SCHEDA TECNICA

Infoblox Threat Defense™ Advanced

Il DNS protettivo basato su threat intelligence predittiva protegge tutto, ovunque, prima dell'impatto

IL DNS È IL PRIMO PUNTO DI PREVENZIONE PER TUTTI GLI ATTACCHI INFORMATICI

Il DNS è il primo punto di rilevamento e prevenzione per tutti gli attacchi informatici. Che si tratti di un'email di phishing, un messaggio smishing o una vulnerabilità sfruttata, quasi ogni attacco genera una query DNS verso un dominio dannoso. Di conseguenza, il DNS fornisce un potente punto centralizzato di visibilità e controllo per proteggere un'intera impresa, inclusi utenti, dispositivi, IoT/OT e carichi di lavoro, sia on-premise, nel cloud o all'edge.

Come primo passo di qualsiasi comunicazione, il rilevamento e il blocco delle attività di minaccia a livello DNS aiuta a fermare il traffico dannoso prima che raggiunga gli strumenti a valle e attivi gli avvisi. Correlando i dati DNS con il contesto di dispositivi e risorse, i team NetOps e SecOps ottengono una visibilità più approfondita su ciò che accade nei loro ambienti, migliorando sia l'efficienza operativa che il livello di sicurezza.

LE TRADIZIONALI SOLUZIONI DI "RILEVAMENTO E RISPOSTA" NON SONO PIÙ EFFICACI

Gli attori di minacce utilizzano sempre più l'AI per lanciare campagne più prolifiche, sofisticate e furtive. Generano malware monouso, realizzati in modo unico, che rendono inefficaci gli strumenti tradizionali di "rilevamento e risposta", i quali aspettano un'infezione del "paziente zero". Ogni attacco si trasforma in uno scenario di "paziente zero" in cui non esiste alcuna firma o comportamento noto. Gli strumenti di "rilevamento e risposta" spesso agiscono troppo tardi nella kill chain per prevenire danni. Quindi, è necessario un approccio preventivo diverso. Una che blocca le minacce prima che entrino nell'ambiente o si muovano lateralmente. Questo non solo blocca gli attacchi precocemente, ma riduce anche il carico sui tradizionali strumenti di "rilevamento e risposta".

Il DNS funziona come un punto di controllo a monte, offrendo ai team di sicurezza un'opportunità proattiva per rilevare e bloccare le minacce in anticipo, prima che raggiungano utenti, carichi di lavoro o endpoint.

SICUREZZA PREVENTIVA CON DNS

Infoblox Threat Defense™ Advanced offre un **approccio preventivo** unico al rilevamento delle minacce. Uno che non si basa sul "paziente zero". Utilizza una combinazione di **threat intelligence predittiva** che blocca l'infrastruttura degli attori di minacce prima che venga utilizzata come arma e analisi algoritmica/ML delle query DNS nelle reti dei clienti per fornire protezione prima dell'impatto. Attraverso l'identificazione rapida delle risorse coinvolte negli incidenti di sicurezza, le integrazioni degli ecosistemi e gli spazi di lavoro intuitivi, consente un rilevamento più rapido, una risposta più rapida e un maggiore ritorno sull'investimento (ROI) dagli investimenti in sicurezza esistenti.

DATI E CIFRE

- Monitora **204.000** cluster di attori di minacce in tempo reale e in continua crescita
- Riduce il tasso di falsi positivi allo **0,0002%**
- Blocca **l'82%** delle minacce prima della prima query
- Offre protezione in media **68,4** giorni prima di un attacco
- Blocca **5 volte più** domini ad alto/medio rischio rispetto agli strumenti che si limitano a cercare un comportamento dannoso noto
- Fa risparmiare in media **500 ore di analisi SOC** al mese*
- Consente di realizzare **400.000 dollari** di risparmi sulla produttività all'anno*
- Riduce decine di migliaia di avvisi a poche unità*

Il SANS SOC 2025 Survey ha rivelato che sette dei 10 principali ostacoli che impediscono il pieno utilizzo del SOC riguardano gli avvisi, l'integrazione degli strumenti e la carenza di competenze.

*Basato su dati reali dei clienti.

