Forcepoint

Scheda dati

Prevenzione delle intrusioni con Next-Gen Firewall di Forcepoint

Il sistema di prevenzione delle intrusioni di Forcepoint è tra i più apprezzati del settore per la protezione delle reti aziendali distribuite, dai data center alle filiali e fino al cloud.

Le soluzioni per la sicurezza di rete di Forcepoint offrono uno dei sistemi di prevenzione dalle intrusioni (IPS) più solidi del settore. Ottimamente classificato nei test indipendenti, Forcepoint Next-Gen Firewall può essere adottato come dispositivo IPS autonomo di livello 2 o come parte di una soluzione Next-Gen Firewall completa di livello 3 in ambiente fisico, virtuale e cloud. Contrasta evasioni, exploit e malware che gli hacker usano per fare breccia e insediarsi nelle reti aziendali.

Tutta l'efficacia e la velocità di un'architettura unica

Forcepoint Next-Gen Firewall usa un approccio dinamico basato su flussi per condurre ispezioni che vanno ben oltre il semplice controllo dei pacchetti. Ricostruisce ed esamina i payload reali, riconoscendo le tecniche di evasione che occultano exploit e malware.

In più la decrittografia granulare e ad alta velocità smaschera gli attacchi che tentano di nascondersi nel traffico SSL/TLS. Forcepoint analizza ogni flusso di payload, decodificando i vari livelli dei protocolli per identificare header, metadati e configurazioni anomale o malformate.

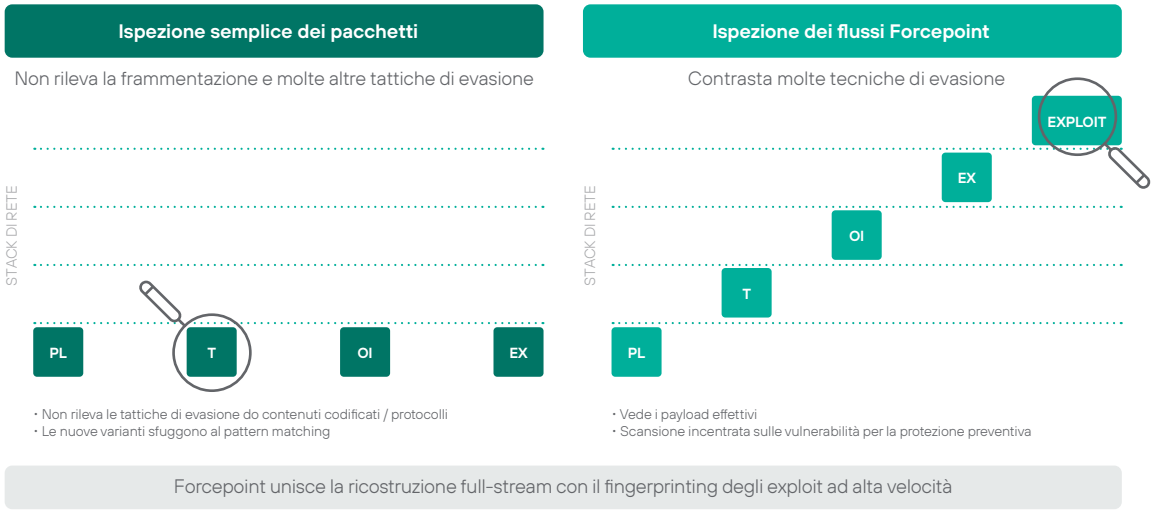
Forcepoint si avvale quindi di tecniche avanzate per esaminare i contenuti delle trasmissioni e rilevare eventuali segni di exploit che puntano a sfruttare le vulnerabilità in molti tipi di sistemi. Diversamente dai pesanti meccanismi basati su firme e pattern, l'approccio più sofisticato di Forcepoint permette di identificare questi attacchi con un'impronta digitale (fingerprint) semplice e concisa. Le impronte vengono associate usando un automa a stati finiti deterministico (DFA) ad alta velocità, su misura per ciascun contesto di protocollo; il DFA consente di integrare le nuove impronte con un impatto pressoché impercettibile sulle risorse della CPU.

