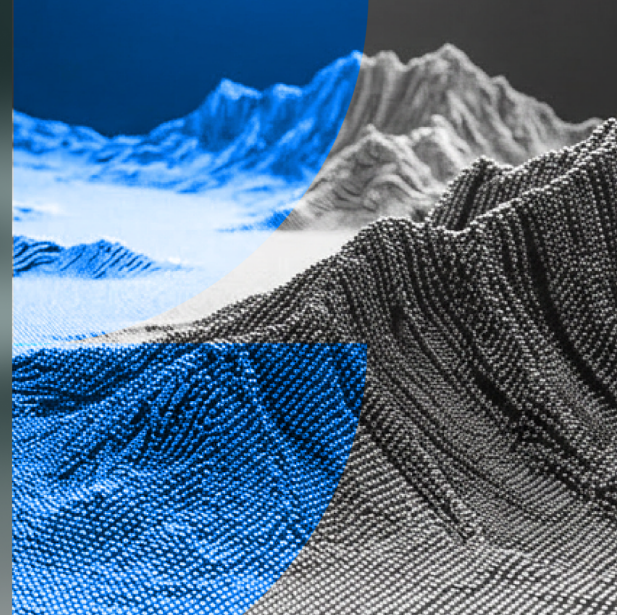


Proofpoint Collaboration Security Prime

Sicurezza completa e continua della collaborazione nell'era dell'IA



Vantaggi principali

- Blocca la più ampia gamma di minacce con un'efficacia del 99,999%
- Contiene le violazioni dell'account in pochi minuti, sia che la minaccia abbia origine da un'email, sia veicolata tramite altri vettori o provenga da un fornitore compromesso
- Riduce del 40% i clic su link dannosi effettivi nei sei mesi successivi all'implementazione
- Previene il furto d'identità e disattiva i domini fotocopia prima che raggiungano i tuoi clienti
- Riduce il costo totale di proprietà del 40% grazie al consolidamento della piattaforma

Questa suite di soluzioni fa parte della piattaforma Human-Centric Security integrata di Proofpoint volta a proteggere persone e dati nell'ambiente di lavoro agentico.

Panoramica

L'IA ha trasformato il panorama per tutti. I criminali informatici la utilizzano per lanciare attacchi più innovativi e personalizzati, con una sofisticazione e un'ampiezza maggiori. Campagne come la violazione dell'email aziendale (BEC, Business Email Compromise) sono aumentate del 27%, e il phishing generato dall'IA ora registra un tasso di clic 4,5 volte superiore a quello del phishing tradizionale. Gli utenti sono diventati più vulnerabili ai contenuti generati dall'IA, mentre i difensori sono sopraffatti dalla classificazione degli avvisi per priorità e dagli strumenti frammentati.

Le aziende hanno bisogno di un approccio fondamentalmente diverso, progettato per l'era agentica, in cui strumenti e assistenti basati sull'IA si affiancano alla forza lavoro estesa a livello di email, strumenti di messaggistica istantanea e applicazioni cloud, ampliando così la superficie d'attacco già sfruttata dai criminali informatici.

Purtroppo, numerose aziende sono costrette a adottare un approccio frammentato alla sicurezza, basato su prodotti isolati. Ciò crea ulteriori lacune nelle loro difese, isola i team e aumenta la complessità operativa.

Per difendersi dagli attacchi su larga scala ottimizzati dall'IA, che si verificano su più canali e in diverse fasi, nonché per proteggere le interazioni affidabili - che si tratti di interazioni tra esseri umani, tra esseri umani e assistenti IA, o tra esseri umani e applicazioni cloud - le aziende hanno bisogno di un approccio più completo. Proofpoint Collaboration Security Prime può aiutarle. Proofpoint Prime unifica rilevamento e neutralizzazione delle minacce nell'intero ambiente di lavoro agentico.