BLOCCA LE MINACCE PRIMA DELL'IMPATTO

Infoblox Threat Defense applica la threat intelligence DNS predittiva con analisi algoritmiche e basate su machine learning sul traffico DNS in tempo reale per bloccare l'attività delle minacce prima che influiscano sulla rete, spesso rilevando minacce che altri strumenti non riescono a rilevare. Bloccando le minacce a livello DNS, Infoblox aiuta anche a ridurre il volume degli avvisi e il carico di lavoro sugli strumenti di sicurezza a valle, con i clienti che segnalano una riduzione fino al 50% degli avvisi sui firewall di nuova generazione (NGFW) e sui sistemi di rilevamento e risposta degli endpoint (EDR).

> *"Il DNS sicuro potrebbe ridurre la capacità del 92% degli attacchi di malware di distribuire con successo malware su una determinata rete."*
>
> **Anne Neuberger,**
> **Direttrice della sicurezza informatica Direzione,**
> **National Security Agency (NSA)**

Funzionalità principale	Descrizione	Infoblox Threat Defense	NGFW	SASE	EDR
Resolver sicuro a livello aziendale e registrazione delle query DNS	Utilizza i dati delle query DNS per individuare e bloccare i domini	●	◑	◑	◑
Monitoraggio completo del comportamento DNS	Monitora tutti i tipi di record DNS alla ricerca di attività dannose	●	●	◔	○
Rilevamento e rimozione di domini lookalike/ doppleganger	Attenua la superficie di attacco dei lookalike/doppleganger	●	○	◑	○
Zero Day DNS Protection	Identifica domini nuovi o emergenti che potrebbero rappresentare una minaccia per la tua organizzazione	●	◑	◑	○
Rilevamento del tunneling DNS basato sul comportamento	Rileva i tunnel DNS utilizzati per l'esfiltrazione/infiltrazione dei dati, le comunicazioni C2, ecc.	●	◑	◑	○
Protezione proattiva dei domini sospetti/ ad alto rischio	Identifica e blocca preventivamente i domini sospetti che potrebbero essere utilizzati in future campagne dannose	●	◑	◑	◑
Arricchimento automatico del contesto nativo	Correla il contesto di rete senza la necessità di installare client o di sinkholing (utente, dispositivo, IP sorgente, posizione, indirizzo MAC, VLAN)	●	◑	◑	◑
Rilevamento e distruzione dei Threat Distribution Systems (TDS)	Identifica l'infrastruttura TDS posta in essere dagli attori di minacce e non soltanto i singoli domini, questo permette di contrastare gli attori di minacce che usano i domini a rotazione per evitare il rilevamento	●	◔	○	○

Figura 1. Funzionalità esclusive di Threat Defense che altri strumenti non sono in grado di gestire completamente

CARATTERISTICHE PRINCIPALI DI THREAT DEFENSE

- **Monitoraggio di "protezione prima dell'impatto".** Consente a CISO e team di sicurezza di eseguire la loro strategia di sicurezza preventiva e di riferire al consiglio di amministrazione con metriche chiare e quantificabili sulle minacce neutralizzate prima dell'impatto, ottenendo vantaggi in termini di tempo critico e riducendo il carico sul Security Operation Center (SOC).
- **Rilevazione di risorse e integrazione dell'inventario.** Identificazione rapida delle risorse coinvolte negli incidenti di sicurezza per una valutazione e una risposta più rapide agli incidenti.
- **Area di lavoro di sicurezza.** Interfaccia utente semplificata e intuitiva che consente ai team di sicurezza di comprendere cosa accade nel loro ambiente e suggerire modi per ridurre i rischi per la sicurezza.
- **Modalità di rilevamento.** Per una facile implementazione e proof of concept, senza modificare l'infrastruttura IT o di rete esistente.

POTENZIA LA SICUREZZA PREVENTIVA CON L'INTELLIGENCE PREDITTIVA

Infoblox è il leader nella creazione di threat intelligence DNS originale. L'azienda adotta un approccio preventivo, non solo difensivo, utilizzando le sue intuizioni per tracciare l'infrastruttura degli attori di minacce mentre viene costruita e interrompere il crimine informatico alla fonte, spesso prima ancora che venga lanciato un attacco.

