Infoblox
CONTROL YOUR NETWORK

Threat Insight

DATASHEET

Key Features

- **Real-time streaming analytics of live DNS queries:** Unique patented technology examines TXT and host.subdomain records in DNS queries, and analyzes queries and responses using entropy, lexical methods, time series, and other factors to detect data exfiltration.
- **Active blocking of data exfiltration attempts:** Adds destinations associated with data exfiltration to the blacklist and blocks communications with those domains; sends Grid-wide updates to all Infoblox members with DNS firewalling/ RPZ capability— thereby scaling protection.
- **Visibility:** Helps quickly pinpoint infected devices and/or rogue employees trying to steal data; provides identifying information such as user name (with Infoblox Identity Mapping), device IP and MAC address, and device type.
- **Automated security response through integrations:** Provides indicators of compromise (data exfiltration attempts) to leading endpoint solutions such as Carbon Black to accelerate and automate security response.

Prevent Data Exfiltration via DNS

Theft of sensitive data is one of the most serious risks to an enterprise. DNS is frequently used as a pathway for data exfiltration, because common security products do not inspect it. Infoblox Threat Insight detects and automatically blocks attempts to steal sensitive data via DNS without the need for endpoint agents or additional network infrastructure.

The Challenge

DNS is increasingly used as a pathway for data exfiltration either by malware-infected devices or by rogue employees. According to a recent DNS security survey, 46 percent of respondents experienced DNS exfiltration and 45 percent experienced DNS tunneling. DNS tunneling is the tunneling of IP protocol traffic through DNS port 53—which is often not even inspected by firewalls, even next-generation firewalls—most likely for purposes of data exfiltration. Malicious insiders either establish a DNS tunnel from within the network or encrypt and embed chunks of the data in DNS queries. Data is decrypted at the other end and put back together to get the valuable information.

The data that the hackers are after could be regulated data related to compliance standards, personally identifiable information (PII) such as social security numbers, or intellectual property that gives an organization a competitive advantage over its rivals. When sensitive information is stolen, it causes financial and legal woes, not to mention the huge negative impact to brand. According to a Ponemon Institute study in 2015, the average consolidated cost of a data breach is $3.8M, which includes investigative and forensic efforts and resolution and consequences of customer defection. This is an average—recent breaches have cost victims a lot more.

The Infoblox Solution

DNS is a critical Threat Insight element and can be used as an effective enforcement point against data exfiltration. Threat Insight is a unique patented 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. Available as an optional module with Infoblox DNS Firewall, Threat Insight 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.

Active Blocking of Data Exfiltration Attempts

Threat Insight automatically blocks communications to destinations associated with data exfiltration attempts by adding the destinations associated with data exfiltration to the blacklist in DNS Firewall. In addition, it scales enforcement to all parts of the network through Grid-wide update to all Infoblox members with DNS firewalling/RPZ capability.

Integrated into DNS

Unlike approaches that analyze log data in batches and after the compromise, Threat Insight is built directly into a DNS appliance, which is in the path of exfiltration, and provides real-time detection and blocking. There is no need for additional network infrastructure, agents, or new inline appliances.

Infoblox
CONTROL YOUR NETWORK

Threat Insight

DATASHEET

Why Infoblox

- This is the first and only DNS infrastructure to use built-in analytics to detect and block data exfiltration. Now Infoblox can detect even the most sophisticated methods that embed data directly in DNS queries.
- As the infrastructure provider of choice for enterprises, Infoblox provides solutions that are in a unique position in the network to protect against data exfiltration and have the ability to scale protection to all parts of the network.
- Infoblox can stop DNS-based exfiltration without endpoint software or additional network infrastructure changes. No additional box needs to be placed and configured in the network. The DNS server itself can be used for protection.

Visibility

Threat Insight provides visibility into infected devices or potential rogue employees trying to steal data. It provides identifying information such as user name (through Identity Mapping), device IP and MAC address, and device type. Reports can be accessed through the Infoblox Reporting and Analytics server.

Unique Patented Technology

Threat Insight is a patented technology that uses machine learning and performs real-time streaming analytics on live DNS queries to detect data exfiltration. It examines host.subdomain and TXT records in DNS queries and uses entropy, lexical analysis, time series, and other factors to determine presence of data in queries.

Automated Security Response with Integrations

When an endpoint is trying to exfiltrate data, DNS Firewall provides indicators of compromise to endpoint remediation solutions such as Carbon Black. Using this intelligence, Carbon Black automatically bans the malicious processes from future execution and quarantines the infected endpoint. This accelerates security response. Infoblox also exchanges security event information with Cisco Identity Services Engine (ISE) and provides robust restful APIs, which can be used to enrich your SIEM with additional contextual data.

