

proofpoint®

EBOOK

Proofpoint e Microsoft: insieme per una maggior sicurezza

Rafforza la sicurezza di Microsoft 365
grazie al rilevamento avanzato delle
minacce e al filtraggio di spam e graymail



PROOFPOINT
E MICROSOFT:
INSIEME PER UNA
MAGGIOR SICUREZZA

Rafforzamento della protezione del tuo ambiente Microsoft 365

Protezione avanzata contro gli
attacchi informatici elusivi

Gateway email sicuro o API?
Proofpoint ti permette
di scegliere

Perché scegliere Proofpoint?

Rafforzamento della protezione del tuo ambiente Microsoft 365

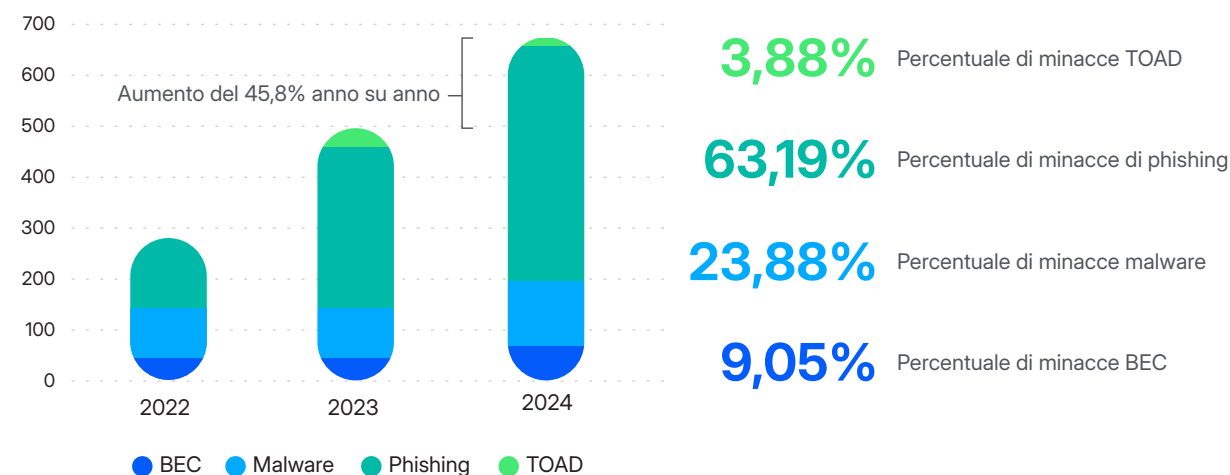
Non importa se disponi di funzionalità di base di sicurezza dell'email Microsoft o hai effettuato l'upgrade a Microsoft Defender per Office 365. Con l'adozione diffusa di Microsoft 365 come piattaforma professionale, gli attacchi sono destinati ad aumentare. L'email è oggi il punto di partenza per un ampio numero di attacchi informatici, perciò il rafforzamento della tua sicurezza dell'email Microsoft dovrebbe essere una priorità assoluta.

Uno dei motivi per cui queste tendenze sono così allarmanti è che gli attacchi trasmessi via email continuano a essere un problema per molte aziende, anche quelle che utilizzano le difese incorporate di Microsoft. Le valutazioni della sicurezza dell'email di Proofpoint rivelano che le minacce avanzate possono ancora eludere il rilevamento di Microsoft. Di conseguenza, le aziende sono ancora esposte alle minacce come le seguenti:

- Phishing avanzato
- Malware
- Violazione dell'email aziendale (BEC, Business Email Compromise)
- Codici QR
- URL dannosi
- Attacchi tramite telefonate (TOAD, Telephone-Oriented Attack Delivery)

Protezione ininterrotta contro le minacce in aumento

Minacce avanzate rilevate da Proofpoint nelle valutazioni delle minacce



PROOFPOINT E MICROSOFT: INSIEME PER UNA MAGGIOR SICUREZZA

Rafforzamento della
protezione del tuo ambiente
Microsoft 365

Protezione avanzata contro
gli attacchi informatici elusivi ●

Gateway email sicuro o API?
Proofpoint ti permette
di scegliere

Perché scegliere Proofpoint?



Protezione avanzata contro gli attacchi informatici elusivi

Phishing, URL dannosi e malware

I criminali informatici continuano a inviare una gran quantità di link e allegati dannosi via email, che possono essere bloccati solo con una protezione avanzata dell'email.

