

proofpoint.

Proteggere Microsoft 365

Dieci motivi per scegliere Proofpoint
per proteggere le distribuzioni cloud

proofpoint.com/it





INTRODUZIONE

Molte aziende stanno migrando verso il cloud e hanno bisogno di supportare i loro dipendenti, sempre più dispersi e spesso in telelavoro. Per molte di loro, Microsoft 365 rappresenta un modo totalmente nuovo di operare, che richiede un approccio completamente nuovo alla sicurezza e alla conformità.

Gli attuali attacchi informatici prendono di mira le persone, ovunque lavorino e qualsiasi sia il dispositivo che utilizzano. I clienti di Microsoft 365 si rivolgono a Proofpoint per il suo approccio alla sicurezza e alla conformità incentrato sulle persone. Ecco perché.

Introduzione

1 Protezione avanzata dell'email

2 Sicurezza dei dati

3 Protezione completa

4 Protezione contro i ladri di account

5 Visibilità e sicurezza del cloud

6 Risposta ultrarapida agli incidenti

7 Archiviazione intelligente

8 Formazione sulla sicurezza

9 Servizio di assistenza di prim'ordine

10 Sicurezza integrata

Protezione avanzata e più rapida dell'email



La migliore difesa contro gli attacchi informatici è quella in grado di neutralizzare le minacce alla fonte. Questo è il motivo per cui aiutiamo i clienti di Microsoft 365 a bloccare un maggior numero di minacce e email indesiderate, prima che raggiungano le caselle di posta degli utenti.

Gli attacchi via email oggi si presentano sotto varie forme. Possiamo aiutarti a bloccarli tutti.

Con un tempo medio di analisi inferiore ai tre minuti, blocchiamo gli allegati dannosi prima che i tuoi utenti abbiano la possibilità di interagirvi e senza interrompere il loro lavoro. Supportiamo un'ampia gamma di tipi di file, inclusi PDF e HTML, non solo i documenti di Office.

La nostra protezione contro il malware si integra anche con le nostre funzioni di rilevamento degli URL. L'analisi predittiva degli URL permette di valutare e neutralizzare gli URL pericolosi prima che vengano recapitati e quando gli utenti fanno clic. Puoi bloccare gli allegati che contengono link pericolosi e riscrivere gli URL sospetti in qualsiasi file: testo (.txt), rich-text (.rtf) o HTML.

Ciò detto, alcuni attacchi via email non utilizzano affatto il malware. Ecco perché la nostra soluzione globale e integrata blocca anche i tentativi di violazione dell'email aziendale (BEC, Business Email Compromise) e di violazione degli account email (EAC, Email Account Compromise). Possiamo contrastare tutte le tattiche utilizzate dai criminali informatici. La nostra soluzione ti offre una visibilità approfondita sulle attività e sui comportamenti dannosi degli utenti. Inoltre, automatizza passaggi fondamentali del processo di risposta agli incidenti per aiutarti a proteggere tutti i tuoi utenti.

La nostra soluzione intercetta un maggior numero di minacce basate sugli URL con il sandboxing multi-livello basato sull'analisi statica e dinamica. Rileva sia il codice dannoso che i siti web di phishing delle credenziali - anche quelli che utilizzano tecniche di aggiramento dell'ambiente sandbox - che altri approcci basati su macchine virtuali non riescono a rilevare.

Per gli utenti e i siti web ad alto rischio, la nostra tecnologia di isolamento degli URL apre i link sconosciuti inclusi nelle email in un ambiente sicuro e autonomo per tenere le minacce al di fuori del tuo ambiente.

Introduzione

1 Protezione avanzata dell'email

2 Sicurezza dei dati

3 Protezione completa

4 Protezione contro i ladri di account

5 Visibilità e sicurezza del cloud

6 Risposta ultrarapida agli incidenti

7 Archiviazione intelligente

8 Formazione sulla sicurezza

9 Servizio di assistenza di prim'ordine

10 Sicurezza integrata

Mantieni la conformità, evitando di incorrere in sanzioni, senza le seccature tipiche delle tradizionali soluzioni di prevenzione della fuga di dati (DLP). Semplifichiamo la creazione, l'applicazione e l'implementazione di policy unificate per l'email e le applicazioni cloud per mantenere i tuoi dati sicuri e conformi.

