SOLUTION NOTE

INFOBLOX FOR PROTECTIVE DNS

OVERVIEW

With cybercrime expected to cost the world $10.5 trillion by 2025, and the increasing worry about stronger and more frequent cyberattacks, government bodies such as NCSC (National Cyber Security Centre) in the U.K. and CISA (Cybersecurity & Infrastructure Security Agency) in the US have provided strong guidelines around and in some cases mandated the use of Protective DNS Services (PDNS). PDNS promotes the use of DNS protocol and architecture as a security control point that analyzes DNS queries and takes action to mitigate threats such as malware C&C, ransomware, DGAs, phishing and more.

It's no surprise that governments are emphasizing the use of DNS for security. It is a well known fact that 90% of malware uses DNS to progress the attack, and using threat feeds and analytics at the DNS level can effectively block such activities early in the kill chain. Benefits of using a PDNS service include:

- Blocking malicious sites - PDNS prevents users and devices from accessing sites hosting malware, ransomware and other malicious content, and blocks C&C to contain active threats.
- Scale - A core capability of PDNS is the ability to use threat intelligence to allow or block DNS resolution and DNS can act upon millions of threat indicators, providing protection at scale.
- Visibility and Context - By using DNS logs, and additional context from related technologies such as DHCP and IP Address Management, security operations teams can get a lot more context on threats which helps reduce response times.
- Anywhere protection - PDNS can help protect not just assets and users within corporate networks but also remote/home workers and branch locations that don't have on-premises security stack protecting them.

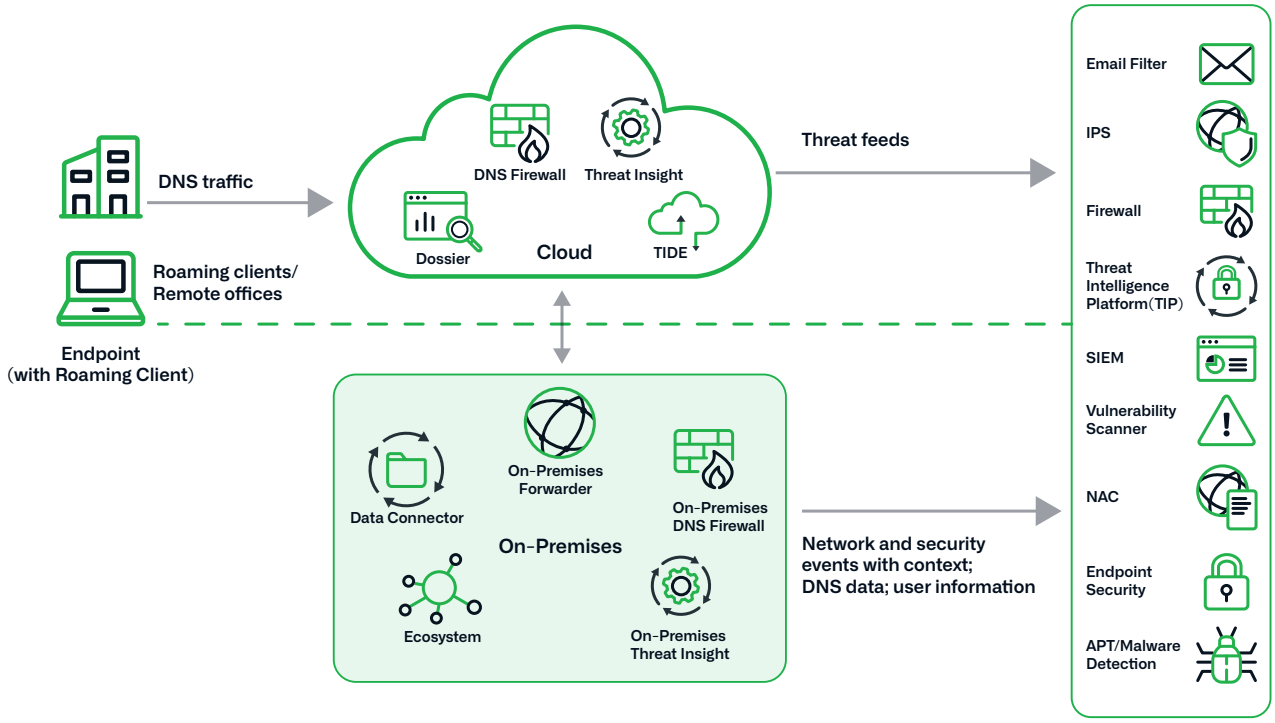
NCSC offers PDNS services free of charge to central government departments in the US, emergency services, NHS organizations, ministry of defense and local authorities. It also strongly recommends private industry to use a commercial PDNS provider for protection against cyberthreats. CISA in the US also outlined the benefits of using a PDNS service and assessed several commercial PDNS providers.

In addition to the US and the U.K., governments around the world are urging public and private companies in their countries to invest in cybersecurity to avoid expensive operational disruption and costs associated with security breaches. Saudi Arabia is one of those countries that has recognized the threat and has been gearing up to combat cyberattacks, ranking second on the Global Cybersecurity Index.

BLOXONE® THREAT DEFENSE AS A PDNS SOLUTION

BloxOne Threat Defense operates at the DNS level to see threats that other solutions miss and stops attacks earlier in the threat lifecycle. Through pervasive automation and ecosystem integrations, it drives efficiencies in SecOps, uplifts the effectiveness of the existing security stack, secures digital and work-from-anywhere efforts and lowers the total cost for cybersecurity.

	Key benefits
1	**Shifting Left of Protection.** BloxOne Threat Defense detects and blocks most malware earlier in the threat cycle, even before endpoint security, CASB, NGFW and NDR, because it sees the threat first as soon as a device requests a connection to an Internet location that could be malicious. This effectively "shifts left" protection, reducing security incident related endpoint downtime by 47% and sending fewer alerts to the SIEM due to early blocking. BloxOne Threat Defense detects/blocks a broad range of threats such as data exfiltration, DGAs, phishing, ransomware and botnets using an unparalleled mix of aggregated threat intelligence with patented machine learning models.
2	**Automating Threat Response.** BloxOne Threat Defense integrates with most security ecosystem tools, including ServiceNow, SIEM, SOAR, NAC and Vulnerability management, via RESTful APIs for automated and faster response to detected events, while making those tools more effective. Organizations get better ROI out of their existing investments.
3	**Reduction in SecOps effort through better context.** BloxOne Threat Defense can reduce security operations effort by 34% by providing critical telemetry on threats. BloxOne Threat Defense can pull contextual information from Infoblox on-prem or cloud DDI (DHCP/DNS/IP Address Management) for assessing threat exposure and severity, and tracking a threat back to the originating source on their network. The what, when and why of each threat is presented with deep insight which saves manual time and effort for SecOps as they investigate a threat. In addition, DNS based threat intelligence can be added to the ecosystem to enrich the data they already have.
4	**Protecting OT/IoT.** OT systems are often unpatched and run legacy applications. IoT devices are non-standard devices where endpoint security can't always be deployed. EDR/XDR solutions have limited or no visibility on OT/IoT. BloxOne Threat Defense protects OT/IoT systems using DNS-layer security to offer protection against malware and data theft.
5	**Asset and Application Discovery.** BloxOne Threat Defense provides asset and application discovery, and allows admins to proactively manage applications as approved/unapproved, helping to control shadow IT. This is done based on DNS communications without the need for agents and can be implemented quickly because no server/client applications need to be installed. In addition, the solution connects security events with user application usage and puts security events into context using DDI data.



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