Infoblox
NEXT LEVEL NETWORKING

SOLUTION NOTE

Raise Network Security to the Next Level

SUMMARY

We are becoming increasingly dependent on secure network connectivity. Half the world's population uses the Internet.[1] By 2021, global IP traffic is projected to exceed three zettabytes a year.[2] By 2030, the number of Internet of Things (IoT) devices is expected to reach 125 billion.[3] In just the past ten years alone, malware attacks have totaled 780 million.[4] Traditional network management and security solutions are not able to keep up in the face of rising complexity and escalating network-based attacks. With signature security, reliability and automation capabilities from Infoblox, you can take network security to the next level to stop malware, protect your infrastructure and data and remediate threats faster.

Potential Gaps in Modern Networks

Modern networks are distributed with one or more main office locations, branch offices, and data centers. They have a mix of physical, virtual, and cloud components with applications running either in local datacenters or in a public/hybrid cloud. Endpoints are connecting to corporate applications and resources from remote locations. Organizations have SOC teams deploying and managing several security tools that filter different types of traffic known to present risks. Despite the variety and breadth of security tools, there are still several gaps in security, including:

- No protection against DNS-based data exfiltration, command-and-control (C&C) callbacks, or DDoS attacks on DNS servers
- Little visibility into what's on the extended network—new or unmanaged devices on the network hiding vulnerabilities, virtual workloads being spun up or spun down on a daily basis, roaming devices connecting to suspicious sites before spreading malware inside the corporate network
- Lack of network context for prioritizing alerts, knowledge of which threats to address first, or ability to leverage critical DNS data to analyze threats

The SANS Institute, a leading authority in security best practices, provides a framework for critical security controls that companies can follow to improve their security posture. It's no surprise that visibility and inventory of devices and software top the list. At the end of the day, you can only protect what you can see.

The other area that creates security gaps is DNS. DNS is one of your network's most critical assets—and most vulnerable. Frankly, every part of your network, which in our digital era means every part of your business, depends on the security and availability of DNS services. For example, in one way or

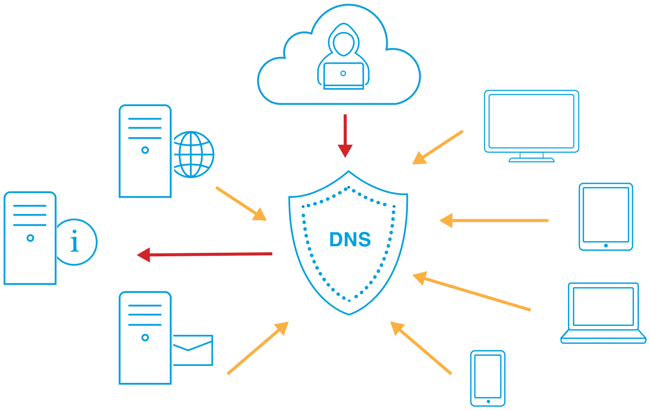


Figure 1: DNS is a vulnerable network asset that is as essential to digital organizations as it is to hackers and cybercriminals.

[1] International Telecommunications Union, 2015 estimate
[2] Cisco white paper, The Zettabyte Era: Trends and Analysis, June 2017
[3] IHS Markit, The Internet of Things: a movement, not a market, October 2017
[4] RightScale, 2018 State of the Cloud Survey, January 2018

another any digital communication, access to an application or service, or ecommerce customer transaction involves your DNS infrastructure. Hackers and cybercriminals have figured this out. Whether they use DNS to try to map out your network, plan an attack, or deploy botnets or malware to communicate with malicious (C&C) servers, DNS is just as essential to the bad guys as it is to your business (Fig 1).

Approach to Next Level Security

The most effective network security solutions enable you to close the security gaps mentioned previously by addressing the following three areas:

1. **Infrastructure protection** to maintain application and service availability
2. **Data protection and malware mitigation** for safeguarding devices and data
3. **Threat containment and operations** to optimize and automate security activities

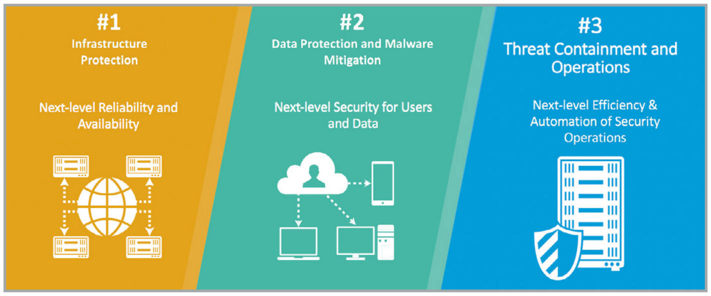

#1
Infrastructure Protection
Next-level Reliability and Availability
#2
Data Protection and Malware Mitigation
Next-level Security for Users and Data
#3
Threat Containment and Operations
Next-level Efficiency & Automation of Security Operations

Figure 2: Three aspects of security

Infrastructure Protection

Ensuring application and service availability are critical elements of any infrastructure protection solution. To accomplish this end, the best solutions enable you to protect critical network elements against a wide range of attacks. In addition, they give you the ability to automatically discover non-compliant and vulnerable network devices and enhance visibility across your physical, virtual, and cloud network infrastructure.