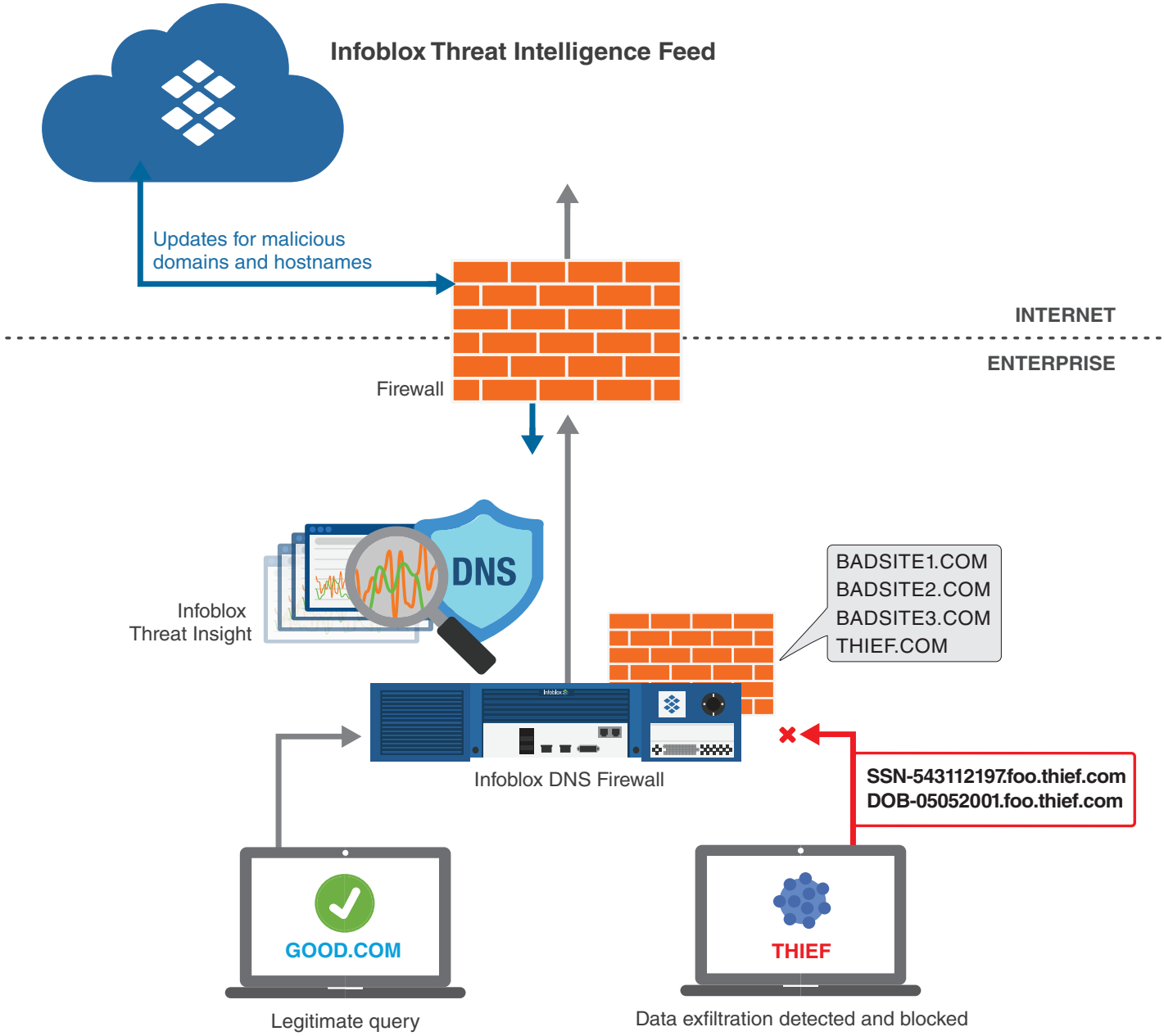
Solution Components

Software	Data exfiltration protection with Threat Insight
Other Products Needed with Threat Insight	To ensure not just detection of data exfiltration, but also enforcement of protection, Threat Insight must be deployed with Infoblox DNS Firewall. Threat Insight will create an RPZ entry in all Infoblox appliances running DNS Firewall, to include domains associated with data exfiltration.
Delivery Option: Hardware or Software	Threat Insight can run on physical or virtual Infoblox appliances. **Note:** this only works on the following Infoblox models: PT-1405, TE-1415/V1415, TE-1425/V1425, TE-2210/v2210, 2215/v2215, TE-2220/v2220, 2225/v2225, PT-2200, PT-2205, IB-4010/v4010, V4015, TE-V4010/V4015, PT-4000, IB-4030-DCAGRID-AC/DC, IB-4030-DCAGRID-T1-AC/DC, IB-4030-DCAGRID-T2-AC/DC, and IB-4030-DCAGRID-T3-AC/DC.

Infoblox
CONTROL YOUR NETWORK

Threat Insight

DATASHEET



Infoblox DNS Firewall with Threat Insight

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