

# Forcepoint Zero Trust Content Disarm and Reconstruction per Web Gateway

Navigare nel web senza timori

## Sfide

- › Le aziende sono compromesse da minacce zero day che le invadono prima che le difese basate sul rilevamento riescano a identificarle, oppure da minacce del tutto sconosciute che vanno a segno senza mai essere individuate chiaramente.
- › I contenuti scaricati dal web possono contenere minacce che causano malfunzionamenti delle applicazioni e danno agli hacker il controllo sui sistemi aziendali.
- › Gli upload sul web possono contenere più informazioni di quante un'azienda voglia divulgare e danneggiano il business rendendo pubblica la proprietà intellettuale.

## Soluzione

- › L'esclusiva tecnologia Zero Trust CDR di Forcepoint presume che tutti i dati siano pericolosi o comunque non sicuri: non prova neanche a distinguere tra "buoni" e "cattivi". Ecco perché è l'unica vera soluzione Zero Trust.
- › Zero Trust CDR può essere integrato in pochi istanti in ogni difesa web preesistente.

## Vantaggi

- › Contenuti sempre sicuri e senza minacce trasferiti oltre i confini del web
- › Blocco delle minacce sconosciute
- › Trasformazione della sicurezza web
- › Esperienza di navigazione più ricca
- › Integrazione trasparente
- › Blocco dei malware
- › Lotta alla steganografia
- › Protezione senza confronti

Le organizzazioni dipendono dal web per condividere informazioni essenziali per i processi chiave di business e per condurre transazioni. Le difese web perimetrali esistenti (gateway web e firewall) non riescono a tenere testa alla marea di minacce zero-day, note e sconosciute nascoste in documenti e immagini di business. Lasciato incontrollato, questo vettore d'attacco è una minaccia esistenziale per le imprese. I documenti e le immagini scaricati dagli utenti contengono minacce che possono causare malfunzionamenti delle applicazioni e dare agli hacker il controllo sui sistemi aziendali. I documenti e le immagini caricati possono contenere più informazioni di quante un'azienda voglia divulgare e danneggiano il business rendendo pubblica la proprietà intellettuale. A oggi nessuno ha trovato un modo per arginare il flusso delle minacce.

### Blocco delle minacce sconosciute

Firewall, gateway e difese web perimetrali esistenti costituiscono una prima linea di difesa e rilevano le minacce note cercando le firme di exploit o comportamenti non sicuri già individuati in precedenza. 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, oppure da minacce del tutto sconosciute che vanno a segno senza mai essere individuate chiaramente.

Zero Trust Content Disarm and Reconstruction (CDR) per Web Gateway 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 del web. 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 web

Zero Trust CDR per Web Gateway funziona estraendo le informazioni di business da documenti e immagini nel flusso di navigazione sul web. I dati che trasportano le informazioni vengono eliminati insieme a tutte le eventuali minacce. Al loro posto vengono creati documenti e immagini nuovi, poi 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 alle 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 isolamento delle minacce, l'esclusiva tecnologia Zero Trust CDR di Forcepoint presume che tutti i dati siano ostili o non sicuri: non prova neanche a distinguere i "buoni" dai "cattivi".

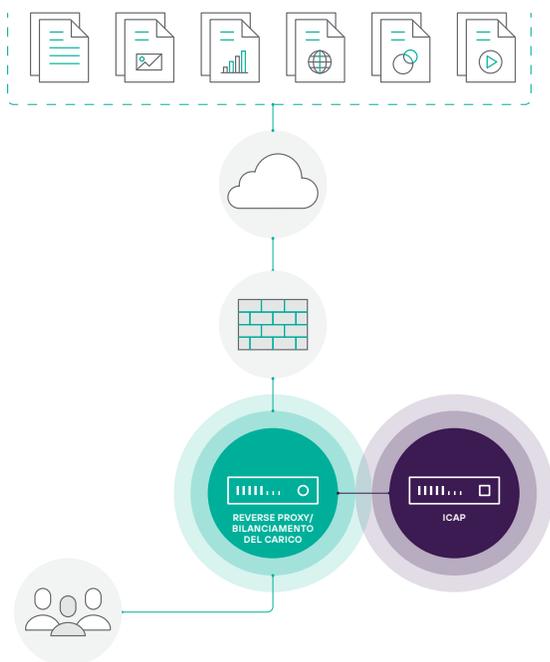
### Esperienza di navigazione più ricca

Mentre i team addetti alla sicurezza combattono contro cybercriminali che sembrano stare sempre un passo avanti, a soffrire sono gli utenti aziendali. Il tempo speso a gestire gli allarmi di sicurezza dovuti a falsi positivi oppure in attesa che i documenti siano controllati e resi disponibili ostacola i processi di business e limita la produttività. E quando un attacco va a segno, le operazioni di remediation sono costose e lunghe.

Zero Trust CDR per Web Gateway arricchisce la user experience su web e social media perché offre l'accesso tempestivo alle informazioni aziendali che gli utenti devono leggere e condividere per completare transazioni, il tutto senza che i contenuti consumati pongano alcun rischio di compromissione.

