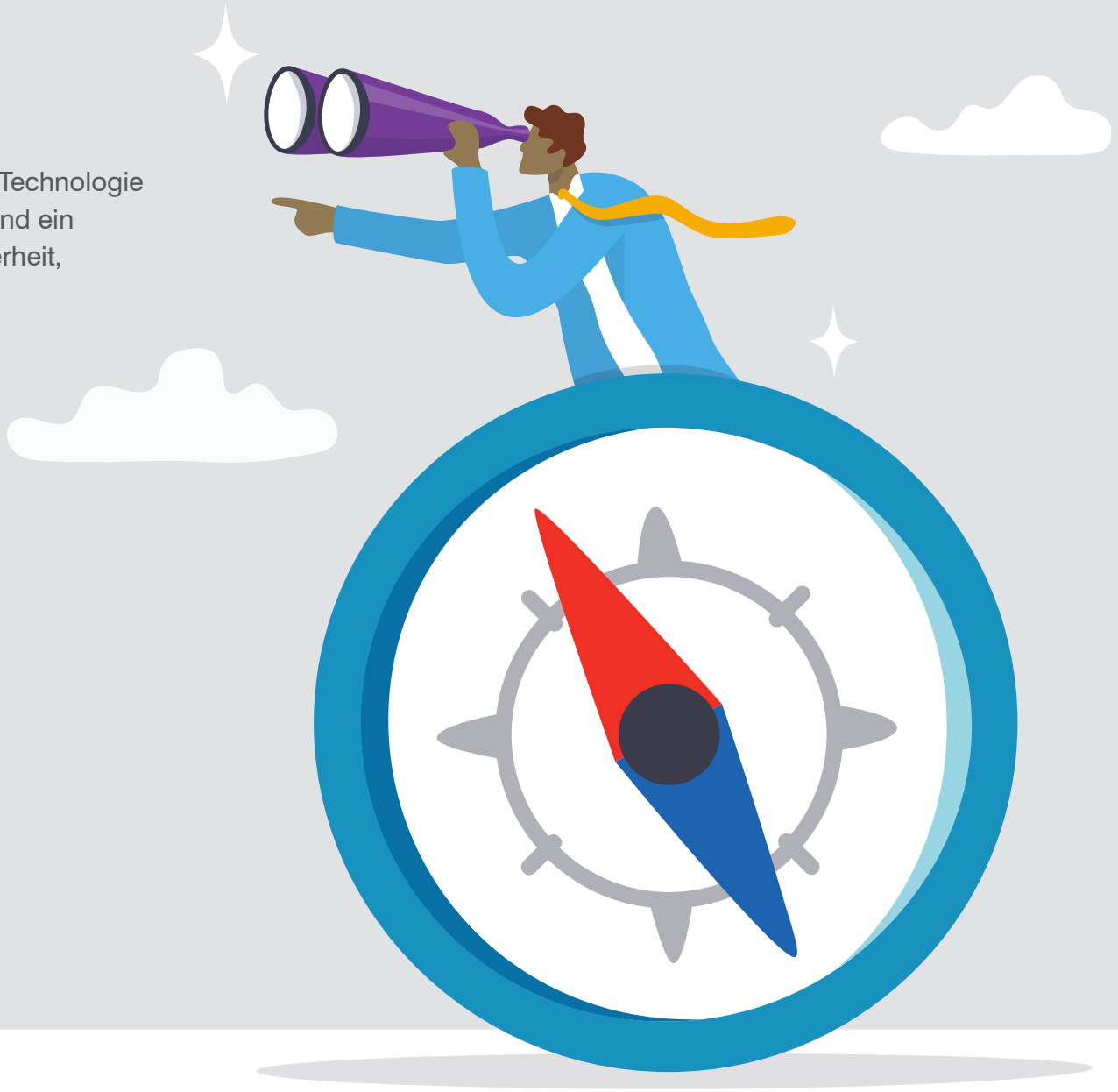
Die größten Forschungsuniversitäten

Die meisten dieser Unternehmen sind auch Abonnenten von Microsoft 365 E3 oder E5. Während sie sich also bei der Produktivität auf Microsoft verlassen, setzen sie bei der Sicherheit auf Proofpoint.

GRUND 10

Branchenführend

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



Wir entwickeln kontinuierlich Innovationen, um Microsoft 365-Umgebungen vor einer Vielzahl von Bedrohungen zu schützen – und zwar auch vor neuen und zukünftigen Angriffstechniken. Wir verfügen über einen der größten Datensätze in der Cybersicherheitsbranche und können daher Bedrohungen schneller erkennen und effektiver abwehren.

