DATENBLATT

Infoblox Threat Defense™ Advanced

Schützendes DNS, unterstützt durch prädiktive Bedrohungsintelligenz, schützt alles und überall – bevor es zu negativen Auswirkungen kommt.

DNS IST DER FRÜHESTE PRÄVENTIONSPUNKT FÜR ALLE CYBERANGRIFFE

DNS ist der erste Erkennungs- und Präventionspunkt für alle Cyberangriffe. Ob er mit einer Phishing-E-Mail, einem Smishing-Text oder einer ausgenutzten Sicherheitslücke beginnt – fast jeder Angriff erzeugt eine DNS-Anfrage an eine bösartige Domain. Daher bietet DNS einen leistungsstarken, zentralen Punkt der Transparenz und Kontrolle, um ein ganzes Unternehmen abzusichern, einschließlich Benutzer, Geräte, IoT/OT und Workloads, egal ob vor Ort, in der Cloud oder am Edge.

Als erster Schritt jeder Kommunikation hilft die Erkennung und Blockierung von Bedrohungsaktivitäten auf der DNS-Ebene, bösartigen Datenverkehr zu stoppen, bevor er nachgelagerte Tools erreicht und Warnungen auslöst. Durch die Korrelation von DNS-Daten mit dem Geräte- und Asset-Kontext erhalten NetOps- und SecOps-Teams einen besseren Einblick in das Geschehen in ihren Umgebungen und verbessern so sowohl die Betriebseffizienz als auch die Sicherheitslage.

TRADITIONELLE „ERKENNEN UND REAGIEREN“-LÖSUNGEN SIND NICHT MEHR EFFEKTIV

Bedrohungsakteure setzen zunehmend KI ein, um produktivere, raffiniertere und heimlichere Kampagnen zu starten. Sie generieren einzigartig gestaltete Einweg-Malware, die herkömmliche „Erkennen und Reagieren“-Tools, die auf eine „Indexpatient-Infektion warten, unwirksam macht. Jeder Angriff wird zu einem „Indexpatient“-Szenario, bei dem es keine Signatur und kein bekanntes Verhalten gibt. „Erkennen und Reagieren“-Tools greifen in der Kill Chain oft zu spät ein, um Schäden zu verhindern. Daher ist ein anderer präventiver Ansatz erforderlich. Ein Ansatz, der Bedrohungen stoppt, bevor sie in die Umgebung eindringen oder sich seitlich bewegen. Dadurch werden nicht nur Angriffe früher abgewehrt, sondern auch die Belastung traditioneller „Erkennen und Reagieren“-Tools verringert.

DNS fungiert als Upstream-Kontrollpunkt und bietet Sicherheitsteams die proaktive Möglichkeit, Bedrohungen früher zu erkennen und zu blockieren, bevor sie Benutzer, Workloads oder Endpunkte erreichen.

PRÄVENTIVE SICHERHEIT MIT DNS

Infoblox Threat Defense™ Advanced bietet einen einzigartigen **präventiven Ansatz** zur Bedrohungserkennung, der nicht auf „Indexpatient“ angewiesen ist. Es nutzt eine Kombination aus **prädiktiver Bedrohungsintelligenz**, die die Infrastruktur von Bedrohungsakteuren blockiert, bevor sie als Waffe eingesetzt wird, und algorithmischen/ML-basierten Analysen von DNS-Abfragen in Kundennetzwerken, um Schutz vor Auswirkungen zu bieten. Durch die schnelle Identifizierung von an Sicherheitsvorfällen beteiligten Assets, Ökosystemintegrationen und intuitiven Arbeitsbereichen ermöglicht es eine schnellere Erkennung, schnellere Reaktion und einen höheren ROI Ihrer bestehenden Sicherheitsinvestitionen.