Infoblox's solution for infrastructure protection provides the following:

Single pane of glass visibility of extended infrastructure—See every network asset, IP address switch port, VLAN, username, and topology with unmatched clarity and consolidate your core network infrastructure into a single, comprehensive authoritative database. View attack points and patterns, identify new or unmanaged devices quickly, and manage devices intelligently as they grow.

Automatic detection of vulnerable devices—Easily identify new devices as soon as they join the network and quickly flag non-compliant devices which could hide vulnerabilities. The solution automatically remediates configuration issues and uniformly enforces compliance mandates and security policies.

Protection against the widest range of DNS-based attacks—The solution automatically detects and stops the widest range of DNS attacks, including reflection, DDoS, NXDOMAIN, amplification, TCP/UDP/ ICMP floods, tunneling, reconnaissance, cache poisoning, and protocol anomalies. It detects DNS hijacking, provides alerts, and maintains DNS integrity to ensure availability even under attack by allowing legitimate DNS traffic to proceed while blocking malicious activity.

Automatic notications using ecosystem integrations—The solution enriches your security infrastructure with information on network changes and the industry's most inclusive array of curated threat intelligence. It automatically shares attack event information across your third-party ecosystem through more than thirty API-level vendor integrations, including endpoint, security information and event management (SIEM) and Network Access Control (NAC) solutions. For example, the solution can automatically notify your vulnerability scanner when a virtual workload is spun up or automatically trigger a scan on a new device as soon as it joins the network.

Centralized reporting for analysis and planning—Infoblox provides detailed reporting, enabling your security teams to automatically harness rich network data to gain insights that drive more effective planning and elevate your security response.

Data Protection and Malware Mitigation

Malware uses DNS at various stages of the cyber kill chain to penetrate the network, infect devices, propagate laterally and exfiltrate data. In a recent survey by SC Magazine, 46% of respondents experienced DNS-based data exfiltration while 45% said they experienced DNS tunneling. More than 90% of malware uses DNS to carry out campaigns once it has breached the perimeter. Disrupting this kill chain and preventing DNS-based data exfiltration requires the following:

- Enhanced DNS security that closes pathways that most traditional network security solutions inadequately protect
- A multi-pronged approach to threat detection
- Centralized and consolidated visibility into the network

Infoblox's solution for Data Protection and Malware Mitigation addresses the security gaps in your DNS that expose your network to escalating risks. In addition to DNS security, the solution also provides:

Disruption of the cyber kill chain to prevent malware proliferation—The solution proactively contains the spread of malware, including phishing and ransomware, and stops C&C communications at the DNS choke point. It enforces policy using extensive, up-to-date threat intelligence that has been aggregated, verified, and curated by an Infoblox threat research team. Through API integrations, it also shares DNS indicators of compromise with your security ecosystem such as next-generation endpoint protection (NGEP), NAC, vulnerability scanners, and SIEM to prevent lateral movement of threats to speed remediation. Available as an on-premises solution or as a service delivered from the cloud, the solution protects devices at headquarters, in remote and branch offices or while roaming.

Detection and prevention of known and zero-day data exfiltration—The Infoblox solution uses a combination of signatures, machine learning algorithms, and behavioral analytics to detect not just standard DNS tunnels, but also zero-day techniques that hide in the shadows by occurring in low volumes or unfolding slowly over long periods of time.

Deep visibility into your extended network— Get unified visibility into infected endpoints wherever they are—on premises or in the cloud. Infoblox also provides actionable context, including user name, MAC address, device type, and lease history to hasten remediation.

Reporting and mining of valuable DNS data— Infoblox provides detailed and centralized reporting for on-premises and cloud-delivered solutions, enabling you to automatically monitor and analyze your network, devices and applications and see granular details about malicious interactions and infected devices all in one place to bolster the effectiveness of your security operations

Threat Containment and Operations

Eliminating silos between networking and security technologies and improving the ROI from existing security investments is at the heart of Infoblox's Threat Containment and Operations solution. The solution brings situational awareness and context to security events by gathering and analyzing a broader set of data, to find events that pose the greatest harm to an organization quickly and prioritize them for remediation. The solution optimizes threat intelligence, automates remediation, shares context required to prioritize threats and bridges silos.

