SOLUTION NOTE

Infoblox Ecosystem Exchange

Reducing Threat Response Time and Costs with Enhanced Productivity and Automation

SUMMARY

Infoblox Ecosystem Exchange is a highly connected set of integrations that enable organizations to eliminate silos, optimize security orchestration, automation and response (SOAR) solutions and improve the ROI of their entire cybersecurity ecosystem, including third-party, multi-vendor assets. It reduces the time it takes to respond to threats as well as the cost through enhanced automation and real-time, two-way data sharing enabled by extensive APIs.

Infoblox as Part of the Cybersecurity Ecosystem

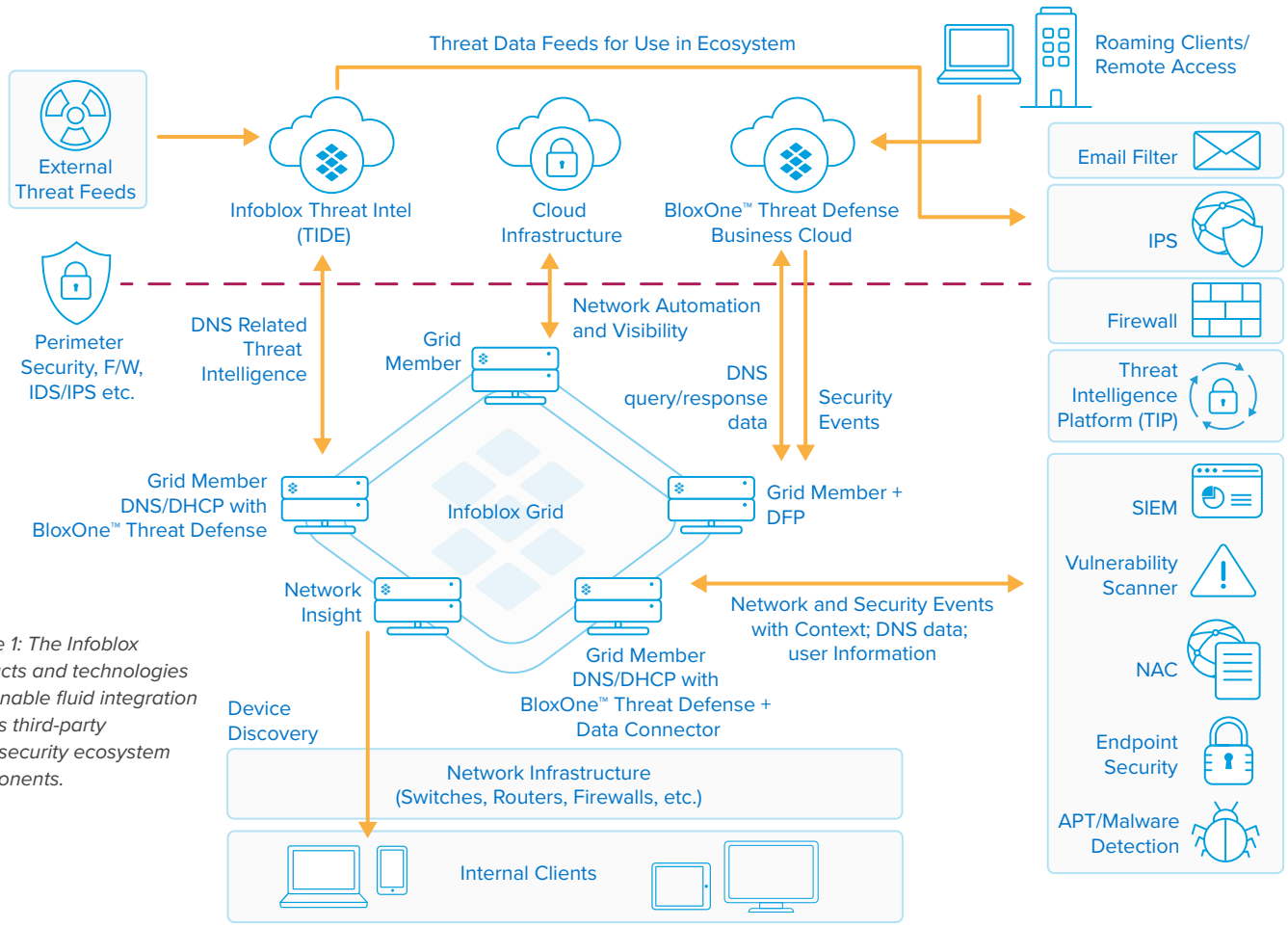

Figure 1: The Infoblox products and technologies that enable fluid integration across third-party cybersecurity ecosystem components.

Infoblox's extensive integrations enable the broader cybersecurity ecosystem to work in unison to detect and remediate threats (Figure 1). They combine aggregated, curated threat intelligence, more than 30 API-level vendor integrations and pervasive automation, enabling network and security teams to:

- Gain centralized visibility into devices and DNS- based threat vectors across on-premises, virtual and cloud deployments, including VMWare, AWS, Azure, Cisco ACI and OpenStack
- Orchestrate common security policy across the infrastructure
- Decrease time to remediation by up to two-thirds
- Reduce costs associated with manual intervention and human error
- Reduce the number of alerts teams must review
- Make threat analysts up to three times more productive
- Optimize SOAR solutions by automatically sharing contextual threat information
- Improve the effectiveness of threat intelligence across the ecosystem
- Lower cost of SIEM solutions by sending only suspicious DNS data to these platforms
- Get better ROI from existing network security investment

Ecosystem Technology	Integration Overview	Benefits
Advanced Threat Detection (FireEye NX Series)	• 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 (ThreatConnect, Cisco Threat Intelligence Director, Check Point Threat Cloud, Windows Server 2016)	• 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) (LogRhythm, Splunk, McAfee ESM, IBM, QRadar, Micro Focus ArcSight)	• 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 (Qualys, Rapid7, Tenable Security Center)	• 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

Network Access Control (NAC) (Cisco, ISE, Aruba ClearPass, ForeScout)	• 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 (Carbon Black, McAfee ePO)	• 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) (Palo Alto Networks)	• 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 (McAfee)	• 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 (Phantom Cyber)	• SOAR solution receives information on IP address, network devices and malicious events from Infoblox • SOAR uses that information to block/un-block/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 (ServiceNow)	• 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)
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.

Infoblox
NEXT LEVEL NETWORKING

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com