Securing Your Business with DNS Servers That Protect Themselves

Infoblox
CONTROL YOUR NETWORK

Summary: The Infoblox DNS security product portfolio mitigates attacks on DNS/DHCP servers by intelligently recognizing various attack types and dropping attack traffic while responding only to legitimate queries. The products also disrupt advanced persistent threats (APTs) and malware that use DNS to communicate with malicious domains, and provide protection against data exfiltration via DNS. Infoblox External DNS Security, Infoblox Internal DNS Security, and Infoblox DNS Firewall use a secure platform and integrate with industry standard ecosystems to deliver comprehensive protection and response.

Built-in Protection for Your DNS Infrastructure

If your external Domain Name System (DNS) server goes down, your entire network is shut off from the Internet, so your business depends on having DNS servers that continue to respond to queries even when they are under attack. Neustar's annual DDoS report for 2015 estimates an average financial damage of as high as $100,000 per hour of outage. Companies that experience extended service disruptions lose revenue, customers, and brand value.

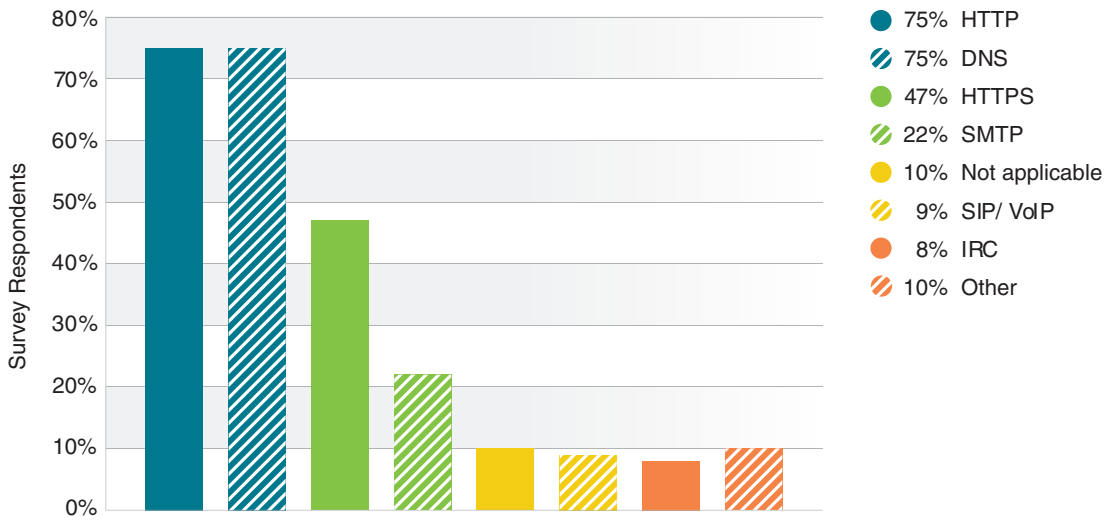
Unfortunately the DNS protocol—and the open-source software and commodity servers most organizations use to manage DNS services—have easily exploited vulnerabilities that defenses such as next-generation firewalls, secure web gateways, and incident detection and prevention systems do little to protect against. The only sure method of securing DNS servers is to build protection into the servers themselves.

As the leader in DNS, Infoblox has embraced this self-protecting server approach to deliver the most effective solution on the market for protecting your mission-critical DNS services from attack.

The Increasing Exploitation of DNS Vulnerability

In Arbor Networks' latest Worldwide Infrastructure Security Report, DNS is tied with HTTP as the top target of application-layer DDoS attacks. Moreover, the same report states that DNS is the number one vector used for amplification/reflection attacks.

Targets of Application-Layer Attacks



Source: Arbor Networks Inc.

Securing Your Business with DNS Servers That Protect Themselves

Infoblox
CONTROL YOUR NETWORK

Fighting a Battle on Two Fronts

Threats can come from the Internet or from within the firewalls inside an organization's network. Key threat vectors are: attacks on critical DNS and DHCP infrastructure, APTs and malware that use DNS as a communication path, and data exfiltration via DNS. To protect against the loss of trust, possible lawsuits, remediation costs, compliance penalties, and diminished revenue a successful attack can cause, DNS servers need to be protected from both outside-in and inside-out threats:

- To mitigate attacks on external authoritative servers, the servers themselves need to intelligently recognize various attack types and drop the attack traffic while responding to legitimate queries.
- To detect infrastructure attacks that affect internal DNS and DHCP servers and cause significant disruption such as downtime and cache and resource exhaustion, the recursive servers must be able to identify and drop these attacks as well as block traffic to misbehaving domains and servers that are usually set up as part of these attacks.
- To detect malware/APT infections before they spread or cause further damage, DNS servers can be leveraged to automatically block infected endpoints from communicating to malicious domains.
- To detect data exfiltration via a DNS tunnel or directly embedded in the DNS queries, the servers need intelligence to detect DNS tunneling attempts and detect any misuse of DNS queries.