In questo modo puoi:

- Rilevare prima le nuove minacce generate dall'IA con una maggiore visibilità sulla superficie d'attacco
- Bloccare con fiducia grazie a una precisione all'avanguardia e un basso numero di falsi positivi
- Fornire una protezione prima e dopo la consegna, nei browser e negli ambienti agentici
- Proteggere le comunicazioni aziendali ovunque si verifichino, nelle chat, nelle applicazioni e negli agenti
- Contenere le violazioni degli account in pochi minuti, non giorni.

Rilevamento più tempestivo delle nuove minacce grazie a una maggiore visibilità

I nuovi attacchi, generati dall'IA, si evolvono più rapidamente di quanto le difese tradizionali riescano a intercettarle. In questo modo riescono ad aggirare i filtri legacy e raggiungono le persone tramite l'email, le piattaforme di collaborazione e le applicazioni cloud.

Proofpoint Collaboration Security Prime colma questa lacuna grazie a una protezione continua che copre l'intero ciclo di vita delle minacce, dalla fase precedente alla consegna a quella successiva alla consegna nell'architettura dell'email, e dal momento del clic alla connessione, su tutti i canali utilizzati dai collaboratori.

Proofpoint Prime protegge contro la più ampia gamma di minacce, tra cui:

- Phishing avanzato, inclusi il phishing delle credenziali d'accesso e il phishing di callback
- BEC e furto d'identità del CEO
- Distribuzione del malware
- Attacchi tramite codice QR
- Attacchi tramite telefonata (TOAD)
- Invio in massa di email
- Ransomware
- Takeover degli account
- Abuso di servizi legittimi
- Attacchi generati dall'IA e tecniche di exploit dell'IA, come l'iniezione di prompt

Al cuore di questa protezione c'è Proofpoint Nexus® AI, il motore di rilevamento più avanzato del settore. Addestrato con uno dei più grandi set di dati del settore, Nexus AI valuta oltre 1.000 attributi per messaggio. Combina cinque tipi di modelli: modelli linguistici, grafici relazionali, machine learning, threat intelligence e computer vision. Tali modelli lavorano insieme e apprendono continuamente da ogni verdetto.

Il risultato è un'efficacia di rilevamento del 99,999% e il tasso di falsi positivi più basso del settore, consentendo di bloccare le minacce reali senza sovraccaricare i team con informazioni superflue.

Protezione contro la violazione degli account

Le violazioni degli account non si limitano alle email di phishing. L'IA permette ai criminali informatici di sferrare più facilmente gli attacchi di raccolta delle credenziali d'accesso ben oltre la casella email, dalla creazione di pagine di accesso identiche a quelle originali, all'elusione dell'autenticazione a più fattori tramite l'invio in massa di prompt automatizzati.

In un ambiente di lavoro basato sulla collaborazione e assistito da agenti, è fondamentale contrastare queste minacce in ogni fase: prima, durante e dopo la violazione.

Proofpoint Collaboration Security Prime aiuta a prevenire le violazioni prima che si verifichino. SSO Password Guard di Proofpoint Prime rileva quando i collaboratori riutilizzano la loro password aziendale su siti non professionali,

chiudendo una delle vie di accesso più comuni per gli attacchi basati sulle credenziali d'accesso e estendendo la protezione oltre le email fino al browser stesso.

Quando la prevenzione non è sufficiente, Proofpoint Prime rileva le violazioni mentre si verificano. Correla i segnali di identità e post-accesso provenienti da Microsoft 365, Google Workspace e Okta per identificare gli account che mostrano segni di violazione.

Una volta identificata una violazione, Proofpoint Prime ti aiuta a analizzarla e contenerla in pochi minuti, non giorni, limitando il raggio d'azione prima che un criminale informatico possa spostarsi ulteriormente nell'ambiente.

