SOLUTION NOTE

INFOBLOX ECOSYSTEM EXCHANGE

Reduce MTTR with automation

SUMMARY

Infoblox Ecosystem Exchange is a set of integrations that unifies your security ecosystem, enabling seamless data exchange and automated response across diverse solutions. The extensive integration enables the broader cyber security ecosystem to work in unison to detect and remediate threats. It empowers organizations to:

- **Break down silos:** Eliminate information barriers between your networking and security tools such as , SIEMs, firewalls, endpoint security tools and others .
- **Optimize SOAR:** Simplify and improve security workflows by sharing real-time network and threat context with Security Orchestration, Automation and Response (SOAR) tools
- **Enhance threat detection and response:** Gain a unified view of threats across your entire network and respond quickly with automated actions.

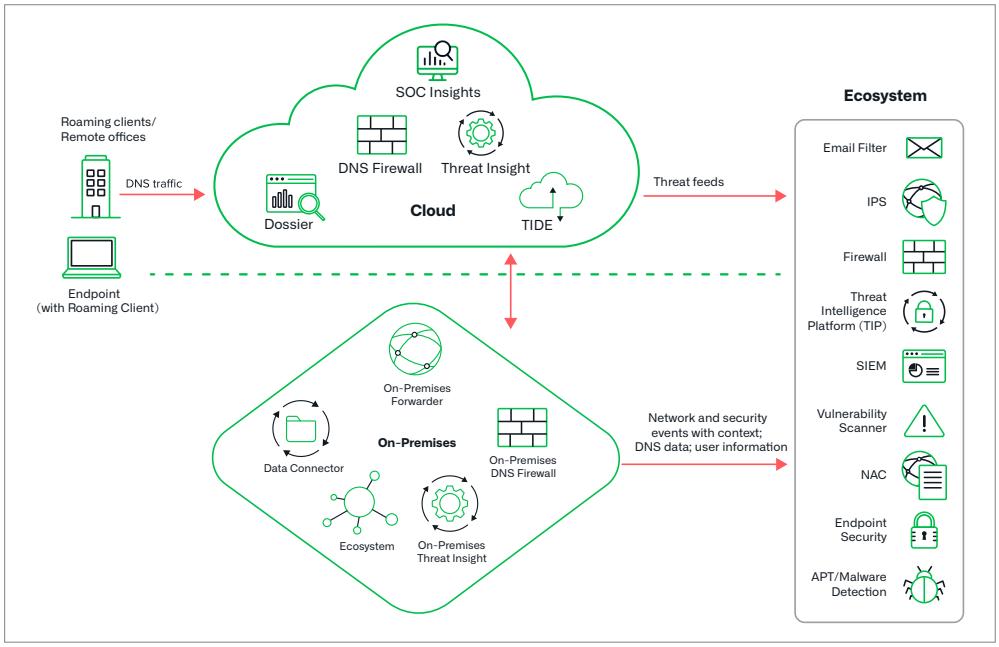

Figure 1: Infoblox hybrid architecture enables protection everywhere and deployment anywhere

The Exchange relies on a comprehensive set of APIs that cover various functionalities:

- **Threat Intelligence (TI) APIs:** Share unique DNS threat data between Infoblox tools and your other security solutions. For example, you can retrieve malicious domains, IP addresses and other threat indicators identified by Infoblox BloxOne® Threat Defense and send them to SIEM, firewall or endpoint security for enhanced protection and consistent policy enforcement.

- **Security Automation APIs:** Trigger automated actions in response to threats. It serves as a bridge between Infoblox's security capabilities and your broader security ecosystem, allowing for streamlined workflows and enhanced threat response.
- **Data Management APIs:** Automate and integrate DNS, DHCP, and IPAM (DDI) tasks into your broader IT workflows, streamlining operations and enhancing network visibility
- **Configuration Management APIs:** Automate the configuration of Infoblox devices and integrate them with your existing IT tools.

The benefits of using the Infoblox Ecosystem Exchange include:

- **Reduced risk of security breaches:** By breaking down silos and improving collaboration between security tools, the Exchange makes it more difficult for attackers to exploit vulnerabilities.
- **Improved operational efficiency:** Automated workflows and reduced manual work lead to significant time savings and improved efficiency for security teams.
- **Increased ROI:** By getting more value out of your existing security tools, the Exchange helps you maximize your security investment.

Ecosystem Technology	Integration Overview	Benefits
Advanced Threat Detection	• BloxOne® Threat Defense automatically shares information with advanced threat detection solutions on incidents involving advanced persistent threat (APT) activity and malicious domains • Infoblox then automatically blocks, logs events or takes appropriate action on these threats	• Enables flexible policy enforcement • Rapidly identifies infected devices • Builds defense and remediation into IT systems and processes
Threat Intelligence Sharing	• Infoblox Threat Intelligence Data Exchange (TIDE) sends information on malicious host names, IP addresses and URLs to the threat intelligence platform (TIP) • TIP enables blocking and monitoring of more threats	• Reduces the number of alerts that require review • Improves situational awareness for network and security organizations • Enhances overall security posture
Security Information and Event Management (SIEM)	• Infoblox sends information on IP addresses, infected devices and suspicious DNS requests and responses to SIEM • SIEM can use this information to perform analysis and take action	• Provides consolidated visibility into device activity regardless of where log data was generated • Supplies context for more accurate prioritization of security events • Improves operational efficiency of network ops and IT teams
Vulnerability Management	• Infoblox sends information on IP addresses, network devices and malicious events to vulnerability management • Vulnerability management uses that information to automatically trigger scans, enabling easier compliance and accelerated remediation	• Provides near-real-time visibility into new devices as they join the network • Automates and accelerates responses to network changes and malicious events • Improves ROI on security investments already made

