Infoblox
CONTROL YOUR NETWORK

Context-Aware Security from the Core

SOLUTION NOTE

Summary

Today's networks are constantly evolving, getting more complex and subject to frequent paradigm shifts. From hyperconnectivity with more than 21 billion connected devices expected by 2020[1] that are increasing the attack surface, to transformational shifts in deployment models such as hybrid cloud and SDN driving complexity, to business demands for 24x7x365 digital presence—the digital transformation is happening faster than you think. This complexity along with the constantly evolving nature of threats is leading to more breaches, attacks, longer times to resolve incidents, and increased risk to your business. What's needed are solutions that work together to protect your infrastructure, your users, and your data, provide visibility, and help resolve threats faster. These solutions must reduce your day-to-day operational load, not add to it. Infoblox solutions for security address these challenges with actionable intelligence and context-aware security delivered form the core of your network.

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:

- 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
- No protection against DNS-based data exfiltration, command-and-control callbacks, DDoS attacks on DNS servers

SANS, 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 tops the list. At the end of the day, you can't protect what you can't see.

The other gap in security is DNS—the critical yet vulnerable asset. Frankly, every part of your network, which in the digital era means every part of your business, is driven by DNS. Any communication, access to an application or service, or transaction from a customer around ecommerce in some form or fashion is going to involve your DNS infrastructure. Hackers have figured this out. Whether DNS is used to try and map out your network, plan an attack, or have botnets or malware communicate to C&C servers, DNS becomes just as critical to that hacker as it is to your business.

1. Gartner report: http://www.gartner.com/newsroom/id/3165317

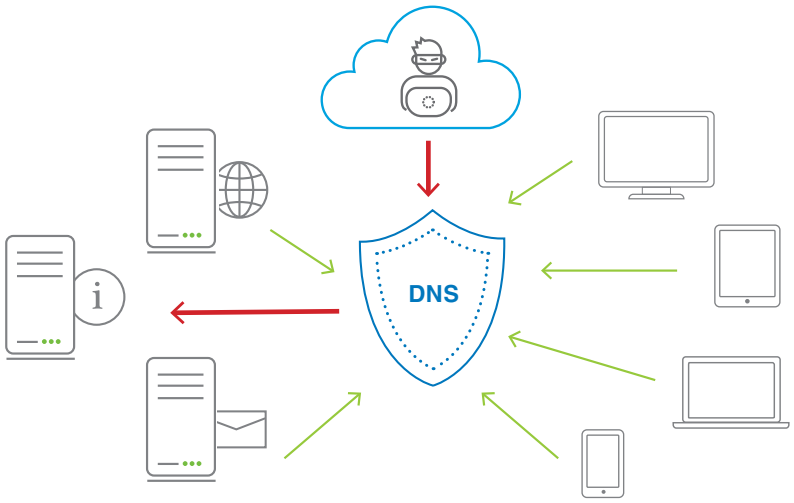


Figure 1: DNS—the critical yet vulnerable asset

Approach to Context-Aware Security

There are three aspects in security that all organizations should consider in order to close the security gaps identified above:

1. **Infrastructure protection** for better application and service availability
2. **Data protection and malware mitigation** for protecting devices and data
3. **Threat containment and operations** for better efficiency and optimization of security operations

Figure 2: Three aspects of security

Infoblox
CONTROL YOUR NETWORK

Context-Aware Security from the Core

SOLUTION NOTE

Infrastructure Protection

Any solution that offers infrastructure protection must help ensure application and service availability. It should include ability to protect critical network elements against a wide range of attacks, automatically discover non-compliant and vulnerable network devices, and provide visibility into your physical and virtual network.

Infoblox's solution for infrastructure protection provides the following:

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

- **Detection of vulnerable devices**—The solution has the ability to easily identify new devices as soon as they join the network and non-compliant devices which could hide vulnerabilities. It 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 ensures application availability even under attack.

- **Automatic notification of network changes to the security ecosystem**—The solutions enriches your security infrastructure with intelligence including threat data and network changes. The notifications also include sharing attack event information with SIEMS and NACs via easy-to-consume APIs, syslog, and SNMP. For example, you can notify your vulnerability scanner when a virtual workload is spun up or when a new device joins the network to trigger scanning.

