DATASHEET

BloxOne® Threat Defense Advanced

Stärken und optimieren Sie Ihre Sicherheitslage von Grund auf

DER BEDARF AN GRUNDLEGENDER SICHERHEIT IN GROSSEM MASSSTAB

Das traditionelle Sicherheitsmodell ist in der heutigen Welt des digitalen Wandels unzureichend.

- Die Grenzen haben sich verschoben, und Ihre Benutzer greifen von überall aus direkt auf Cloud-basierte Anwendungen zu.
- Das Internet der Dinge (IoT) führt zu einer explosionsartigen Zunahme von Geräten, die keine herkömmlichen Endpoint-Technologien zum Schutz akzeptieren.
- Die meisten Sicherheitssysteme sind komplex und lassen sich nicht ohne weiteres auf das Niveau skalieren, das zum Schutz dieser dynamischen Umgebungen erforderlich ist.

Was Unternehmen brauchen, ist eine skalierbare, einfache und automatisierte Sicherheitslösung, die das gesamte Netzwerk schützt, ohne dass eine zusätzliche Infrastruktur bereitgestellt oder verwaltet werden muss.

INFOBLOX BIETET EINE SKALIERBARE PLATTFORM, DIE IHRE BESTEHENDEN INVESTITIONEN IN DIE BEDROHUNGSABWEHR MAXIMIERT

Infoblox BloxOne Threat Defense Advanced, eine umfassende Lösung für DNS Detection and Response (DNSDR), erkennt Bedrohungsaktivitäten, die von anderen Lösungen übersehen werden. Es stoppt Angriffe, bevor sie stattfinden, indem es DNS-Bedrohungsdaten im Vorfeld von Kampagnen aufspürt und so die Lieferketten von Angreifern unterbricht. Intelligente Ökosystem-Integrationen und Automatisierung reduzieren den manuellen Aufwand, während die einzigartigen KI-gestützten Analysen von Infoblox Analysten erlauben, sich auf das Wesentliche zu konzentrieren. Zudem liefern sie Erkenntnisse, die die MTTR reduzieren, den ROI vorhandener Sicherheitstools erhöhen und die SecOps-Effizienz als Ganzes steigern.

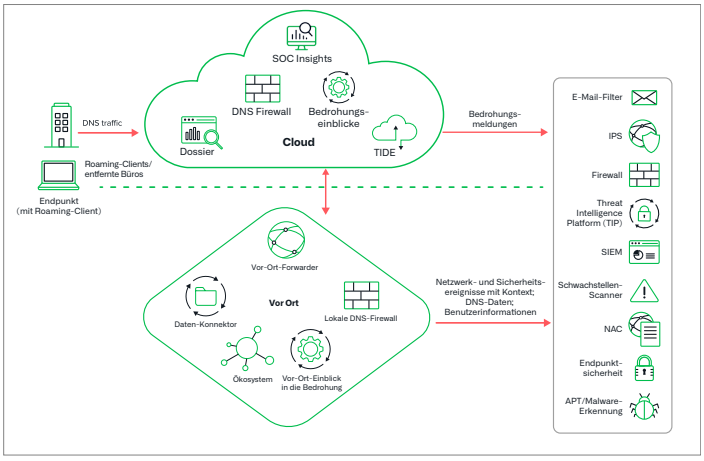


Abbildung 1: Die Hybridarchitektur von Infoblox ermöglicht Schutz überall und Einsatz überall

WICHTIGE FÄHIGKEITEN

- Erkennen und blockieren Sie Exploits, Phishing, Ransomware und andere moderne Malware, die andere Lösungen übersehen
- Schützen Sie Benutzer und Geräte unabhängig von Plattform oder Betriebssystem auf der DNS-Ebene, einschließlich BYOD, IoT und ICS.
- Entdecken Sie risikoreiche Anwendungen und verwalten Sie Ihre Schatten-IT, Insider, Compliance und andere Risiken
- Vermeiden Sie Datenexfiltrations-techniken dank Analysen mit maschinellem Lernen und KI, einschließlich DNS-basierter Datenexfiltration, DGA und DNSMessenger.
- Beschränken Sie den Nutzer-zugang zu unangemessenen oder unerwünschten Webinhalten und verfolgen Sie die Aktivitäten
- Schützen Sie Ihre Marke mit Lookalike Domain Monitoring für Ihre wertvollsten Internetobjekte
- Beschleunigen Sie Untersuchungen um das Dreifache und optimieren Sie die Reaktion auf Bedrohungen und die Bedrohungssuche.
- Verbessern Sie die Transparenz: Präzise Sichtbarkeit und umfassender Netzwerkkontext durch Integration mit IPAM-Metadaten für optimales Verständnis und Korrelation von Ereignissen
- Mit SOC Insights können Sie die Untersuchung und Reaktion auf die wichtigsten Bedrohungen beschleunigen und die MTTR mit KI-gestützten Einblicken reduzieren.

