SCHEDA TECNICA

BloxOne® Threat Defense Advanced

Rafforza e ottimizza la tua strategia di sicurezza dalle fondamenta

LA NECESSITÀ DI UNA SICUREZZA FONDAMENTALE SU LARGA SCALA

Il modello di sicurezza tradizionale è inadeguato nel mondo odierno delle trasformazioni digitali.

- Il perimetro è cambiato e i tuoi utenti accedono direttamente alle applicazioni basate su cloud da qualsiasi luogo.
- L'IoT porta a un'esplosione di dispositivi che non accettano le tecnologie endpoint tradizionali per la protezione.
- La maggior parte dei sistemi di sicurezza sono complessi e non raggiungono facilmente il livello necessario per proteggere questi ambienti dinamici.

Ciò di cui le organizzazioni hanno bisogno è una soluzione di sicurezza scalabile, semplice e automatizzata che protegga l'intera rete senza la necessità di implementare o gestire infrastrutture aggiuntive.

INFOBLOX FORNISCE UNA PIATTAFORMA SCALABILE CHE MASSIMIZZA L'INVESTIMENTO ESISTENTE NELLA DIFESA DALLE MINACCE

Infoblox BloxOne Threat Defense Advanced è una soluzione completa di DNS Detection and Response (DNSDR), rileva l'attività delle minacce che altre soluzioni non rilevano e blocca gli attacchi prima che si verifichino con informazioni sulle minacce DNS pre-campagna per interrompere le catene di approvvigionamento degli aggressori. Le integrazioni intelligenti dell'ecosistema e l'automazione riducono lo sforzo manuale, mentre le esclusive analisi basate sull'AI di Infoblox concentrano gli analisti su ciò che conta di più e forniscono informazioni che riducono l'MTTR, aumentano il ROI degli strumenti di sicurezza esistenti ed elevano l'efficienza complessiva di SecOps.

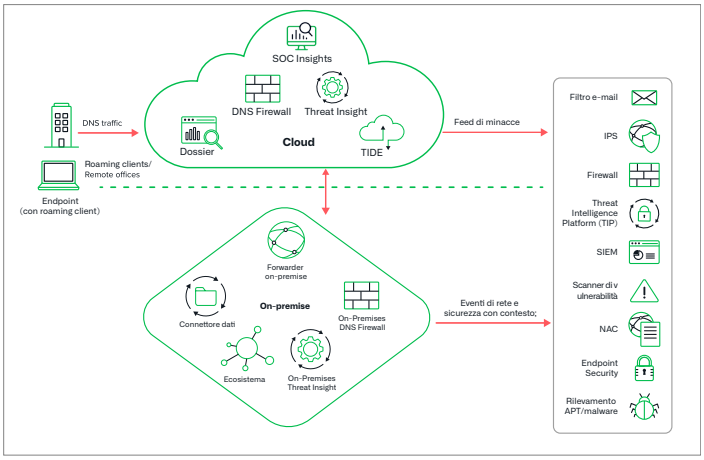


Figura 1: L'architettura ibrida Infoblox consente la protezione ovunque e l'implementazione ovunque

FUNZIONALITÀ PRINCIPALI

- Rileva e blocca exploit, phishing, ransomware e altri malware moderni che altre soluzioni non riescono a rilevare
- Proteggi utenti e dispositivi, indipendentemente dalla piattaforma o dal sistema operativo, a livello DNS, inclusi BYOD, IoT e ICS
- Scopri le applicazioni ad alto rischio e gestisci i rischi Shadow IT, Insider, Compliance e altri
- Previeni le tecniche di esfiltrazione dei dati con analisi AI/machine learning, compresa l'esfiltrazione dei dati basata su DNS, DGA e DNSMessenger
- Limita l'accesso dell'utente a contenuti web inappropriati o indesiderati e monitora l'attivitày
- Proteggi il tuo marchio con il monitoraggio dei domini Lookalike per le tue proprietà Internet più preziose
- Accelera di 3 volte le indagini e semplifica le attività di risposta alle minacce e di caccia alle minacce
- Migliora la visibilità: ottieni una visibilità precisa "e un ricco contesto di rete" grazie all'integrazione con i metadati delle risorse IPAM per una comprensione e una correlazione ottimale degli eventi
- SOC Insights ti consente di avviare rapidamente l'indagine e la risposta alle minacce che contano di più e di ridurre l'MTTR con informazioni basate sull'AI