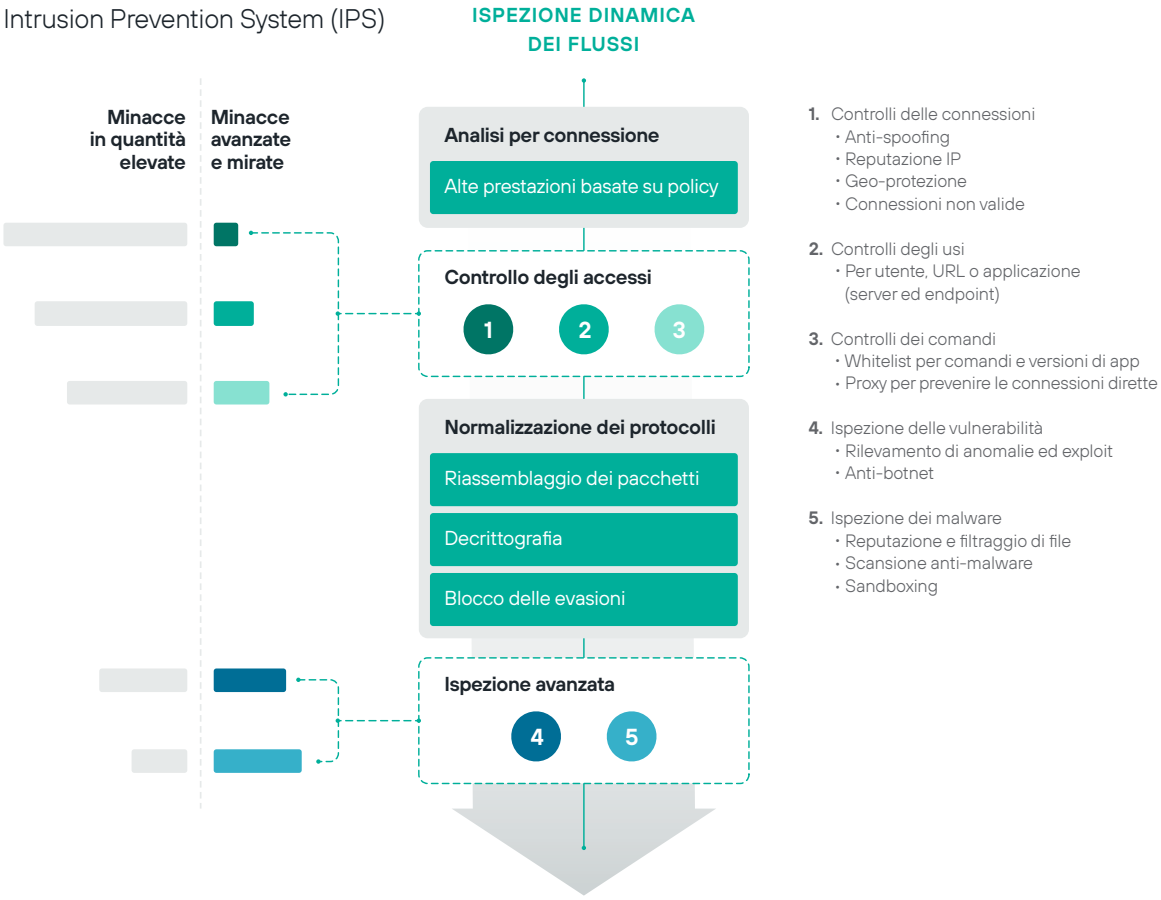
Aggiornamenti continui per anticipare le mosse degli hacker

Il team di ricerca globale di Forcepoint analizza costantemente feed di informazioni, report sulle vulnerabilità provenienti da fonti diverse e una varietà di sistemi di test per esaminare exploit e vulnerabilità. Le nuove impronte vengono pubblicate sul servizio cloud e scaricate automaticamente dai sistemi di sicurezza di rete Forcepoint. Questo approccio proattivo dà ai team IT il tempo necessario per analizzare le patch di recente divulgazione e adottare le strategie di remediation senza temere compromissioni immediate.

Alt alle minacce Zero-Day e ai contenuti indesiderati

I prodotti per la sicurezza di rete di Forcepoint offrono molteplici livelli di difesa da attacchi sconosciuti e contenuti indesiderati. I file trasmessi vengono sottoposti a rigorosi test di reputazione e malware e le nuove minacce, come gli attacchi zero-day, possono essere identificate mediante la nostra tecnologia di sandboxing estremamente avanzata. Forcepoint è tra i pionieri per la classificazione e il filtraggio di contenuti e siti web; con i nostri firewall e dispositivi IPS, le organizzazioni riescono più facilmente a rispettare i regolamenti sul posto di lavoro, limitare l'esposizione dei dati personali e, soprattutto, a impedire del tutto ai loro utenti di accedere a siti web pericolosi.





Resilienza fail-open

I dispositivi Forcepoint supportano tutta una serie di schede di rete modulari, ad esempio le interfacce fail-open che assicurano la continuità del traffico anche se s'interrompe l'alimentazione del Next-Gen Firewall.