ZAHLEN UND FAKTEN

- Überwacht **204K** Echtzeit-Cluster von Bedrohungsakteuren, die weiter wachsen
- Reduziert die Falsch-Positiv-Rate auf **0,0002 %**
- Blockiert **82 %** der Bedrohungen vor der ersten Abfrage
- Bietet Schutz **68,4** Tage vor einem Angriff im Durchschnitt
- Blockiert **5X mehr** Domains mit hohem/mittlerem Risiko im Vergleich zu Tools, die nur nach bekanntem bösartigem Verhalten suchen
- Spart durchschnittlich **500 Stunden für SOC-Analysten** pro Monat*
- Hilft bei der Realisierung von **400.000 $** an Produktivitätseinsparungen pro Jahr*
- Reduziert Zehntausende von Warnungen auf eine Handvoll*

Die SANS 2025 SOC-Umfrage ergab, dass sieben der zehn größten Hindernisse, die eine vollständige SOC-Nutzung verhindern, Warnungen, Tool-Integration und Fachkräftemangel betreffen.

*Basierend auf echten Kundendaten.

BLOCKIEREN SIE BEDROHUNGEN, BEVOR SIE SICH NEGATIV AUSWIRKEN

Infoblox Threat Defense wendet prädiktive DNS-Bedrohungsinformationen mit algorithmischen/maschinellen Lernanalysen auf DNS-Verkehr in Echtzeit an, um Bedrohungsaktivitäten zu blockieren, bevor sie sich negativ auf Ihr Netzwerk auswirken. Dabei werden häufig Bedrohungen erkannt, die von anderen Tools nicht erkannt werden. Indem Infoblox Bedrohungen auf der DNS-Ebene stoppt, trägt es auch dazu bei, das Warnvolumen und die Arbeitsbelastung auf nachgelagerten Sicherheitstools zu reduzieren, wobei Kunden von einer Reduzierung der Alarme um bis zu 50 % auf Next-Generation Firewall (NGFW)- und Endpoint Detection and Response (EDR)-Systemen berichten.

> *„Sicheres DNS könnte die Fähigkeit von 92 % der Malware-Angriffe verringern, erfolgreich Malware in einem bestimmten Netzwerk zu verteilen.“*
>
> **Anne Neuberger,**
> **Director of the Cybersecurity Directorate,**
> **National Security Agency (NSA)**

Wichtige Fähigkeit	Beschreibung	Infoblox Threat Defense	NGFW	SASE	EDR
Unternehmensweiter sicherer Resolver und DNS-Abfrageprotokollierung	Verwendet DNS-Abfragedaten, um Domänen zu identifizieren und zu blockieren	●	◑	◑	◑
Umfassende Überwachung des DNS-Verhaltens	Überwacht alle DNS-Eintragstypen auf böswillige Aktivitäten	●	●	◔	○
Erkennung und Entfernung von Lookalike-/ Doppelgänger-Domänen	Minderung der Angriffsfläche für Lookalike/Doppelgänger-Angriffe	●	○	◑	○
Zero-Day-DNS-Schutz	Identifiziert neue oder aufkommende Domänen für Ihr Unternehmen, die eine Bedrohung darstellen könnten	●	◑	◑	○
Verhaltensbasierte DNS-Tunneling-Erkennung	Erkennt DNS-Tunnel, die für Datenexfiltration/-infiltration, C2-Kommunikation usw. genutzt werden	●	◑	◑	○
Proaktiver Schutz vor verdächtigen/ hochrisikoreichen Domänen	Identifiziert und blockiert verdächtige Domänen präventiv, die wahrscheinlich in zukünftigen bösartigen Kampagnen verwendet werden	●	◑	◑	◑
Automatische, native Kontextanreicherung	Korreliert den Netzwerkkontext ohne die Notwendigkeit von Clients oder Sinkholing (Benutzer, Gerät, Quell-IP, Standort, MAC-Adresse, Virtual Local Area Network)	●	◑	◑	◑
Proaktive Erkennung und Störung von Bedrohungsverteilungssystemen (TDS)	Identifiziert die TDS-Infrastruktur von Bedrohungsakteuren, nicht nur einzelne Domänen. So werden Bedrohungsakteuren, die sich über zahlreiche Domänen hinweg bewegen, um der Entdeckung zu entgehen, abgewehrt.	●	◔	○	○