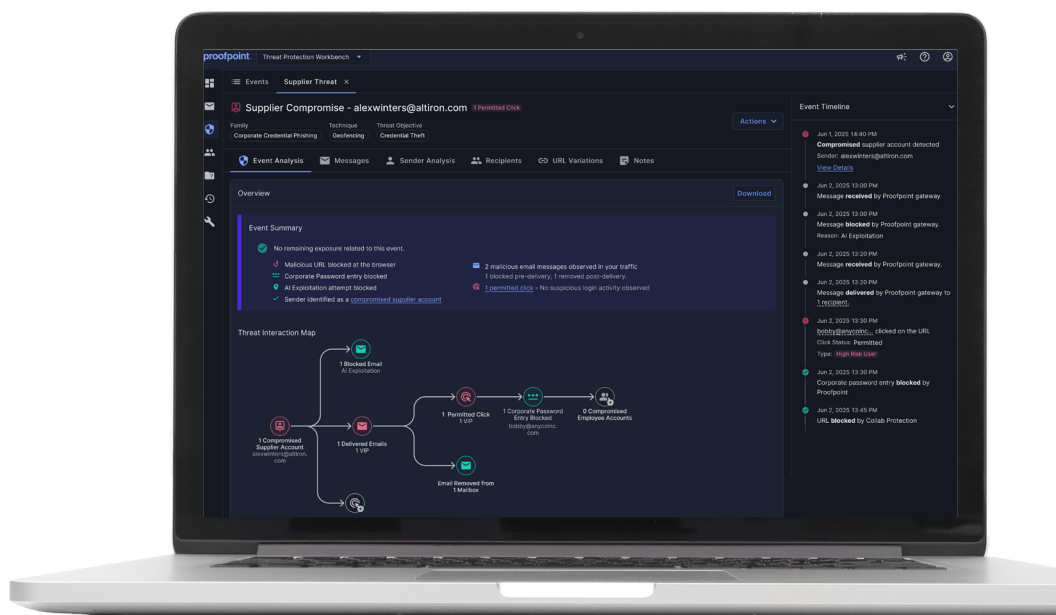


Figura 1. Proofpoint Collaboration Security Prime blocca e correla le minacce a livello di email, messaggistica e collaborazione, cloud e canali dei fornitori.

I modelli Nexus® AI sono addestrati con uno dei set di dati più vasti e diversificati del settore della sicurezza informatica.

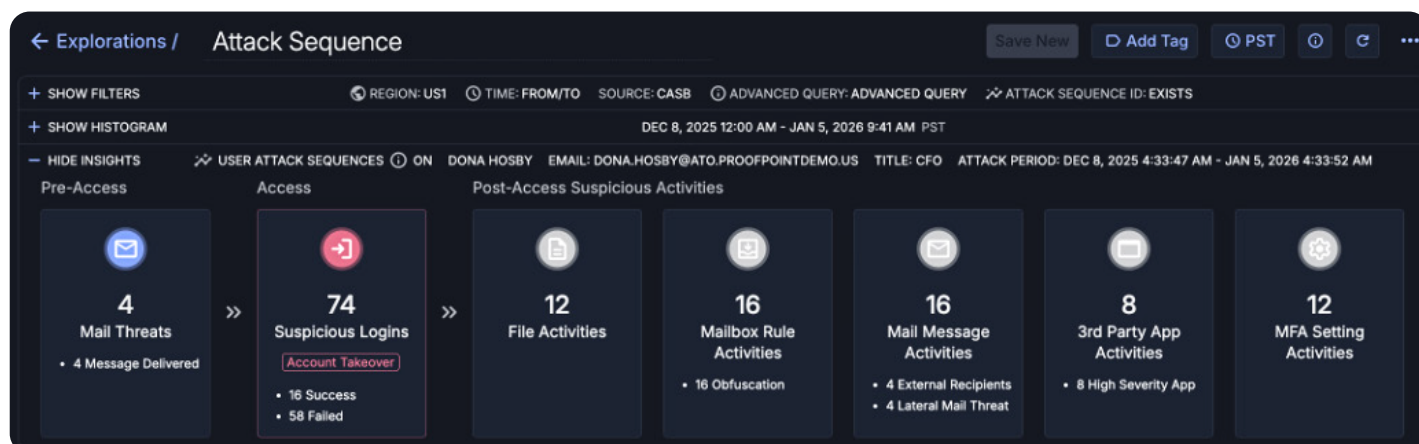


Figura 2. Proofpoint Collaboration Security Prime offre visibilità sulle sequenze di attacco e automatizza il contenimento.

