SCHEDA TECNICA

Infoblox Advanced DNS Protection

Riduci al minimo le interruzioni dell'attività causate da attacchi basati su DNS

SFIDA: INTERRUZIONI DEL SERVIZIO

Il DNS è fondamentale per ogni organizzazione perché fornisce la connettività di rete mission-critical necessaria per gestire un'azienda. Se il server DNS esterno si arresta, l'intera rete viene disattivata da Internet. L'interruzione del DNS interferisce o arresta le applicazioni IT critiche, come e-mail, siti web, VoIP e Software as a Service (SaaS). Poiché nel 2020 un numero significativo della forza lavoro ha iniziato a lavorare in remoto, si è verificato un enorme picco di attacchi DDoS. Il DNS continua a essere uno dei principali servizi presi di mira dagli attacchi DDoS perché è fondamentale per mantenere un'azienda online. Oltre alla perdita di fiducia da parte dei clienti, gli attacchi DDoS riusciti possono costare a un'organizzazione centinaia di migliaia di dollari di entrate perse al mese.

Infoblox offre la più ampia gamma di protezione sul mercato per proteggere i tuoi servizi DNS vitali dagli attacchi, garantendo la disponibilità del 99,999% da cui dipende la tua organizzazione. Offre una visibilità centralizzata su chi sta utilizzando la rete, su quali dispositivi si trova e dettagli sull'attacco per garantire una risposta rapida.

SOLUZIONE: PROTEGGI LA TUA AZIENDA DALLE INTERRUZIONI CAUSATE DA ATTACCHI BASATI SU DNS

Con Infoblox Advanced DNS Protection (ADP), la tua azienda è sempre attiva e funzionante, anche in caso di attacco basato su DNS. Infoblox blocca la più ampia gamma di attacchi, come attacchi volumetrici, NXDOMAIN, exploit e dirottamento DNS. A differenza degli approcci che si basano sull'overprovisioning dell'infrastruttura o sulla semplice limitazione della velocità di risposta, Advanced DNS Protection rileva e mitiga gli attacchi DNS in modo intelligente rispondendo solo a query legittime grazie all'utilizzo di una threat intelligence costantemente aggiornata, senza la necessità di implementare patch di sicurezza. Con Infoblox, puoi portare l'affidabilità della rete a un livello superiore, assicurando che la tua infrastruttura critica, e la tua azienda, continuino a funzionare in ogni momento.

CARATTERISTICHE PRINCIPALI

Riduci le interruzioni dell'attività: Infoblox Advanced DNS Protection (ADP) monitora, rileva e blocca continuamente tutti i tipi di attacchi DNS, inclusi gli attacchi volumetrici, gli attacchi non volumetrici, come gli exploit DNS e il dirottamento DNS, rispondendo al contempo a query legittime. Mantiene inoltre l'integrità DNS, che gli attacchi di dirottamento DNS possono compromettere. Infoblox fornisce una solida base per la sicurezza, garantendo una disponibilità del 99,999% per la tua rete.

Adattati alle minacce in evoluzione: Infoblox ADP utilizza la tecnologia Infoblox Threat Adapt™ per aggiornare automaticamente la protezione contro le minacce nuove e in evoluzione non appena emergono. Threat Adapt applica analisi e ricerche indipendenti all'evoluzione delle tecniche di attacco, compreso ciò che gli specialisti delle minacce di Infoblox hanno osservato nelle reti dei clienti, per aggiornare la protezione. Adatta automaticamente la protezione per riflettere le modifiche alla configurazione DNS.

ABILITARE DOT E DOH

La comunicazione tra il resolver del client DNS (stub) e il server DNS locale (resolver ricorsivo) non è crittografata. Le comunicazioni non criptate sono soggette allo snooping, all'intercettazione e all'esfiltrazione dei dati, altrimenti noto come problema di sicurezza dell'"ultimo miglio" del DNS. In risposta, il settore ha realizzato DNS over TLS (DoT) e DNS over HTTPS (DoH) per fornire privacy e crittografia tra i client DNS e i server DNS Internet esterni. L'implementazione della crittografia tramite il resolver DNS nella rete consente di mantenere il controllo dell'esperienza di rete dell'utente, fornendo al contempo sicurezza e filtro dei contenuti in base ai requisiti dei criteri di sicurezza. ADP ottimizza la crittografia DNS con il motore di pacchetti ad alte prestazioni chiamato Fast Path in modo da poter terminare le connessioni DoT e DoH crittografate sulla rete.