L'analisi algoritmica integrata, il nostro motore di identificazione intelligente e i dizionari ti consentono di concentrarti sulla definizione e la gestione delle policy per i dati specifiche per la tua azienda.

I nostri flussi di lavoro DLP pronti all'uso semplificano l'identificazione, la gestione e la segnalazione delle violazioni. La nostra soluzione offre anche funzionalità avanzate che semplificano notevolmente la sicurezza e la conformità dei dati. Ecco alcuni esempi:

- Conferma di lettura
- Corrispondenza esatta dei dati a più colonne
- Crittografia push/pull
- Semplice processo di revoca delle chiavi
- Funzionalità TLS di emergenza

Non importa quanto complesse siano le tue esigenze di sicurezza dei dati, non sarai ostacolato da blocchi tecnici.

Sicurezza dei dati

per l'email e il cloud



2

Introduzione

1 Protezione avanzata dell'email

2 Sicurezza dei dati

3 Protezione completa

4 Protezione contro i ladri di account

5 Visibilità e sicurezza del cloud

6 Risposta ultrarapida agli incidenti

7 Archiviazione intelligente

8 Formazione sulla sicurezza

9 Servizio di assistenza di prim'ordine

10 Sicurezza integrata

Protezione completa

contro i tentativi di violazione delle email aziendali e degli account email

3



Alcune minacce non utilizzano file dannosi. Gli attacchi di violazione dell'email aziendale (BEC) e violazione degli account email (EAC) sono due aspetti di un problema che costa alle aziende ben 26 miliardi di dollari¹.

Poiché questi attacchi possono assumere diverse forme, non esiste un approccio unico in grado di neutralizzarli tutti. Uno strumento di sicurezza può sconfiggere uno o due tipi di tattica, lasciandoti però indifeso contro una moltitudine di altri attacchi.

Ecco perché hai bisogno di una soluzione in grado di gestire ogni aspetto di queste minacce ingannevoli e difficili da rilevare. La nostra soluzione globale integrata è in grado di neutralizzare tutte le tattiche di attacco utilizzate dagli hacker. La nostra soluzione ti offre una visibilità approfondita sulle attività e sui comportamenti dannosi degli utenti. Inoltre, automatizza passaggi fondamentali del processo di risposta agli incidenti per aiutarti a proteggere tutti i tuoi utenti.

¹ FBI. "Business Email Compromise: The \$26 Billion Scam." (Violazione dell'email aziendale: una truffa da 26 miliardi di dollari), settembre 2019.

Introduzione

1 Protezione avanzata dell'email

2 Sicurezza dei dati

3 Protezione completa

4 Protezione contro i ladri di account

5 Visibilità e sicurezza del cloud

6 Risposta ultrarapida agli incidenti

7 Archiviazione intelligente

8 Formazione sulla sicurezza

9 Servizio di assistenza di prim'ordine

10 Sicurezza integrata

Nelle mani sbagliate, un account cloud può trasformarsi in un'arma formidabile.

