Summary: Infoblox External DNS Security defends against the widest range of DNS-based threats such as volumetric attacks, NXDOMAIN, exploits, and DNS hijacking. Unlike approaches that rely on infrastructure over-provisioning or simple response-rate limiting, External DNS Security intelligently detects and mitigates DNS attacks while responding only to legitimate queries. Moreover, Infoblox is the only vendor to provide the ability (Infoblox Threat Adapt™ technology) to automatically update its defenses against new and evolving threats as they emerge, without the need for patching.

Continuously Block New and Evolving DNS Attacks While Responding to Legitimate Requests

DNS servers are mission-critical infrastructure, and they have to continue to respond to queries even when they are under attack. If your external DNS server goes down, your entire network is shut off from the Internet. DNS is now tied with http as the number one targeted service for application-layer attacks and is the number one protocol used in reflection/amplification attacks according to leading security reports. The damage is costly, and Neustar estimates upward of $100,000 an hour as the cost resulting from a DDoS attack, not including customer defection and damage to brands.

Attackers look for the weakest links in your network, and the Domain Name System (DNS) protocol is easy to exploit. As a result, attacks designed to bring down DNS servers and consume network bandwidth—and to interfere with or shut down critical IT applications such as email, web sites, VoIP, and software as a service (SaaS)—are on the rise. Another common threat is DNS hijacking, which compromises the integrity of DNS.

As the leader in DNS, Infoblox delivers the widest range of protection on the market for guarding your mission-critical DNS services from attack.

The Threat Landscape

To underscore the seriousness of the danger DNS attacks present to your business, we’d like to highlight a few of the most common threats.

**DNS reflection/DrDos attacks** use third-party DNS servers (open resolvers) to propagate a DoS or DDoS attack.

**DNS amplification attacks** use specially crafted queries to create amplified responses to flood their victims with traffic.

**TCP, UDP, and ICMP floods** deny service on layer 3, bringing a network or service down by flooding with large volumes of traffic.

**DNS-based exploits** exploit vulnerabilities in the DNS software.

**Protocol anomalies** cause servers to crash by sending malformed packets and queries.

**Reconnaissance probes** are attempts to get information on the network environment before launching a large DDoS or other type of attack.

**DNS hijacking** attacks override a domain's registration information, usually at the domain's registrar, to point to a rogue DNS server.

**NXDOMAIN attacks** send a flood of queries to a DNS server to resolve non-existent domain names, causing the server's cache to fill up with NXDOMAIN results and slowing response time for legitimate requests.
Protect against the Widest Range of DNS Attacks

Many IT organizations today use load-balancers, IPS and firewall devices, generic DDoS protection solutions, and cloud-based solutions to try to counter DNS-based attacks. But all of these approaches are limited in what they can and cannot protect. Most of them are external solutions that are “bolted on” rather than built from the ground up to secure DNS against attacks. None of them can compare to the effectiveness of a purpose-built, DNS-specific defense solution.

The Power of Infoblox External DNS Security

External DNS Security solution components include:

- **Infoblox Advanced Appliance**: A DNS server that is purpose-built with security in mind. It has enhanced processing and dedicated compute for threat mitigation.

- **Infoblox External DNS Security Service**: The software, in conjunction with Threat Adapt technology, to provide protection against existing and new threats to the DNS server.

Figure 1: Infoblox External DNS Security provides unique protection against DNS-based attacks.
The Fortified DNS Server—the Best Protection against DNS-based Attacks
The Infoblox Advanced Appliance is a fortified DNS server with security built in. It leverages dedicated compute to filter out attacks before they reach the DNS server application.

Protection against the Widest Range of Attacks
Infoblox External DNS Security continuously monitors, detects, and drops all types of DNS attacks—including volumetric attacks and non-volumetric attacks such as exploits and DNS hijacking—while responding to legitimate queries. It also maintains DNS integrity, which can be compromised by DNS hijacking attacks.

Infoblox Threat Adapt Technology
Infoblox External DNS Security uses Infoblox Threat Adapt technology to keep the protection updated automatically against new and evolving threats as they emerge. Threat Adapt uses independent analysis and research on evolving attack techniques, including what we have seen in customer networks, to update protection, and automatically morphs protection to reflect DNS configuration changes.

Global Visibility of Attacks with Reporting
Through comprehensive reports and alerts, External DNS Security provides detailed views on attack points across the network and attack sources, providing the intelligence needed to take action. The reports can be accessed through the Infoblox Reporting Server.

Quick Deployment
External DNS Security is fast and easy to get up and running. Once installed, it starts blocking attacks immediately—even if an attack is already in progress.

Note: External DNS Security can also be deployed in a trial or proof-of-concept mode, either in line in monitor mode to detect and monitor attacks without actually blocking them, or in out of-band mode using port mirroring to detect attacks.

The Sooner You Act, the Safer Your Business Is
Security built in is better than security bolted on. There is no better place to defend against DNS-based attacks than from within the DNS servers they target. And the only solution built with this in mind is Infoblox External DNS Security.

Contact us today to find out more about the widest range of protection available for your DNS servers.

About Infoblox
Infoblox (NYSE:BLOX), headquartered in Santa Clara, California, delivers network control solutions, the fundamental technology that connects end users, devices, and networks. These solutions enable more than 7,000 enterprises and service providers around the world to transform, secure, and scale complex networks. Infoblox (www.infoblox.com) helps take the burden of complex network control out of human hands, reduce costs, and increase security, accuracy, and uptime.