DATENBLATT

BloxOne™ Threat Defense Advanced

So verstärken und optimieren Sie Ihr Sicherheitskonzept von Grund auf

DIE WICHTIGSTEN FUNKTIONEN

- Schutz bestehender Netzwerke und transformativer Technologien wie SD-WAN, IoT und Cloud unter Verwendung vorhandener Infrastruktur
- **Verhinderung von Datendiebstahl:** Erkennen und Blockieren von DNS-basiertem Datendiebstahl, Domain Generation Algorithms (DGA), DNSMessenger und Fast-Flux-Angriffen mittels analysebasierte Machine-Learning-Funktionen
- **Erkennen und Blockieren von Malware-Aktivitäten:** Blockieren bösartiger Kommunikationen zu C&Cs, Verhinderung der Malware-Ausbreitung
- **Kategorisierung von Webinhalten und Durchsetzung von Richtlinien für den Web-zugriff:** Einschränkung des Benutzerzugriffs auf bestimmte Website-Kategorien
- **Automatisierte Reaktion bei Vorfällen: um zwei Drittel schnellere Fehlerbehebung** und schnellere Reaktion auf Bedrohungen, da diese zuerst blockiert und anschließend mittels REST API oder lokaler Integrationen mit dem Rest des Ökosystems geteilt werden
- **Zugriff auf Daten mittels S3-Bucket:** Export der Aktivitätsprotokolle in Amazon S3-Buckets und einfache Nutzung von Daten in gängigen Formaten (CSV, JSON und CEF)
- **Schnellere Untersuchung von Bedrohungen und schnelleres Threat-Hunting:** automatische Recherche von Bedrohungsdaten aus Dutzenden von Quellen, für eine schnellere Auswertung und somit **3-mal effizientere** Bedrohungsanalyse

Warum heute solide, skalierbare Sicherheitslösungen gefragt sind

Im Zeitalter der digitalen Transformation hat das traditionelle Sicherheitsmodell endgültig ausgedient.

- Die Netzwerkgrenzen haben sich verschoben. Ihre User greifen heute direkt auf cloudbasierte Anwendungen zu – von jedem beliebigen Ort aus.
- SD-WAN treibt die Netzwerktransformation voran und Niederlassungen stellen eine direkte Verbindung zum Internet her, ohne dass sie den kompletten Sicherheitsstack der Zentrale passieren können.
- Das Internet der Dinge (IoT) hat zu einer explosionsartigen Zunahme von Geräten geführt, die mit herkömmlichen Endpoint-Protection nicht geschützt werden können.
- Die meisten Sicherheitssysteme sind komplex und lassen sich nicht ohne Weiteres skalieren, um diese dynamischen Umgebungen zu schützen.

Hinzu kommt, dass Sicherheitsteams chronisch unterbesetzt sind (einem aktuellen ISC2-Bericht zufolge **fehlen weltweit 2,93 Millionen Fachkräfte in der IT-Sicherheit**). Sie nutzen isolierte Tools und manuelle Prozesse zur Erfassung von Informationen nutzen und Tag für Tag auf Hunderte bis Tausende Warnmeldungen reagieren müssen.

Unternehmen brauchen eine einfache, skalierbare und automatisierte Sicherheitslösung, die das gesamte Netzwerk schützt, ohne zusätzliche Infrastruktur zu implementieren oder zu verwalten.

Infoblox bietet eine skalierbare Plattform, die Ihre bisherigen Investitionen in den Bedrohungsschutz maximiert

Infoblox BloxOne Threat Defense Advanced verstärkt und optimiert Ihr Sicherheitskonzept von Grund auf. Das Produkt schützt Ihre bestehenden Netzwerke, SD-WAN Umgebungen, IoT und die Cloud und sorgt so für einen maximalen Unternehmensschutz. Mit einer hybriden Architektur, sorgt es für einen flächendeckenden Schutz und unterstützt zusätzlich SOAR-Lösungen (Security Orchestration, Automation and Response). Somit wird die Zeit für die Analyse und Eliminierung von Cyberbedrohungen um ein Vielfaches verkürzt, sowie die Performance des gesamten Sicherheitsökosystems optimiert und die Gesamtkosten für den Bedrohungsschutz im Unternehmen reduziert.