Abbildung 1. Einzigartige Funktionen von Threat Defense, die andere Tools nicht vollständig abdecken können

WICHTIGE FUNKTIONEN VON THREAT DEFENSE

- **„Präventischutz"-Monitor.** Damit können CISOs und Sicherheitsteams ihre präventive Sicherheitsstrategie umsetzen und dem Vorstand mit klaren, quantifizierbaren Kennzahlen über die vor der Auswirkung neutralisierten Bedrohungen Bericht erstatten – ein entscheidender Zeitvorteil und eine Entlastung des Security Operations Center (SOC).
- **Asset-Erkennung und Bestandsintegration.** Schnelle Identifizierung von Assets, die an Sicherheitsvorfällen beteiligt sind, für eine schnellere Bewertung und Reaktion auf Vorfälle.
- **Sicherheits-Arbeitsbereich.** Vereinfachte und intuitive Benutzeroberfläche, die es Sicherheitsteams ermöglicht, zu verstehen, was in ihrer Umgebung vor sich geht, und Möglichkeiten zur Verringerung von Sicherheitsrisiken vorzuschlagen.
- **Erkennungsmodus.** Für eine einfache Bereitstellung und einen Proof of Concept, ohne die bestehende IT- oder Netzwerkinfrastruktur zu ändern.

STÄRKEN SIE DIE PRÄVENTIVE SICHERHEIT MIT PRÄDIKTIVER INTELLIGENZ

Infoblox ist der führende Anbieter von Original-DNS-Threat-Intelligence. Das Unternehmen verfolgt einen präventiven, nicht nur defensiven Ansatz, indem es seine Erkenntnisse nutzt, um die Infrastruktur von Bedrohungsakteuren zu verfolgen, während sie aufgebaut wird, und Cyberkriminalität an der Quelle zu unterbrechen, oft bevor ein Angriff überhaupt gestartet wird.

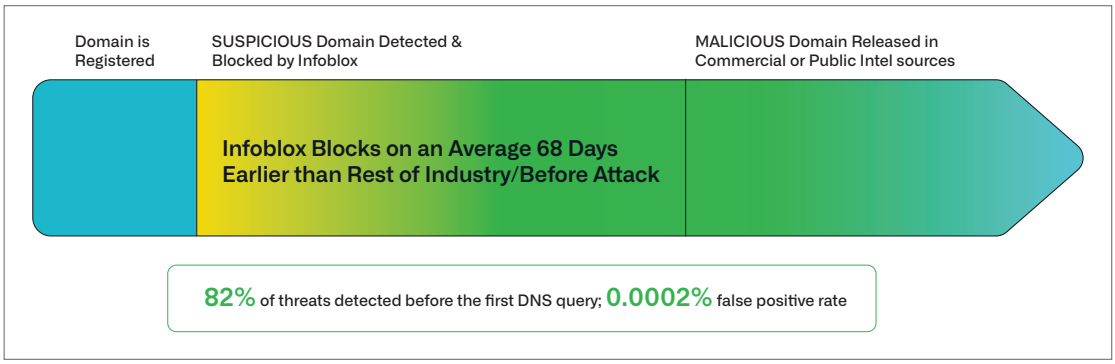

Abbildung 2. Infoblox Threat Intelligence kann vor Bedrohungen schützen, bevor der Rest der Sicherheitsbranche dies kann.

Wie Infoblox originale DNS-Bedrohungsinformationen erstellt

DNS-Experten: Infoblox entdeckt Bedrohungsakteure, die sich im DNS verstecken, indem es weiß, wo es suchen muss. Beginnend mit hochriskanten oder verdächtigen Domänen, verbindet das Team die Punkte, um die Infrastruktur der Angreifer zu identifizieren und sie zu verfolgen, während sie sich entwickelt und neue Bedrohungen auftauchen, bevor sie anderswo erkannt werden.

