FALLSTUDIE

Führende SIEM-Datenplattform erweitert globale Zuverlässigkeit, Transparenz und Sicherheit in hybriden Netzwerken mit Infoblox

ÜBERSICHT

Dieses in den USA ansässige Unternehmen produziert Software zum Suchen, Überwachen und Analysieren maschinengenerierter Daten über eine webbasierte Schnittstelle.

Seine Lösungen — darunter eines der führenden Sicherheitsinformations- und Event-Management-Tools (SIEM) auf dem Markt — helfen dabei, Echtzeitdaten in einem durchsuchbaren Repository zu erfassen, zu indexieren und zu korrelieren, aus dem Warnmeldungen, Dashboards, Berichte und Visualisierungen generiert werden können. Das Unternehmen verwendet maschinengenerierte Daten zur Identifizierung von Datenmustern, um Kennzahlen bereitzustellen, Probleme zu diagnostizieren und Informationen für Geschäftsabläufe bereitzustellen. Das Unternehmen, das seit 2015 Kunde von Infoblox und OEM-Partner ist, musste vor Kurzem seine DNS-, DHCP- und IPAM-Plattform (DDI) aktualisieren und erweitern, um den globalen Betrieb zu unterstützen und seine Sicherheit zu verbessern. Es entschied sich für die DDI-integrierte Infoblox-Lösung „BloxOne® Threat Defense Advanced“, um seine Infrastruktur, Daten und Benutzer vor Malware, Ransomware und DNS-Datenexfiltration zu schützen.

SITUATION

Globale Zuverlässigkeit und Expansion

2015 ersetzte das Unternehmen seine Microsoft DNS- und DHCP-Plattform durch Infoblox DDI, um die Netzwerkverfügbarkeit und Zuverlässigkeit zu verbessern. Dabei wurde das Unternehmen zum OEM-Technologieanbieter für das Datensuch- und Visualisierungstool von Infoblox, Infoblox Reporting and Analytics. Im Jahr 2021 war es jedoch Zeit für eine technische Aktualisierung des Netzwerks. Das IT-Team des Unternehmens zog kurzzeitig EfficientIP in Betracht, doch aufgrund des guten Rufs und der Erfolgsbilanz von Infoblox in Sachen Zuverlässigkeit erneuerte das Unternehmen die Partnerschaft mit Infoblox und begann mit dem Aufbau seiner 21 Regionen rund um den Globus. Die Expansion in die Cloud war Teil einer Modernisierungsinitiative und einer Road Map, aber die oberste Priorität des Unternehmens war die Verbesserung der Kernnetzdienste. Das IT-Team wünschte sich autorisiertes IPAM, eine einzige Kontrollebene, eine einheitliche Verwaltung, die Reduzierung von überflüssigen Netzwerk-Tools und Overhead, vereinfachte Arbeitsabläufe und schnelle Skalierbarkeit. Dementsprechend baute das Unternehmen seine Dienste gemeinsam mit Infoblox weiter aus, ausgehend von der Prämisse, dass „Vertrauen schwer zu gewinnen und leicht zu verlieren ist“.

> *„Wie man so schön sagt: Vertrauen ist schwer zu gewinnen, aber leicht zu verlieren.“ Glücklicherweise bietet Infoblox eine sichere, zuverlässige erstklassige DDI-Lösung, der wir vertrauen können. Es ist die Plattform unserer Wahl für globale Netzwerkkonsistenz, eine zentrale Sicht auf die Steuerebene und das Maß an Skalierbarkeit, das wir für unsere expandierenden globalen Regionen benötigen. Und BloxOne Threat Defense mit seinen Ökosystemintegrationen, Dossier und Threat Insight ist einfach zu implementieren und zu verwenden. Es schützt uns, unsere Daten, unsere Infrastruktur und unsere Benutzer vor Malware, Ransomware, Bedrohungen durch Datenexfiltration und den böswilligen Akteuren, denen wir täglich ausgesetzt sind.“*
>
> **IT Team Leader**