MASSIMIZZA L'EFFICIENZA DEL SECURITY OPERATION CENTER

Riduci i tempi di risposta agli incidenti

- Blocca automaticamente le attività nocive e fornisci i dati delle minacce al resto dell'ecosistema di sicurezza per indagini, quarantena e riparazione
- Ottimizza la tua soluzione SOAR utilizzando dati contestuali di rete e threat intelligence, e sfrutta le integrazioni dell'ecosistema Infoblox (un fattore critico di SOAR) per ridurre i tempi di risposta alle minacce e l'OPEX
- Utilizza le funzionalità di Infoblox SOC Insights per sapere quali eventi contano di più con le analisi basate sull'AI che vanno oltre le semplici dashboard classificate in base al rischio di malware

Unisci la politica di sicurezza con la portabilità della threat intelligence

- Raccogli e gestisci dati di threat intelligence da fonti interne ed esterne e distribuiscili ai sistemi di sicurezza esistenti
- Riduci il costo dei feed delle minacce e migliora l'efficacia della threat intelligence nell'intero stack di sicurezza

Indagine e ricerca delle minacce più rapide

- Avvia rapidamente l'indagine e la risposta alle minacce che contano di più e riduci l'MTTR con informazioni basate sull'AI che vanno oltre le semplici dashboard classificate in base al rischio di malware
- Rende il tuo team di analisti delle minacce 3 volte più produttivo mettendo a disposizione degli analisti della sicurezza indagini automatizzate sulle minacce, approfondimenti sulle minacce correlate e prospettive di ricerca aggiuntive da fonti informatiche esperte, per prendere decisioni rapide e precise sulle minacce

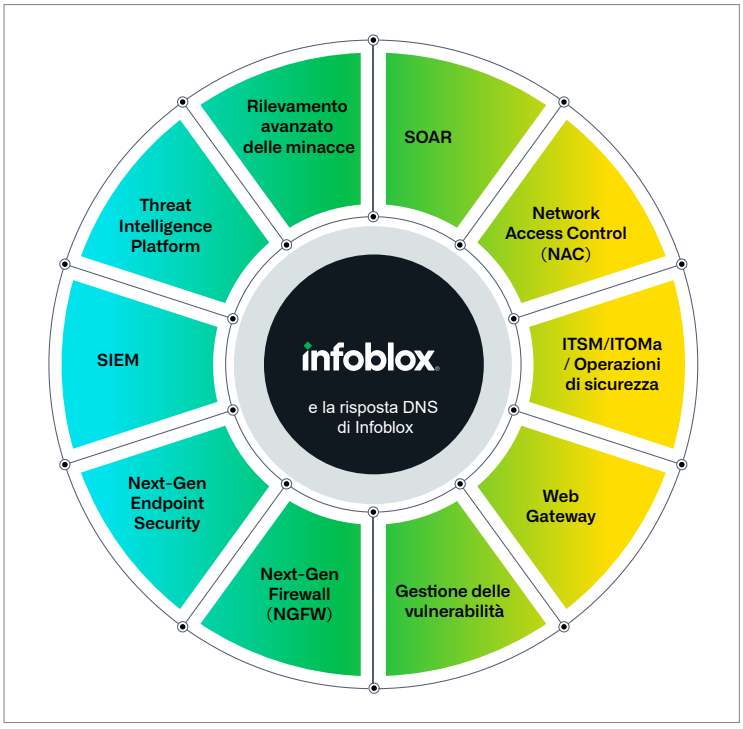
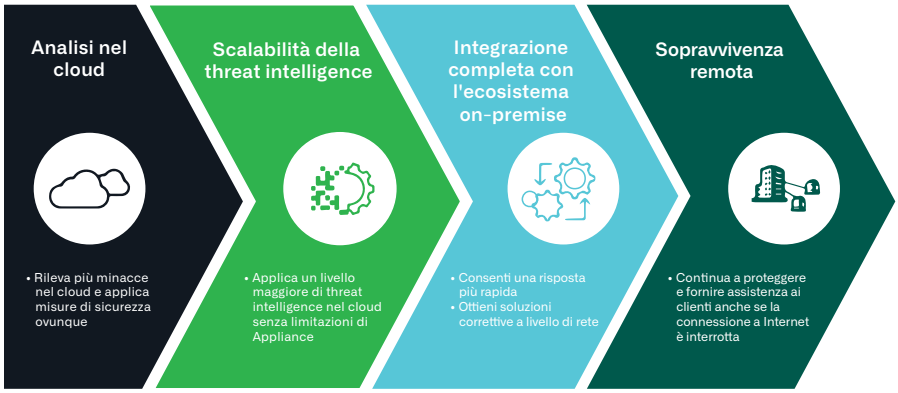


