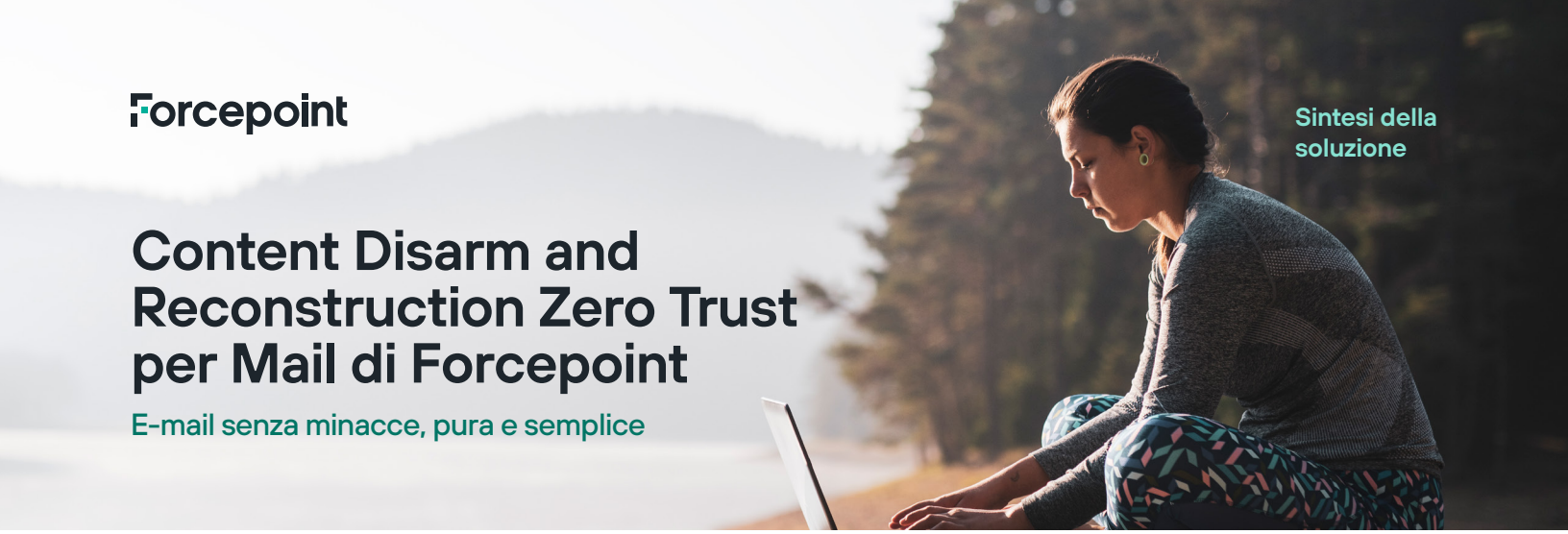
Forcepoint



Sintesi della soluzione

# Content Disarm and Reconstruction Zero Trust per Mail di Forcepoint

## E-mail senza minacce, pura e semplice

### Sfide

- Lotta contro gli attacchi di phishing – CISCO ha segnalato che nel 2021 il 90% delle violazioni dei dati è stato conseguenza del phishing.
- Exploit zero-day

### Soluzione

- Potenzia la sicurezza e-mail con Content Disarm and Reconstruction (CDR) Zero Trust: l'unico mezzo per sconfiggere le minacce note, sconosciute e zero-day presenti nei contenuti quando attraversano i confini delle e-mail.

### Vantaggi

- Recapita messaggi e allegati e-mail sicuri e senza minacce oltre il perimetro della rete senza bisogno di rilevare le minacce o impedire agli utenti di accedere ai contenuti necessari per il loro lavoro. Exploit zero-day, ransomware, exploit steganografici, malware senza file e minacce inerenti in file polimorfi vengono tutti rimossi.
- Compatibile con soluzioni preesistenti di Email Security Gateway, filtri antispam e tecnologia antivirus perimetrale, si integra in trasparenza nella tua strategia di difesa perimetrale, offrendo una risposta a basso rischio e basso costo per la protezione totale dalle minacce veicolate dai contenuti.

