LÖSUNGSHINWEIS

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

DNS-, DHCP- UND IPAM (DDI)-LÖSUNG AUF GCP

Mit Google Cloud können Unternehmen durch einen hybriden Cloud-Ansatz, der lokale Umgebungen mit öffentlichen Cloud-Diensten wie Google Cloud Platform kombiniert, Flexibilität und Kosteneinsparungen erzielen. Die Verwaltung kritischer Netzwerkdienste (DNS, DHCP und IP-Adressverwaltung (DDI)) in dieser Umgebung kann jedoch zu Ineffizienzen und eingeschränktem Einblick in virtuelle Netzwerke, VLANs, IP-Adressen und DNS-Einträge sowie zu größeren Sicherheitsherausforderungen aufgrund der verteilten Natur der Infrastruktur führen. Ohne eine unternehmenstaugliche Lösung zur Automatisierung und Zentralisierung der DDI-Verwaltung kann es zu Serviceverzögerungen, Inkonsistenzen und Sicherheitslücken kommen. Infoblox-Lösungen für Google Cloud Platform können bei der Lösung dieser Hybrid-Cloud-Herausforderungen helfen.

Infoblox DDI- und BloxOne® Threat Defense (Abbildung 1) ermöglicht 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.

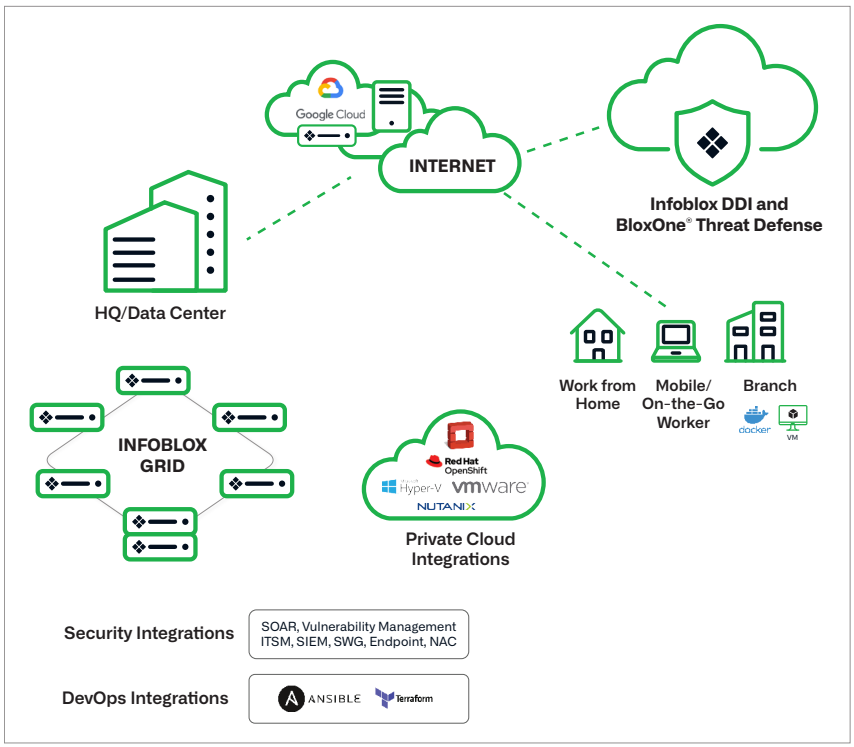


Abbildung 1 : Infoblox DDI and BloxOne® Threat Defense-Lösung

VORTEILE

Branchenführende DNS- und IP-Adressverwaltung für GCP

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

Verbesserte Erkennung und Transparenz

Beseitigen Sie tote Winkel mit automatischer Erkennung sowie einheitlicher und forensischer Transparenz von virtuellen Netzwerken und Maschinen auf GCP.

Stellen Sie die Konsistenz sicher

Infoblox IPAM sorgt für Konsistenz in Hybrid- und On-Premise-Netzwerken sowie GCP.

Sicherheit der Spitzenklasse

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

Infoblox DDI macht die IP-Adressverwaltung (IPAM) einfach

Infoblox hat seine Cloud-Automatisierungsplattform auf Google Cloud Platform ausgeweitet 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. On-Premise und Public Cloud) von einem zentralen Kontrollpunkt aus verwalten und so für mehr Effizienz, Koordination und Umsetzung der Richtlinieneinhaltung sorgen.