At Infoblox we are well aware that to protect against DNS-based attacks, you must fight a two-front war. Based on this knowledge—and on our extensive experience helping our customers around the world manage and secure DNS services—we offer a complete solution that protects you on both fronts.

The Infoblox Solution

Infoblox's DNS security portfolio consists of Infoblox External DNS Security, which shields networks from cyberattacks; Internal DNS Security, which protects internal servers from attacks, APTs, malware, and data exfiltration; and Infoblox DNS Firewall, which blocks APT and malware communication from within the network. Running on purpose-built DNS appliances, these solutions effectively protect both your external and internal DNS and DHCP infrastructure. In addition, Infoblox security products leverage continual, automatic updates to protect against new and evolving attacks and emerging malicious domains and networks.

Protection from the Platform Up

Protection starts with the hardware—Infoblox purpose-built appliances hardened for security during the manufacturing process and certified for Common Criteria Level EAL-2. One-click enablement and automatic key refresh eliminate the usual complexity of implementing DNS Security (DNSSEC).

Guarding against Outside-In Attacks

Infoblox External DNS Security provides defense against the widest range of DNS-based attacks such as volumetric attacks, NXDOMAIN, exploits, and DNS hijacking attacks. This provides secure, highly available, and trustworthy DNS services even when your network is under attack. External DNS Security uses Infoblox Threat Adapt™ technology to keep the protection updated automatically against new and evolving threats as they emerge.

Through comprehensive reports, the solution gives you a centralized view of attacks that are happening on your network. These reports include details like number of events by category, rule, severity, member-trend analysis, and time-based analysis. Since every enterprise has different DNS traffic-flow patterns that can vary based on seasonality, time of day, or geography, Infoblox External DNS Security provides tunable traffic thresholds for fine-tuning protection parameters based on your unique traffic patterns.