Protezione delle tue comunicazioni aziendali di fiducia

I criminali informatici utilizzano spesso tattiche di furto d'identità per inserirsi nelle comunicazioni aziendali di fiducia, sia attraverso lo spoofing diretto dei domini, dei domini fotocopia o di account di fornitori compromessi. Quando la tua azienda o i suoi partner subiscono un furto d'identità o una violazione, i tuoi collaboratori e i tuoi clienti vengono esposti ai rischi, il tuo marchio può subire gravi danni.

Proofpoint Collaboration Security Prime può aiutarti a ridurre in modo proattivo questi rischi di furto d'identità. Ti offre una visibilità completa su tutte le email in uscita inviate utilizzando i tuoi domini di fiducia, incluse quelle inviate da terze parti. Hai accesso non solo a potenti strumenti, ma anche a consulenti esperti che ti guideranno attraverso ogni fase dell'implementazione dell'autenticazione delle email. Ciò ti aiuta a conseguire la piena conformità DMARC e a impedire ai criminali informatici di violare i tuoi domini.

La nostra protezione va oltre le email generate dagli utenti e include un ambiente dedicato sicuro per l'inoltro di messaggi generati dalle applicazioni e le email inviate da fornitori SaaS terzi per tuo conto.

Nel caso di minacce provenienti dai fornitori, Proofpoint Prime impedisce che i tuoi collaboratori vengano sfruttati da criminali informatici che utilizzano account di terze parti compromessi. Identifica le attività sospette che provengono da account di fornitori e applica protezioni adattive, come indicatori di avviso e isolamento degli URL, per ridurre i rischi senza interrompere le comunicazioni aziendali legittime.

Proofpoint Prime fornisce inoltre funzionalità avanzate di rilevamento di domini fotocopia. Monitora Internet in modo dinamico alla ricerca di domini che assomigliano molto ai tuoi. Fornisce anche informazioni dettagliate sulla loro registrazione e sul loro possibile uso improprio.

Non ci limitiamo al rilevamento. Possiamo operare per tuo conto per smantellare i domini e gli URL dannosi grazie alle nostre solide relazioni con gli enti di registrazione, fornitori di servizi di hosting e di domini di primo livello. I nostri professionisti gestiscono l'intero processo, permettendo ai tuoi team di concentrarsi sulle operazioni aziendali strategiche.