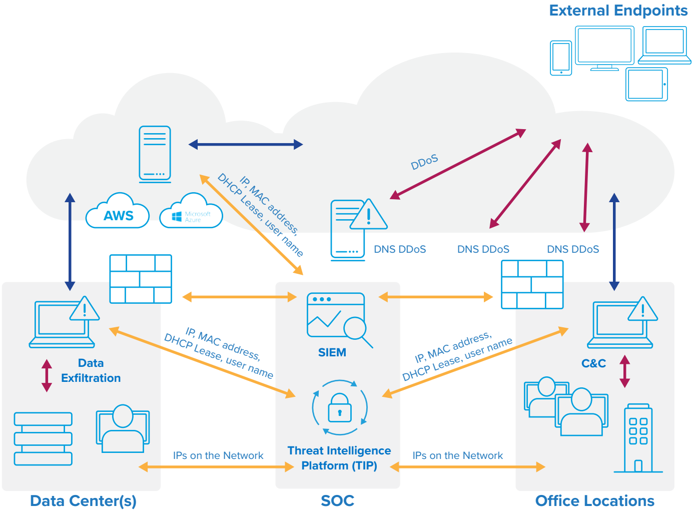


Figure 3: : Making modern networks agile and secure

Threat Intelligence optimization—Automatically enforce security policy through timely, consolidated and far-reaching threat intelligence that is aggregated from multiple sources, verified, and curated by an in-house threat research team. The solution enables you to eliminate conflicts that can slow your response. It automatically distributes trusted threat intelligence across your security infrastructure providing you with a single source of truth about impending risk.

Security orchestration—Security orchestration involves automatically sharing network events and indicators of compromise at the device level in real time across the multi-vendor cybersecurity ecosystem. Extensive Infoblox API-level integrations enable more than two-dozen endpoint, SIEM and NAC vendor solutions to exchange security event data to accelerate attack detection and remediation (Fig. 4).

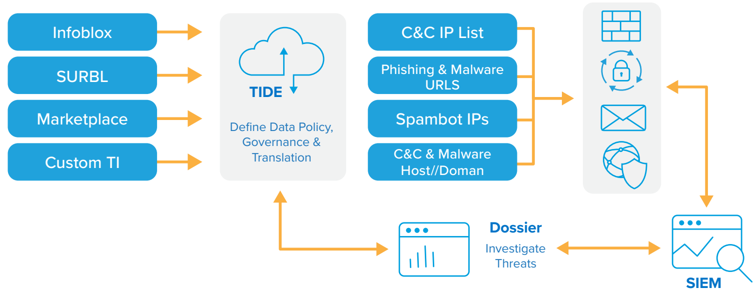
Rapid triage—With Infoblox, your security analysts and researchers can rapidly prioritize genuine threats faster and reduce time-draining false positives. Threat intelligence from Infoblox provides timely context (including type of malware, domain registration information, and associated malicious campaigns) that threat analysts and incident responders can access either through our portal or through an Infoblox API. The solution provides the ability to apply information from multiple sources on an individual indicator, including antivirus analysis, domain reputation score, passive DNS, and "who is' information, to name just a few.

Mining valuable historical DNS data for security and troubleshooting—DNS, DHCP, and IPAM (DDI) data is a gold mine that your organization can use for forensics and for enhancing security operations. DDI data reveals associations between devices and users, the destinations users visit in a specific period, and which assets in your network are most in need of protection. Through the Infoblox solution, your security operations teams can determine the scope of a security incident, or automate correlation of network context and data with security events (Fig 5).

Conclusion

Infoblox solutions enable your organization to bring security, reliability and automation to the next level by tightly integrating networking and security architectures. It provides extensive threat intelligence; the industry's broadest set of API vendor integrations; and centralized visibility across extended third-party network infrastructure. It empowers security practitioners to mitigating DNS-based threats rapidly and efficiently using signature, reputation and behavioral analytics, and by automatically sharing threat event information throughout the cybersecurity ecosystem.

Learn more about the solution at https://www.infoblox.com/solutions/network-security/



RESULT: Single-source of TI management • Faster triage • Threat prioritization

Figure 4: Leveraging threat intelligence across entire security infrastructure

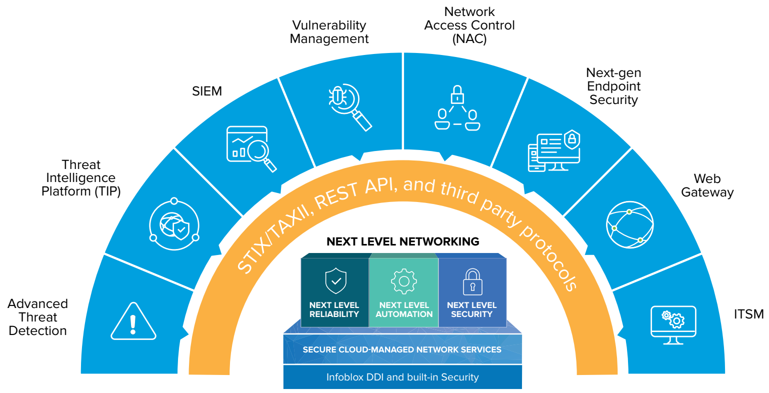

Advanced Threat Detection
Threat Intelligence Platform (TIP)
SIEM
Vulnerability Management
Network Access Control (NAC)
Next-gen Endpoint Security
Web Gateway
ITSM
STIX/TAXII, REST API, and third party protocols
NEXT LEVEL NETWORKING
NEXT LEVEL RELIABILITY
NEXT LEVEL AUTOMATION
NEXT LEVEL SECURITY
SECURE CLOUD-MANAGED NETWORK SERVICES
Infoblox DDI and built-in Security

Figure 5: Accelerating incident handling and response with Infoblox Next Level Automation

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