

# Bundle Proofpoint

**Proteggi i tuoi collaboratori. Difendi i tuoi dati.**

Proofpoint offre un approccio unico alla sicurezza informatica incentrato sulle persone, che inizia con l'identificazione dei tuoi VAP™ (Very Attacked People ovvero le persone più attaccate) e la valutazione del rischio che ognuno di essi rappresenta per la tua azienda. I nostri bundle Proofpoint Threat Protection e Proofpoint Information Protection ti offrono soluzioni complete che si adattano all'attuale panorama delle minacce, rafforzano le tue risorse ed evolvono con la tua strategia di sicurezza. Questo documento ti fornisce una panoramica su questi bundle e spiega come possono aiutarti a proteggere i tuoi collaboratori e a difendere i tuoi dati.

## Intelligenza artificiale e machine learning alimentate dal grafico delle minacce Nexus

Proofpoint sfrutta l'intelligenza artificiale e il machine learning per proteggere utenti e dati. Sfruttando l'Intelligenza Artificiale e il machine learning nella nostra suite di prodotti, forniamo ai nostri clienti una protezione completa e costantemente aggiornata contro un'ampia gamma di minacce esterne. Sfruttiamo quasi due decenni di esperienza nell'intelligenza artificiale, nel machine learning e nell'elaborazione dei dati con la piattaforma di intelligenza artificiale che alimenta le soluzioni Proofpoint. Le nostre soluzioni sono così in grado di eliminare efficacemente un ampio spettro di rischi legati a sicurezza informatica e conformità.

Il nostro stack di rilevamento e la nostra threat intelligence si contraddistinguono dalla concorrenza grazie ai modelli di machine learning addestrati dal grafico delle minacce Nexus di Proofpoint che include oltre un bilione di nodi. Il grafico delle minacce Nexus ha accesso a enormi set di dati relativi alla sicurezza informatica che coprono email, cloud, reti, domini e altro ancora. I membri del nostro team interno che si occupano di elaborazione dei dati hanno conseguito dottorati e master in informatica nell'ambito della sicurezza informatica. Provengono inoltre dalla pubblica amministrazione e dal mondo accademico. Abbiamo collaborato con le principali università per essere all'avanguardia nell'elaborazione dei dati. Il team lavora sulle nostre soluzioni per la protezione contro le minacce, la protezione delle informazioni e l'archiviazione e la conformità in collaborazione con i ricercatori sulle minacce. Questa collaborazione massimizza l'efficacia del nostro motore di machine learning.

## Bundle Proofpoint Threat Protection - Proteggi i tuoi collaboratori

Proteggi i tuoi collaboratori dalle minacce che li prendono di mira. Integrando molteplici controlli a livello di email, cloud, utenti e fornitori, la piattaforma Proofpoint Threat Protection offre una protezione completa contro phishing, attacchi BEC/frodi via email, malware e ransomware. Questa piattaforma integrata alimentata dall'intelligenza artificiale, fornisce visibilità ineguagliata sulla tua superficie d'attacco, una protezione più efficace contro le minacce moderne e risultati operativi positivi. Tutti i bundle possono essere distribuiti facilmente grazie alle offerte Inline+API o basata sui record MX. Tutti offrono la stessa potente protezione.

### Presentazione di Proofpoint Threat Protection

FUNZIONALITÀ	COMPONENTE	PX	P0	P1	P1+
Implementazione e gestione	<ul style="list-style-type: none"> <li>On premise, ibrido o cloud</li> <li>Inline+API o basato sui record MX</li> </ul>	<ul style="list-style-type: none"> <li>Solo M365 Cloud</li> <li>Solo Inline+API</li> </ul>	✓	✓	✓
Violazione dell'email aziendale (BEC, Business Email Compromise)	Analisi comportamentale e della reputazione basata su IA/ML	✓	✓	✓	Dashboard dei rischi legati ai fornitori
Phishing, ransomware e malware	Analisi comportamentale e della reputazione basata su IA/ML	✓	✓	✓	✓
	Riscrittura degli URL e sandboxing al momento del clic		✓	✓	✓
	Sandboxing degli allegati		✓	✓	✓
Takeover degli account	Visibilità sui takeover degli account	✓	✓	✓	✓
	Indagine post-accesso sotto forma di visualizzazione cronologica	+	+	+	+
	Correzione degli ambienti cloud ed email	+	+	+	+
Segnalazione e neutralizzazione delle email	Strumento mSOAR automatico	✓	✓	✓	✓
	Casella email automatizzata per la segnalazione di abusi	✓*	✓	✓	✓
	Segnalazione delle email da parte degli utenti	✓	Visualizzazione di avvisi per le email sospette		
Dashboard delle minacce e degli utenti	Informazioni sulle minacce, inclusi i VAP	✓	✓	✓	✓
	Dashboard sui rischi legati agli utenti		✓	✓	✓
Integrità delle email in arrivo e configurazione	Antispam, antivirus e antigraymail		✓	✓	✓
	Funzionalità destinate ai dirigenti/VIP		✓	✓	✓
	Policy personalizzate		✓	✓	✓
Difese approfondite degli utenti	Isolamento dei clic sulle email riscritte	+	VAP		Tutti
	Formazione di sensibilizzazione alla sicurezza informatica	+	+	✓	✓
Autenticazione delle email e protezione interna	Implementazione DMARC, informazioni fruibili	+	+	+	✓
	Protezione contro le email interne dannose	+	+	+	< 5.000 utenti

