INFOBLOX AND GOOGLE CLOUD PLATFORM: PERFORMANCE AND PROTECTION FOR HYBRID CLOUD ENVIRONMENTS

DNS, DHCP AND IPAM (DDI) SOLUTION ON GCP

Google Cloud empowers organizations to achieve agility and cost savings through a hybrid cloud approach, which combines on-premises environments with public cloud services like Google Cloud Platform. However, managing critical network services - DNS, DHCP, and IP Address Management (DDI) across this environment can introduce inefficiencies and limited visibility into virtual networks, VLANs, IP addresses, and DNS records, and increased security challenges due to the distributed nature of the infrastructure. Without an enterprise-grade solution to automate and centralize DDI management, service delays, inconsistencies, and security gaps can arise. Infoblox solutions for Google Cloud Platform can help resolve these hybrid cloud challenges.

Infoblox DDI and BloxOne® Threat Defense solution (Figure 1) enables organizations to centrally manage and secure critical network services and protect against threats across hybrid cloud environments while protecting investments, optimizing ROI and scaling to meet future business requirements.
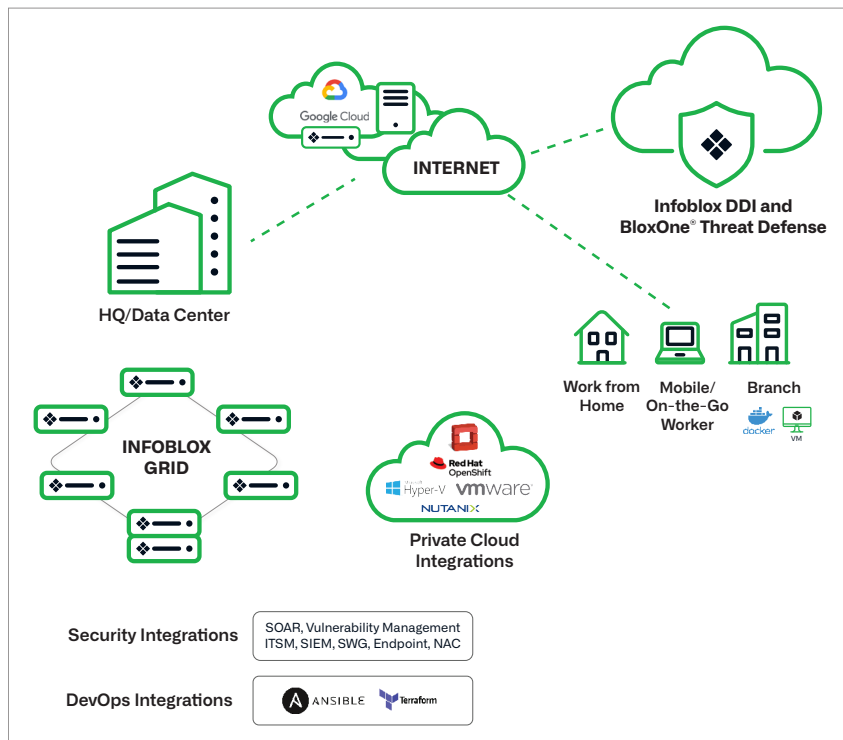

Figure 1 : Infoblox DDI and BloxOne® Threat Defense Solution

BENEFITS

Gain Industry-Leading DNS and IP Address Management for GCP
Automate provisioning, deprovisioning and modifications of DNS records for GCP workloads.

Improve Discovery and Visibility
Eliminate blind spots with automated discovery, unified and forensic visibility of virtual networks and machines on GCP.

Ensure Consistency
Infoblox IPAM ensures consistency across hybrid, on-prem networks, and GCP.

Best-in-Class Security
BloxOne Threat Defense provides robust DNS-based security to detect, block and resolve security threats.

Infoblox DDI makes IP Address Management(IPAM) simple

Infoblox has extended its cloud automation platform to Google Cloud Platform, enabling better visibility, automation, and control across private, hybrid, and public multi-cloud environments. With Infoblox IPAM, you can manage multiple IPAM systems (such as on-prem and public cloud) from a central control point, ensuring greater efficiency, coordination, and implementation of policy compliance.