MAXIMIEREN SIE DIE EFFIZIENZ DES SECURITY OPERATION CENTER

Reaktionszeit auf Vorfälle verkürzen

- Automatische Blockierung bösartiger Aktivitäten und Bereitstellung der Bedrohungsdaten für den Rest Ihres Sicherheits-Ökosystems zur Untersuchung, Quarantäne und Behebung
- Optimieren Sie Ihre SOAR-Lösung mithilfe von kontextbezogenen Netzwerk- und Bedrohungsdaten und Infoblox-Ökosystem-Integrationen (eine wichtige Voraussetzung für SOAR) - reduzieren Sie die Reaktionszeit auf Bedrohungen und die Betriebskosten.
- Nutzen Sie die Fähigkeiten von Infoblox SOC Insights, um herauszufinden, welche Ereignisse am wichtigsten sind – mit KI-gestützten Analysen, die über einfache Dashboards mit Malware-Risikoeinstufung hinausgehen.

Vereinheitlichung der Sicherheitsrichtlinien mit der Portabilität von Bedrohungsinformationen

- Sammeln und Verwalten von Bedrohungsdaten aus internen und externen Quellen und Verteilen dieser Daten an bestehende Sicherheitssysteme
- Senkung der Kosten für Bedrohungsmeldungen bei gleichzeitiger Verbesserung der Effektivität von Bedrohungsinformationen im gesamten Sicherheitsstack

Schnellere Bedrohungsuntersuchung und Bekämpfung

- Beschleunigen der Untersuchung und Reaktion auf die wichtigsten Bedrohungen und Reduzieren der MTTR mit KI-gesteuerten Erkenntnissen, die über einfache Dashboards mit Malware-Risikoeinstufung hinausgehen
- Macht Ihr Team von Bedrohungsanalysten **3-mal produktiver,** indem es Sicherheitsanalysten mit automatisierten Bedrohungsuntersuchungen, Einblicken in verwandte Bedrohungen und zusätzlichen Forschungs-perspektiven von Cyber-Experten ausstattet, um schnelle und präzise Entscheidungen über Bedrohungen zu treffen

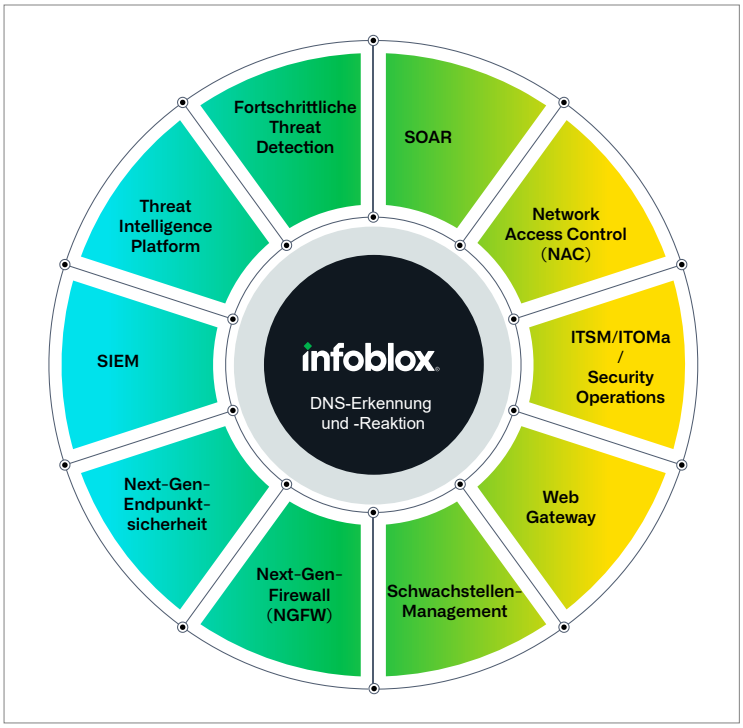
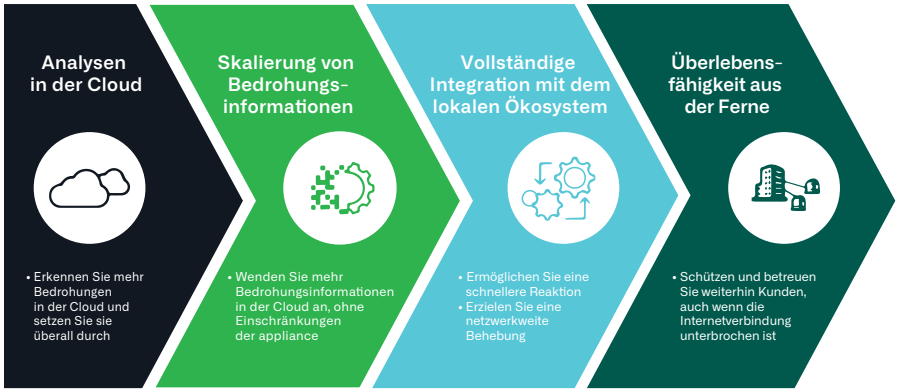