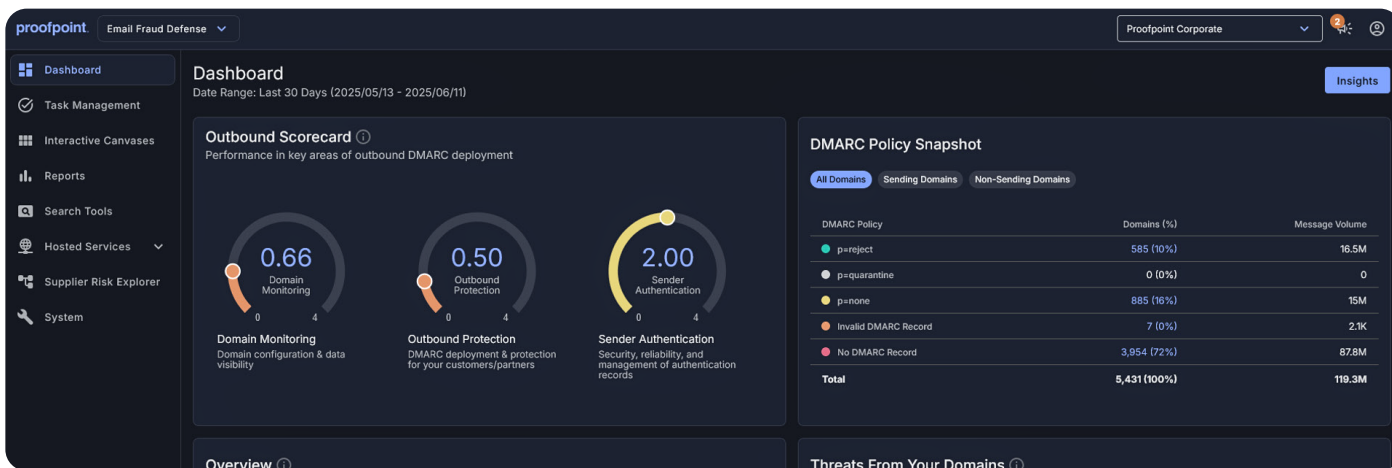


Figura 3. Proofpoint Collaboration Security Prime offre visibilità sulle minacce di furto d'identità, come lo spoofing del dominio e i domini fotocopia dannosi.

Rafforzamento della resilienza degli utenti grazie a consigli basati sui rischi

Con il lavoro che diventa sempre più collaborativo e dinamico, è fondamentale che i collaboratori dimostrino una maggior resilienza nei confronti degli attacchi informatici. Perciò è necessario andare oltre una formazione incentrata sulla conformità per includere la gestione dei rischi legati agli utenti - una formazione in tempo reale che riflette il modo in cui gli utenti lavorano e i rischi reali che si trovano ad affrontare.

Collaboration Security Prime rafforza la resilienza degli utenti in modo sistematico, non attraverso una formazione una tantum, ma attraverso un ciclo continuo legato ai rischi reali.

Tutto inizia con l'identificazione dell'obiettivo. Lo Human Resilience Workbench capta i segnali di comportamento e di rischio da tutta la piattaforma, identificando automaticamente gli utenti ad alto rischio, i nuovi assunti e i collaboratori che si lasciano ingannare più facilmente, in modo che i team della sicurezza possano concentrare l'attenzione dove è più importante.

Da lì, Proofpoint Prime stimola comportamenti più sicuri nel momento in cui il rischio è più elevato. Grazie al sistema ThreatFlip ottimizzato dall'IA, trasforma le minacce reali attive in simulazioni istantanee con un solo clic, mostrando ai collaboratori come appare esattamente un attacco nel momento stesso in cui lo affrontano e non settimane dopo in un modulo di formazione generico.

Infine, Proofpoint Prime dimostra l'impatto. I punteggi di rischio e il benchmarking offrono agli amministratori una chiara visibilità sulle aree in cui i comportamenti stanno migliorando e su quelle in cui permangono delle lacune. Le aziende che adottano questo approccio registrano una riduzione del 40% dei clic su link dannosi reali nei sei mesi successivi all'implementazione, a dimostrazione del fatto che è la resilienza, e non la sola sensibilizzazione, a generare un cambiamento duraturo.

