DATASHEET

Threat Insight

PREVENT DATA EXFILTRATION VIA DNS

Theft of sensitive data is one of the most serious risks to an enterprise. One of the most commonly used pathways for data exfiltration is DNS. That's because it plays a central role in all IP-based communication and conventional security products are not designed to inspect it or adequately protect 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 exploited as an attack vector for data exfiltration either by malware-infected devices or by rogue employees. According to 2018 global DNS threat report, 33 percent of respondents experienced data theft via DNS and 20 percent experienced DNS tunneling. Used primarily for data exfiltration, DNS tunneling involves moving IP protocol traffic through DNS port 53—which firewalls, even next-generation firewalls, often do not inspect. 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 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. The theft of sensitive information can cause everything from financial and legal woes, to substantial and lasting brand damage.

According to a 2018 Ponemon Institute study, the average consolidated cost of a data breach is $3.86 million, which increased by 6.4 percent from 2017. Recent breaches have cost some victims much more.

THE INFOBLOX SOLUTION

Threat Insight uses patented technology that detects and automatically blocks data exfiltration via DNS without requiring endpoint agents or extra network infrastructure. It uses real-time streaming analytics of live DNS queries and machine learning to accurately detect the presence of potential data exfiltration activity within data queries. Threat Insight provides protection against data exfiltration that uses sophisticated DNS tunneling techniques as well as protection against DNSMessenger, DGA and fast flux.

KEY CAPABILITIES

Real-time streaming analytics of live DNS queries:
Using unique patented technology, examines TXT and host.subdomain records in DNS queries; 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; send Grid-wide updates to all Infoblox members with DNS firewalling/ response policy zone (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 addresses and device type

Automated security response through integrations:
Provides indicators of compromise (e.g., data exfiltration attempts) to leading endpoint solutions such as Carbon Black to accelerate and automate security responses

Active Blocking of Data Exfiltration Attempts

Threat Insight automatically blocks communications to destinations associated with data exfiltration attempts by adding the destinations to a blacklist for the RPZ-based mitigation. In addition, it scales enforcement to all parts of the network through the Infoblox Grid, which distributes updates to all Infoblox members with DNS firewall/RPZ capability.

Active Blocking of Data Exfiltration Attempts

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 addresses 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 the presence of suspicious data in queries.

Automated Security Response with Integrations

When an endpoint is trying to exfiltrate data, Infoblox 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. These actions accelerate security responses. Infoblox also exchanges security event information with Cisco Identity Services Engine (ISE) and provides robust restful APIs, which can enrich an enterprise's SIEM with additional contextual data.

Automated Security Response with Integrations

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 BloxOne™ Threat Defense. Threat Insight will create an RPZ entry in all Infoblox appliances running security.
Delivery Option: Hardware or Software	Threat Insight can run on physical or virtual Infoblox appliances. Note: It 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 THREAT INTELLIGENCE FEED

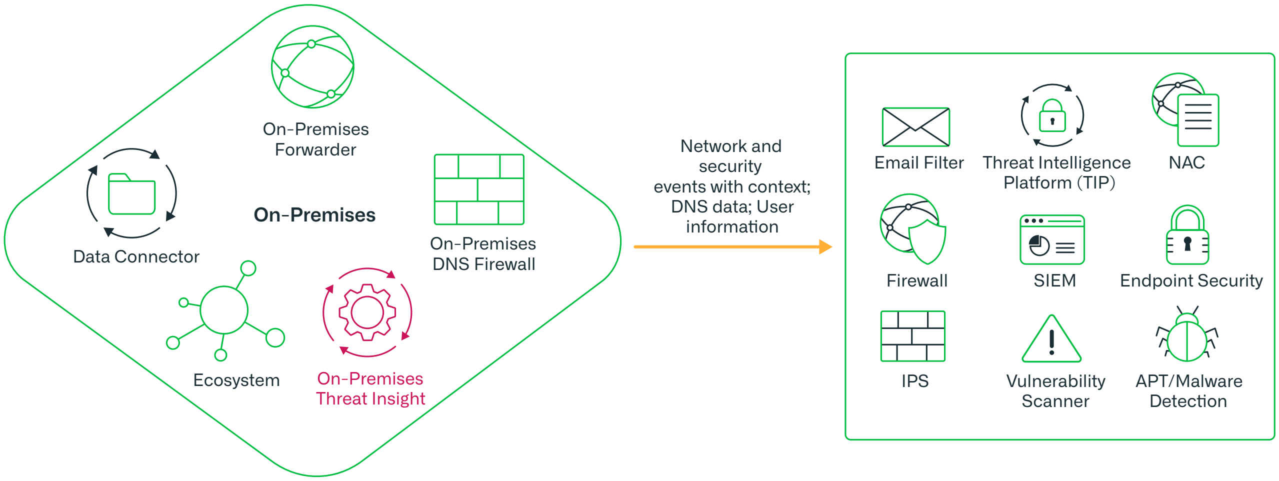

Figure 1: Infoblox Cloud Network Automation is deployed on fully virtualized Cloud Platform Appliances that runon ESXi, Hyper-V, or XenServer hypervisors

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com