Ecosystem Technology	Integration Overview	Benefits
Network Access Control (NAC)	• Infoblox provides information on IP addresses, network devices and DNS security events • NAC solutions can use that information to get context to better prioritize threats and take more immediate action (such as removing a device from the network) to shorten time to containment	• Expands visibility into network infrastructure, users and devices • Provides vital context for threat prioritization • Enables consistent policy enforcement
Next Generation End-point Security	• Infoblox detects DNS-based malware communications and informs next generation endpoint security technologies • These products can identify the malicious processes, quarantine the endpoint or take other actions • For added protection, endpoint security solutions can incorporate Infoblox client agents	• Quickly identifies and prevents DNS-based endpoint communications to malicious domains • Automatically responds to endpoint threats, reducing dwell time • Enables mass deployment of Infoblox endpoint agent for DNS security and streamlines workflows
Next Generation Firewall (NGFW)	• NGFW receives malicious host names, IP addresses and URLs from Infoblox TIDE • NGFW enables customer to block or monitor threats	• Reduces the number of alerts to review • Improves situational awareness for network and security organizations • Strengthens overall security posture
Web Gateway	• BloxOne Threat Defense blocks DNS-based data exfiltration, as well as DNS requests to malicious domains before forwarding the traffic to McAfee Web Gateway • The web gateway then scans traffic for further inspection with URL filtering, SSL and more	• Unifies domain blocking and http security for broader protection • Speeds detection of malicious traffic originating from infected endpoints, regardless of its location • Complements web gateway with DNS-based threat intelligence
Security Orchestration, Automation and Response	• SOAR solution receives information on IP address, network devices and malicious events from Infoblox • SOAR uses that information to block/unblock/check domain, check information about IP/host/network/domain in IPAM • Infoblox automatically enriches IPAM with data from security tools and events	• Integrates disparate security tools and provides vendor-neutral threat intelligence for all devices • Automates and produces faster response with full set of threat intelligence APIs • Enhances and improves incident response with better threat intelligence • Improves security processes by integrating with other systems via SOAR
ITSM/ITOM/Security Operations	• Infoblox sends information on new devices, networks and IP addresses to ITSM/ITOM/Security Operations • Network and security admins can view devices and events discovered by Infoblox in a single place	• Provides at-a-glance dashboard views into devices and endpoints joining and leaving the network • Enables proactive identification of network issues to accelerate responses to network changes and security events

AUTOMATING WORKFLOWS THROUGH CLOUD ECOSYSTEM INTEGRATION

Networks ops teams may have hundreds of network tools in their environment. Often, these tools work in silos, making it very difficult to see the full range of diverse network assets in a single place. Today's organizations also use varied deployments and architectures, from physical to virtual to cloud. Infoblox ecosystem integration enables networkers to gain a consolidated view of assets and architectures, while automating common workflows to speed response times and improve agility.

Infoblox network automation and cloud eocystem integrations enable organizations to:

- Unify domain blocking and http security for broader protection
- Speed detection of malicious traffic originating from infected endpoints, regardless of its location
- Complement web gateway with DNS-based threat intel

Ecosystem Technology	Integration Overview	Benefits
Cloud Management Platforms (Cisco, VMWare)	• Infoblox automation enables quick spin ups of VMWare instances • Cloud management platforms can incorporate DDI automation into their workflows • Infoblox automation ties into service management solution from Cisco and VMWare	• Enables faster provisioning of new users joining the network • Provides unified visibility across diverse assets and infrastructure • Facilitates and automates policy enforcement
Service Provider Services (Nokia)	• Infoblox NIOS integrates with Nokia Cloud Band to accelerate Network Functions Virtualization (NFV) development and implementation • The Cloud Band NFV system orchestrates the deployment of Infoblox Virtual Appliances in the network	• Simplifies network operations by automating infrastructure and Infoblox DDI appliance lifecycle management processes • Accelerates deployment with a pre-integrated solution that combines Infoblox DDI software with Nokia's NFV infrastructure solution
Public Cloud (AWS, Azure, VMWare)	• Infoblox and public cloud exchange information with each other to provide unified visibility and management across all platforms • Infoblox and public cloud integration enables automation of IPAM and DNS provisioning	• Provides consolidated views into IP and DNS information for virtual machines (VMs) located on-premises or in the cloud • Enables centralized management of DNS servers on-premises and in the cloud • Ensures efficient utilization of cloud resources across multiple clouds (Azure, AWS, VMWare, OpenStack)

Ecosystem Technology	Integration Overview	Benefits
Private Cloud (OpenStack)	• Infoblox integration enables automatic provisioning of the next available IP address and DNS record when creating VMs and automatically releases IPs and DNS records when destroying VMs • Private cloud spins up VM on Hypervisor (e.g., KVM) and VM makes DHCP request after it starts up	• Ensures consistency and visibility in hybrid deployments (on-premises, virtual and/or cloud) • Reduces manual processes • Speeds time to deployment
Next Generation Data Centers (Cisco, Nutanix)	• Infoblox provides IPAM and DDI provisioning workflows • Integration between DDI and next generation data center products provides consolidated environment and provisioning flexibility	• Automates manual tasks • Enables faster response to network changes • Provides better ROI for existing network investments • Offers flexibility and helps consolidate operations

Note: The integrations require one or more relevant Infoblox products to be able to pass necessary information to the tools mentioned above. Infoblox integrations support a variety of options including REST APIs, STIX/TAXII, JSON, XML and CSV formats, syslog and third-party propriety methods, to ensure interoperability.

To learn more, please visit Technology Alliance Partner page.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240209v1