DATASHEET

Infoblox advanced DNS protection

Minimize business disruptions caused by DNS-based attacks

CHALLENGE: SERVICE DISRUPTIONS

DNS is foundational to every organization because it provides mission-critical network connectivity necessary to run a business. If your external DNS server goes down, your entire network is shut off from the Internet. DNS disruption interferes with or shuts down your critical IT applications, such as email, websites, VoIP and software as a service (SaaS). As a significant number of the workforce started working remotely in 2020, there was a huge spike in DDoS attacks. DNS continues to be a leading targeted service for DDoS, because it's critical to keeping a business online. In addition to loss of customer trust and confidence, successful DDoS attacks can cost an organization hundreds of thousands of dollars in lost revenue per month.

Infoblox delivers the widest range of protection on the market for guarding your vital DNS services from attack, ensuring the five nines availability your organization depends on. It provides centralized visibility into who is using the network, which devices they are on and details about the attack to ensure a rapid response.

SOLUTION: SAFEGUARD YOUR BUSINESS FROM DISRUPTIONS CAUSED BY DNS-BASED ATTACKS

With Infoblox Advanced DNS Protection (ADP), your business is always up and running, even under a DNS-based attack. Infoblox blocks the widest range of attacks, such as volumetric attacks, NXDOMAIN, exploits and DNS hijacking. Unlike approaches that rely on infrastructure overprovisioning or simple response-rate limiting, Advanced DNS Protection intelligently detects and mitigates DNS attacks while responding only to legitimate queries by using constantly updated threat intelligence, without the need to deploy security patches. With Infoblox, you can take network reliability to the next level by ensuring that your critical infrastructure—and your business—keep working at all times.

KEY FEATURES

Reduce Business Disruptions: Infoblox Advanced DNS Protection (ADP) continuously monitors, detects and stops all types of DNS attacks—including volumetric attacks non-volumetric attacks, such as DNS exploits and DNS hijacking—while responding to legitimate queries. It also maintains DNS integrity, which DNS hijacking attacks can compromise. Infoblox provides a solid foundation for security, enabling five nines availability for your network.

Adapt to Evolving Threats: Infoblox ADP uses Infoblox Threat Adapt™ technology to automatically update protection against new and evolving threats as they emerge. Threat Adapt applies independent analysis and research to evolving attack techniques, including what Infoblox threat specialists have seen in customer networks, to update protection. It automatically adapts protection to reflect DNS configuration changes.

ENABLING DOT AND DOH

Communication between the DNS client (stub) resolver and local DNS server (recursive resolver) is unencrypted. Unencrypted communications are subject to data snooping, interception and exfiltration -- otherwise known as DNS's "last mile" security problem. In response, the industry initiated DNS over TLS (DoT) and DNS over HTTPS (DoH) to provide privacy and encryption between DNS clients and external Internet DNS servers. Implementing encryption through the DNS resolver on your network allows you to remain in control of your user's network experience while providing security and content filtering per your security policy requirements. ADP optimizes DNS encryption for our high-performance packet engine called Fast Path so you can terminate encrypted DoT and DoH connections on your network.