### Garanzia di contenuti digitalmente puri

Mentre l'uso del web e dei social media continua a definire ogni singolo aspetto del business, oggi è più importante che mai assicurare che i contenuti che viaggiano nel digitale siano sicuri, puliti e privi di minacce. Qualsiasi azienda in grado di crearsi agli occhi di utenti, business partner e clienti una reputazione di affidabilità per contenuti puliti e sicuri si differenzierà in un contesto sempre più caratterizzato da minacce fuori controllo.



Zero Trust CDR per Web Gateway fa esattamente questo, assicurando alle aziende la possibilità di sfruttare i vantaggi di web e social media, con la certezza di gestire contenuti non contaminati.

### Integrazione trasparente con le difese esistenti

Zero Trust CDR per Web Gateway si integra in trasparenza con le difese web perimetrali, i gateway web e i firewall esistenti usando il protocollo standard ICAP. Distribuita come "sidecar", la soluzione è configurata in modo che il web gateway o il firewall passi documenti e immagini a un server [Forcepoint Gateway eXtension \(GX\)](#) su ICAP, dove vengono trasformati per eliminare ogni eventuale minaccia nascosta e poi essere rinviati al gateway per il recapito all'utente.

L'integrazione con la difesa web perimetrale preesistente chiede solo pochi istanti ed esistono file di integrazione precostituiti per tutta una serie di firewall e web gateway tra i più diffusi, in modo da rendere il processo ancora più semplice.

### 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 il web è il vettore perfetto per l'infiltrazione.

Zero Trust CDR per Web Gateway assicura agli utenti aziendali la possibilità di caricare e scaricare documenti e immagini commerciali sul web in totale tranquillità grazie alla particolare trasformazione che subiscono. Ogni documento e ogni immagine vengono trasformati e resi innocui.

### Alt alle fughe dei dati nascosti con la steganografia nelle immagini

La steganografia è una tecnica che permette di nascondere dei dati in file apparentemente innocui. È un modo per codificare un messaggio segreto all'interno di un altro messaggio, detto vettore; soltanto la persona a cui è destinato il messaggio segreto è in grado di interpretarlo. Oggi si sta diffondendo sempre più lo stegware, ovvero l'utilizzo della steganografia da parte degli hacker per scopi criminali. Sul Dark Web è disponibile sotto forma di kit malware-as-a-service già pronti. Lo stegware è stato utilizzato in campagne di malvertising per estorcere denaro a migliaia di utenti e rovinare la reputazione di siti di news tra i più seri. È stato utilizzato in associazione a siti web di social media per rubare risorse materiali di valore, nascondendole in immagini apparentemente innocue. Tutte pessime notizie per i professionisti IT che si affidano a strumenti per identificare i dati non sicuri, visto che la steganografia è impossibile da rilevare.

Zero Trust CDR per Web Gateway assicura che ogni immagine vista da un'utente che naviga sul web o comunicata tramite social media sia completamente libera da contenuti occultati utilizzando lo stegware. Il processo di trasformazione distrugge qualsiasi contenuto nascosto, rendendo l'immagine inutile per l'aggressore. Zero Trust CDR per Web Gateway rafforza le iniziative pubbliche e di prevenzione della perdita dei dati già esistenti, ad esempio il Regolamento Generale sulla Protezione dei Dati (GDPR), in quanto impedisce del tutto le fughe di dati occultati nelle immagini tramite la steganografia.

### Alt ai Command and Control Channel (CnC)

Gli attacchi informatici più sofisticati e nocivi spesso prevedono la creazione di un Command and Control Channel (CnC) tra il criminale che opera da remoto e una o più workstation all'interno della rete aziendale. Spesso questi canali vengono stabiliti quando una stazione di lavoro già compromessa contatta un server remoto, ad esempio usando un'immagine su una piattaforma social, oppure quando un malware prima sconosciuto viene introdotto in una rete aziendale camuffato da legittimo documento di lavoro.

Zero Trust CDR per Web Gateway provvede a bloccare qualsiasi tentativo di stabilire un CnC. Il processo di trasformazione rimuove tutte le minacce eventualmente nascoste in documenti, immagini web e social media. Una dashboard forense permette di vedere le copie di documenti e immagini "com'erano prima e dopo", favorendo l'identificazione dei comportamenti sospetti e mettendo alle strette gli utenti.

### Una soluzione configurabile su misura

Insieme ai partner rivenditori di Forcepoint, il team di soluzioni Forcepoint offre un ricco ventaglio di servizi professionali per massimizzare l'investimento nella tecnologia Zero Trust CDR. Possiamo aiutarti a definire la portata, pianificare, installare, configurare e gestire la tua soluzione Zero Trust CDR per Web Gateway.

Il servizio di assistenza tecnica Forcepoint si assicura che tutto funzioni perfettamente durante e dopo la distribuzione. Il nostro team di esperti in soluzioni vanta notevoli competenze e la possibilità di attingere a un ricchissimo database di informazioni che gli permettono di operare come un'estensione naturale del team in-house di ogni cliente.

### Riepilogo: una protezione senza confronti

Siamo sulla soglia di una rivoluzione tecnologica. Bersagliate da una serie incalzante di attacchi informatici, le organizzazioni sono obbligate a riconsiderare ogni aspetto delle loro strategie digitali di acquisizione, condivisione e transazione.



Per maggiori informazioni, consulta  
Forcepoint Zero Trust CDR