Infoblox
CONTROL YOUR NETWORK

Infoblox Advanced DNS Protection

DATASHEET

Key Features

- **Protection against the widest range of DNS-based attacks:** Continuously monitors, detects, and drops various types of DNS attacks, including volumetric and exploit attacks, and maintains DNS integrity.
- **Automatically update protection against evolving threats:** Uses Threat Adapt™ technology to deliver the latest threat intelligence and morph protection to reflect changes in DNS configuration—all without downtime or patching.
- **Global visibility of attacks:** Provides detailed central view of attack points and patterns across the entire network, leveraging Infoblox Reporting and Analytics.
- **Flexible deployment options:** Provides flexible deployment options as a subscription add-on to virtual and hardware Trinzic appliances or as specialized advanced appliances.
- **Enhanced processing for threat mitigation:** Features a dedicated compute (dedicated network packet inspection hardware) for threat mitigation blocks attacks before they reach the DNS server application.

Protection Against the Widest Range of External and Internal DNS Attacks

DNS: One of the Fastest Growing Attack Vectors

Security, availability, and integrity are the top three concerns regarding DNS infrastructure. Attackers seek weakest links and pressure points to harm or illegally exploit businesses, and since the Domain Name System (DNS) protocol is not protected by legacy security systems, it is easy to exploit. As a result, cyberattacks on DNS are on the rise.

DNS distributed denial of service (DDoS) attacks are designed to bring down external and internal DNS servers and consume network resources, affecting the availability of critical IT applications such as email, web sites, VoIP, and software as a service (SaaS). DNS is now the number one targeted service for application-layer attacks and is the number one protocol used in reflection/amplification attacks, according to leading security reports. The damage is costly, and Forrester Research estimates upward of $100,000 an hour as the cost resulting from a DDoS attack, not including customer defection and damage to brands.

Also, it is important to preserve the integrity and availability of the DNS to ensure pre-processing of DNS traffic to filter out attacks while responding to legitimate DNS requests in parallel.

Mitigating the Problem with Infoblox Advanced DNS Protection

Infoblox Advanced DNS Protection provides defense against the widest range of DNS-based attacks such as DNS DDoS, exploits, NXDOMAIN, DNS data exfiltration (through known tunnels), and DNS hijacking attacks. Unlike approaches that rely on infrastructure over-provisioning or simple response-rate limiting, Advanced DNS Protection intelligently detects and mitigates DNS attacks while responding only to legitimate queries. Moreover, it uses Infoblox Threat Adapt™ technology to automatically update its defense against new and evolving threats as they emerge to deliver Actionable Network Intelligence.

Solution Components

- **Infoblox Appliances**
  - Advanced PT Appliance: Special-purpose appliance that has dedicated processing power for the Advanced DNS Protection Service. The PT Appliance is a fortified DNS server with security built in. It leverages dedicated compute to filter out attacks before they reach the DNS server or application. These are DNS appliances only; they do not include DHCP and IPAM.
  - Trinzic hardware and virtual appliances: Consist of Trinzic TE-1410/1420/815/825/1415 appliances with ADP software subscription add-on. Virtual appliances are supported on VMWare and KVM.
- **Advanced DNS Protection Service:** The software plus Threat Adapt technology provides ongoing protection against existing and new threats to the DNS server.

Infoblox
CONTROL YOUR NETWORK

Infoblox Advanced DNS Protection

DATASHEET

Benefits

Prevent DNS Service Disruption

Advanced DNS Protection continuously monitors, detects, and drops various types of DNS attacks—including volumetric attacks such as floods and NXDOMAIN and non-volumetric attacks such as exploits and anomalies—while responding to legitimate queries. It maintains DNS integrity, which can be compromised by DNS hijacking attacks.

Adapt to Evolving Threats

Advanced DNS Protection uses Infoblox Threat Adapt technology to keep the protection updated automatically against new and evolving threats as they emerge and to deliver Actionable Network Intelligence. Threat Adapt uses independent analysis and research on evolving attack techniques, including what's seen in customer networks, to update protection. It also automatically morphs protection to reflect DNS configuration changes.

Utilize Data for Threat Management

Through comprehensive reports and alerts, Advanced DNS Protection features central and detailed views of attack points across the network and attack sources, providing the intelligence needed to take action. The reports can be accessed through Infoblox Reporting and Analytics.