#### LEGENDA

- ✓ Incluso nel bundle
- + Disponibile a costi aggiuntivi

\* Disponibile a breve, solo cloud

## Descrizioni dei bundle Proofpoint Threat Protection

BUNDLE	PANORAMICA	DESCRIZIONE	FUNZIONALITÀ INCLUSE
<b>PX</b>	<p>Protezione dell'email semplice, rapida e basata sull'intelligenza artificiale per Microsoft 365</p> <p>Ideale per le aziende più piccole che desiderano aumentare la sicurezza nativa di Microsoft 365 e semplificare l'amministrazione della sicurezza delle email con impostazioni preconfigurate</p> <p>Implementazione in pochi minuti con la modalità Inline+API</p>	<p>Proofpoint PX è disponibile solo per le istanze cloud di Microsoft 365. È il modo più rapido e semplice per godere della miglior sicurezza dell'email e cloud del settore. Grazie alla combinazione di machine learning, analisi comportamentale e threat intelligence, PX rileva, blocca con precisione e pone rimedio a spear phishing, violazioni dell'email aziendale (BEC, Business Email Compromise), attacchi alla supply chain e ransomware che eludono i controlli di sicurezza di Microsoft.</p>	<p>Funzionalità di rilevamento e neutralizzazione automatizzate guidate dall'intelligenza artificiale che integra le protezioni native di Microsoft</p>
<b>P0</b>	<p>Sicurezza avanzata di cloud ed email</p> <p>Ideale per le aziende vittime di minacce più mirate e per quelle che necessitano di ulteriori personalizzazioni e configurazioni</p>	<p>Neutralizza le minacce trasmesse via email lungo l'intera catena di attacco, dal rilevamento alla risposta. È inclusa la possibilità di automatizzare la gestione della casella di posta per gli abusi rimuovendo le email di phishing dannose segnalate dagli utenti. Vengono eliminate anche le minacce come il phishing, gli attacchi BEC, le frodi dei fornitori, il ransomware e altro malware. Questa soluzione offre visibilità su chi è stato attaccato e sulla tecnica di attacco utilizzata. Ti permette di stabilire se gli utenti colpiti fanno clic su un messaggio di phishing o lo segnalano e se sono stati compromessi.</p>	<p>Tutte le funzionalità di PX e:</p> <ul style="list-style-type: none"> <li>• Opzioni di implementazione più flessibili (ibrida o on premise)</li> <li>• Gestione del flusso di email con personalizzazione tramite la console di gestione completa</li> <li>• Protezione avanzata al momento del clic per gli attacchi basati su allegati e URL, con TAP URL Isolation for VAP</li> <li>• Visualizzazione di avvisi HTML per le email sospette con tasto "Report Suspicious"</li> <li>• Integrità delle email degli utenti che include antispam, antivirus, antigraymail e altri controlli</li> <li>• Dashboard integrata per i rischi legati agli utenti con i controlli consigliati (Nexus People Risk Explorer)</li> </ul>
<b>P1</b>	<p>Protezione contro le minacce avanzate</p> <p>Ideale per le aziende che devono formare i loro collaboratori grazie a funzionalità di difesa aggiuntive integrate</p>	<p>Insegna agli utenti finali a resistere meglio alle minacce che li colpiscono. Migliora la protezione contro le minacce grazie a un solido programma di formazione di sensibilizzazione alla sicurezza informatica che si integra con i tuoi controlli di sicurezza per l'email e include simulazioni di attacchi di phishing, valutazioni della cultura e delle conoscenze, corsi di formazione completi e materiali di sensibilizzazione.</p> <p>Adatta il programma di formazione fornito agli utenti in base alle minacce effettive che li prendono di mira. Sfrutta l'intero catalogo di formazione e gli strumenti interattivi studiati per modificare il comportamento degli utenti finali. I bundle includono simulazioni delle minacce volte a testare la risposta degli utenti agli attacchi di phishing utilizzando migliaia di modelli, oltre 40 lingue e 13 categorie. Queste simulazioni permettono di creare una linea di condotta per la sicurezza, di insegnare ai collaboratori a evitare i rischi legati alla sicurezza e di monitorare i progressi. Puoi visualizzare l'avanzamento del tuo programma in una dashboard specifica per i CISO. Vengono messe in evidenza le metriche più importanti per i responsabili della sicurezza.</p>	<p>Tutte le caratteristiche di P0 e Proofpoint Security Awareness Training Enterprise</p>