Securing Your Business with DNS Servers That Protect Themselves

Infoblox
CONTROL YOUR NETWORK

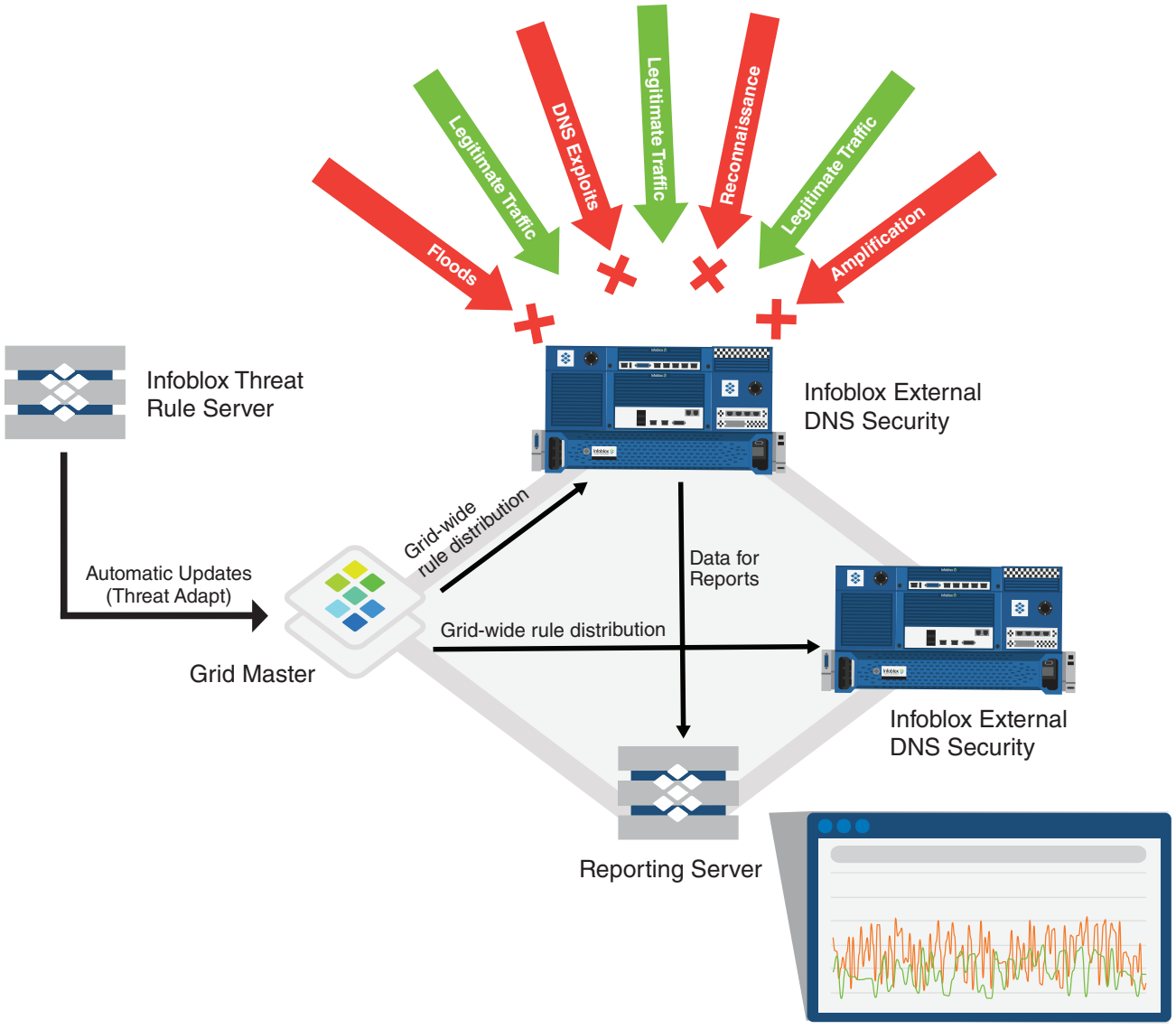


Figure 1: Infoblox External DNS Security provides unique protection against DNS-based attacks.

Guarding against Inside-out Attacks

Infoblox Internal DNS Security is an easy-to-deploy, appliance-based solution that protects mission-critical DNS and DHCP infrastructure from attacks, stops APT and malware communications, and prevents data exfiltration—without the need for endpoint agents or changes to your network architecture. It combines the Infoblox automated threat intelligence feed with enterprise-grade DNS to provide ongoing protection against new and evolving threats.

In addition to providing protection, Internal DNS Security also accelerates remediation by pinpointing infected devices and uses Identity Mapping to provide the user names associated with the infected devices.

