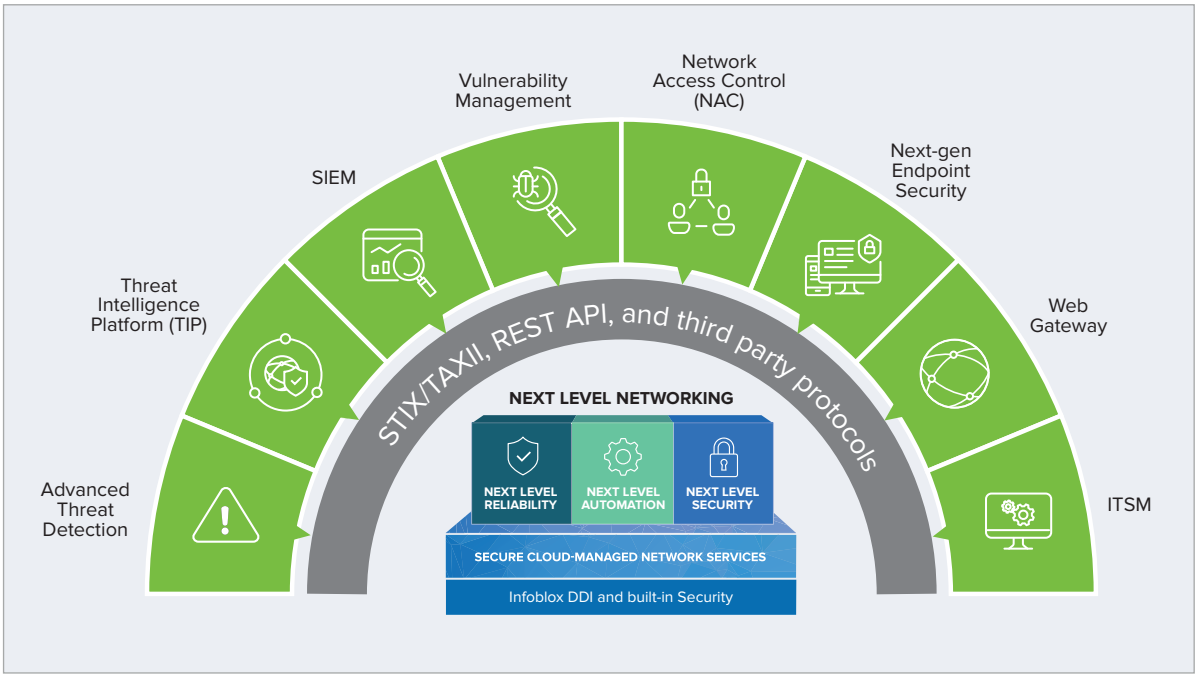
SOLUTION NOTE

Infoblox Ecosystem Exchange

Infoblox Ecosystem Exchange is a highly-interconnected set of ecosystem integrations that extend security, increase agility, and provide situational awareness for more efficient operations, on-premises and in the cloud. It provides visibility across the entire network including virtualized or cloud deployments, removes silos between network and security teams, improves agility, automates IT workflows, enables faster remediation to threat and network changes, and provides better ROI on IT and security investments already made.

Cybersecuriry Ecosystem



Infoblox integrations with the broader security ecosystem allow customers to:

- Gain visibility into DNS threats and get proactive protection against cyberattacks
- Improve speed of response by threat intelligence and DNS indicators of compromise sharing
- Prioritize response based on critical contextual data
- Get better ROI from security investments already made

Ecosystem Technology	Integration Overview	Benefits
Advanced Threat Detection (FireEye NX Series)	• Advanced threat detection solutions share advanced persistent threats (APTs) communication to malicious domains with Infoblox ActiveTrust® • Infoblox then blocks, logs events, or takes appropriate action on these threats	• Flexible policy enforcement • Identification of infected devices • Defense and remediation built into IT systems and processes
Threat Intelligence Sharing (ThreatConnect, Cisco Threat Intelligence Director, Check Point Threat Cloud, Windows Server 2016)	• Threat intellgience platforms (TIPs) receive malicious host names, IP addresses, and URLs from Infoblox TIDE • TIPs can enable blocking and monitoring of more threats	• Reduces the number of alerts to review • Improves situational awareness in an organization • Improves overall security posture
SIEM (LogRhythm, Splunk, McAfee ESM)	• SIEM vendors receive information on IP address, DNS requests and responses, and infected devices from Infoblox • This information can be used by SIEMs to perform analysis and take action	• Unified visibility into device activity regardless of where log data was generated • Context and prioritization—visibility into security events, threat intelligence feed of malicious zdomains and IP addresses • Improve efficiency of network ops and IT teams
Vulnerability Management (Qualys, Rapid7, Tenable Security Center)	• Vulnerability management receives information on IP addresses, network devices, and malicious events from Infoblox • Vulnerability management uses that information to trigger scan, enabling ease of compliance and accelerated remediation	• Near-real time visibility into new devices getting added to the network • Automated/faster response to network and malicious events • Improve ROI on security investments already made
Network Access Control (NAC) (Cisco ISE, ForeScout)	• Infoblox provides information on IP addresses, network devices and DNS security events • NAC solutions can use that information to get context to prioritize threats and take action (such as knocking a device off the network) reducing time to containment	• Expand visibility of network, users, and devices • Context for prioritization of threats • Consistent policy enforcement
Next-generation End-point Security (Carbon Black, McAfee)	• Infoblox detects malware communications being made via DNS and informs next-generation end-point security technologies • These products can identify the malicious processes, quarantine the endpoint, or take other actions • Infoblox client agent can be deployed using endpoint security solutions	• Identify and prevent DNS-based endpoint communications to malicious domains • Automatically respond to endpoint threats, reducing dwell time • Enables mass deployment of Infoblox endpoint agent for DNS security and streamlines workflows
Next Generation Firewall (Palo Alto Networks)	• NGFW receives malicious host names, IP addresses, and URLs from Infoblox TIDE • Enable customers to block or monitor threats	• Reduce the number of alerts to review • Improves situational awareness in an organization • Improves overall security posture
Web Gateway (McAfee)	• Infoblox ActiveTrust Cloud blocks DNS-based data exfiltration and DNS requests to malicious domains before forwarding the traffic to McAfee Web Gateway • 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 their location • Compliments web gateway with DNS based threat intelligence

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 cloud and hybrid systems, 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