Infoblox DDI(Figure 2) has recently added integration with **GCP internal ranges** to help you efficiently manage IP addresses for your on-premises and GCP networks at scale through automation.
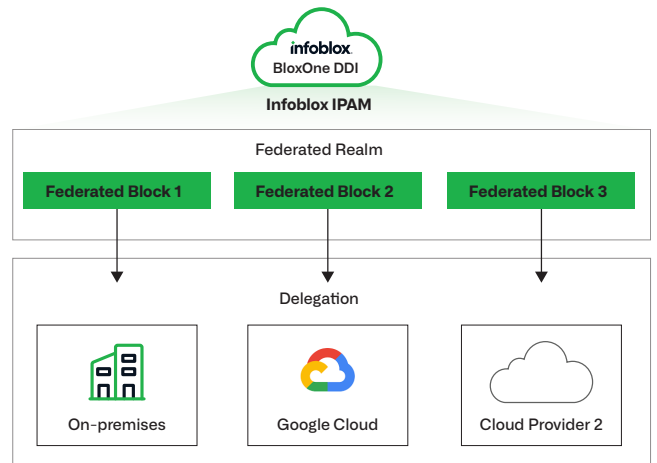

Figure 2 : Infoblox DDI and Infobox IPAM

BloxOne® Threat Defense elevates network security and stops cyber threats

Along with the consistent visibility, automation and management of critical network services, Infoblox solutions help provide best-in-class DNS-based security for workloads running on-premises and in the cloud. Infoblox BloxOne® Threat Defense(Figure 3) provides hybrid protective DNS services to secure networks, devices and users from cyberthreats on- and off- premises, including remote locations and home offices.
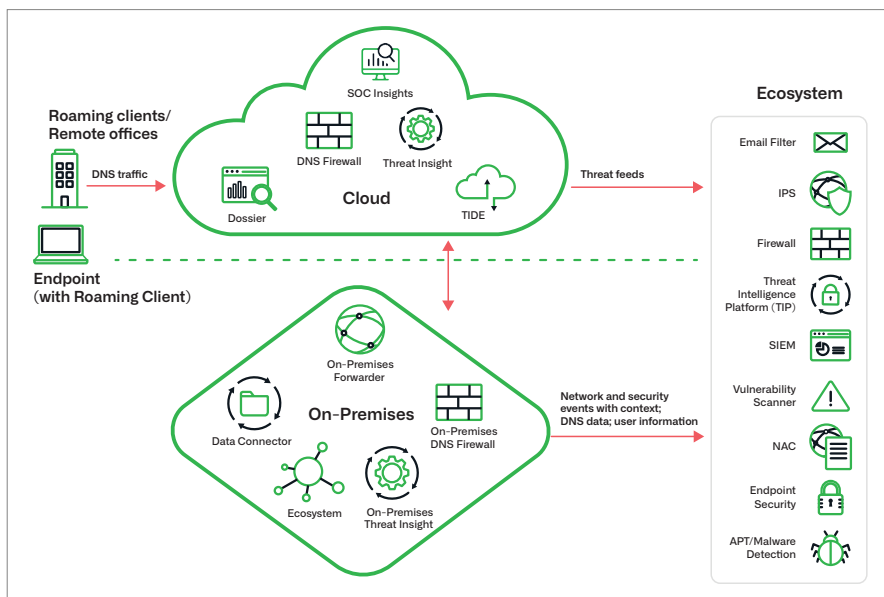
DNS Threat Detection and Response

BloxOne® Threat Defense analyzes DNS queries to detect and block malware C&C communications, suspicious domains, DNS-based data exfiltration, phishing, ransomware and advanced threats such as domain generation algorithms (DGAs) and look-alike domains. The solution leverages Infoblox Threat Intel, which is unique DNS-centric threat intelligence, and inspection of customer network DNS traffic to identify threat actors and block their domains before they launch attacks.

Ecosystem Integrations

BloxOne® Threat Defense also helps with faster threat response by using APIs and native out-of-the-box integrations with security ecosystem tools, including SIEM, SOAR, ITSM, vulnerability scanners,

NAC and endpoint security. The solution significantly improves security posture for hybrid environments. Leveraging DDI data, BloxOne Threat Defense uses valuable network context, such as which part of the network and which workloads are compromised, to quickly identify and initiate remediation action before the threat spreads laterally.