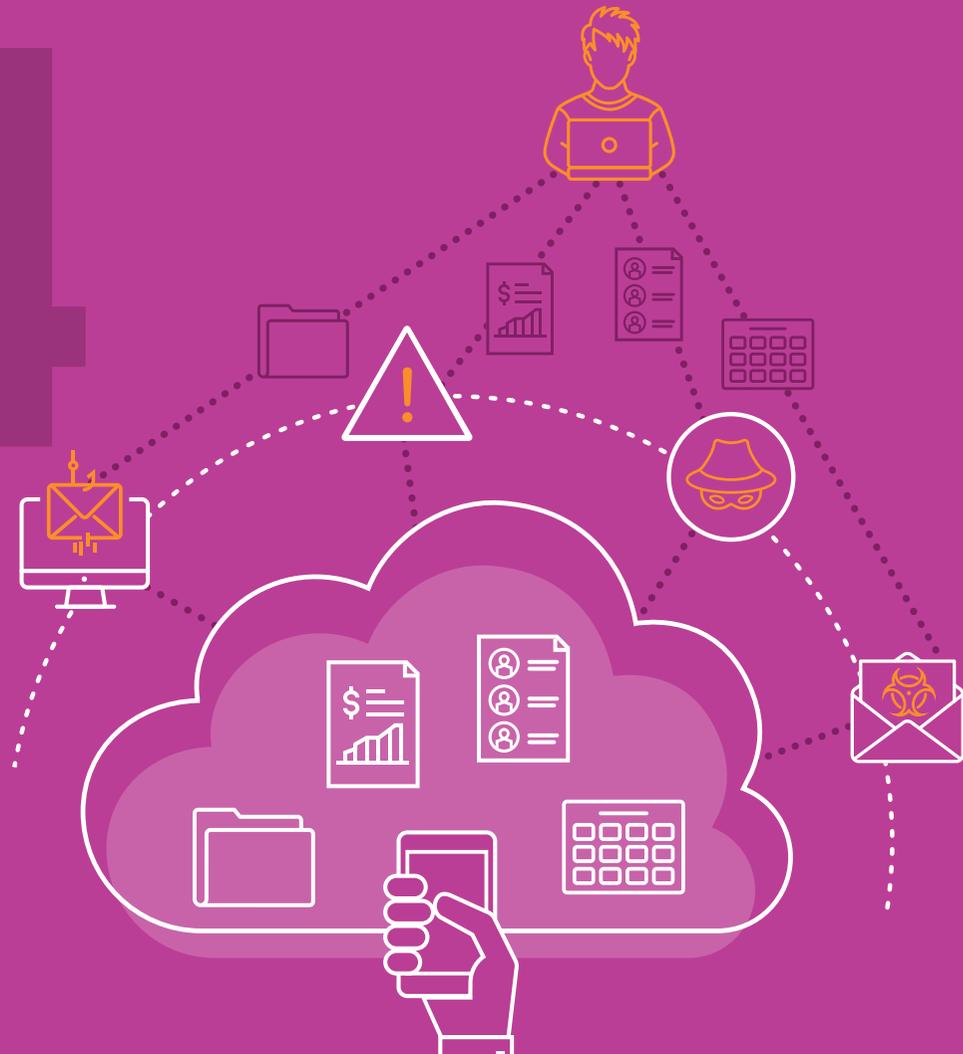
Gli hacker che assumono il controllo degli account dei tuoi utenti possono fare ciò che vogliono con i dati sensibili a cui hanno accesso. Chiunque prenda il controllo di un account email può approfittarsi delle persone che lo ritengono attendibile, dentro e fuori il tuo ambiente.

Grazie al nostro approccio multi-livello, ti aiutiamo a proteggere il tuo account Microsoft 365 con avvisi in tempo reale delle attività sospette, attività di remediation automatiche e controlli dell'accesso in base al livello di rischio. Quando si verifica un incidente, puoi analizzare le attività e gli allarmi passati utilizzando la nostra dashboard intuitiva. Policy efficaci ti segnalano i problemi in tempo reale, applicano le misure necessarie agli account violati, mettono in quarantena i file dannosi e applicano un'autenticazione basata sul rischio, quando necessario.