Abbildung 2: BloxOne Threat Defense lässt sich in das gesamte Cybersicherheits-Ökosystem integrieren

> *„Heutzutage gibt es viel zu viel Ransomware, Spyware und Adware, die eingeschleust wird, wenn Internetnutzer auf Links klicken. Die Cloud-Sicherheitslösung von Infoblox verhindert, dass Benutzer auf bösartige Websites weitergeleitet werden, schützt Rechner davor, infiziert zu werden, und erhöht die Sicherheit der Benutzer.“*
>
> **Senior System Administrator und Network Engineer, City University of Seattle**

SCHUTZ, WO IMMER SIE GERADE SIND – DURCH DEN HYBRID-ANSATZ



Analysen in der Cloud

- Nutzen Sie die umfassenderen Verarbeitungsmöglichkeiten der Cloud, um ein breiteres Spektrum an Bedrohungen zu erkennen, einschließlich Datenexfiltration, Domain Generation Algorithm (DGA), Fast Flux, dateilose Malware, Dictionary DGA und mehr, indem Sie auf maschinellem Lernen basierende Analysen einsetzen.
- Erkennen Sie Bedrohungen in der Cloud und setzen Sie sie überall durch, um den Hauptsitz, das Rechenzentrum, entfernte Büros oder Roaming-Geräte zu schützen.

Skalierung von Bedrohungsinformationen

- Nutzen Sie einen umfassenden Informationsschatz aus der Infoblox-Forschung und von Drittanbietern, um Richtlinien vor Ort oder in der Cloud durchzusetzen, und verteilen Sie diese automatisch an die übrige Sicherheitsinfrastruktur.
- Wenden Sie mehr Bedrohungsinformationen in der Cloud an, ohne große Investitionen in mehr Sicherheits-Appliances für jeden Standort tätigen zu müssen

Leistungsstarke Integrationen in Ihr Sicherheits-Ökosystem

- Sie erhalten die Möglichkeit einer vollständigen Integration mit lokalen Sicherheitstechnologien von Infoblox und Drittanbietern, was netzwerkweite Remediation ermöglicht und den ROI dieser Technologien verbessert.

Überlebensfähigkeit/Resilienz aus der Ferne

- Sollte es jemals zu einer Unterbrechung Ihrer Internetverbindung kommen, kann das Infoblox-System vor Ort das Netzwerk weiterhin sichern.

Mehr über die Art und Weise, wie BloxOne Threat Defense Ihre Daten und Infrastruktur schützt, erfahren Sie unter: https://www.infoblox.com/products/bloxone-threat-defense

DER ROI VON INFOBLOX SECURITY

Entlastung der strapazierten Sicherheitsgeräte

- Reduzieren Sie die Belastung überlasteter Perimeter-Sicherheitsgeräte wie Firewalls, IPS und Web-Proxies, indem Sie Ihre bereits verfügbaren DNS-Server als erste Verteidigungslinie nutzen
- **Bis zu 60-fache Reduzierung des an** NGFWs gesendeten Datenverkehrs*

Verbesserung des ROI bestehender Investitionen

- Profitieren Sie von benachbarten/ergänzenden Produkten durch den bidirektionalen Austausch von Bedrohungs- und Angreiferinformationen
- Wenn Sie DNS-Daten an SIEM senden, reduzieren Sie die Kosten für SIEM-Lösungen, indem Sie nur verdächtige DNS-Daten an diese Plattformen senden

Automatisierung

- Reduzieren Sie die Kosten für menschliche Eingriffe/Fehler mithilfe von Automatisierung
- Überwinden Sie den Mangel an qualifizierten Ressourcen - 60 % weniger Anforderungen an Ihr Team bei der Implementierung (Konfiguration in Stunden statt in Monaten) und beim Betrieb, sowohl was die Fähigkeiten als auch die Kosten betrifft
- Erhöhen Sie die Produktivität Ihrer Bedrohungsanalysten um das Dreifache mit einer einfach zu bedienenden, zentralen Konsole für tiefgreifende Bedrohungsdaten

**Basierend auf echten Kundendaten*

infoblox.

Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Hauptsitz der Gesellschaft
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240122v1