infoblox

Threat Intel

SOLUTION NOTE

Threat Insight

Real Time Inspection of Enterprise Network DNS Traffic to Detect Unknown Threats

THE CHALLENGE

Data exfiltration: DNS is used for data exfiltration and malware command and control (C2). Compromised devices transmit DNS queries to an actor-controlled name server that embes data within the hostname, and they receive commands through the DNS responses. The exfiltrated data can include proprietary information, personally identifiable information (PII), and network information. The compromised device may receive commands to accomplish a range of tasks, including establishing additional communications channels and deleting information on the compromised device. The theft or destruction of sensitive information can cause everything from financial and legal woes to lasting brand damage.

Domain Generation Algorithms (DGAs): DGAs are algorithms encoded within certain types of malware. When an end host is infected with this malware, these algorithms are programmed to generate several pseudorandom domain names, and the malware cycles through them quickly to find one that it can use to communicate with the attacker's C2. This allows for the attacker to evade detection and blocking by traditional reputation-based solutions. DGAs are commonly used to distribute malware, adware, phishing campaigns etc.

Zero Day DNS™: Threat actors are increasingly targeting enterprise networks using freshly registered domains, often before it is even known that the domain has been created. Zero Day DNS creates a zero trust model for DNS that operates in near-real time to identify emerging threats at scale.

These scenarios highlight the need for near real-time detection of threats tailored to an individual network.

THE INFOBLOX SOLUTION

Threat Insight uses patented technology that inspects live DNS traffic from customer networks going to the Internet to detect and automatically block threats such as data exfiltration via DNS, DGAs and Zero Day DNS. Threat Insight also provides protection against fast flux and fileless malware(DNS messenger).

- Detects communications over DNS
- Detects transmission of data/unknown threats in DNS queries
- Is near real time
- Examines all DNS records (e.g., A, AAAA, CNAME, MX, NS, SOA, TXT, etc.)

KEY CAPABILITIES

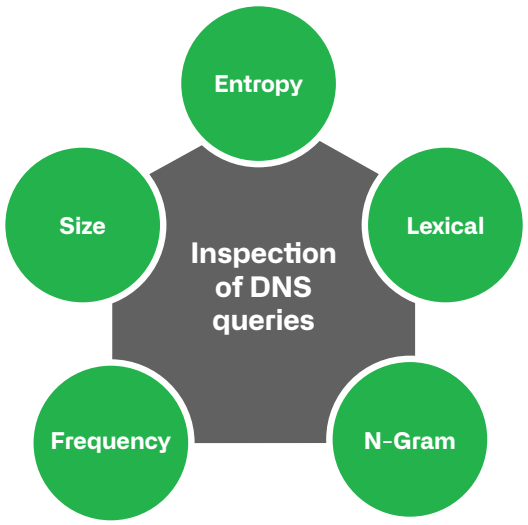
Real-time streaming inspection of enterprise DNS queries
Using unique patented technology, examines domain names and record content of DNS queries; analyzes queries and responses using entropy, lexical methods, time series and other factors to detect threats.

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/ response policy zone (RPZ) capability — thereby scaling protection.

Active blocking of Domain Generation Algorithms
Detects and blocks Domain Generation Algorithms that cannot otherwise be detected via reputation methods alone.

Block Emerging Threats with Zero Day DNS
Squash rapid fire attacks with a zero trust model for DNS that identifies and blocks newly created domains in near real time.

Note: Zero Day DNS detection is only available for BloxOne Threat Defense Advanced customers.



Unique Patented Technology
Threat Insight is a patented technology that uses machine learning and performs real-time streaming inspection on live DNS queries.

Software	Protection with Threat Insight
Other Products Needed with Threat Insight	To ensure not just the detection of these threats but also the enforcement of protection, Threat Insight must be deployed with BloxOne® Threat Defense. Threat Insight will create an RPZ entry for each of the threats.
Delivery Option: Hardware or Software or in the cloud	On-premises 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. However, there are limitations to the protection capabilities for on-premises Threat Insight. Threat Insight can also run in the Cloud for BloxOne Threat Defense Cloud and BloxOne Threat Defense Advanced customers, which offers maximum protection.

infoblox.

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

Version: 20240408v1