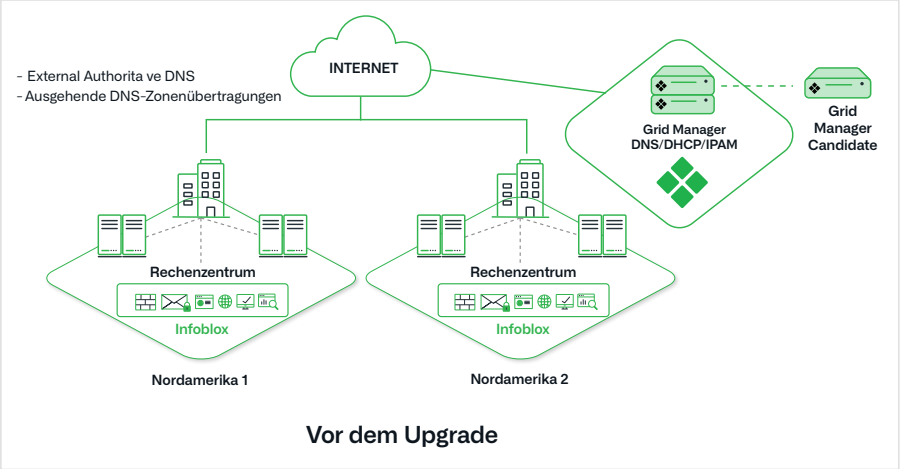

Abbildung 1: Netzwerkarchitektur vor der Modernisierung mit Infoblox

HERAUSFORDERUNG

Ausbau der Dienste zur Erhöhung der Zuverlässigkeit, Transparenz und Sicherheit auf der ganzen Welt

Dank Infoblox hatte das Unternehmen mit keinen größeren Netzwerkkonflikten, Ausfällen oder Sicherheitsvorfällen zu kämpfen und konnte sich auf die Aktualisierung der NIOS DDI-Technologie konzentrieren, um die Netzwerktransparenz, -sicherheit und -verfügbarkeit auf andere Standorte rund um den Globus auszuweiten. Es spezifizierte zentrale Verwaltung, IP-Adressmanagement (IPAM) auf Unternehmensebene und DHCP-Failover für eine „Always-On"-Serviceverfügbarkeit. Das Unternehmen benötigte außerdem ein internes autoritatives DNS und einen sicheren rekursiven DNS-Dienst für ausgehende Abfragen. Während die Automatisierung keine Priorität hatte, konzentrierte sich das IT-Team stattdessen auf die Beseitigung von überflüssigen Tools, Wartungsarbeiten und Gemeinkosten. Sie legten jedoch auch Wert auf On-Demand-Transparenz für historische Audits und Compliance, Nutzungs- und Leistungsmetriken, DNS-Sicherheitswarnungen und Kapazitätsplanung.

Angesichts der zunehmenden Sicherheitsbedrohungen räumte das Unternehmen der Verschärfung seiner Sicherheitslage Priorität ein. Es entschied, dass DDI-integrierte Sicherheit die richtige Lösung ist, um seine Infrastruktur, Daten, Partner und Benutzer vor Command and Control, Ransomware, Malware, Domain Generation Algorithm (DGA), Fast Flux, DNS-Messenger und Datenexfiltration über DNS zu schützen. Sowohl die Netzwerk- als auch die Sicherheitsanforderungen erforderten einen Übergang von der bestehenden Bereitstellung (siehe Abbildung 1) zu einer modernisierten DDI-Architektur der Enterprise-Klasse (siehe Abbildung 2).