Protezione

contro i ladri di account Microsoft 365

4



Introduzione

1 Protezione avanzata dell'email

2 Sicurezza dei dati

3 Protezione completa

4 Protezione contro i ladri di account

5 Visibilità e sicurezza del cloud

6 Risposta ultrarapida agli incidenti

7 Archiviazione intelligente

8 Formazione sulla sicurezza

9 Servizio di assistenza di prim'ordine

10 Sicurezza integrata

Visibilità e sicurezza ottimali per il cloud



Il “perimetro umano” ha preso il posto del tradizionale perimetro di rete. I tuoi dipendenti condividono dati sensibili senza supervisione, utilizzano app cloud non autorizzate e un gran numero di dispositivi personali.

Questo è il motivo per cui adottiamo un approccio incentrato sulle persone per la protezione contro le minacce nel cloud, per individuare i dispositivi della Shadow IT (IT ombra) e governando le app cloud e di terze parti che utilizzano OAuth.

Grazie a una ricca intelligence sulle minacce che copre diversi canali e dati contestuali specifici per l'utente, andiamo ben oltre la sicurezza nativa di Microsoft 365 per salvaguardare gli utenti, i dati sensibili e le applicazioni cloud dalle minacce esterne e dai rischi di conformità. Identifica i tuoi VAP (Very Attacked People™ ovvero le persone più attaccate) e applica controlli in base al rischio per proteggere i loro account. Classifica i tuoi dati sensibili e rileva autorizzazioni troppo ampie per i file e le condivisioni di dati non autorizzate. Scopri quali sono le applicazioni e i servizi cloud che i tuoi dipendenti utilizzano e controlla il loro accesso a dati e risorse.

Introduzione

1 Protezione avanzata dell'email

2 Sicurezza dei dati

3 Protezione completa

4 Protezione contro i ladri di account

5 Visibilità e sicurezza del cloud

6 Risposta ultrarapida agli incidenti

7 Archiviazione intelligente

8 Formazione sulla sicurezza

9 Servizio di assistenza di prim'ordine

10 Sicurezza integrata

Più a lungo una minaccia persiste nel tuo ambiente Microsoft 365, maggiore è il danno che può causare.

Ecco perché una risposta rapida ed efficace agli incidenti è fondamentale per mantenere protetta la tua azienda. La nostra soluzione Threat Response Auto-Pull (TRAP) rimuove le email dannose dalla casella email dei tuoi utenti, anche se sono già state consegnate o inoltrate ai colleghi.

TRAP arricchisce inoltre gli avvisi di sicurezza con informazioni forensi permettendo al tuo team di sicurezza di verificare e risolvere gli incidenti in modo più rapido ed efficiente. TRAP si avvale di un patrimonio di informazioni di threat intelligence che include dati in tempo reale raccolti da milioni di caselle email in tutto il mondo. Integriamo anche informazioni di threat intelligence provenienti dalla piattaforma Emerging Threats e da fonti di terze parti.

Inoltre, supportiamo un'ampia gamma di sistemi email - non solo Microsoft 365 - e le nostre soluzioni si integrano perfettamente con gli strumenti di sicurezza che già utilizzi, come per esempio Okta e CyberArk.

