Key Features

- **Adaptive malware protection:** Detects and disrupts malware communications with command and control (C&C) servers and reduces exposure to data exfiltration
- **Automated and actionable 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 and analytics to aid remediation:** Integrates with Infoblox Reporting and Analytics to provide top RPZ hits, top malicious hostnames, and users
- **Actionable threat intelligence:** 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 actionable security event information with NAC solutions such as Cisco Identity Services Engine (ISE) to automate security response and quarantine infected endpoints.

Infoblox DNS Firewall is the leading DNS-based network security solution which effectively contains and controls malware communications and prevents data exfiltration, thereby securing 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), actionable 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 actionable 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 actionable 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 recursion enabled.

Trinzic models:
- IB Series: IB-800, IB-1400, IB-2200, IB-4000, and IB-4030
- PT Series: PT-1400/1405, PT-2200/2205, and PT-4000
- TE Series (physical and virtual appliances): TE-100, TE-810/815/820/825, TE-1410/1415/1420/1425, TE-2210/2215/2220/2225, and TR-4010/TR-4010-10GE

**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.
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 security and easing incident response efforts.
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

© 2017 Infoblox, Inc. All rights reserved. DS-0157-01 1706 - DNS Firewall