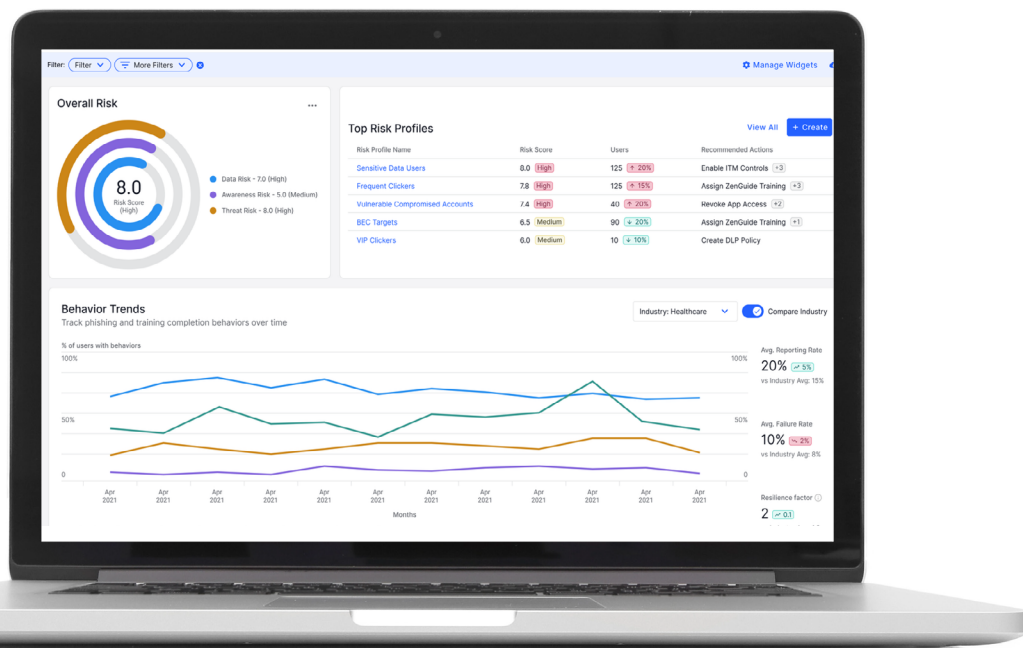


Figura 4. Proofpoint Collaboration Security Prime offre visibilità sul comportamento reale degli utenti, che permette di fornire formazione mirata e basata sui rischi.

Semplificazione delle operazioni di sicurezza

Con l'estendersi delle minacce oltre le email per colpire strumenti di collaborazione, piattaforme cloud ed ecosistemi dei fornitori, i team della sicurezza sono chiamati a fare sempre di più con meno risorse. In questo contesto, soluzioni isolate scollegate non facilitano loro il compito. Non solo aumentano la complessità, ma rallentano anche i tempi di risposta e aumentano i costi operativi. Tutto ciò rende più difficile ridurre i rischi su larga scala.

Proofpoint Collaboration Security Prime semplifica le operazioni di sicurezza unificando il rilevamento e l'analisi delle minacce e automatizzando i flussi di lavoro e la risposta. Grazie a integrazioni native, Threat Protection Workbench utilizza integrazioni native per riunire informazioni relative al rilevamento e analisi dettagliate degli attacchi provenienti da email, messaggi, piattaforme di collaborazione, account cloud ed ecosistemi dei fornitori. I team possono così indagare sugli incidenti e intraprendere azioni decisive, il tutto da un unico spazio di lavoro unificato per la massima efficienza.

Proofpoint Prime aiuta inoltre i team a stabilire le priorità in modo efficace. La Threat Interaction Map correla le minacce e gli eventi di sicurezza nei punti di controllo e fornisce una mappa visiva dei percorsi di attacco. Questo consente agli analisti di identificare rapidamente gli incidenti più critici. In parallelo, ispeziona automaticamente i messaggi segnalati dagli utenti, neutralizza i contenuti dannosi e fornisce un feedback agli utenti. Ciò permette di ridurre gli interventi manuali e di rafforzare i comportamenti sicuri degli utenti.

Il risultato? Una risposta più rapida e una minore complessità operativa. Inoltre, il tuo team della sicurezza può fare di più con meno, senza sacrificare la protezione.

Scelta del giusto livello di protezione

Proofpoint Collaboration Security Prime è disponibile in diversi livelli, consentendoti di scegliere una protezione in base al profilo di rischio e alle esigenze operative della tua azienda. Ogni livello si basa su quello precedente.

La copertura va dalle minacce email di base ai canali di collaborazione, alla violazione degli account, alla riduzione dei rischi legati alle persone fino alla protezione avanzata del marchio.

Scopri le
funzionalità
disponibili nella
pagina seguente.