Bedrohungsexpertise: Infoblox versteht, wie böswillige Akteure vorgehen und wie sich Bedrohungen wie Malware, Ransomware, Phishing und DNS-basierte Exploits manifestieren. Dieses Know-how ermöglicht prädiktive Systeme, die Lookalike-Domains, DNS-Command-and-Control-Aktivitäten (C2), Registered Domain Generation Algorithms (RDGAs) und andere verdächtige Verhaltensweisen erkennen.

Data Science: Infoblox wendet maschinelles Lernen und fortschrittliche Data Science auf riesige Mengen an DNS-Abfragedaten an. Dies ermöglicht nahezu in Echtzeit Schutz vor Datenexfiltration, Domain-Generierungsalgorithmen (DGAs) und einer Vielzahl von schwer fassbaren Bedrohungen.

INTELLIGENTER ARBEITEN MIT SOC INSIGHTS

Von Alarmmüdigkeit und Analysten-Burnout bis hin zu langwierigen Untersuchungs- und Reaktionsbemühungen bietet Infoblox Threat Defense dem SOC mit dem zusätzlichen SOC Insights-Paket erhebliche Entlastung.

- Helfen Sie Analysten, das Wesentliche zu erkennen, mit KI-gestützten Analysen, die Hunderttausende von Warnmeldungen auf eine Handvoll Erkenntnisse reduzieren.
- Automatisieren Sie die Erfassung und Korrelation von Protokollen, Bedrohungsinformationen und anderen Daten, damit Analysten mit der Untersuchung und Reaktion beginnen können.
- Beschleunigen Sie die Reaktion auf Vorfälle mit Asset-Entdeckung und Bestandsintegration, damit Analysten betroffene Geräte schneller identifizieren können.

Abbildung 3. Infoblox Threat Intel hat überraschende Forschungsdaten über das zunehmende Risiko von Lookalike-Domains geteilt.

EXPORTIEREN SIE WERTVOLLE DNS-LOGS IM GROSSEN MASSSTAB

Mit Infoblox können Sie hochpräzise DNS-Abfragen und Ereignisdaten ganz einfach an Ihr SIEM, SOAR oder Ihren Data Lake senden, um zentrale Sichtbarkeit und schnellere Bedrohungskorrelation zu ermöglichen.

- Filtern und leiten Sie nur hochwertige DNS-Ereignisse weiter, um die Kosten für die SIEM-Erfassung und das Rauschen von Warnmeldungen zu reduzieren.
- Streamen Sie angereicherte DNS-Protokolle in Echtzeit mit dem Infoblox Cloud Data Connector.
- Verbessern Sie die Erkennung und Reaktion in Ihrem gesamten Ökosystem, indem Sie jedem Tool den Kontext geben, den es benötigt.
- Tauschen Sie Daten über zertifizierte, bidirektionale Integrationen nahtlos mit anderen Tools aus und verbessern Sie so die durchgängige Erkennung, Triage und Reaktion.

SCHNELLERE ERMITTLUNGEN MIT DOSSIER

Dossier bietet Analysten ein leistungsstarkes, einheitliches Recherchetool, um Bedrohungen zu validieren, anhand von Kompromissindikatoren (IOCs) zu orientieren und Untersuchungen zu beschleunigen, ohne zwischen verschiedenen Plattformen wechseln zu müssen.

- Konsolidieren Sie interne, Infoblox- und Drittanbieter-Bedrohungsinformationen in einer intuitiven Benutzeroberfläche.
- Untersuchen Sie schnell IOCs und decken Sie damit verbundene Bedrohungen mit integrierter Anreicherung und Linkanalyse auf.
- Reduzieren Sie die Untersuchungszeit um bis zu 67 %, indem Sie die manuelle Datenerfassung und den Kontextwechsel eliminieren.

