Internal DNS Security

Key Features

- **Deep Inspection of DNS Traffic**
  Detects and drops various types of DNS attacks such as volumetric, exploits, and DNS tunneling; detects and blocks potential data exfiltration through DNS

- **Adaptive APT and Malware Protection**
  Uses unique threat intelligence feed to detect APTs and malware and disrupts APT and malware communication with external command-and-control servers

- **Automated Threat Intelligence Feed**
  Automatically updates protection based on research on evolving attacks, APTs, malware threats, and intelligence gained from customer deployments

- **Contextual Reporting**
  Provides a detailed view of attack points and patterns across the entire network and of APT- and malware-infected endpoints, with drill-down analytics

- **Hardware-accelerated Threat Mitigation**
  Delivers dedicated network packet-inspection hardware for threat mitigation to block attacks before they reach the DNS server application

- **Patented Infoblox Grid™**
  Automates all appliance configurations and updates, enabling rapid, automated security policy rollout to all Infoblox Advanced Appliances

Protect Data and Critical Network Infrastructure from Targeted Attacks

Today's targeted attacks pose threats to both data and infrastructure inside your enterprise. Internal DNS Security protects mission-critical DNS infrastructure from attacks, stops APTs and malware from using DNS, and prevents data exfiltration. Unlike alternative solutions, it combines enterprise-grade DNS with unique automated threat intelligence feed to provide ongoing protection against new and evolving threats.

The Challenge

More and more attacks are originating from inside the network and targeting internal DNS. These attacks could be volumetric DNS DDoS attacks that cause downtime, or they could be harder-to-detect low-volume attacks that stay under the radar but eventually cause resource exhaustion on internal DNS servers. Attacks lead to catastrophic system failure, business downtime, and lost productivity. APTs are increasingly becoming sophisticated and use DNS to communicate with command-and-control servers, making them harder to detect with traditional tools.

DNS is also a leading vector for data exfiltration. Data can be exfiltrated via DNS tunneling or within the DNS queries themselves. According to a leading IT security magazine, a recent survey of 300 enterprise IT decision makers showed that close to 46 percent experienced data exfiltration via DNS, and another 45 percent experienced DNS tunneling. When sensitive information is stolen, it causes financial and legal woes, not to mention the huge negative impact to brand.

The Infoblox Solution

DNS is a critical infrastructure element that has a unique position in the network. This makes it an optimal enforcement point for protection and response against threats like DNS attacks, APTs, malware, and data exfiltration.

Infoblox Internal DNS Security is an easy-to-deploy, appliance-based solution that protects mission-critical DNS 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.

Resilient Network Infrastructure

Internal DNS Security continuously monitors, detects, and drops internal DNS attacks such as DNS DDoS, exploits, DNS tunneling, and cache poisoning. The solution uses hardware-accelerated threat mitigation that maintains service availability even under extreme attack.
Internal DNS Security

Protection against APTs and Malware
Internal DNS Security disrupts APT and malware communication with external command-and-control servers by intercepting DNS queries associated with malware. Internal DNS Security can work with third-party advanced threat detection technologies such as FireEye.

Protection against Data Exfiltration
Internal DNS Security prevents data exfiltration through DNS. It can detect and stop exfiltration of sensitive information via DNS tunneling or within the DNS queries themselves.

Automated Threat Intelligence Feed
Internal DNS Security uses Infoblox’s automated threat intelligence feed to keep your protection updated automatically against new and evolving DNS attacks, APTs, and malware as they emerge—without intervention, downtime, or patching.

Contextual Reporting
Through comprehensive reports, Internal DNS Security provides visibility into attack points and types and devices infected by APTs and malware with drill-down analytics, enabling timely and effective response to threats. The reports can be accessed through the Infoblox Reporting Server.

Solution Components

<table>
<thead>
<tr>
<th>Software</th>
<th>Advanced DNS attack protection, APT and malware protection, and data exfiltration protection Adapter for integration with FireEye NX Series included, allowing automatic response to FireEye-detected threats</th>
</tr>
</thead>
</table>
| Feeds and services                    | Infoblox automated threat intelligence feeds:  
  • DNS attack signature feeds  
  • APTs, and malware site feeds |
| Delivery option—hardware              | Infoblox Advanced Appliances with deep packet inspection hardware for line-rate protection against DNS DDoS attacks, vulnerabilities, and other threats. Models include PT-1400, PT-2200, and PT-4000. Refer to the hardware datasheet for specifications. |

Why Infoblox

- As the infrastructure provider of choice for enterprises, we develop solutions that are in a unique position in the network to protect against APTs, malware, and data exfiltration.
- Infoblox combines DNS protocol awareness and a threat feed to provide intelligent protection and response to threats.
- No endpoint software or network changes are needed for threat mitigation.

Why Infoblox

- As the infrastructure provider of choice for enterprises, we develop solutions that are in a unique position in the network to protect against APTs, malware, and data exfiltration.
- Infoblox combines DNS protocol awareness and a threat feed to provide intelligent protection and response to threats.
- No endpoint software or network changes are needed for threat mitigation.

No endpoint software or network changes are needed for threat mitigation.
Internal DNS Security

Infoblox Automated Threat Intelligence Feed Service

Updates for DNS-based attacks and malicious domains

INTERNET

ENTREPRISE

Infoblox Internal DNS Security

SSN-543112197.foo.thief.com
DOB-05052001.foo.thief.com
BADSITE1.COM
BADSITE2.COM
BADSITE3.COM

Figure 1: Infoblox Internal DNS Security with Infoblox Reporting Server
Delivery Options
Appliances come in three physical platforms. Choose the appliance that fits your network environment. They offer both AC and DC power supply options. The PT-4000 comes in 1 GigE and 10 GigE versions.

Next Steps
Internal DNS Security provides complete protection for your internal DNS servers and leverages Infoblox technology's unique place in the network as an enforcement point for protection against today's advanced targeted attacks.

Learn more at www.infoblox.com/InternalDNSSecurity.

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.