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

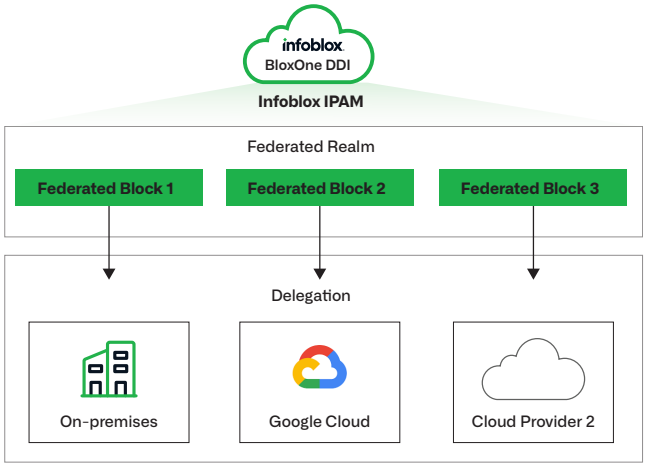
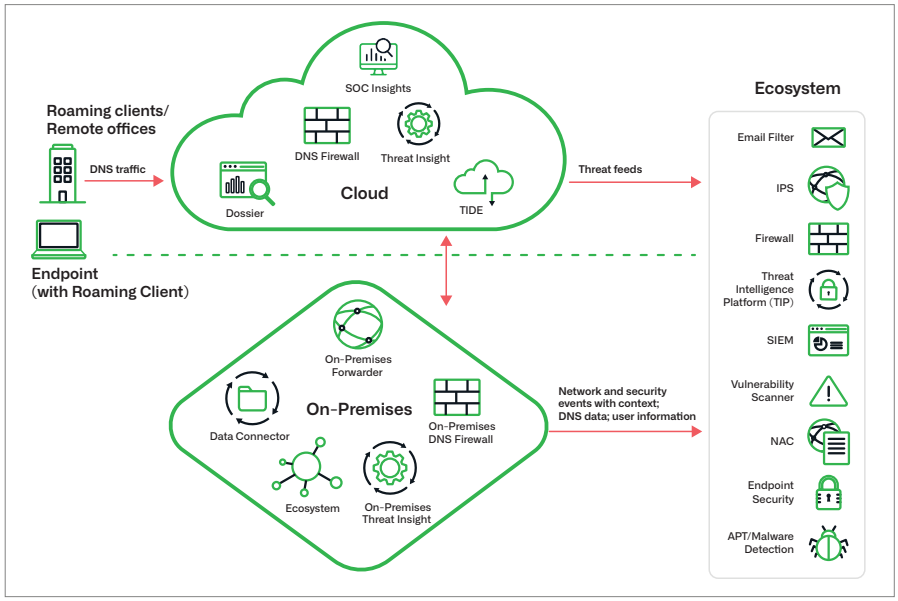


Abbildung 2: Infoblox DDI und Infoblox IPAM

BloxOne® Threat Defense verbessert die Netzwerksicherheit und wehrt Cyber-Bedrohungen ab

Zusätzlich zur konsistenten Transparenz, Automatisierung und Verwaltung kritischer Netzwerkdienste tragen die Infoblox-Lösungen zu erstklassiger DNS-basierter Sicherheit für Workloads bei, die lokal und in der Cloud ausgeführt werden. Infoblox BloxOne® 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.



DNS-Bedrohungserkennung und -reaktion

BloxOne® Threat Defense analysiert DNS-Anfragen, um Malware-C&C-Kommunikation, verdächtige Domains, DNS-basierte Datenexfiltration, Phishing, Ransomware und fortgeschrittene Bedrohungen wie Domain-Generierungsalgorithmen (DGAs) und Look-alike-Domains zu erkennen und zu blockieren. Die Lösung nutzt Infoblox Threat Intel, eine einzigartige DNS-zentrierte Bedrohungsanalyse, sowie die Untersuchung des DNS-Traffics im Kundennetzwerk, um Bedrohungsakteure zu identifizieren und ihre Domains zu blockieren, bevor sie Angriffe starten.

Ökosystemintegrationen

BloxOne® Threat Defense trägt auch zu einer schnelleren Reaktion auf Bedrohungen bei, indem es APIs und native, sofort einsetzbare Integrationen mit Sicherheits-Ökosystem-Tools wie SIEM, SOAR, ITSM, Schwachstellen-Scannern, NAC und Endpunktsicherheit nutzt. Die Lösung verbessert die Sicherheitslage in hybriden Umgebungen erheblich. Durch die Nutzung von DDI-Daten nutzt BloxOne Threat Defense wertvollen Netzwerkkontext, z. B. welcher Teil des Netzwerks und welche Arbeitslasten gefährdet sind, um schnell Abhilfemaßnahmen 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: 20240403v1