**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). According to leading security reports, DNS is the second most targeted service for application-layer attacks, with 72 percent of enterprises impacted in 2018. Neustar estimates the cost resulting from a distributed denial of service (DDoS) attack carried out through DNS to be greater than $220,000 an hour, not including customer defection and damage to brands. Attackers look for the weakest links in your network. The DNS protocol is easy to exploit for DDoS or DNS hijacking, compromising the integrity of DNS.

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.

- **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 or as specialized advanced appliances.

- **Lower Your Costs**: Infoblox Software ADP leverages existing hardware, which means customers only need to upgrade software that runs on the hardware resulting in minimal incremental cost for upgrades.
Solution Components

Infoblox Appliances

- **Advanced PT Appliance**: special-purpose appliance that has dedicated processing power for Advanced DNS Protection. The PT Appliance is a fortified DNS server with security built in. It leverages dedicated compute resources to filter out attacks before they reach the DNS server or application. This is a DNS appliance only and does not include DHCP and IPAM.

- **Infoblox Trinzic Hardware and Virtual Appliances**: consist of existing Trinzic TE-1410/1420/2210/2220 appliances as well as newer Trinzic TE-815/825/1415/1425/2215/2225/4015/4025 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.

Get Started on an Evaluation

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

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>
<thead>
<tr>
<th>Attack Name</th>
<th>Type</th>
<th>How It Works</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS reflection/DDoS attacks</td>
<td>Volumetric</td>
<td>Using third-party DNS servers (open resolvers) to propagate a DoS or DDoS attack</td>
</tr>
<tr>
<td>DNS amplification</td>
<td>Volumetric</td>
<td>Using a specially crafted query to create an amplified response to flood the victim with traffic</td>
</tr>
<tr>
<td>TCP/UDP/ICMP floods</td>
<td>Volumetric</td>
<td>Denial of service on layer 3 by bringing a network or service down by flooding it with large amounts of traffic</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>Volumetric</td>
<td>Flooding the DNS server with requests for non-existent domains, causing cache saturation and slower response time</td>
</tr>
<tr>
<td>Random sub-domain (slow drip attacks), domain lock-up attacks, phantom</td>
<td>Low-volume</td>
<td>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</td>
</tr>
<tr>
<td>domain attacks</td>
<td>stealth</td>
<td></td>
</tr>
<tr>
<td>DNS-based exploits</td>
<td>Exploits</td>
<td>Attacks that exploit vulnerabilities in the DNS software</td>
</tr>
<tr>
<td>DNS cache poisoning</td>
<td>Exploits</td>
<td>Corruption of the DNS cache data with a rogue address</td>
</tr>
<tr>
<td>Protocol anomalies</td>
<td>Exploits</td>
<td>Causing the server to crash by sending malformed packets and queries</td>
</tr>
<tr>
<td>Reconnaissance</td>
<td>Exploits</td>
<td>Attempts by hackers to get information on the network environment before launching a large DDoS or other type of attack</td>
</tr>
<tr>
<td>DNS hijacking</td>
<td>Exploits</td>
<td>Attacks that override domain registration information to point to a rogue DNS server</td>
</tr>
<tr>
<td>Data exfiltration (using known tunnels)</td>
<td>Exploits</td>
<td>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</td>
</tr>
</tbody>
</table>
Appliance Options

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

Software ADP: Available on Physical and Virtual Platforms
Software ADP is a software add-on to Trinzic TE-1410/1420/2210/2220 appliances as well as newer Trinzic TE-815/825/1415/1425/2215/2225/4015/4025 appliances.

PT - 1405
PT - 2205
PT - 4000
TE - 4015/4025
TE - 2215/2225
TE - 1415/1425
TE - 2210/2220
TE - 1410/1420
TE - 815/TE 825