Per saperne di più, visita il sito [proofpoint.com/it](https://www.proofpoint.com/it)

Informazioni su Proofpoint. Inc. Proofpoint, Inc. è un'azienda leader globale nella cybersecurity incentrata sulle persone e sugli agenti, che protegge il modo in cui persone, dati e agenti IA si connettono tramite email, cloud e strumenti di collaborazione. Proofpoint è un partner di fiducia per oltre 80 aziende della classifica Fortune 100, oltre 10.000 grandi imprese e milioni di aziende più piccole, per contrastare le minacce, prevenire la perdita di dati e rafforzare la resilienza di persone e processi di IA. La piattaforma di collaborazione e sicurezza dei dati di Proofpoint aiuta aziende di tutte le dimensioni a proteggere e responsabilizzare i propri collaboratori in modo che possano adottare l'IA in modo sicuro e con fiducia. Per saperne di più, visita www.proofpoint.com/it.

Seguici: [LinkedIn](#)

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

Tutti i livelli della soluzione Proofpoint Collaboration Security sono disponibili per le implementazioni API e gateway email sicuro. La disponibilità delle funzionalità può variare a seconda del modello di implementazione.

	Funzionalità disponibili	Core Email Protection	Collaboration Security Tier 2	Collaboration Security Tier 3	Collaboration Security Prime
Sicurezza dell'email	Protezione contro attacchi BEC, phishing, phishing di callback e malware	✓	✓	✓	✓
	Stack di rilevamento multilivello ottimizzato da Nexus AI	✓	✓	✓	✓
	Dati senza pari sulle minacce provenienti da oltre 2,8 milioni di clienti	✓	✓	✓	✓
	Sandboxing di allegati e URL	✓	✓	✓	✓
	Riscrittura di URL e sandboxing al momento del clic	Gateway email sicuro	Gateway email sicuro	Gateway email sicuro	Gateway email sicuro
	Isolamento dei clic sospetti sugli URL riscritti	VAP*	Tutti gli utenti*	Tutti gli utenti*	Tutti gli utenti*
	Antispam e rilevamento di graymail	✓	✓	✓	✓
	Visualizzazione di avvisi contestuali per le email sospette	✓	✓	✓	✓
	Strumenti adattivi di integrità dell'email con apprendimento automatico in base al comportamento degli utenti	✓	✓	✓	✓
	Policy di instradamento delle email configurabili	Gateway email sicuro	Gateway email sicuro	Gateway email sicuro	Gateway email sicuro
	Correzione automatica dei messaggi	✓	✓	✓	✓
	Casella di posta per gli abusi automatizzata	✓	✓	✓	✓
	Persone più attaccate (VAP™), criminali informatici e threat intelligence mondiale	✓	✓	✓	✓
Protezione contro le minacce multicanale e in più fasi	Rilevamento e correzione degli account cloud compromessi		✓	✓	✓
	Blocco degli URL dannosi inviati tramite applicazioni di messaggistica e collaborazione		✓	✓	✓
	Rilevamento dell'uso improprio delle password aziendali su siti web a rischio o non approvati		✓	✓	✓
	Protezione contro gli account fornitori compromessi		✓	✓	✓
Resilienza umana e sensibilizzazione alla sicurezza informatica	Automazione della formazione basata sul livello di rischio			✓	✓
	Rafforzamento della sensibilizzazione dei collaboratori tramite simulazioni basate su minacce reali			✓	✓
	Conversione delle minacce attive in simulazioni sicure			✓	✓
	Rilevamento e classificazione in base alle priorità degli utenti a rischio in base ai comportamenti, ai dati di telemetria sulle minacce e ai ruoli			✓	✓
Protezione contro il furto d'identità	Prevenzione degli usi impropri del marchio tramite l'autenticazione delle email				✓
	Rilevamento e neutralizzazione dei domini fotocopia dannosi				✓
	Relay sicuro delle email generate dalle applicazioni (250 GB)				✓

SEG = Solo implementazione del gateway di posta sicuro

* = Disponibile solo per le implementazioni SEG.