Infoblox
CONTROL YOUR NETWORK

DNS Firewall

DATASHEET

Key Features

- **Adaptive malware protection:** Detects and disrupts malware communications with command and control (C&C) servers and reduces exposure to data exfiltration
- **Automated threat intelligence feed:** Provides up-to-date protection with Infoblox Threat Intelligence Feed, which automatically updates RPZ policy
- **Active blocking of data exfiltration attempts when used with Infoblox Threat Insight:** Adds domain destinations to a blacklist as they are discovered and blocks communications
- **Infected device identification:** Leverages Infoblox DHCP fingerprinting to identify infected devices for remediation, reducing threat impact early in the cyber kill chain
- **Rich reporting to aid remediation:** Integrates with Infoblox Reporting and Analytics to provide top RPZ hits, top malicious hostnames, and users
- **Threat context:** Infoblox Security Portal includes a threat lookup tool search engine that provides actionable data on threat severity and confidence level plus threat context
- **Automated threat response through integration** with leading security solutions such as FireEye and Carbon Black and exchange of security event information with NAC solutions such as Cisco ISE

Infoblox DNS Firewall is the leading DNS-based network security solution which effectively contains and controls malware communications and prevents data exfiltration, thereby protecting your assets and business. It also provides insights on threats, helps isolate infected devices for remediation, and stays current with the evolving threat landscape through an automated threat intelligence feed.

The Challenge

Malware has become increasingly sophisticated and is circumventing traditional defenses. According to a recent security study, over 91% percent malware uses DNS to gain command and control, to exfiltrate data, and to redirect traffic. Traditional protection methods do not intercept DNS communications to malicious locations, so a DNS security layer is required.

The Infoblox Solution

Infoblox DNS Firewall is the leading DNS-based network security solution which contains and controls malware that uses DNS to communicate with C&Cs and botnets. DNS Firewall works by employing DNS Response Policy Zones (RPZs), automated threat intelligence, and the optional Infoblox Threat Insight to prevent data exfiltration. Also—collaborating with Infoblox DHCP for device fingerprinting, with Infoblox Identity Mapping for capturing the user name tied to an infected device, and with Infoblox IP address management—DNS Firewall provides valuable information to help pinpoint infected devices for remediation.

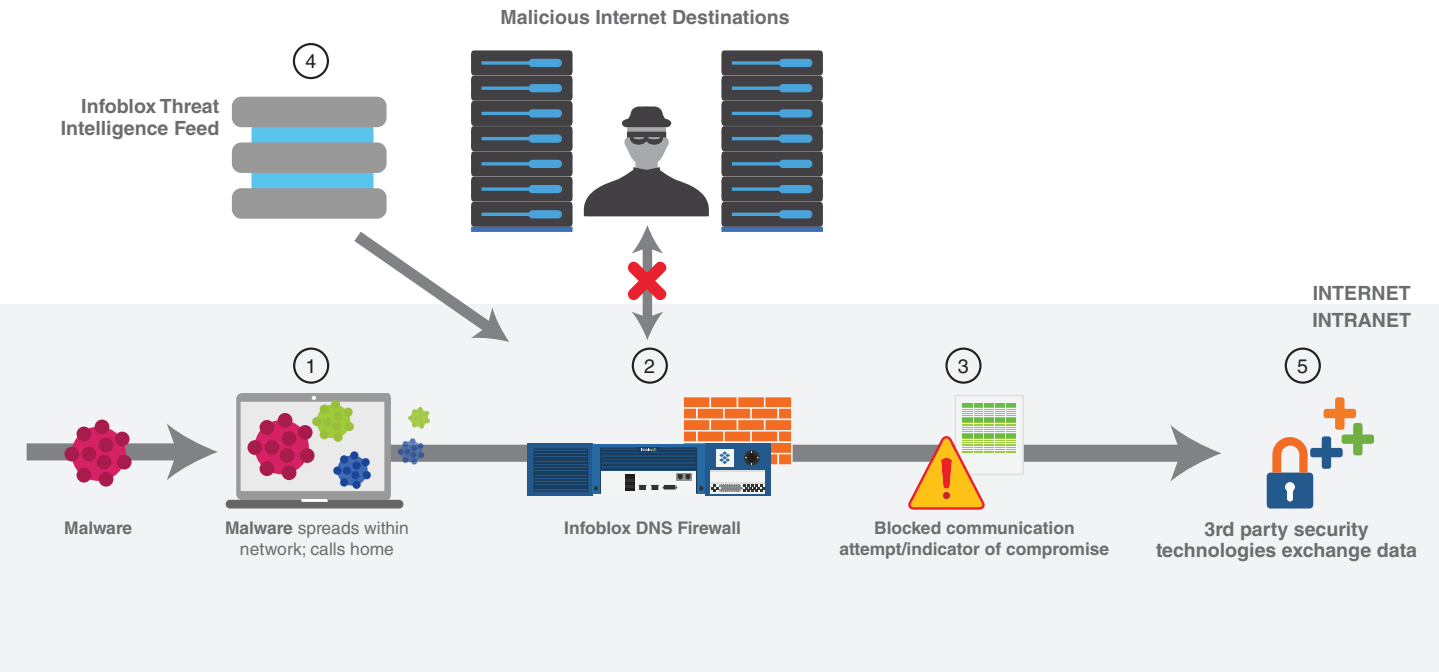
Furthermore, Infoblox is the industry's first and only DDI vendor to seamlessly integrate DNS Firewall with leading security solutions such as FireEye and Carbon Black and exchange valuable security event information with NAC solutions such as Cisco Identity Services Engine (ISE) to automate security response and quarantine infected endpoints.