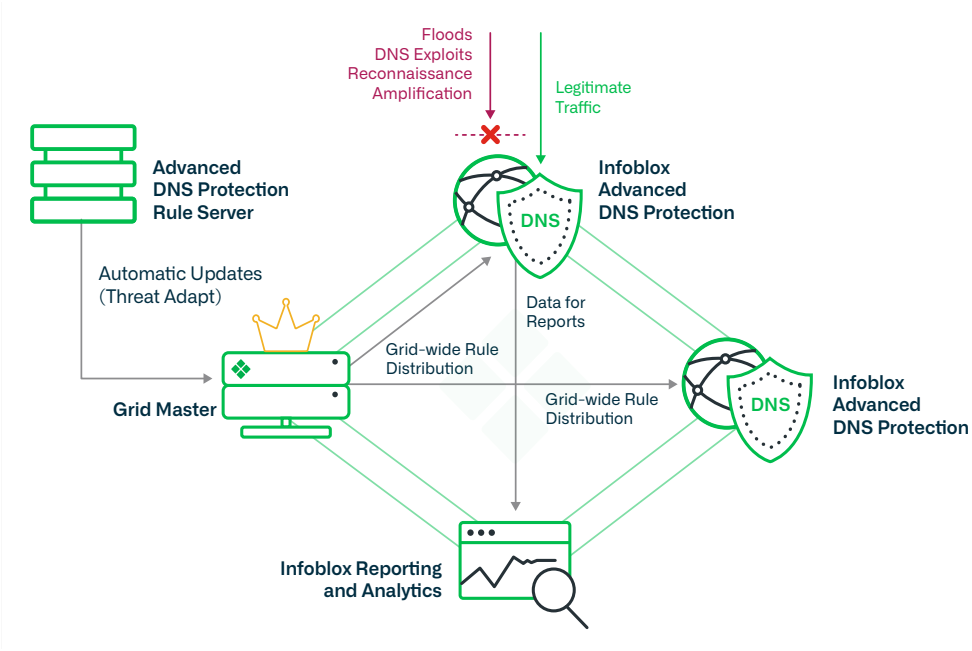

Figure 1: Infoblox Advanced DNS Protection provides a unique defense against DNS-based attacks.

KEY FEATURES (CONT'D.)

Gain Single-Pane-of-Glass Visibility:
With Infoblox, your organization can easily view prior or current DNS attacks and improve operational efficiency through our rapid threat remediation. Infoblox Advanced DNS Protection also provides a single view of attack points across the network and attack sources, supplying the intelligence necessary for threat management. It is integrated with our DNS solution.

Deploy Flexibly:
With Infoblox, you have the option of deploying as a subscription add-on to virtual and physical Trinzic appliances.

WHAT OUR CUSTOMERS SAY

"Service incidents from DDoS attacks have been cut in half, and customer complaints about lengthy page load times have been significantly reduced"

—VP of Customer Support, Large Service Provider

"I've been using Infoblox for DNS, DHCP, and IP address management for four years. It's a solid product. We've moved resources around because the product works so well. Our global footprint is managed by 1.5 FTE–and that's 65 devices."

—Manager of Global Infrastructure, Adobe

TABLE 1:
SUMMARY OF ATTACK TYPES THAT ADVANCED DNS PROTECTION (ADP) DEFENDS AGAINST

Attack Name	Type	How It Works
DNS reflection/DDoS attacks	Volumetric	Using third-party DNS servers (open resolvers) to propagate a DoS or DDoS attack
DNS amplification	Volumetric	Using a specially crafted query to create an amplified response to flood the victim with traffic
TCP/UDP/ICMP floods	Volumetric	Denial of service on layer 3 by bringing -a network or service down by flooding it with large amounts of traffic
NXDOMAIN	Volumetric	Flooding the DNS server with requests for non-existent domains, causing cache saturation and slower response time
Random sub-domain (slow drip attacks), domain lock-up attacks, phantom domain attacks	Low-volume stealth	Flooding the DNS server with requests for phantom or misbehaving domains that are set up as part of the attack, causing resource exhaustion, cache saturation, outbound query limit exhaustion and degraded performance
DNS-based exploits	Exploits	Attacks that exploit vulnerabilities in the DNS software
DNS cache poisoning	Exploits	Corruption of the DNS cache data with a rogue address
Protocol anomalies	Exploits	Causing the server to crash by sending malformed packets and queries
Reconnaissance	Exploits	Attempts by hackers to get information on the network environment before launching a large DDoS or other type of attack
DNS hijacking	Exploits	Attacks that override domain registration information to point to a rogue DNS server
Data exfiltration (using known tunnels)	Exploits	Attack involves tunneling another protocol through DNS port 53, which is allowed if the firewall is configured to carry non-DNS traffic—for the purposes of data exfiltration

APPLIANCE OPTIONS

Software ADP: Available on Physical and Virtual Platforms

Software ADP is a software add-on to Trinzic TE-815/825/1415/1425/ 2215/2225/4015/4025 appliances.

TE - 4015/4025

TE - 1415/1425

TE - 2215/2225

TE - 815/TE 825

Get Started on an Evaluation

60-day free software ADP evaluation with temporary license for customers will be made available through your Account Managers/SEs.

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