Securing Your Business with DNS Servers That Protect Themselves

Infoblox
CONTROL YOUR NETWORK

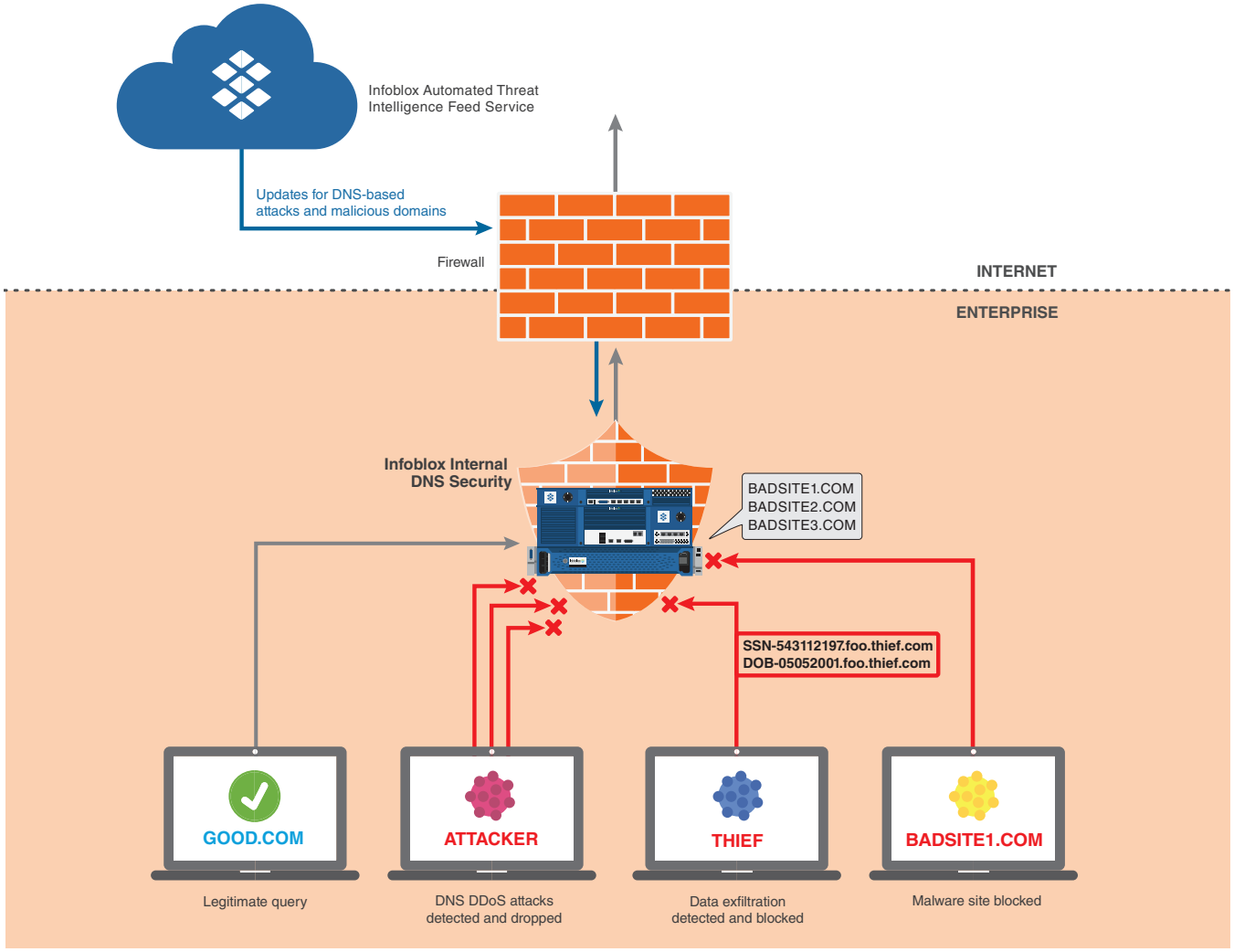


Figure 2: Infoblox Internal DNS Security provides protection for mission-critical DNS infrastructure from attacks, stops APT and malware communications, and prevents data exfiltration.

Protecting against APTs and Identifying Malicious Devices

The Infoblox DNS Firewall protects against APT-driven and malware-driven DNS queries to malicious domains by disrupting the ability of infected devices to communicate with botnets or command-and-control servers.

DNS Firewall uses threat intelligence derived from internal and external sources. Infoblox provides threat intelligence on known malicious domains, IP addresses, and networks via a threat-update service that derives data from 39+ feed sources, both public and proprietary. In addition, DNS Firewall uses external threat intelligence, including from the FireEye NX series.

Just as Internal DNS Security does, DNS Firewall enables client IP-based policy enforcement to provide granular protection.