Risposta agli incidenti

ultrarapida in tutta l'azienda



Introduzione

1 Protezione avanzata dell'email

2 Sicurezza dei dati

3 Protezione completa

4 Protezione contro i ladri di account

5 Visibilità e sicurezza del cloud

6 Risposta ultrarapida agli incidenti

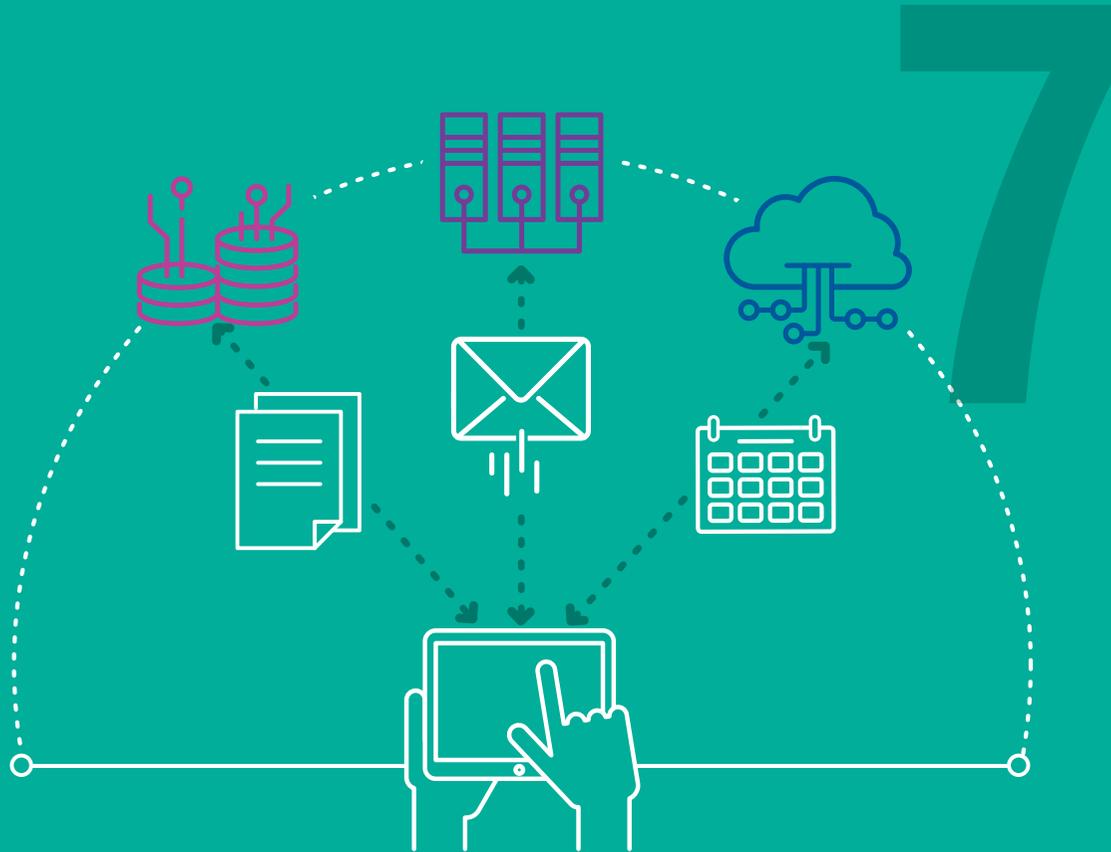
7 Archiviazione intelligente

8 Formazione sulla sicurezza

9 Servizio di assistenza di prim'ordine

10 Sicurezza integrata

Archiviazione intelligente e ultrarapida



Se il tuo sistema di archiviazione non ti permette di recuperare rapidamente i dati di cui hai bisogno, in ultima analisi non ti è di alcuna utilità. Indipendentemente dalle dimensioni dei tuoi archivi, ti garantiamo un tempo di ricerca di 20 secondi o ancora meno.

La nostra soluzione di archiviazione cloud supporta oltre 500 tipi di file on premise e nel cloud, non soltanto le email. Inoltre, non limitiamo il numero di file di e-discovery o archivi che sei tenuto a conservare a fini legali, né il numero di esportazioni di dati che puoi includere - sia che si tratti di 10.000 o di 100.000 caselle email (o più).

Introduzione

1 Protezione avanzata dell'email

2 Sicurezza dei dati

3 Protezione completa

4 Protezione contro i ladri di account

5 Visibilità e sicurezza del cloud

6 Risposta ultrarapida agli incidenti

7 Archiviazione intelligente

8 Formazione sulla sicurezza

9 Servizio di assistenza di prim'ordine

10 Sicurezza integrata

I tuoi utenti sono l'obiettivo principale dei criminali informatici, e anche il tuo principale fattore di rischio. Offri loro una formazione di sensibilizzazione alla sicurezza all'avanguardia per trasformarli in un caposaldo della tua difesa.

Basato su metodi didattici collaudati ed efficaci, i nostri corsi di formazione permettono di modificare i comportamenti dei tuoi utenti aiutandoli a identificare, rifiutare e segnalare le email dannose.