BUNDLE	PANORAMICA	DESCRIZIONE	FUNZIONALITÀ INCLUSE
P1+	<p>Protezione completa contro le minacce veicolate tramite email e nel cloud</p> <p>Ideale per le aziende che hanno bisogno di protezione avanzata per email e cloud tramite informazioni fruibili e funzionalità di sicurezza avanzate</p>	<p>Rafforza la protezione dalle frodi dei domini e dell'email, inclusi gli attacchi BEC, per bloccare gli attacchi di spoofing delle email in ingresso e in uscita inviate per conto della tua azienda. Gli attacchi BEC possono utilizzare diverse tecniche di furto d'identità. Devi adottare un approccio multilivello alla sicurezza per proteggere i tuoi collaboratori, i tuoi clienti e i tuoi partner commerciali. La soluzione BEC integrata di Proofpoint prende in considerazione tutte le tecniche utilizzate dai criminali informatici, ti offre una visibilità completa sull'ecosistema email e i controlli per bloccare questi attacchi prima che raggiungano la casella email.</p> <p>Vai oltre l'implementazione DMARC per identificare i rischi di frode posti dai tuoi fornitori. Proofpoint fornisce una visibilità unica sui rischi legati ai fornitori per aiutarti a neutralizzare gli attacchi complessi alla supply chain. Identifica automaticamente i tuoi fornitori e valuta il livello di rischio dei domini che utilizzano per inviare email ai tuoi utenti. Integrando i dati della piattaforma di protezione contro le minacce, indichiamo il volume dei messaggi, le minacce rilevate dai domini dei fornitori, così come i messaggi bloccati dai domini fotocopia dannosi dei tuoi fornitori.</p> <p>Inoltre, le aziende con meno di 5.000 collaboratori possono godere di una visibilità in tempo reale sulle email interne dannose inviate da account compromessi e neutralizzarli automaticamente. Puoi identificare rapidamente gli account compromessi e gli utenti interessati.</p>	<p>Tutte le funzionalità di P1 e:</p> <ul style="list-style-type: none"> <li>• Proofpoint Email Fraud Defense (EFD)</li> <li>• Proofpoint Supplier Risk Explorer</li> <li>• Proofpoint TAP URL Isolation per tutti gli utenti</li> <li>• Internal Mail Defense per le aziende con meno di 5.000 dipendenti</li> </ul>

## Bundle Proofpoint Information Protection - Difendi i tuoi dati

Modernizza la tua soluzione di prevenzione della perdita di dati (DLP) grazie al nostro bundle Proofpoint Enterprise DLP. Questo bundle adotta un approccio incentrato sulle persone. Fornisce un contesto arricchito su contenuti, comportamenti e minacce per ottenere informazioni fruibili sulla perdita di dati e per prevenirle. Fornisci ai tuoi team della sicurezza e della conformità la telemetria su email, cloud ed endpoint. Questo consente loro di affrontare tutti gli scenari di perdita di dati incentrati sulle persone, tutto in un'unica soluzione.

Proofpoint Enterprise DLP include:

- **Proofpoint Email DLP:** previene le perdite di dati grazie a policy integrate, all'analisi dell'impronta digitale dei file e alla funzione di correzione automatica Smart Send.
- **Proofpoint Cloud App Security Broker (CASB):** offre protezione contro le minacce nel cloud e previene le perdite di dati nel cloud, inclusa la condivisione eccessiva di dati sensibili, il controllo delle applicazioni di terze parti e supporto per la gestione delle applicazioni non approvate (Shadow IT).
- **Proofpoint Endpoint DLP e Proofpoint Insider Threat Management (ITM):** per il 3% degli utenti. Mitiga i rischi interni grazie a questo agent endpoint leggero. Previene i comportamenti dannosi e negligenti dei dipendenti, degli utenti con privilegi e di terze parti.

### PER SAPERNE DI PIÙ

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

#### INFORMAZIONI SU PROOFPOINT

Proofpoint 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 il 75% 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](https://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.