La protezione che mantiene attiva la tua azienda

I criminali informatici perfezionano di giorno in giorno le loro capacità di penetrare all'interno di reti aziendali, applicazioni, data center ed endpoint. Una volta all'interno, possono impossessarsi di proprietà intellettuale, dati dei clienti e altri dati rientranti in particolari categorie, causando danni irreversibili alla tua affidabilità e alla reputazione.

Gli attacchi lanciati su internet non si limitano più soltanto a diffondere degli exploit delle vulnerabilità. Accade sempre più spesso che nuove tecniche riescano ad aggirare il rilevamento dei dispositivi di sicurezza tradizionali, anche di firewall noti finora considerati affidabili.

Queste strategie di evasione agiscono su più livelli per occultare exploit e malware, rendendoli invisibili alla tradizionale ispezione dei pacchetti signature-based. Con le evasioni, anche attacchi di vecchia data, magari bloccati per anni, possono essere utilizzati improvvisamente per compromettere i sistemi interni.

L'approccio di Forcepoint è diverso. Il nostro motore IPS, leader dell'industria, è studiato per tutti e tre gli stadi di difesa della rete: lotta alle evasioni, rilevamento degli exploit delle vulnerabilità e blocco dei malware. Può essere applicato in trasparenza a monte dei firewall già esistenti, per aggiungere protezione senza interferenze, oppure come parte della nostra soluzione Next-Gen Firewall completa, per offrire una strategia di sicurezza all-in-one.

Tutti i prodotti per la sicurezza di rete Forcepoint vengono aggiornati costantemente, sono gestiti centralmente e possono condividere dashboard e policy di sicurezza su tutta la rete, senza soluzione di continuità. Con Forcepoint, la tua organizzazione sarà al sicuro – in totale affidabilità, coerenza ed efficienza – a tutti i livelli: data center, rete di uffici, filiali o ambienti cloud.

Risultati

- Meno violazioni
- Più sicurezza, senza interferenze
- Meno esposizione alle nuove vulnerabilità, mentre i team IT preparano la distribuzione delle nuove patch
- Maggiore sicurezza per il lancio di filiali, cloud o data center
- Minore costo totale di proprietà (TCO) per l'infrastruttura di sicurezza e della rete

Funzioni chiave

- Implementazione come Next-Gen Firewall di livello 2, IPS di livello 2 o come parte di una soluzione Next-Gen Firewall di livello 3
- Sistemi IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) per proteggere e difendere
- Ispezione dei flussi per analizzare i paylod reali
- Pionieri nelle strategie di difesa anti-evasione
- Decrittografia ad alta velocità con controlli granulari della privacy
- Rilevamento di usi scorretti e anomalie dei protocolli
- Rilevamento di exploit e malware tramite DFA ad alta velocità
- Rilevamento di attacchi DoS (Denial-Of-Service)
- Difese anti-bot
- Sandboxing zero-day tramite dispositivi locali oppure su cloud
- Filtraggio degli URL leader del settore
- Interfacce di rete fail-open per i dispositivi

Specifiche di Forcepoint Next-Gen Firewall

PIATTAFORME SUPPORTATE	
Dispositivi	Molteplici serie di dispositivi modulari per l'implementazione presso data center, edge di rete e filiali
Infrastruttura cloud	Amazon Web Services, Microsoft Azure
Appliance virtuali	Sistemi x86 a 64 bit; VMware ESXi, VMware NSX, Microsoft Hyper-V e ambienti virtualizzati KVM
Modalità di implementazione	IPS autonomo (livello 2, con moduli di interfaccia di rete fail-open opzionali), parte di NGFW (livello 3)
Contesto virtuale	Virtualizzazione per separare i contesti logici con policy e interfacce distinte

