LÖSUNGSHINWEIS

INFOBLOX UND GOOGLE CLOUD: LEISTUNG UND SCHUTZ FÜR HYBRIDE CLOUD-UMGEBUNGEN

DNS-, DHCP- UND IP-ADRESSMANAGEMENT-(DDI)-LÖSUNG AUF DER GOOGLE CLOUD

Google Cloud befähigt Organisationen, Agilität und Kosteneinsparungen durch einen hybriden Cloud-Ansatz zu erreichen, der lokale Umgebungen mit öffentlichen Cloud-Diensten wie Google Cloud kombiniert. Die Verwaltung kritischer Netzwerkdienste – DNS, DHCP und IP-Adressverwaltung (DDI) – in dieser Umgebung kann jedoch zu Ineffizienzen und eingeschränkter Sichtbarkeit bei virtuellen Netzwerken, VLANs, IP-Adressen und DNS-Einträgen führen und aufgrund der verteilten Natur der Infrastruktur zu erhöhten Sicherheitsherausforderungen führen. Ohne eine Unternehmenslösung zur Automatisierung und Zentralisierung der DDI-Verwaltung können Serviceverzögerungen, Inkonsistenzen und Sicherheitslücken auftreten. Infoblox-Lösungen für Google Cloud können Ihnen helfen, diese Herausforderungen der Hybrid-Cloud zu bewältigen.

Infoblox DDI- und Infoblox Threat Defense™-Lösungen (Abbildung 1) ermöglichen es Unternehmen, kritische Netzwerkdienste zentral zu verwalten und abzusichern und sich vor Bedrohungen in hybriden Cloud-Umgebungen zu schützen, während sie gleichzeitig ihre Investitionen schützen, den ROI optimieren und für künftige Geschäftsanforderungen skalieren.

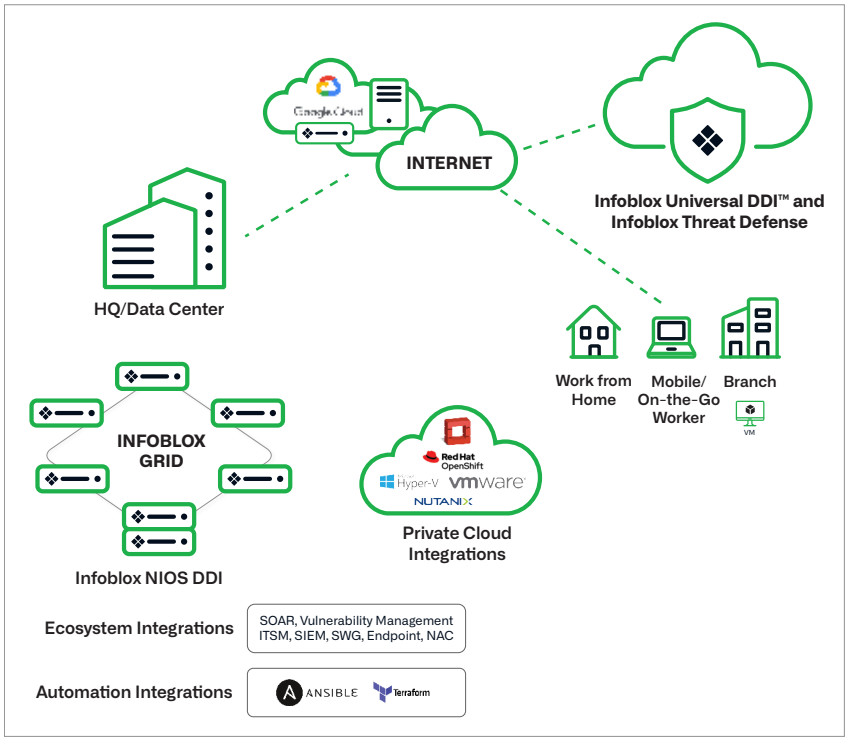

Abbildung 1. Infoblox DDI- und Infoblox Threat Defense-Lösungen

VORTEILE

Profitieren Sie von branchenführendem DNS- und IP-Adressmanagement (IPAM) für Google Cloud

Automatisieren Sie die Bereitstellung, Deprovisionierung und Änderung von DNS-Einträgen für Google Cloud-Workloads.

Verbesserte Erkennung und Transparenz

Beseitigen Sie tote Winkel mit automatischer Erkennung sowie einheitlicher und forensischer Transparenz von virtuellen Netzwerken und Maschinen in Google Cloud.

Stellen Sie die Konsistenz sicher

Infoblox IPAM sorgt für Konsistenz in Hybrid- und On-Premises-Netzwerken sowie der Google Cloud.

Sicherheit der Spitzenklasse

Threat Defense bietet eine zuverlässige DNS-basierte Sicherheit, um Sicherheitsbedrohungen zu erkennen, zu blockieren und zu beseitigen.

Infoblox DDI vereinfacht IPAM

Infoblox erweitert die DDI-Dienste auf Google Cloud und ermöglicht damit eine bessere Transparenz, Automatisierung und Kontrolle in privaten, hybriden und öffentlichen Multi-Cloud-Umgebungen. Mit Infoblox IPAM können Sie mehrere IPAM-Systeme (z. B. vor Ort und in der Public Cloud) von einem zentralen Kontrollpunkt aus verwalten, was eine höhere Effizienz, Koordination und Einhaltung der Richtlinien gewährleistet.