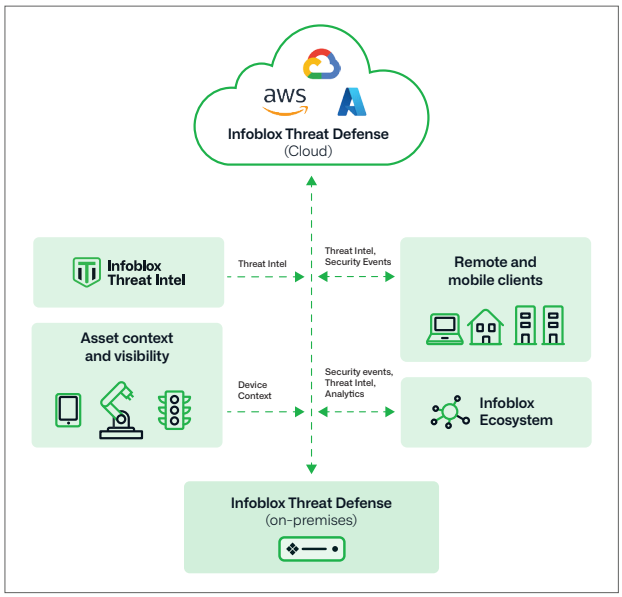

Abbildung 4. Die Hybridarchitektur von Infoblox ermöglicht Schutz überall und Einsatz überall, um der heutigen KI-gestützten Bedrohungslandschaft entgegenzuwirken.

SCHÜTZEN SIE IHRE MARKE VOR GEZIELTER TÄUSCHUNG

Infoblox bietet zwei integrierte Funktionen – Lookalike-Domain-Überwachung und Domänenabsicherungsdienste – die dazu beitragen, Ihre Marke, Kunden und Mitarbeiter vor auf Täuschung basierenden Cyberangriffen zu schützen. Zusammen bieten sie Ihnen einen Überblick über neu auftretende Bedrohungen und die Möglichkeit, schnell und effektiv gegen bösartige Domains vorzugehen, bevor sie Ihr Unternehmen beeinträchtigen.

Überwachung von Lookalike-Domains

Bleiben Sie den Angriffen auf Ihre Marke oder vertrauenswürdige Dritte immer einen Schritt voraus.

- Erkennen Sie Domains, die registriert wurden, um sich als Ihr Unternehmen, Ihre Lieferkette oder kundenorientierte Eigenschaften auszugeben.
- Identifizieren Sie Domains, die in Phishing- und Betrugskampagnen verwendet werden, die auf Ihre Mitarbeiter oder Kunden abzielen.
- Überwachen Sie hochpriorisierte Domänen auf Änderungen der Risikolage und erhalten Sie Echtzeitwarnungen.

Dienste zur Domänenabsicherung

Validieren Sie schnell bösartige Domains, die in freier Wildbahn aktiv sind, und entfernen Sie sie.

- Bestätigen und dokumentieren Sie bösartige Aktivitäten durch menschlich geführte Vorfallvalidierung und zusammenfassende Berichterstattung.
- Stimmen Sie sich mit globalen ISPs, Hosting-Providern und Aufsichtsbehörden ab, um eine schnelle Deaktivierung zu gewährleisten – oft innerhalb von 24 Stunden.
- Überwachen Sie entschärfte Bedrohungen 30 Tage lang nach der Entfernung, um Reaktivierungsversuche zu erkennen und zu entfernen, ohne zusätzliche Kosten.
- Bekämpfen Sie eine Reihe von Bedrohungstypen, darunter Phishing, Malware-Hosting, C2-Infrastruktur und gestohlene Daten.

Um mehr über die Methoden zu erfahren, mit denen Infoblox Threat Defense Ihre Daten und Infrastruktur schützt, besuchen Sie bitte https://www.infoblox.com/de/products/threat-defense/.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1 408 986 4000
www.infoblox.com/de

Version: 20250121v1