DIE WICHTIGSTEN FUNKTIONEN

- **Verbesserte Transparenz:** hohe Transparenz und aussagekräftige Kontextinformationen zum Netzwerk einschließlich IPAM- und Asset-Metadaten zu Ihren Netzwerksystemen, um Ereignisse besser einordnen zu können
- **Executive Reporting:** Einfach zu konsumierender, visuell aufschlussreicher Überblick über den Sicherheitsstatus mit Informationen auf Unternehmensebene für Führungskräfte

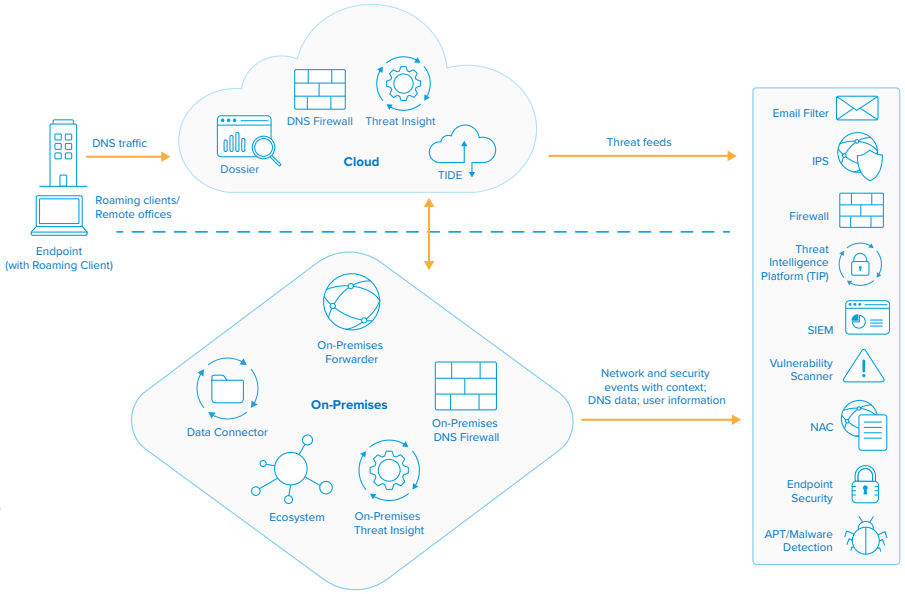


Abbildung 1: Die hybride Architektur von Infoblox schützt jede Umgebung und lässt sich überall implementieren.

Maximierung der Effizienz im Security-Operations-Center

Kürzere Reaktionszeit bei Vorfällen

- Blockieren Sie automatisch bösartige Aktivitäten und stellen Sie Ihrem restlichen Sicherheitsökosystem die Bedrohungsdaten für Analyse- oder Quarantänezwecke zur Verfügung.
- Optimieren Sie Ihre SOAR-Lösung mit Hilfe der Infoblox-Ökosystem-Integration, mit Bedrohungsdaten und Kontextinformationen zum Netzwerk. Auf diese Weise reduzieren Sie die Reaktionszeit bei Bedrohungen sowie die Betriebskosten.
- Verringern Sie die Anzahl der zu überprüfenden Warnmeldungen, sowie irrelevante Informationen von Ihren Firewalls.

Einheitliche Sicherheitsrichtlinien mit flächendeckender Bereitstellung von Bedrohungsinformationen

- Erfassen und verwalten Sie kumulierte Bedrohungsdaten aus internen und externen Quellen und leiten Sie diese an bestehende Sicherheitssysteme weiter.