Securing Your Business with DNS Servers That Protect Themselves

Infoblox
CONTROL YOUR NETWORK

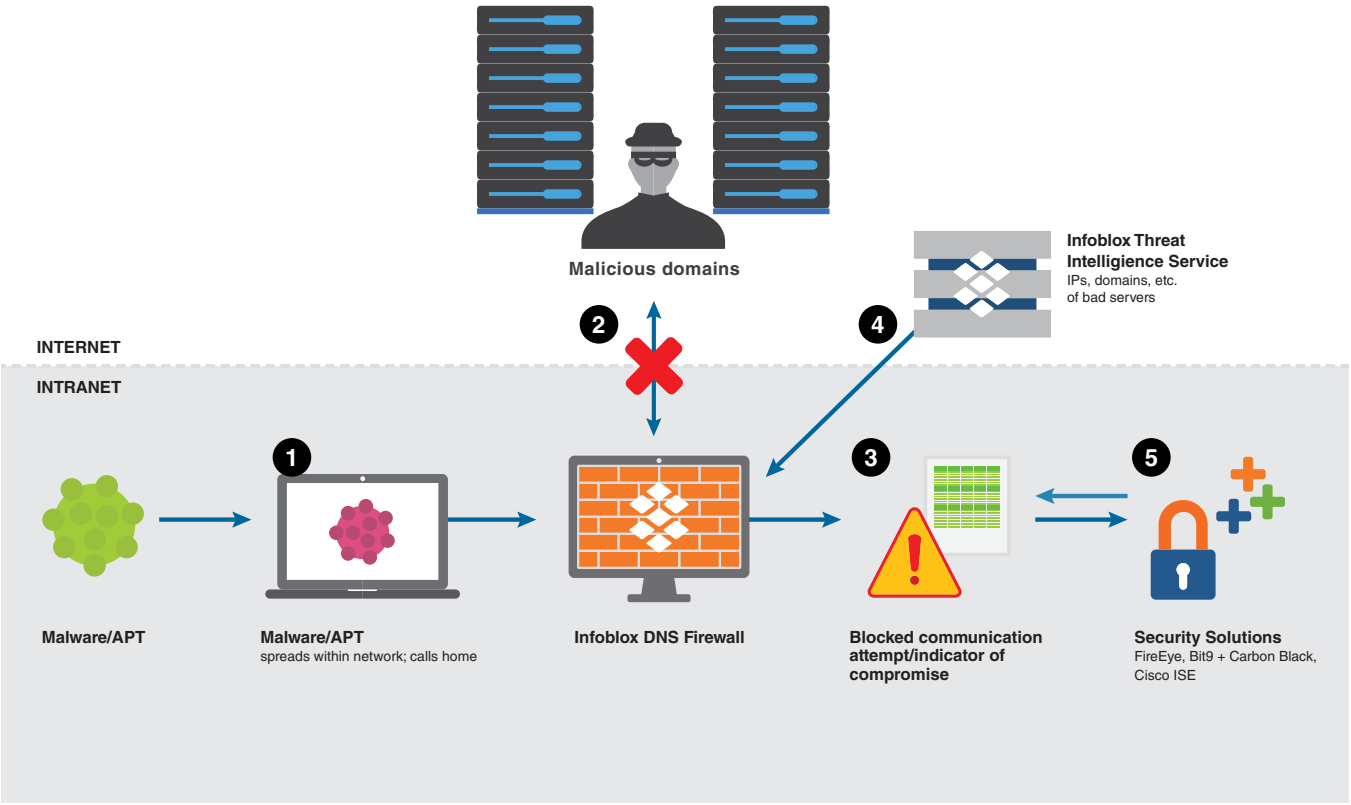


Figure 3: Infoblox DNS Firewall provides comprehensive protection against APTs and malware that use DNS to reach out to malicious domains.

Preventing Data Exfiltration via DNS

DNS is frequently used as a pathway for data exfiltration, because common security products do not inspect it. Infoblox DNS Threat Analytics is a unique technology that detects and automatically blocks data exfiltration via DNS without the need for endpoint agents or additional network infrastructure. It uses real-time streaming analytics of live DNS queries and machine learning to accurately detect presence of data in queries. When used as an option with the Infoblox DNS Firewall or Infoblox Internal DNS Security products, DNS Threat Analytics provides protection against both DNS tunneling and sophisticated data exfiltration techniques. *Infoblox is the only vendor to offer DNS infrastructure with built-in analytics for protection of your data.*

Automated Threat Response through Integrations

Security professionals are inundated with siloed technologies that help with one aspect of security detection or response—but these solutions don't work well together or communicate with each other. Infoblox helps automate and accelerate security response by integrating Infoblox DNS Firewall with leading security solutions such as FireEye and Bit9 + Carbon Black and exchanging valuable security event information with network access control (NAC) solutions such as Cisco Identity Services Engine (ISE), which, based on the event severity and the policies deployed, can quarantine an infected device.

Securing Your Business with DNS Servers That Protect Themselves

Infoblox
CONTROL YOUR NETWORK

Don’t Become the Next Highly Publicized Victim.

The impact of DNS-based attacks is apparent to anyone who follows IT-related news on line.

In 2014, American Express discovered a data breach that exposed names and account numbers for roughly 76,000 customers. JPMorgan Chase revealed that customer data had been exposed in a large-scale attack that targeted major financial institutions.In early 2015, America’s second largest health insurance company, Anthem, was also attacked, with data of about 80 million customers compromised and financial losses estimated at up to $100M USD. All of these attacks were publicized over multiple news outlets for several days.

Can your business afford the downtime, customer ire, lost revenue, and bad publicity that goes with this kind of disruption? If not, then contact us today to find out more about how you can defend against the most dangerous threats your network faces.

Infoblox Product Warranty and Services

Infoblox delivers critical network services that protect Domain Name System (DNS) infrastructure, automate cloud deployments, and increase the reliability of enterprise and service provider networks around the world. As the industry leader in DNS, DHCP, and IP address management, the category known as DDI, Infoblox (www.infoblox.com) reduces the risk and complexity of networking.

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