LÖSUNG

Netzwerkmodernisierung, Sichtbarkeit, Sicherheit und Skalierbarkeit

Mit einem sehr kleinen IT-Personal benötigte das Unternehmen Einfachheit und Zuverlässigkeit nach dem Motto „Einrichten und vergessen". Die DDI-Plattform für Unternehmen von Infoblox umfasste eine Kombination aus Hardware und virtuellen, sicherheitsoptimierten Appliances zur besseren Übersicht und Verwaltung seines Netzwerks. Sie setzten Grid Manager und Grid Manager Candidate ein, einschließlich vollständig verwaltetem IPAM und internem autorisierendem DNS auf einem HA-Mitglied für optimale Transparenz. Das

KUNDENPROFIL:

- Als globales Unternehmen mit über 7.500 Mitarbeitern, 850 Patenten und Verfügbarkeit in 21 Regionen weltweit bietet dieses Softwareunternehmen eine offene, erweiterbare Datenplattform, die gemeinsame Nutzung von Daten in jeder Umgebung unterstützt. Das bedeutet, dass alle Teams im Unternehmen eine kontextbezogene Netzwerkeinsicht für jede Interaktion und jeden Geschäftsprozess erhalten.

SITUATION:

- Das Unternehmen wollte die Zuverlässigkeit seiner Infrastruktur verbessern, indem es die Redundanz erhöhte und DNS Security in sein SIEM-Angebot integrierte, um die Betriebszeit und die Verfügbarkeit von Anwendungen zu gewährleisten.

HERAUSFORDERUNG:

- IT decision makers realized they needed to expand core network services for single control plane visibility, reliability, management and scalability to serve their end users around the world.

INITIATIVEN:

- Upgrade auf eine moderne, skalierbare DDI-Lösung mit umfassender Netzwerktransparenz, die über eine einzige Kontrollebene verwaltet wird
- Gewährleisten einer kontinuierlichen Betriebszeit, hohen Verfügbarkeit und Redundanz, selbst bei einer Netzwerkmigration.
- Aktivieren von Enterprise-IPAM, internem und externem DNS, DHCP-Failover und Reporting
- Zugriff auf Netzwerkdaten für Audits/Compliance, Leistungs- und Bedrohungsereignisse und vorausschauende Analysen.
- Implementieren integrierter Sicherheits- und Ökosystem-lösungen von DDI, um Partner, verbundene Unternehmen und Endbenutzer vor Malware- und Cybersicherheitsangriffen zu schützen

Netzwerkdesign spezifizierte dedizierte Einheiten für eingehende DNS-Abfragen über das Internet. Ausgehende DNS-Anfragen (DNS DMZ-Cache) wurden zur Auflösung der geolokalen IP-Adresse an die Cloud weitergeleitet. Darüber hinaus ermöglichte das DHCP-Failover-Protokoll eine Standortredundanz, während die HA-Mitglieder für eine maximale Serviceverfügbarkeit sorgten, insbesondere für VoIP-Implementierungen in seinem globalen Netzwerk.

Die Cloud Network Automation von Infoblox wurde für Sichtbarkeit, Verwaltung und Kontrolle in den öffentlichen Cloud-Diensten von AWS hinzugefügt. Außerdem wurde DNS Traffic Control (DTC) für die Verwaltung des Netzwerkverkehrs, die Betriebszeit von Anwendungen, die einfache Bereitstellung neuer Dienste und die API-Integration hinzugefügt.

Es überrascht nicht, dass das Unternehmen auch Infoblox Reporting and Analytics intensiv genutzt hat. Diese Lösung war hilfreich für Warnmeldungen, Dashboards und Berichte für eine bedarfsgerechte Netzwerktransparenz, Network Insight und verbesserte Reaktionszeiten. Die umfangreichen DDI-Metadaten des Unternehmens waren nicht mehr im Netzwerk vergraben, sondern sichtbar, zugänglich und nützlich für die Suche, prädiktive Analysen und grafische Visualisierungen für Endpunkte, Leistung, Sicherheitsforensik, Zugriffsprotokollierung sowie Audit und Compliance, um eine konsistente Transparenz und Betriebszeit zu unterstützen.