Di solito gli utenti aziendali hanno una funzionalità e-mail che consente di scambiare messaggi dal posto di lavoro con utenti sia interni all'azienda che esterni, su internet. Le e-mail possono avere contenuti complessi: spesso gli utenti inviano messaggi in HTML e includono formattazione, collegamenti ipertestuali, colori, immagini e allegati. Tutto ciò comporta per l'organizzazione il rischio che le e-mail veicolino malware nascosto nei contenuti complessi.

Gli Email Security Gateway tradizionali si affidano al rilevamento delle potenziali minacce e si stanno dimostrando inadeguati per il livello di sofisticazione degli attacchi moderni.

**Blocco delle minacce sconosciute**

I gateway e le difese e-mail perimetrali esistenti (che includono antivirus, threat intelligence, sandbox e filtri antiSPAM) costituiscono una prima linea di difesa, rilevando le minacce note attraverso la ricerca delle firme di exploit già individuati in precedenza o di comportamenti non sicuri. Ma fin troppo spesso le aziende sono compromesse da minacce zero day – che le invadono prima che le difese basate sul rilevamento riescano a identificarle – o da minacce del tutto sconosciute che vanno a segno senza nemmeno essere individuate.

Zero Trust CDR per la posta è l'unico modo per sconfiggere non solo le minacce note, ma anche quelle sconosciute e zero-day, nascoste nei contenuti che attraversano il perimetro delle e-mail. Infatti non si affida né alla detonazione nelle sandbox né al rilevamento, ma utilizza un esclusivo processo di trasformazione per assicurare la protezione totale.

**Trasformazione della sicurezza e-mail**

Zero Trust CDR per la posta funziona in questo modo: estrae le informazioni di business da documenti e allegati e-mail prima che superino il tuo perimetro esterno. I dati che trasportano le informazioni vengono eliminati insieme a tutte le eventuali minacce. Al loro posto vengono creati messaggi e allegati completamente nuovi, e solo questi saranno recapitati all'utente. A spostarsi da un capo all'altro sono soltanto contenuti sicuri. I criminali non riescono a trovare varchi e le aziende ricevono i contenuti di cui hanno bisogno.

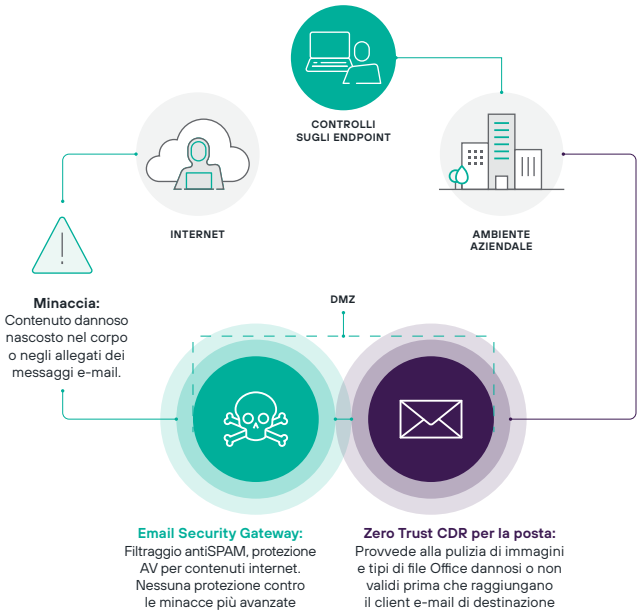
Questo processo è detto "trasformazione". È praticamente invincibile: risponde alla esigenze del team addetto alla sicurezza, perché le minacce vengono rimosse, e a quelle degli utenti aziendali, che acquisiscono le informazioni che gli occorrono.

Zero Trust CDR è l'unico modo per assicurare che le minacce siano eliminate dai contenuti. Evitando il ricorso ai paradigmi falliti del rilevamento e dell'isolamento delle minacce, l'esclusiva tecnologia Zero Trust CDR di Forcepoint presume che tutti i dati siano pericolosi o non sicuri: non prova neanche a distinguere tra "buoni" e "cattivi".

### Estensione della difesa esistente

Zero Trust CDR per la posta estende una soluzione Email Security Gateway e Email Server esistente rimuovendo le minacce dai corpi delle e-mail e dai tipi di file che di solito vengono allegati ai messaggi (immagini, documenti Microsoft Office e PDF). Zero Trust CDR per la posta può essere distribuito in locale e nel cloud.

Zero Trust CDR per la posta va a integrare i controlli di sicurezza e-mail preesistenti, inserendo un componente extra nel flusso del traffico e-mail in entrata e in uscita.