Proofpoint utilizza il sandboxing predittivo, l'estrazione di URL, il rilevamento delle elusioni, l'isolamento del browser e una gamma di altre tecniche avanzate per offrire la difesa più efficace contro questi payload dannosi.

Protezione contro gli attacchi BEC

Gli attacchi di furto d'identità senza payload, come gli attacchi BEC, sono tra i più difficili da rilevare perché queste email spesso sembrano legittime.

I motori Proofpoint NexusAI analizzano le relazioni degli utenti e il loro linguaggio ricercando anche altri potenziali indicatori di minaccia. La mancata corrispondenza degli attributi dell'intestazione, un circuito di riscontri DMARC e il comportamento del mittente forniscono informazioni preziose che utilizziamo per bloccare le minacce BEC.

Protezione contro gli attacchi TOAD

Negli attacchi TOAD (Telephone-Oriented Attack Delivery), noti anche come phishing di callback, i criminali informatici inviano email che cercano di convincere i destinatari a chiamare un call center fasullo.

Queste minacce possono essere difficili da rilevare perché raramente includono payload dannosi. I motori Proofpoint NexusAI utilizzano machine learning e computer vision per ricercare indicatori di minacce noti per bloccare tali minacce (numeri di telefono dannosi, codici QR e furti d'identità basati sulle immagini, ecc.).

PROOFPOINT E MICROSOFT: INSIEME PER UNA MAGGIOR SICUREZZA

Rafforzamento della
protezione del tuo ambiente
Microsoft 365

Protezione avanzata contro
gli attacchi informatici elusivi ●

Gateway email sicuro o API?
Proofpoint ti permette
di scegliere

Perché scegliere Proofpoint?

La stragrande maggioranza dei clienti Microsoft che desiderano rafforzare la sicurezza della propria email sceglie Proofpoint. L'85% delle aziende della classifica Fortune 100 - e oltre 1,88 milioni di clienti in tutto il mondo - ci ha scelto come partner di sicurezza privilegiato.

Proofpoint eccelle nei report di analisi come il Magic Quadrant di Gartner. Nell'ultimo report di Gartner *sulle funzionalità essenziali delle piattaforme di sicurezza dell'email*, Proofpoint si è classificata al primo posto in quattro dei cinque casi d'uso¹.

Proofpoint Core Email Protection blocca il 99,99% delle minacce veicolate tramite email, spam e graymail. Il nostro stack di rilevamento multilivello Proofpoint Nexus combina grafici delle relazioni, machine learning, computer vision e analisi semantica. È alimentato dai dati sulle minacce

provenienti da oltre 3 bilioni di email che analizziamo ogni anno. Di conseguenza, può prevenire la maggior parte delle minacce attuali più avanzate, tra cui:

- Attacchi BEC
- Takeover degli account
- Minacce dei codici QR
- Furto d'identità
- Phishing laterale

Proofpoint Core Email Protection va oltre il blocco delle minacce. Aiuta anche i team della sicurezza, che usufruiscono di flussi di lavoro ottimizzati basati sugli avvisi e di funzionalità di ricerca integrate. Inoltre, le email segnalate dagli utenti vengono bonificate automaticamente e gli utenti ricevono formazione in tempo reale ogni volta che segnalano un'email sospetta.



“La piattaforma [Proofpoint] eccelle nella protezione di base dell'email grazie alle sue solide funzionalità di rilevamento delle minacce basate sull'IA, analisi multilivello dei contenuti e sandboxing avanzato”².

GARTNER

1. Gartner, *Critical Capabilities for Email Security Platforms Report* (Report sulle funzionalità essenziali delle piattaforme di sicurezza dell'email), gennaio 2025.
2. Ibid.

**PROOFPOINT
E MICROSOFT:
INSIEME PER UNA
MAGGIOR SICUREZZA**

Rafforzamento della
protezione del tuo ambiente
Microsoft 365

Protezione avanzata contro
gli attacchi informatici elusivi

Gateway email sicuro o API? ●
**Proofpoint ti permette
di scegliere**

Perché scegliere Proofpoint?

Gateway email sicuro o API?