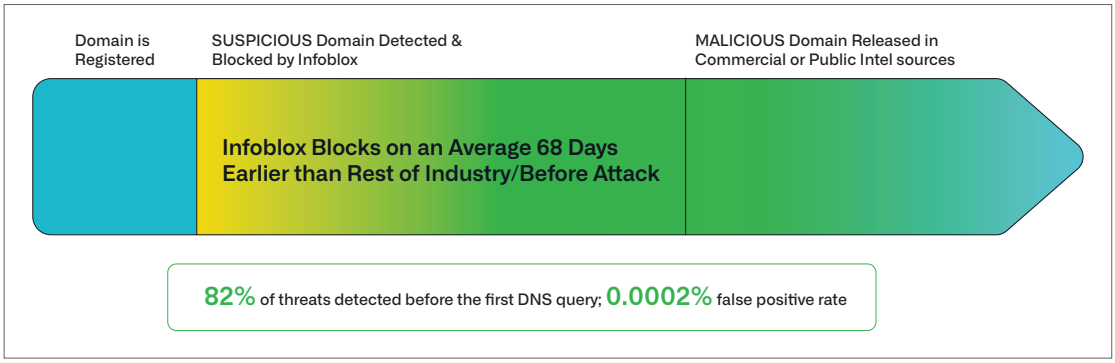

Figura 2. La threat intelligence di Infoblox può proteggere dalle minacce prima del resto del settore della sicurezza

Come Infoblox crea la threat intelligence DNS originale

Esperti di DNS: Infoblox scopre gli attori di minacce nascosti nel DNS sapendo dove cercare. Partendo da domini ad alto rischio o sospetti, il team collega i punti per identificare l'infrastruttura degli aggressori e tracciarla man mano che si evolve e fa emergere nuove minacce, prima che vengano riconosciute altrove.

Competenza sulle minacce: Infoblox comprende come operano gli attori malintenzionati e come si manifestano minacce come malware, ransomware, phishing ed exploit basati su DNS. Tale competenza alimenta sistemi predittivi che rilevano domini lookalike, attività di comando e controllo (C2) DNS, algoritmi di generazione di domini registrati (RDGA) e altri comportamenti sospetti.

Data science: Infoblox applica machine learning e data science avanzata a enormi volumi di dati di query DNS. Ciò consente una protezione quasi in tempo reale contro l'esfiltrazione dei dati, gli algoritmi di generazione di domini (DGA) e un'ampia gamma di minacce evasive.

LAVORA IN MODO PIÙ INTELLIGENTE CON SOC INSIGHTS

Dall'affaticamento degli avvisi e dal burnout degli analisti ai lunghi sforzi di indagine e risposta, Infoblox Threat Defense offre un notevole sollievo al SOC, con il pacchetto aggiuntivo SOC Insights.

- Aiuti gli analisti a comprendere ciò che è più importante con analisi guidate dall'AI che riducono gli avvisi da centinaia di migliaia a una manciata di "informazioni".
- Automatizza la raccolta e la correlazione di log, threat intelligence e altri dati, in modo che gli analisti possano avviare rapidamente le indagini e le risposte.
- Accelera la risposta agli incidenti con la rilevazione di risorse e l'integrazione dell'inventario, aiutando gli analisti a identificare più rapidamente i dispositivi interessati.

Figura 3. Infoblox Threat Intel ha condiviso dati di ricerca sorprendenti sull'aumento del rischio dei domini lookalike

ESPORTA LOG DNS DI ALTO VALORE SU LARGA SCALA

Infoblox semplifica l'invio di dati di query ed eventi DNS ad alta fedeltà al tuo SIEM, SOAR o data lake per una visibilità centralizzata e una correlazione delle minacce più rapida.

- Filtra e inoltra solo gli eventi DNS di alto valore per ridurre i costi di ingestione nel SIEM e il numero di avvisi.
- Trasmetti in streaming i log DNS arricchiti in tempo reale utilizzando Infoblox Cloud Data Connector.
- Migliora il rilevamento e la risposta in tutto il tuo ecosistema fornendo a ogni strumento il contesto di cui ha bisogno.
- Condividi i dati senza problemi con altri strumenti attraverso integrazioni bidirezionali certificate, migliorando il rilevamento, il triage e la risposta end-to-end.