Schnellere Untersuchung von Bedrohungen und schnelleres Threat-Hunting

- Stellen Sie Ihren Sicherheitsanalysten Funktionen zur automatisierten Bedrohungsuntersuchung, Erkenntnisse zu ähnlichen Bedrohungen und zusätzliche Daten von Cyberexperten bereit, um schnelle, genaue Entscheidungen zu Bedrohungen zu treffen. Auf diese Weise können Ihre Bedrohungsanalysten ihre **Produktivität um bis auf das Dreifache steigern**.
- Reduzieren Sie den Analyseaufwand Ihrer Mitarbeiter.

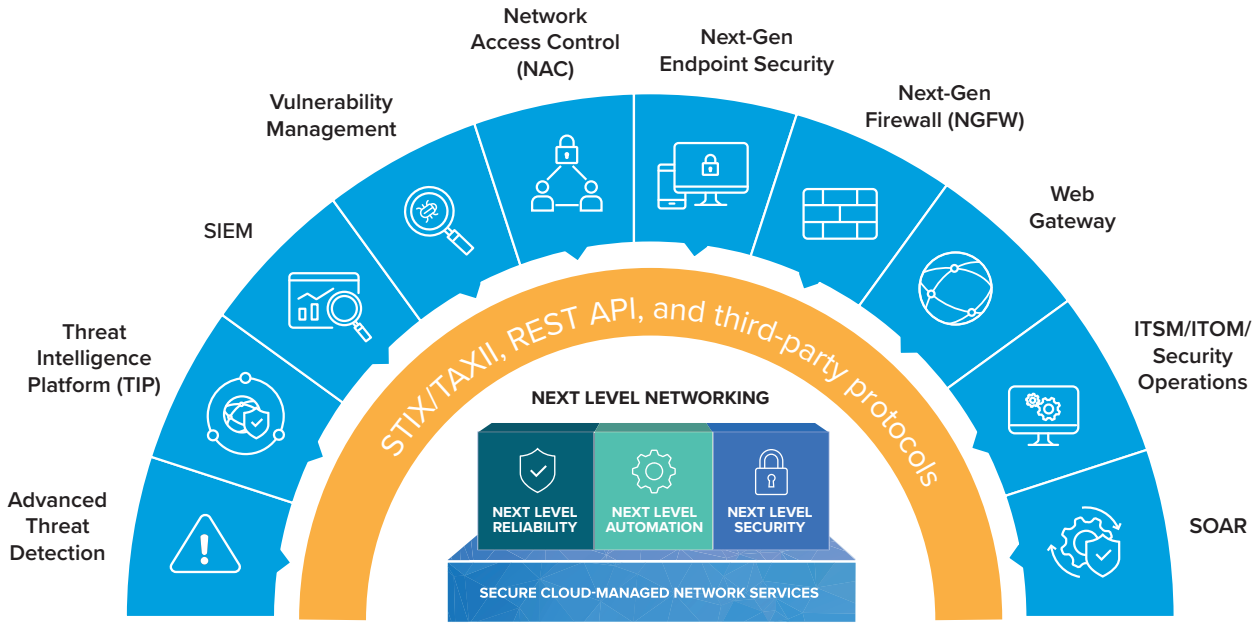


Abbildung 2: Infoblox stellt grundlegende Sicherheitsdaten automatisch und in Echtzeit für alle Komponenten des Sicherheitsökosystems bereit.

„Heutzutage gelangt viel zu viel Ransomware, Spyware und Adware ins Netzwerk – hereingelassen von nichts ahnenden Internetnutzern, die irgendwelche Links öffnen. Die Infoblox-Cloud-Sicherheitslösung verhindert, dass User auf bösartige Seiten zugreifen und Geräte infiziert werden. Auf diese Weise sorgt die Plattform für einen effizienten Schutz der Benutzer.“