Hardware requirements	One or more Infoblox Trinzic (physical) or vNIOS (virtual) appliances with DNS with recursion enabled. Trinzic models: • IB Series: IB-800, IB-1410, IB-2210, and IB-4000 • PT Series: PT-1400, PT-2200, and PT-4000
Software requirements	Infoblox ActiveTrust Standard Subscription License: • 1 license required per recursive/forwarder DNS appliance (one license per appliance, HA pair = 2 licenses) • Includes standard maintenance (Premium, L3+, etc.) • Includes Infoblox Threat Intelligence Feed
Optional services	• Infoblox Reporting and Analytics (appliance) • Infoblox Threat Insight (software license; requires Trinzic appliances: either IB-2210 or higher or PT-2200 or higher) • Infoblox Security Ecosystem Grid License: This enables integration of DNS Firewall with 3rd party security technologies (advanced malware prevention, SIEM, vulnerability management). The license is per NIOS Grid and cost varies by the total number of members on the Grid.

Infoblox
CONTROL YOUR NETWORK

DNS Firewall

DATASHEET



1 An infected device brought into the office. Malware spreads to other devices on network.

2 Malware makes a DNS query to find “home” (botnet / C&C). DNS Firewall looks at the DNS response and takes admin-defined action (disallows communication to malware site or redirects traffic to a landing page or “walled garden” site).

3 Pinpoint. Infoblox Reporting and Analytics lists DNS Firewall action as well as

- User name
- Device IP address
- Device MAC address
- Device type (DHCP fingerprint)
- Device host name
- Device lease history

4 Threat intelligence is regularly updated for up-to-date protection.

5 Additional threat intelligence from sources outside Infoblox can also be used by DNS Firewall and DNS Firewall can likewise share indicators of compromise with other security technologies for enhancing protection and easing incident response efforts.

Infoblox
CONTROL YOUR NETWORK

DNS Firewall

DATASHEET

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 malware.
- Infoblox combines DNS protocol awareness and a high quality malware threat feed to provide intelligent protection and response to threats, and being agentless, scales protection to all parts of the network.
- Infoblox delivers the first and only DNS infrastructure to use built-in analytics to detect and block data exfiltration. Now Infoblox can detect data embedded directly in DNS queries even when the most sophisticated methods are used.
- Integration with Carbon Black enables Infoblox customers to dramatically reduce endpoint response and remediation times associated with DNS Firewall alerts.
- First-to-market interoperability with Cisco pxGrid for seamless data exchange with Cisco ISE delivers improved threat visibility, richer threat mitigation options, and more efficient and effective incident response.

Key Benefits

Security administrators are under pressure to detect and respond to threats as quickly as possible. DNS Firewall aids this effort by proactively detecting and stopping malicious communications, providing insight into infected devices, and adapting protection as threats evolve.

Proactive

DNS Firewall is a purpose-built software application that leverages Infoblox DNS infrastructure that you already have rather than bolting on another security product. It interprets every DNS query, leverages automated threat intelligence to control device communications to known malicious destinations on the Internet, and instantly takes action based on RPZ policy. The optional Threat Insight updates DNS Firewall RPZ policy with domains associated with data exfiltration attempts–effectively preventing sensitive data loss. Furthermore, DNS Firewall performs real-time data sharing with leading security technologies to automatically respond and contain malware more quickly.

Insightful

By using an automated threat intelligence feed, DNS Firewall provides critical threat insight for easily prioritizing and taking action on malware infected devices. Through integration with Infoblox DHCP fingerprinting, IP address management, and Identity Mapping, DNS Firewall provides visibility into compromised devices, including device IP, MAC, OS, and type, and associated users, to help pinpoint infected devices for remediation. The optional Infoblox Reporting and Analytics provides a view of the top RPZ hits, malicious hostnames with which devices attempted to communicate, infected devices, users, and more to help your IT security team prioritize and quickly take action.

Adaptable

Utilizing a cloud-based threat intelligence feed that is regularly refreshed with data on newly discovered malicious Internet destinations, DNS Firewall keeps your network protection up-to-date.

About Infoblox

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