INDAGA PIÙ VELOCEMENTE CON DOSSIER

Dossier fornisce agli analisti un potente strumento di ricerca unificato per convalidare le minacce, fare leva sugli indicatori di compromissione (IOC) e accelerare le indagini, senza la necessità di passare da una piattaforma all'altra.

- Consolida le informazioni sulle minacce interne, di Infoblox e di terze parti in un'unica interfaccia intuitiva.
- Indaga rapidamente sugli IOC e scopri le minacce correlate con l'arricchimento integrato e l'analisi dei collegamenti.
- Riduce i tempi di indagine fino al 67% eliminando la raccolta manuale dei dati e il cambio di contesto.

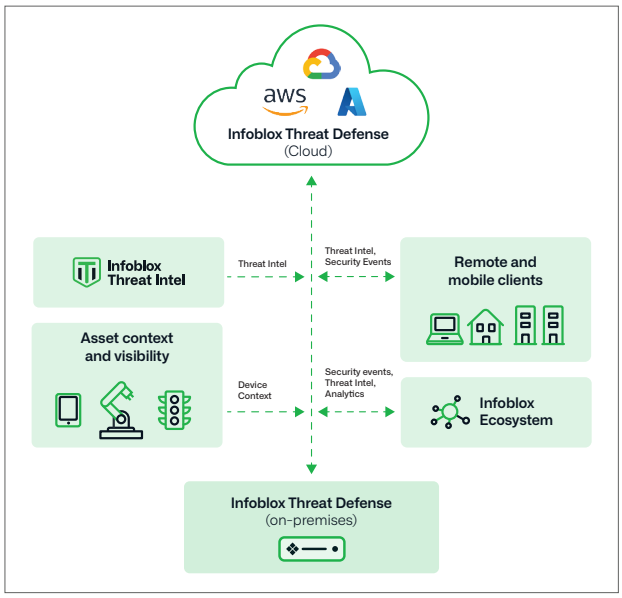

Figura 4. L'architettura ibrida Infoblox consente la protezione ovunque e l'implementazione ovunque per contrastare l'odierno panorama delle minacce basate sull'AI.

PROTEGGI IL TUO MARCHIO DAGLI INGANNI MIRATI

Infoblox offre due funzionalità integrate – monitoraggio dei domini lookalike e servizi di mitigazione dei domini – che aiutano a proteggere il tuo marchio, i clienti e i dipendenti da attacchi informatici basati sull'inganno. Insieme, ti forniscono visibilità sulle minacce emergenti e la capacità di intraprendere azioni rapide ed efficaci contro i domini dannosi prima che influenzino la tua attività.

Monitoraggio dei domini lookalike

Anticipa gli attacchi di impersonificazione che sfruttano il tuo marchio o terze parti fidate.

- Rileva i domini registrati per impersonare la tua azienda, la catena di approvvigionamento o le proprietà rivolte ai clienti.
- Identifica i domini utilizzati nelle campagne di phishing e frode che prendono di mira i tuoi dipendenti o clienti.
- Monitora i domini ad alta priorità per cambiamenti nel profilo di rischio e ricevi avvisi in tempo reale.

Servizi di mitigazione dei domini

Convalida rapidamente e rimuovi i domini dannosi attivi in rete.

- Conferma e documenta le attività dannose tramite la convalida degli incidenti condotta da esseri umani e la reportistica riepilogativa.
- Coordinati con ISP globali, provider di hosting e agenzie di regolamentazione per una rapida rimozione, spesso entro 24 ore.
- Monitora le minacce mitigate per 30 giorni dopo la rimozione per rilevare e rimuovere i tentativi di riattivazione, senza costi aggiuntivi.
- Affronta una gamma di tipi di minacce, tra cui phishing, hosting di malware, infrastrutture C2 e dati rubati.

Per saperne di più sui modi in cui Infoblox Threat Defense protegge i tuoi dati e la tua infrastruttura, visita https://www.infoblox.com/products/threat-defense/.

Sede centrale
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Versione: 20250121v1