Obwohl das Unternehmen über die Sicherheitslösung Cisco Umbrella verfügte, zog es die Idee vor, DNS sowohl als erste Verteidigungsebene als auch zur Bereicherung seiner anderen Toolsets zu verwenden. Die Sicherheitslösung von Infoblox war einfach: Mit DNS beginnen, Threat Intelligence hinzufügen und sie korrelieren, bösartige Akteure blockieren und so andere wichtige Tools zu entlasten. Dementsprechend entschied sich das IT-Team des Unternehmens für die Infoblox-Lösung „BloxOne Threat Defense Advanced“ (Abbildung 2) sowohl vor Ort als auch in der Cloud für aktualisierten Schutz vor Bedrohungen wie Ransomware, DGA, DNS Messenger und Datenexfiltration über DNS. BloxOne Threat Defense fungiert als ein allgemeiner Problemlöser in der Cloud für die geolokale Auflösung zum Schutz der Benutzer und zur Entfernung von Malware. Die Lösung bot außerdem bewährte Sicherheitsfunktionen, die eine fehlende Sicherheitslücke füllten, um DNS zu sichern, Alarmbenachrichtigungen zu verbessern und Geschäftspartner und Benutzer zu schützen. Der IT gefiel die schnelle und einfache Verwaltung, die kontextbezogenen IPAM-Daten in Kombination mit der Bedrohungsabwehr und der DDI-Integration von Infoblox. Das Unternehmen fügte außerdem Dossier und DNS Threat Insight mit seinen ausgefeilten Algorithmen und maschinellem Lernen hinzu, um das Netzwerk ständig auf DNS-Datenexfiltration zu scannen und jede nicht autorisierte DNS-Datenübertragung zu stoppen.

ERGEBNISSE:

- Schaffen von Sicherheit im gesamten Netzwerk mithilfe von sicherem DDI der Enterprise-Klasse
- Gewährleisten von Datenbank-redundanz, Netzwerkstabilität und zuverlässiger Verfügbarkeit
- Integration mit bestehenden Sicherheitsfunktionen bei gleichzeitiger Stärkung der systemweiten Sicherheitslage

INFOBLOX-LÖSUNGEN:

- NIOS DDI mit Failover
- Cloud-Netzwerkautomatisierung
- DNS Traffic Control
- Berichte und Analysen
- BloxOne Threat Defense Advanced
- Ökosystemintegration
- Dossier
- Einblick in die Bedrohung
- Infoblox 2225 HA, 1425, v1425, Security Hardened, BITDA und v5005 virtuelle Reporting-Appliances