### Integrazione trasparente

Zero Trust CDR per la posta è attivo su un server sul lato aziendale di un Email Security Gateway esistente. Le e-mail in arrivo vengono instradate dall'Email Security Gateway a Zero Trust CDR per la posta dove i messaggi vengono trasformati per assicurare che siano liberi da minacce prima di essere recapitati al server della posta aziendale.

### Alt ai malware infiltrati nei contenuti

Oggi i vettori più comuni di malware sono i documenti Office, i file Adobe PDF e le immagini. La complessità di questi formati di file e delle applicazioni per manipolarli li rende un bersaglio ovvio per i criminali. Qualunque sia il malware – ransomware, trojan bancario, kit di accesso remoto e keylogger – gli hacker sanno che il modo migliore per occultare una minaccia zero-day è all'interno di un documento commerciale di uso quotidiano. Tecniche come l'uso di malware senza file e il polimorfismo dei file complicano ulteriormente la gestione delle minacce con sistemi di sicurezza IT convenzionali, basati sul rilevamento; in più l'e-mail è il vettore perfetto per l'infiltrazione.

Zero Trust CDR per la posta usa una tecnica esclusiva per trasformare i file, assicurando così agli utenti aziendali la possibilità di usare l'e-mail in totale serenità. Ogni documento e ogni immagine vengono trasformati e resi innocui.

### Proxy del livello di applicazione

Zero Trust CDR per la posta funziona come proxy del livello di applicazione dual-homed per SMTP. Forma un perimetro sicuro tra la rete aziendale e i sistemi esterni, fungendo da host intelligente sia per il Mail Security Gateway per i messaggi in arrivo sia per il server della posta per i messaggi in uscita. Trasforma tutti i contenuti, incluso MIME e allegati e-mail, per assicurare che possano essere recapitati in sicurezza all'interno della rete aziendale; provvede, inoltre, alla trasformazione delle richieste del portale utenti e delle risposte per l'accesso ai documenti protetti da password e la trasformazione degli allegati protetti da password che vengono ricevuti.

Zero Trust CDR per la posta trasforma i contenuti ricevuti in una rappresentazione interna delle informazioni. I dati originali vengono eliminati e, a partire dalle loro informazioni, vengono creati dei dati nuovi e "sicuri". In questo modo gli attacchi sferrati usando come mezzo i contenuti vengono eliminati anche se non sono noti e le informazioni possono comunque arrivare a destinazione. Questo processo avviene per tutti i contenuti trasformati.

### Allegati protetti da password

In alcune organizzazioni, gli utenti proteggono documenti con password e poi li spediscono tramite internet sotto forma di allegati. Questi documenti rappresentano potenziali minacce in quanto non possono essere trasformati e resi innocui.

Per bilanciare esigenze di business e rischi per la sicurezza, Zero Trust CDR per la posta può essere configurato per non recapitare i messaggi che contengono allegati protetti da password, oppure per rimuovere gli allegati protetti da password presenti nei messaggi. In alternativa, nei casi in cui l'invio di allegati protetti da password sia ritenuto essenziale, si possono configurare dei canali tra specifici utenti o gruppi di utenti per bypassare il processo di trasformazione.

**Messaggi firmati e crittografati**
Se occorre il supporto per messaggi firmati e/o crittografati con S/MIME o PGP, è possibile agire a livello di gateway. I messaggi vengono prima resi innocui con Zero Trust CDR e poi passati a un server di protezione Forcepoint separato per l'apposizione della firma o l'esecuzione della crittografia.

**Macro e contenuti eseguibili**
In alcune organizzazioni, gli utenti si scambiano via e-mail dei documenti Office contenenti macro. Questi documenti rappresentano una potenziale minaccia, perché le macro sono contenuti eseguibili che non possono essere resi innocui dalla trasformazione.

Per bilanciare esigenze di business e rischi per la sicurezza, Zero Trust CDR per la posta può essere configurato per non recapitare i messaggi che contengono macro di Office, oppure per rimuovere gli allegati che contengono macro di Office. In alternativa, nei casi in cui l'invio di documenti Office contenenti macro sia considerato essenziale, si possono configurare dei canali tra specifici utenti o gruppi di utenti per bypassare il processo di trasformazione.

Per maggiori informazioni, consulta Forcepoint Zero Trust CDR

**forcepoint.com/contact**