Proofpoint ti permette di scegliere

Criterio n.1: valorizzazione

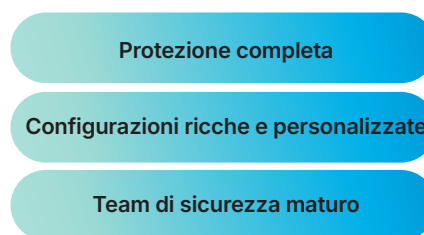
Quando scegliere un'implementazione basata su API

Le implementazioni basate su API di Proofpoint richiedono solo qualche giorno. Ricevi protezione automatizzata entro 48 ore, dopo che il sistema è stato addestrato con un anno di dati degli utenti. La nostra soluzione basata su API è ideale per i team che desiderano una sicurezza informatica dell'email potente ma quasi automatica.

Quando scegliere un gateway email sicuro

Le implementazioni Proofpoint tramite gateway email sicuro possono richiedere qualche settimana, ma contribuiscono a ridurre la maggior parte dei rischi grazie a una protezione prima della consegna, dopo la consegna e al momento del clic. La nostra soluzione basata su un gateway email sicuro fornisce più opzioni di configurazione e personalizzazione della tua implementazione. È ideale per i team che desiderano rafforzare la protezione della loro architettura.

Gateway email sicuro



Criterio n. 2: orientamento Microsoft

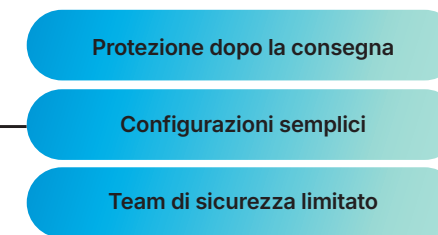
Quando scegliere un'implementazione basata su API

Se desideri rafforzare il gateway email sicuro di Microsoft con la protezione dopo la consegna di Proofpoint, utilizza la nostra integrazione con l'API Microsoft Graph. La soluzione Proofpoint basata su API offre un'esperienza utente in Outlook nativa per le minacce trasmesse via email, lo spam e la graymail.

Quando scegliere un gateway email sicuro

Se desideri sostituire il gateway email sicuro di Microsoft, utilizza Proofpoint. La nostra soluzione basata su gateway email sicuro fornisce protezione prima della consegna, dopo la consegna e al momento del clic grazie a Proofpoint Browser Isolation.

API



Criterio n. 3: complessità dell'infrastruttura email

Quando scegliere un'implementazione basata su API

Se desideri utilizzare il gateway email sicuro Microsoft della tua azienda per l'indirizzamento delle email, scegli la soluzione basata Proofpoint basata su API. In generale, i clienti che scelgono l'API hanno requisiti semplici in termini di infrastruttura email.

Quando scegliere un gateway email sicuro

Se la tua azienda ha un'infrastruttura email sofisticata, scegli un gateway email sicuro. In generale, i clienti che optano per il gateway email sicuro desiderano applicare policy che controllano il flusso delle email e che si basano su condizioni come il dominio del mittente e l'autenticazione.

PROOFPOINT
E MICROSOFT:
INSIEME PER UNA
MAGGIOR SICUREZZA

Rafforzamento della
protezione del tuo ambiente
Microsoft 365

Protezione avanzata contro
gli attacchi informatici elusivi

Gateway email sicuro o API?
Proofpoint ti permette
di scegliere

Perché scegliere Proofpoint? ●

Perché scegliere Proofpoint?

Informazioni su Proofpoint

Protezione delle persone

1,4 Bln

Email analizzate
ogni anno

>1,4 Bln

SMS/MMS analizzati
ogni anno

124 Mln

Attacchi BEC bloccati
ogni mese

>183 Mln

Simulazioni di attacchi
di phishing ogni anno

0,8 Bln

Allegati analizzati
ogni anno

21 Bln

URL analizzati ogni
anno

177 Mln

Attacchi BEC bloccati
ogni anno

Accettazione da parte del mercato

**>1,88
Mln**

di clienti

> 150

ISP e operatori
di telefonia

85%

Aziende
Fortune 100
protette
da Proofpoint

50%

Aziende
Fortune 100
che utilizzano
Proofpoint DLP

>60%

Aziende Fortune
1000 protette
da Proofpoint



proofpoint®

Proofpoint, Inc. è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui l'85% delle Fortune 100, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: www.proofpoint.com/it.

Seguici: [LinkedIn](#)

Proofpoint è un marchio registrato di Proofpoint, Inc. negli Stati Uniti e/o negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.

SCOPRI LA PIATTAFORMA PROOFPOINT →