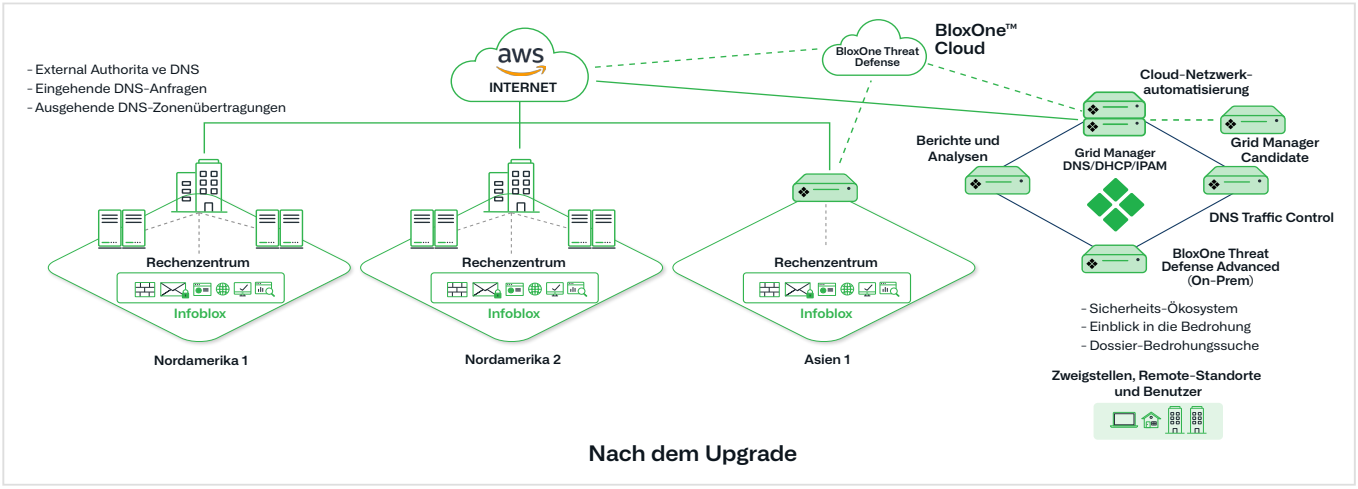

Abbildung 2: Architektur nach dem Upgrade mit modernisiertem DDI, einschließlich Reporting und BloxOne Threat Defense

ERGEBNISSE

Modernisierte Netzwerkdienste bieten Zuverlässigkeit, Transparenz, Sicherheit und globale Skalierbarkeit

Mit dem Infoblox-Update ist das Unternehmen besser aufgestellt, sein Versprechen einzulösen und seinen weltweiten Softwarekunden beispiellose Zuverlässigkeit, Qualität sowie persönlichen Service und Support zu bieten. Es hat jetzt vollständige Netzwerktransparenz, kontinuierliche Anwendungsverfügbarkeit, Betriebszeit und Redundanz sowie konsistentes Unternehmens-DNS für Benutzer vor Ort, außerhalb des Unternehmens und überall verbundene Benutzer. Darüber hinaus trägt die DDI-Modernisierung dazu bei, IT-Investitionen zukunftssicher zu machen, da das Unternehmen seine Migration in die Cloud plant. Der bedarfsgerechte Datenzugriff verbessert die Transparenz und Verwaltung des Netzwerks und beschleunigt die Entscheidungsfindung und Reaktion im Netzwerk – insbesondere für ein kleines IT-Team.

Aus Sicherheitsperspektive ist BloxOne Threat Defense Advanced mit Threat Insight einfach einzurichten und zu verwenden und bietet die DDI-integrierten Metadaten und die Flexibilität, die für erstklassige Sicherheit gegen böswillige Akteure und tägliche Sicherheitsbedrohungen erforderlich sind.

Die Sicherheitslösungen von Infoblox stärken die Sicherheitsfunktionen des Unternehmens und verhelfen ihm zu einer starken Sicherheitsreaktion, nicht nur um Infrastruktur, Daten und Remote-Mitarbeiter zu schützen, sondern auch um das Vertrauen zu schaffen, das für die Expansion neuer Anbieter, Partner und Remote-Benutzer erforderlich ist. BloxOne Threat Defense Advanced mit Dossier und Threat Insight ermöglicht eine schnelle Erkennung, Untersuchung, Abwehr und Behebung von Ransomware, Malware und Datenexfiltration. Diese Sicherheitstools und Integrationen verstärken den Schutz des Netzwerks vor immer häufigeren und komplexeren Sicherheitsbedrohungen im gesamten nationalen Filialnetz des Unternehmens. Indem das Unternehmen die Sicherheit vom Netzwerk aus aufbaut, kann es seine DDI-Metadaten für eine tiefe kontextbezogene Transparenz und Einblicke nutzen, um die Kontrolle und die Sicherheitseffizienz zu verbessern, die Sicherheitskosten zu senken und die Sicherheitstools effektiver zu machen. Mithilfe der zuverlässigen, modernisierten Netzwerk- und Sicherheitsplattformen von Infoblox kann das Unternehmen sein jahrzehntelanges Engagement bei der Verbesserung der Datentransparenz für Sicherheits- und SIEM-Anwendungen auch in Zukunft fortsetzen.

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

+1.408.986.4000
www.infoblox.com