Infoblox DDI (Abbildung 2) wurde kürzlich um die Integration mit **internen Google Cloud-Bereichen** erweitert, damit Sie IP-Adressen für Ihre lokalen und Google Cloud-Netzwerke durch Automatisierung effizient verwalten können.

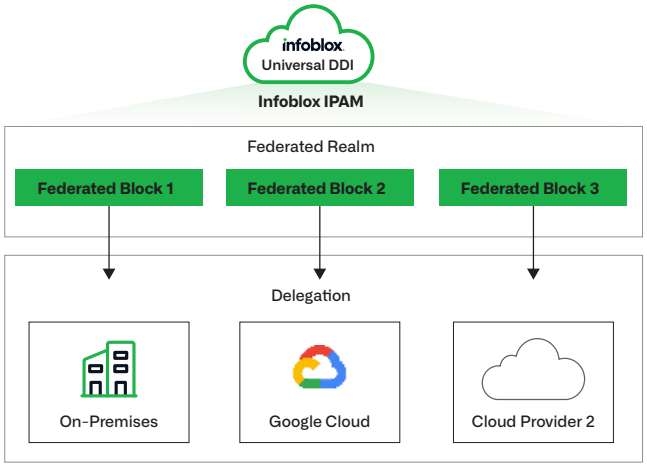

Abbildung 2. Universal DDI und Infoblox IPAM

Infoblox Threat Defense erhöht die Netzwerksicherheit und stoppt Cyberbedrohungen

Zusammen mit der konsistenten Sichtbarkeit, Automatisierung und Verwaltung kritischer Netzwerkdienste bieten die Infoblox-Lösungen erstklassige DNS-basierte Sicherheit für Workloads, die sowohl vor Ort als auch in der Cloud ausgeführt werden. Threat Defense (Abbildung 3) bietet hybride, sicherheitsorientierte DNS-Dienste zum Schutz von Netzwerken, Geräten und Benutzern vor lokalen und externen Cyberbedrohungen, auch an Remote-Standorten und im Homeoffice.

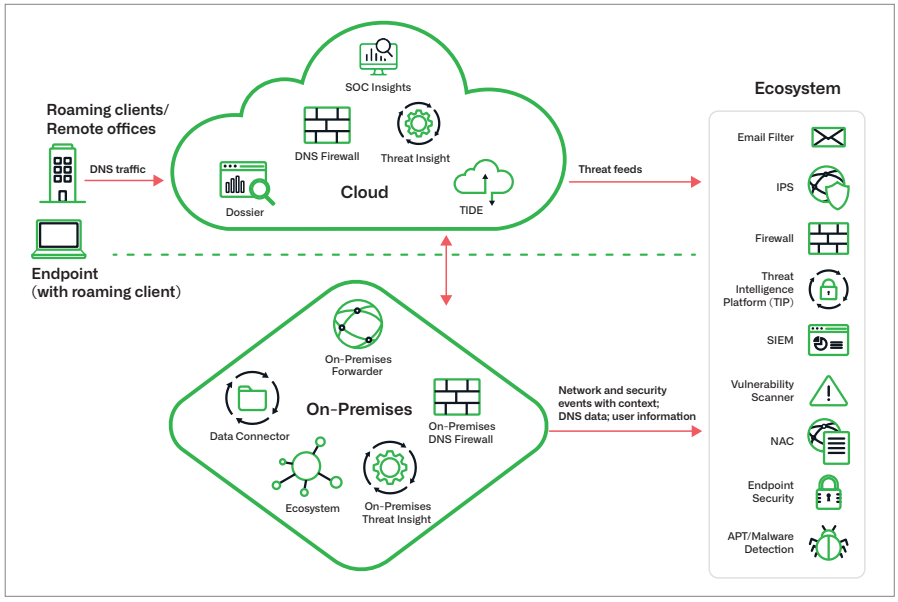

Abbildung 3. Hybride Schutz-DNS-Dienste

DNS-Bedrohungserkennung und -reaktion

Threat Defense analysiert DNS-Abfragen, um Malware-Befehls- und Steuerkommunikation, verdächtige Domains, DNS-basierte Datenexfiltration, Phishing, Ransomware und Advanced Threats wie Domain-Generierungsalgorithmen (DGAs) und Lookalike-Domains zu erkennen und zu blockieren. Die Lösung nutzt Infoblox Threat Intel, eine einzigartige DNS-zentrierte threat intelligence und Überprüfung des DNS-Verkehrs im Kundennetzwerk, um Bedrohungsakteure zu identifizieren und ihre Domänen zu blockieren, bevor sie Angriffe starten.

Ökosystemintegrationen

Threat Defense trägt auch zu einer schnelleren Bedrohungsreaktion bei, indem es APIs und native, sofort einsatzbereite Integrationen mit Sicherheitsökosystem-Tools nutzt, darunter SIEM, SOAR, ITSM, Schwachstellenscanner, NAC und Endpoint-Sicherheit. Die Lösung verbessert die Sicherheitslage für hybride Umgebungen erheblich. Threat Defense nutzt DDI-Daten, um wertvolle Netzwerkkontexte zu verwenden, wie zum Beispiel, welche Teile des Netzwerks und welche Workloads kompromittiert sind, um schnell Remediation-Maßnahmen zu identifizieren und einzuleiten, bevor sich die Bedrohung lateral ausbreitet.

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.

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

+1 408 986 4000
www.infoblox.com

Version: 20250512v2