ISPEZIONE	
Normalizzazione del traffico su più livelli / Ispezione avanzata dell'intero flusso	› Ricostruisce e analizza i payload effettivi per assicurare l'integrità dei flussi di dati › Elimina i segmenti duplicati di livello inferiore che potrebbero creare ambiguità dopo il riassemblaggio
Difesa anti-evasione	Blocca i frammenti fuori ordine, i segmenti sovrapposti, la manipolazione dei protocolli, gli offuscamenti, i trucchi di codifica
Rilevamento dinamico dei contesti	Protocollo, applicazione, tipo di file
Ispezione / manipolazione del traffico in base al protocollo	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, IPv6 encapsulation, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC Classic, OPC UA, Oracle SQL Net, POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP, ispezione integrata con i Sidewinder Security Proxy
Decrittografia granulare del traffico SSL/TLS	› Decrittografia ad alte prestazioni di flussi di server e client HTTPS › Controlli basati su policy per proteggere la privacy degli utenti e limitare l'esposizione dei dati personali per le organizzazioni › Verifiche della validità dei certificati TLS e lista delle esenzioni in base ai nomi di dominio dei certificati
Rilevamento degli exploit delle vulnerabilità	› Indipendente dal protocollo, qualsiasi protocollo TCP/UDP con protezione e rilevamento delle evasioni › Supporto per integrazioni delle firme Snort per personalizzare e migliorare l'assetto globale della sicurezza › Grazie alla strategia sofisticata basata sulle impronte, non occorrono molte firme › Il motore di associazione DFA (automa a stati finiti deterministico) ad alta velocità gestisce velocemente le nuove impronte › Aggiornamento continuo delle impronte da Forcepoint
Fingerprinting personalizzato	› Associazione delle impronte indipendente dal protocollo › Linguaggio delle impronte basato su espressioni regolari con il supporto per applicazioni personalizzate
Ricognizione	Scansione lenta, scansione stealth e TCP/UDP/ICMP in IPv4 e IPv6
Anti-botnet	› Rilevamento basato su decrittografia e analisi delle sequenze di lunghezza dei messaggi › Classificazione degli URL aggiornata automaticamente o segnalazione dei siti botnet agli utenti
Correlazione	Correlazione locale, correlazione server dei registri
Protezione Dos/DDoS	› Rilevamento flood SYN/UDP con limiti di connessioni concorrenti, compressione dei log in base all'interfaccia › Protezione da metodi di richiesta HTTP lenti, limite di connessioni half-open › Separazione di Control Plane e Data Plane
Metodi di bloccaggio	Bloccaggio diretto, reset della connessione, blacklist (locale e distribuita), risposta HTML, ridirezionamento HTTP
Registrazione del traffico	Registrazioni automatiche del traffico / estratti da situazioni di usi scorretti
Aggiornamenti automatici	› Aggiornamenti dinamici costanti tramite il Security Management Center (SMC) di Forcepoint › Aggiorna le patch virtuali e offre indicazioni e prevenzione sulle minacce emergenti

Specifiche di Forcepoint Next-Gen Firewall, continua

CONTROLLO FILE E RILEVAMENTO MALWARE AVANZATI	
Protocolli	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Filtraggio di file	Filtraggio dei file in base alle policy con efficace processo di selezione; supporto per oltre 200 tipi di file in 19 categorie
Reputazione dei file	Controllo della reputazione e bloccaggio di malware in cloud ad alta velocità
Analisi anti-virus sui file	Motore di scansione anti-virus locale*
Sandboxing zero-day	Forcepoint Advanced Malware Detection disponibile per Forcepoint NGFW erogato come servizio cloud, locale o anche come servizio air-gap simile a quello utilizzato da Forcepoint Web Security, Forcepoint Email Security e Forcepoint CASB

FILTRAGGIO DEGLI URL	
Classificazione degli URL	Basata su tecnologia Forcepoint ThreatSeeker Intelligence, uguale a quella utilizzata da Forcepoint Web Security e Forcepoint Email Security
Aggiornamenti automatici	Aggiornamenti costanti a mano a mano che vengono analizzati nuovi siti
Attuazione di policy degli accessi basate su categorie	NGFW URL Filtering di Forcepoint è disponibile come servizio extra in abbonamento

GESTIONE E MONITORAGGIO	
Interfacce di gestione	Sistema di gestione centralizzato di classe enterprise con funzionalità di analisi dei registri, monitoraggio e reporting (per dettagli, leggi la scheda dati di Forcepoint Security Management Center)
Monitoraggio SNMP	SNMPv1, SNMPv2c ed SNMPv3
Acquisizione del traffico	tcpdump della console, acquisizione remota tramite Forcepoint Security Management Center
Comunicazioni di gestione ad alta sicurezza	Comunicazioni gestione-motore con sicurezza a 256 bit
Certificazioni di sicurezza	Profilo di protezione dei dispositivi di rete Common Criteria con firewall di filtraggio stateful dei pacchetti esteso, certificato FIPS 140-2 Crypto, CSPN di ANSSI, USGv6 certificazione di sicurezza primo livello
Endpoint Context Agent	Whitelist e blacklist delle applicazioni client in esecuzione sugli host e sui dispositivi degli utenti finali. Può prevenire le connessioni in uscita dei file non attendibili e abilita controlli granulari personalizzabili in base alle esigenze dell'organizzazione.

*Scansione anti-malware locale non disponibile con i dispositivi 110/115.