Senior System Administrator und Network Engineer,
City University of Seattle

ROI DER INFOBLOX-SICHERHEITSLÖSUNG

Entlastung besonders beanspruchter Sicherheitssysteme

- Entlasten Sie stark beanspruchte Sicherheitssysteme, wie Firewalls, IPS und Web-Proxys, indem Sie Ihre bestehenden DNS-Server als erste Verteidigungslinie nutzen.
- **Bis zu 60-mal weniger Verkehr** an NGFWs

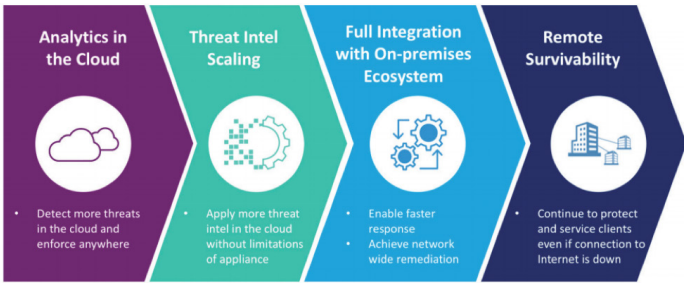
Verbesserung des ROI bei bestehenden Investitionen

- Steigern Sie den Nutzen komplementärer Produkte, indem Sie Bedrohungsdaten in beide Richtungen bereitstellen.
- Wenn Sie DNS-Daten an SIEM weiterleiten: Reduzieren Sie die Kosten der SIEM-Lösungen, indem Sie diesen Plattformen nur verdächtige DNS-Daten zur Verfügung stellen.

Automatisierung

- Reduzieren Sie mithilfe der Automatisierung Kosten für menschliches Versagen und manuelle Prozesse.
- Lösen Sie das Problem mit dem Fachkräftemangel – **60 Prozent weniger Aufwand für Ihr Team** bei der Implementierung und beim Betrieb.
- Erhöhen Sie die Produktivität Ihrer Bedrohungsanalysten um bis auf das Dreifache – mit einer einzigen benutzerfreundlichen Deep-Threat-Intelligence-Konsole für Bedrohungsinformationen.

Hybrider Ansatz bietet umfassenden Schutz unabhängig von der Art der Implementierung



Analysen in der Cloud

- Nutzen Sie Machine-Learning-basierte Analysen und die größere Rechenpower in der Cloud, um ein breites Spektrum an Bedrohungen wie Datendiebstahl, Domain Generation Algorithm (DGA), Dictionary-DGA, Fast-Flux-Angriffe und dateilose Malware zu erkennen.
- Identifizieren Sie Bedrohungen in der Cloud und setzen Sie Richtlinien überall durch, um die Zentrale sowie Datencenter, Niederlassung oder Roaming-Geräte zu schützen.

Systemweite Nutzung von Bedrohungsinformationen

- Nutzen Sie die umfassenden Bedrohungsdaten des Infoblox-Research-Teams und anderer Partnerunternhemen, um Richtlinien lokal oder in der Cloud umzusetzen und leiten Sie diese Informationen automatisch an Ihre gesamte Sicherheitsinfrastruktur weiter.
- Nutzen Sie zusätzliche Bedrohungsinformationen in der Cloud, sodass nicht jeder Standort Geld für weitere Sicherheitssysteme investieren muss.

Leistungsstarke Integration mit Ihrem Sicherheitsökosystem

- Die Umfassende Integration mit lokalen Infoblox- und Drittanbieter-Sicherheitstechnologien ermöglicht eine netzwerkweite Fehlerbehebung und verbessert den ROI dieser Lösungen.

Remote-Survivability/-Resilienz

- Selbst bei einer Störung Ihrer Internetverbindung ist die lokale Infoblox-Lösung weiterhin in der Lage, das Netzwerk zu schützen.

Wenn Sie mehr darüber erfahren möchten, wie Sie mit BloxOne Threat Defense Advanced Ihre Daten und Infrastrukturen schützen können, besuchen Sie uns unter https://www.infoblox.com/products/bloxone-threat-defense

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com