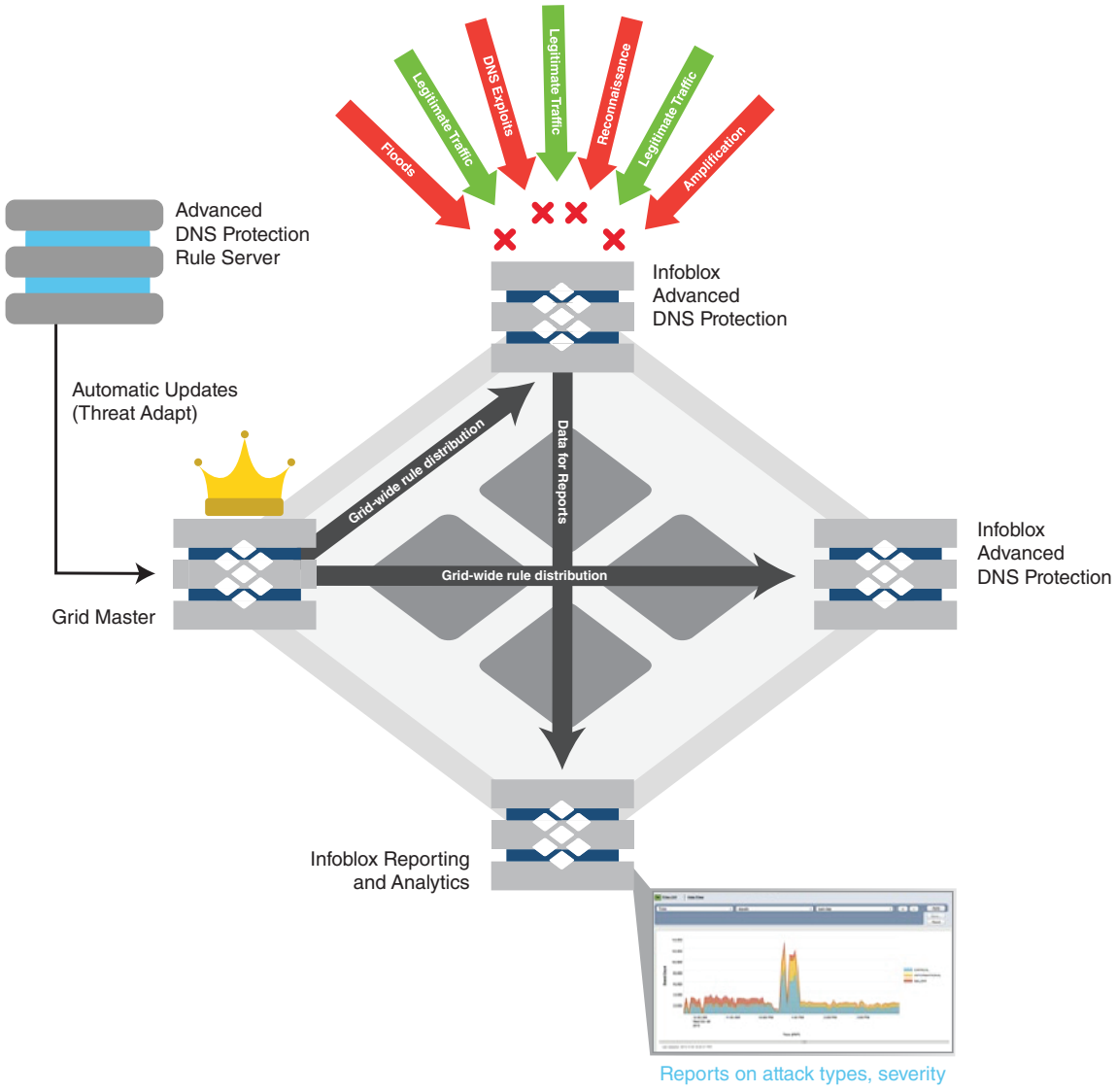
Flexible Deployment Options

It provides flexible deployment options as a subscription add-on to virtual and physical Trinzic appliances or as specialized advanced appliances.

Summary of Attack Types Advanced DNS Protection Protects Against

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



Infoblox
CONTROL YOUR NETWORK

Infoblox Advanced DNS Protection

DATASHEET

Delivery Options

PT Appliances Ship in Five Physical Platforms

The PT Appliances have next-generation programmable processors that provide dedicated compute for threat mitigation. They offer AC and DC power supply options.

Software ADP: Available on Physical and Virtual Platforms

It is a software add-on to Trinzic TE 2225/2215/1425/1415/825/815 or PT 1405/2205 physical and virtual appliances.

PT - 1400

PT - 1405

PT - 2200

PT - 2205

PT - 4000

TE - 815

or

TE - 825

TE - 1415

TE - 1425

TE - 2215

TE - 2225

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