Figura 2: BloxOne Threat Defense si integra con l'intero ecosistema di sicurezza informatica

> *"Al giorno d'oggi ci sono davvero troppi ransomware, spyware e adware che arrivano attraverso i link aperti dagli utenti di Internet. La soluzione di sicurezza cloud di Infoblox aiuta a bloccare gli utenti dai reindirizzamenti che li portano a siti dannosi, impedisce alle macchine di essere infettate e mantiene gli utenti più sicuri."*
>
> **Senior System Administrator and Network Engineer, City University of Seattle**

L'APPROCCIO IBRIDO PROTEGGE LE IMPLEMENTAZIONI OVUNQUE



Analisi nel cloud

- Sfrutta le maggiori capacità di elaborazione del cloud per rilevare una gamma più ampia di minacce, tra cui esfiltrazione di dati, algoritmo di generazione di domini (DGA), fast flux, malware senza file, Dictionary DGA e altro ancora utilizzando l'analisi basata sul machine learning
- Rileva le minacce nel cloud e applica misure di sicurezza ovunque per proteggere sedi centrali, data center, uffici remoti o dispositivi in roaming

Scalabilità della threat intelligence

- Applica l'intelligence completa della ricerca Infoblox e dei fornitori di terze parti per implementare le politiche on-premise o nel cloud e distribuiscila automaticamente al resto dell'infrastruttura di sicurezza
- Applica un livello maggiore di threat intelligence nel cloud senza enormi investimenti in più appliance di sicurezza per ogni sito

Potenti integrazioni con il tuo ecosistema di sicurezza

- Consente la completa integrazione con Infoblox on-premise e tecnologie di sicurezza di terze parti, consentendo la riparazione a livello di rete e migliorando il ROI di tali tecnologie

Sopravvivenza/resilienza da remoto

- In caso di interruzione della connettività Internet, Infoblox on-premise può continuare a proteggere la rete

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

IL ROI DELLA SICUREZZA INFOBLOX

Riduci il carico sui dispositivi di sicurezza oberati

- Riduci il carico sui dispositivi di sicurezza perimetrale oberati come firewall, IPS e proxy web utilizzando i server DNS già disponibili come prima linea di difesa
- **Riduzione fino a 60 volte superiore del traffico** inviato agli NGFW*

Migliora il ROI su investimenti esistenti

- Ottieni più valore dai prodotti adiacenti/complementari condividendoin modo bidirezionale le informazioni sulle minacce e sugli aggressori
- Se si inviano dati DNS al sistema SIEM, riduci il costo delle soluzioni SIEM inviando solo dati DNS sospetti a queste piattaforme

AUTOMAZIONE

- Riduci il costo del tocco/errore umano utilizzando l'automazione
- Supera la mancanza di risorse qualificate: il 60% di richieste in meno al tuo team per l'implementazione (configurazione in ore invece che in mesi) e le operazioni, sia in termini di competenze che di costi
- Rendi i tuoi analisti delle minacce 3 volte più produttivi con un'unica console facile da usare per una threat intelligence approfondita

**Basata su dati reali dei clienti*

infoblox.

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

Versione: 20240122v1