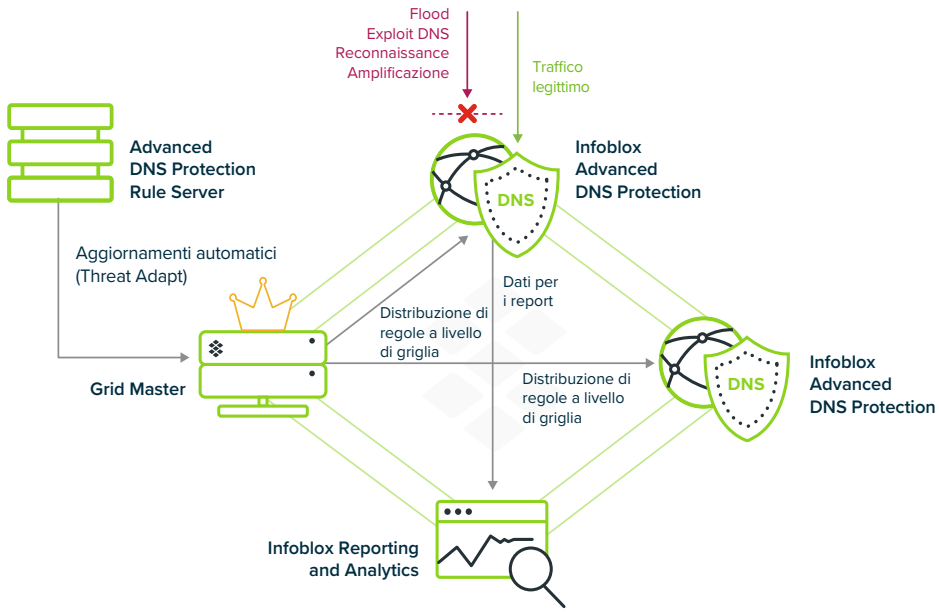

Figura 1: Infoblox Advanced DNS Protection fornisce una difesa unica contro gli attacchi basati su DNS.

CARATTERISTICHE CHIAVE (CONTINUA)

Ottieni visibilità da un unico pannello di controllo:
Con Infoblox, la tua organizzazione può facilmente visualizzare gli attacchi DNS precedenti o attuali e migliorare l'efficienza operativa attraverso il nostro rapido rimedio alle minacce. Infoblox Advanced DNS Protection offre anche una visione unica dei punti di attacco sulla rete e delle fonti di attacco, fornendo l'intelligence necessaria per la gestione delle minacce. È integrato con la nostra soluzione DNS.

Deploy flessibile:
Con Infoblox, hai la possibilità di effettuare il deploy come componente aggiuntivo di abbonamento alle appliance Trinzic virtuali e fisiche.

COSA DICONO I NOSTRI CLIENTI

"Gli incidenti di servizio dovuti ad attacchi DDoS sono stati dimezzati e le lamentele dei clienti sui lunghi tempi di caricamento delle pagine sono stati significativamente ridotti."

—VP of Customer Support, grande Service Provider

"Utilizzo Infoblox per la gestione di DNS, DHCP e indirizzi IP da quattro anni. È un prodotto solido. Abbiamo spostato le risorse perché il prodotto funziona davvero bene. La nostra presenza globale è gestita da 1,5 FTE, ovvero 65 dispositivi."

—Manager of Global Infrastructure, Adobe

TABELLA 1:
RIEPILOGO DEI TIPI DI ATTACCO DA CUI ADVANCED DNS PROTECTION (ADP) DIFENDE

Nome attacco	Tipo	Come funziona
DNS reflection/ DDoS attacks	Volumetrico	Utilizzo di server DNS di terze parti (open resolver) per propagare un attacco DoS o DDoS
Amplificazione DNS	Volumetrico	Utilizzo di una query appositamente predisposta per creare una risposta amplificata per inondare la vittima di traffico
TCP/UDP/ICMP flood	Volumetrico	Denial of service a layer 3 interrompendo una rete o un servizio inondandolo di grandi quantità di traffico
NXDOMAIN	Volumetrico	Inonda il server DNS di richieste di domini inesistenti, con conseguente saturazione della cache e tempi di risposta più lenti
Sottodominio casuale (attacchi "low and slow"), attacchi di blocco del dominio, attacchi di dominio fantasma	Low-volume stealth	Inonda il server DNS con richieste di domini fantasma o che si comportano in modo anomalo configurati come parte dell'attacco, causando l'esaurimento delle risorse, la saturazione della cache, l'esaurimento del limite di query in uscita e il peggioramento delle prestazioni
Exploit basati su DNS	Exploit	Attacchi che sfruttano le vulnerabilità nel software DNS
DNS cache poisoning	Exploit	Alterazione dei dati della cache DNS con un indirizzo non autorizzato
Anomalie del protocollo	Exploit	Causa l'arresto anomalo del server inviando pacchetti e query non validi
Reconnaissance	Exploit	Tentativi da parte degli hacker di ottenere informazioni sull'ambiente di rete prima di lanciare un attacco DDoS di grandi dimensioni o un altro tipo di attacco
Dirottamento hijacking DNS	Exploit	Attacchi che sovrascrivono le informazioni di registrazione del dominio per indirizzare a un server DNS non autorizzato
Esfiltrazione dei dati (utilizzando tunnel noti)	Exploit	L'attacco comporta il tunneling di un altro protocollo attraverso la porta DNS 53, che è consentito se il firewall è configurato per trasportare traffico non DNS, ai fini dell'esfiltrazione dei dati

OPZIONI DI APPLIANCE

Software ADP: disponibile su piattaforme fisiche e virtuali

Software ADP è un componente aggiuntivo software delle appliance Trinzic TE-815/825/1415/1425/2215/2225/4015/4025.

TE - 4015/4025

TE - 1415/1425

TE - 2215/2225

TE - 815/TE 825

Inizia con una valutazione

La valutazione Software ADP gratuita (60 giorni) con licenza temporanea per i clienti sarà resa disponibile tramite i tuoi Account Manager/SE.

Infoblox unisce networking e sicurezza per offrire prestazioni e protezione senza pari. Scelti dalle aziende Fortune 100 e dagli innovatori emergenti, forniamo visibilità e controllo in tempo reale su chi e cosa si connette alla tua rete, in modo che la tua organizzazione funzioni più velocemente e blocchi le minacce in modo più rapido.

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

+1.408.986.4000
www.infoblox.com