Offriamo una vasta biblioteca di contenuti interessanti basati su tecniche di attacco reali. Queste si basano sulle nostre informazioni di threat intelligence. Inoltre, i nostri corsi sono abbastanza flessibili per essere adattati alle sfide di sicurezza specifiche per la tua azienda.

Oltre a questi corsi di formazione di base, proponiamo anche simulazioni di attacchi di phishing e una formazione successiva puntuale per gli utenti che si sono lasciati ingannare. I nostri report semplici e intuitivi ti permettono di monitorare i progressi raggiunti per aiutarti a identificare le aree di miglioramento e contribuire alla crescita dei tuoi utenti.

Formazione sulla sicurezza

che sensibilizza gli utenti, senza mai infastidirli



Introduzione

1 Protezione avanzata dell'email

2 Sicurezza dei dati

3 Protezione completa

4 Protezione contro i ladri di account

5 Visibilità e sicurezza del cloud

6 Risposta ultrarapida agli incidenti

7 Archiviazione intelligente

8 Formazione sulla sicurezza

9 Servizio di assistenza di prim'ordine

10 Sicurezza integrata

Servizio di assistenza di prim'ordine

9



Ogni acquisto include l'installazione completa e la personalizzazione della soluzione, nonché l'accesso alle ultime tendenze e alle best practice del settore.

Offriamo assistenza 24 ore su 24, 7 giorni su 7 per 365 giorni all'anno dopo l'implementazione, senza moduli di servizio aggiuntivi complessi.

La nostra azienda vanta un tasso costante di soddisfazione della clientela superiore al 95% e un tasso di rinnovo annuale di oltre il 90%. Non stupisce che annoveriamo tra i nostri clienti più della metà delle aziende Fortune 100, tra cui:

- Le più grandi banche al mondo
- Le principali catene mondiali della grande distribuzione
- Le principali aziende farmaceutiche
- Gli istituti di ricerca più prestigiosi

Introduzione

1 Protezione avanzata dell'email

2 Sicurezza dei dati

3 Protezione completa

4 Protezione contro i ladri di account

5 Visibilità e sicurezza del cloud

6 Risposta ultrarapida agli incidenti

7 Archiviazione intelligente

8 Formazione sulla sicurezza

9 Servizio di assistenza di prim'ordine

10 Sicurezza integrata

La nostra piattaforma di sicurezza completa e integrata combina una potente protezione del cloud e dell'email per affrontare le sfide attuali più pressanti.

Si integra anche con le soluzioni di importanti fornitori di sicurezza come Palo Alto Networks, Okta e CrowdStrike per ottimizzare il tuo flusso di lavoro e aiutare il tuo team della sicurezza a lavorare meglio e più velocemente.

Insieme, queste soluzioni offrono una sicurezza unificata, incentrata sulle persone in grado di proteggere la tua implementazione cloud. Il nostro collaudato approccio alla sicurezza e alla conformità per Microsoft 365 diminuisce la tua esposizione ai rischi, libera le tue risorse, riduce i costi e migliora l'efficacia delle tue operazioni di sicurezza.

Sicurezza completa e integrata in grado di ottimizzare le operazioni



Introduzione

1 Protezione avanzata dell'email

2 Sicurezza dei dati

3 Protezione completa

4 Protezione contro i ladri di account

5 Visibilità e sicurezza del cloud

6 Risposta ultrarapida agli incidenti

7 Archiviazione intelligente

8 Formazione sulla sicurezza

9 Servizio di assistenza di prim'ordine

10 Sicurezza integrata



PER SAPERNE DI PIÙ

Per maggiori informazioni visita [proofpoint.com/it](https://www.proofpoint.com/it).

INFORMAZIONI SU PROOFPOINT

Proofpoint (NASDAQ: PFPT) è un'azienda leader nella cybersecurity, 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 più della metà delle Fortune 1000, 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.

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