Unser oberstes Ziel ist es, unsere Kunden zufrieden zu stellen. Nachfolgend finden Sie einige der Auszeichnungen, die wir für unsere Arbeit erhalten haben:

- Im Magic Quadrant für Unternehmensdatenarchivierung 2022 das 10. Jahr in Folge als führendes Unternehmen eingestuft
- Gartner Peer Insights Customers‘ Choice 2022 in der Kategorie „Security Service Edge“
- Cybersecurity Excellence Awards Gold Winner 2022 in über 25 Kategorien, darunter Malware-Schutz, Phishing-Schutz, Sicherheit durch künstliche Intelligenz, AWS-Cloud-Sicherheit, Azure-Cloud-Sicherheit, Cloud Access Security Broker, Schutz vor Datenlecks, E-Mail-Sicherheit, Schutz vor Insider-Bedrohungen und Security-Awareness-Programm
- Gewinner des CISO Choice Awards for Premier Security Company 2021, Lösungen für E-Mail- und Cloud-Sicherheit
- Cybersecurity Breakthrough Awards 2021, Anbieter des Jahres für E-Mail-Sicherheitslösungen für Unternehmen (das zweite Jahr in Folge)

Nächste Schritte

Unsere umfassende integrierte Sicherheitsplattform kombiniert leistungsfähigen, effektiven Cloud- und E-Mail-Schutz zur Bewältigung der drängendsten Herausforderungen unserer Zeit. Außerdem bieten wir Ihnen flexible Bereitstellungsoptionen, einschließlich Inline- und API-basierter Optionen. Das bedeutet, dass wir Ihre Microsoft 365-Umgebung schnell und einfach schützen können, ohne Ihre bestehende Infrastruktur stören zu müssen.

Wir integrieren zudem erstklassige Sicherheitsanbieter wie Palo Alto Networks, Okta und CrowdStrike, sodass Sie Ihren Workflow optimieren können und Ihr Sicherheitsteam schneller und besser arbeiten kann.

Das Ergebnis ist eine integrierte, personenzentrierte Sicherheitslösung für Ihre Cloud-Umgebung. Durch unseren bewährten Sicherheits- und Compliance-Ansatz für Microsoft 365 erhalten Sie folgende Vorteile:

- Minimierung von Risiken
- Freigabe von Ressourcen
- Geringere Kosten
- Höhere Effektivität und Effizienz Ihrer Sicherheitsabläufe

Erfahren Sie mehr über Proofpoint und wie wir die Sicherheit Ihrer Microsoft 365-Bereitstellung verbessern können. Informieren Sie sich über personenzentrierte Sicherheit, Datenverlustprävention und Compliance für E-Mail, Cloud, Web und Endpunkte.

Besuchen Sie **proofpoint.com/de/solutions/microsoft-365-security-compliance**.

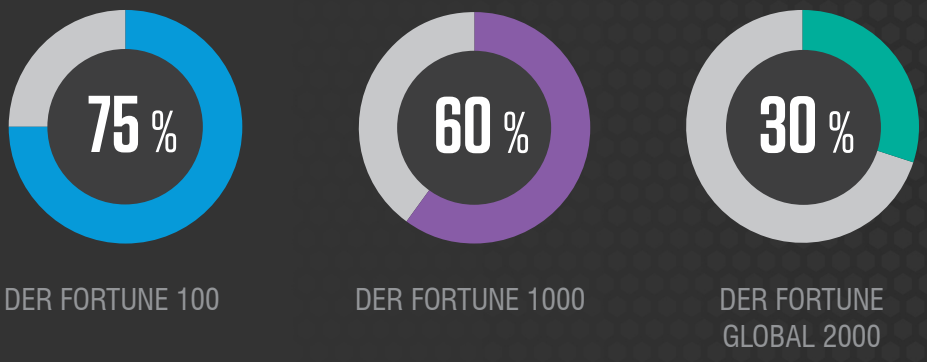
Informationen zu Proofpoint

Proofpoint Nexus Threat Graph verbindet die branchenweit beste Sicherheitsforschung, Technologie und Bedrohungsdaten, um Sie in allen Angriffsphasen zu schützen. Kein anderer Anbieter verfügt über umfangreichere Einblicke in die Mechanismen aktueller Cyberangriffe.

Wir analysieren täglich mehr als:

2,6 Mrd. E-MAILS	**49 Mrd.** URLS	**1,9 Mrd.** ANHÄNGE
1,7 Mrd. MOBILGERÄTE-NACHRICHTEN	**430 Mio.** WEB-DOMAINS	**143.000** SOCIAL-MEDIA-KONTEN

Auf unsere Lösungen vertrauen mehr als:



8.000 GROSSUNTERNEHMEN

200.000 KLEINE UNTERNEHMEN

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU 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 75 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**.

proofpoint.

0503-003-04-03 04/23