- **Centralized reporting for analysis and planning**—Infoblox provides detailed reporting that:
  - Harness rich network data to gain actionable insights for more effective planning and improving security
  - Monitor and analyze your network, devices, and applications
  - Provide details on attacks by severity, category, and time

Data Protection and Malware Mitigation

Malware uses DNS at various stages of the cyber kill chain to penetrate the network including infecting devices, propagating laterally, and exfiltrating data. In a recent survey by *SC Magazine*, 46% of respondents experienced DNS-based data exfiltration while 45% said they experienced DNS tunneling. 91% 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:

- A focus on DNS, a pathway that is often left open and under-protected and therefore exploited by malicious actors for C&C communication and data exfiltration
- Multi-pronged approach to threat detection to include reputation, signatures, and behavior
- Comprehensive visibility into the network

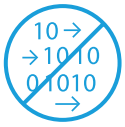
Infoblox
CONTROL YOUR NETWORK

Context-Aware Security from the Core

SOLUTION NOTE

Infoblox's solution for data protection and malware mitigation is designed to address the security gap around DNS. In addition to a focus on DNS, Infoblox's solution provides:

- **Disruption of the cyber kill chain to prevent malware proliferation.** The solution uses a combination of reputation, signature, and behavioral methods to detect threats. It proactively contains the spread of malware including phishing and ransomware; and stops command-and-control communications at the DNS choke point. It enforces policy using up-to-date threat intelligence that has been aggregated, verified, and curated by an in-house threat research team. 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 and for faster remediation. Available as an on-premises solution or as a service delivered from the cloud, the solution protects devices at headquarters, in remote offices/branch offices, or 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 could be low and slow and happen over longer periods of time.

- **Deep visibility into the network.** With Infoblox, you get end-to-end visibility into infected endpoints wherever they are and actionable context, including user name, MAC address, device type, and lease history to hasten remediation.

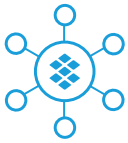
- **Unified reporting and mining valuable historical DNS data.** Infoblox provides detailed and centralized reporting for on-premises and cloud-delivered solutions that:
  - Harness rich network data to gain actionable insights for more effective planning and improving security
  - Monitor and analyze your network, devices, and applications
  - Provide details on malicious activities and infected devices

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 should bring 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.

- **Threat Intelligence optimization.** The solution involves policy enforcement using timely, consolidated, and high-quality threat intelligence that is aggregated from multiple sources, verified, and curated by an in-house threat research team. It allows organizations to incorporate threat intelligence from multiple sources, eliminates conflicts, and distributes uniform threat intelligence to the existing security infrastructure, providing a single source of truth.

- **Security orchestration.** Security orchestration involves automatically sharing network events and indicators of compromise in real time with existing security tools such as next-gen endpoint protection (NGEP), next-gen firewalls (NGFW), network access control (NAC), vulnerability scanners, and SIEM for more effective and timely incident response. For example, when Infoblox detects DNS-based data exfiltration or malware from an infected host, it can automatically notify an endpoint security solution to clean or quarrantine the infected endpoint.



- **Rapid triage.** Infoblox helps security analysts and researchers investigate threats faster by providing a broad range of information and a single source of truth through our partners and marketplace. Infoblox intelligence provides timely context (including type of malware, domain registration information, associated campaigns) that threat analysts and incident responders can leverage, either through our portal or through Infoblox API. Infobloxs' solution provides the ability to gather information from multiple sources on an individual indicator, including antivirus analysis, domain reputation score, passive DNS, and who is information to name a few. This enables the security personnel to focus on the most critical indicators and ignore false positives, thereby freeing up the security personnel to take on other tasks.

- **Mining valuable historical DNS data for security and troubleshooting.** DNS, DHCP, and IPAM (DDI) data is a gold mine that can be used for forensics and security operations. DDI data provides information including association between devices and users, destinations visited in a specified period of time, and criticality of the assets in the network that need to be protected. Operations teams can determine scope of a security incident, or automate correlation of network context and data with security events.

Figure 3: Modern networks —agile and secure

Infoblox
CONTROL YOUR NETWORK

Context-Aware Security from the Core

SOLUTION NOTE

Summary

Infoblox security solutions combine the ability to protect infrastructure to ensure business continuity to protect the most critical assets of the organization—its data—preventing the spread of malware that can impact the integrity of the network and ensuring that the security infrastructure works seamlessly together to remediate threats faster. Infoblox does this by providing visibility into the extended network, mitigating DNS-based threats using a combination of signature, reputation, and behavioral methods, and providing uniform threat intelligence and valuable context from the core of the network.

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

About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com