INFOBLOX: UNLOCKING THE POWER OF DOMAIN NAME SYSTEM FOR SECURITY

EXECUTIVE SUMMARY

While multi-cloud deployments speed digital transformation, they can also introduce complexity for enterprises. These deployments can originate from a variety of scenarios, from acquisitions and vendor lock-in avoidance to tailored services built for specific use cases. Connecting the people, places, and things within modern hybrid work environments across an enterprise also expands attack surfaces inside and outside of network perimeter walls.

Bad actors are becoming more sophisticated, and an overwhelming majority of attacks leverage domain name system (DNS) to install malware, DNS tunneling to steal sensitive data, and lookalike domains to perpetuate phishing schemes. Furthermore, domain generation algorithms (DGAs) are often used to avoid typical threat intelligence. This attack infrastructure leverages the flexibility and scalability of application architectures. However, with the right set of tools and infrastructure-centric threat intelligence, enterprise network and security professionals can also use DNS to increase visibility, identify attacker infrastructure, and thwart attacks before they occur.

Most point security offerings are incomplete, creating blind spots that diminish visibility and allow attackers to exploit vulnerabilities. Enterprises require proactive, powerful security solutions that can reveal and eliminate cyberattacks before they occur while also mitigating and reducing the mean time to resolution of attacks that do materialize — all managed across platforms and domains, spanning on-premises, network edge to cloud. It's a tall order.

DNS Detection and Response has the potential to deliver on all fronts. After all, all communications start with a DNS query, and DNS is a critical service in every enterprise network. DNS also contains user and device access history information, serving as an effective visibility tool and control point to detect malicious traffic and block unwanted communications.

Moor Insights & Strategy believes that DNS Detection and Response delivered through Infoblox offers enterprises an optimal solution. It provides a proactive security capability that is built and optimized for the growing convergence of networking and security,

widespread adoption of SaaS applications that support distributed work and operational models and movement to the cloud for scale, cost, and resiliency considerations.

The Value of a Domain Name System Approach for Security

DNS is a fundamental element of network communications. The convergence of networking and security presents a unique opportunity to leverage the power of DNS given it converts domain names into IP addresses used for all communications over the internet. Access types include laptop PCs and tablets, mobile devices such as connected scanners and readers, IoT sensors, and OT and industrial control systems (ICS).

The variety and scale of IoT and OT devices communicating over the Internet include embedded operating systems and headless configurations, which create deployment and security management challenges. DNS, dynamic host configuration protocol (DHCP) and IP address management (IPAM) services can ultimately come together to provide a wholistic platform to solve the challenges of common network infrastructure complexities and eliminate outages. The integration of these features with cloud service provider (CSP) services also delivers true multi-cloud management and security across disparate cloud networking architectures. This portfolio of functionality simplifies management, integrating on-premises infrastructure across a single pane of glass, drastically improving threat visibility and hardening security.

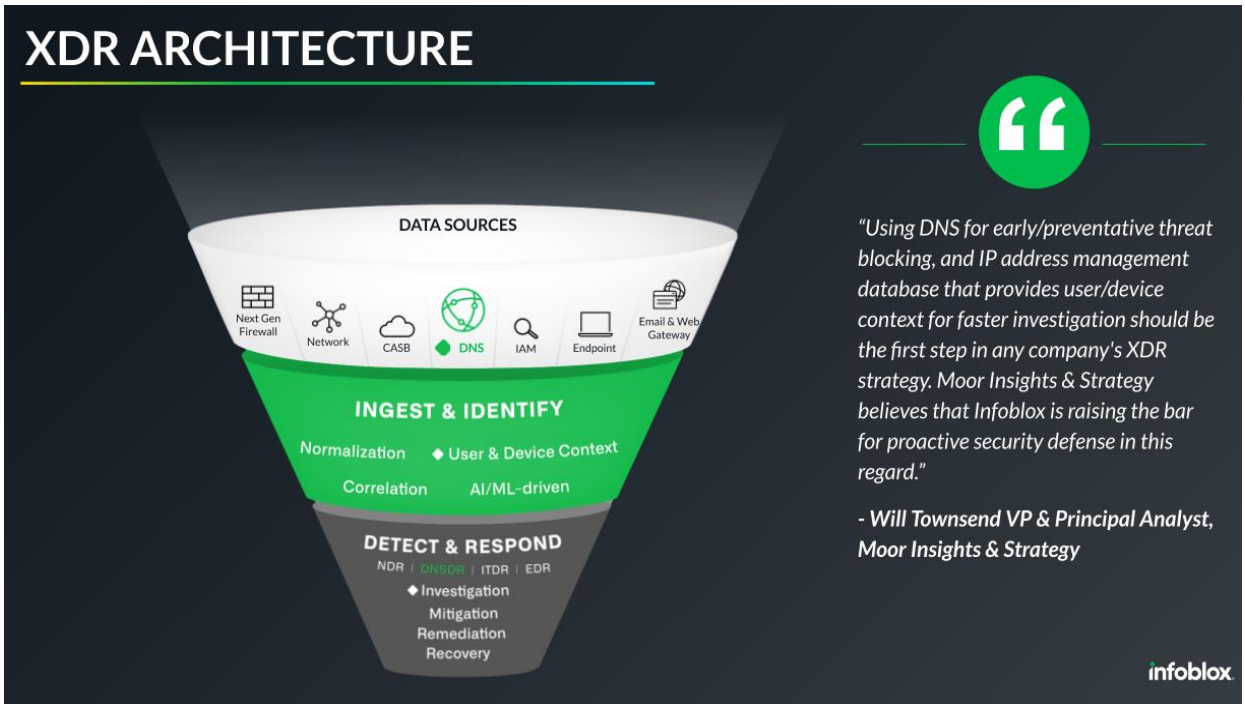
Organizations of all sizes are adopting a zero-trust approach to security based on the NIST cybersecurity framework. In this approach, no device is implicitly trusted, and, by default, access is authenticated to users and applications versus a flat network. DNS can be tightly integrated into zero-trust architectures to improve security resiliency because all cross-domain traffic requires resolution of a domain name with DNS services. DNS can effectively provide a secondary layer of coverage, further safeguarding organizations and ensuring the highest levels of business continuity.

Why Infoblox

Today, Infoblox says it is the ***only*** security infrastructure provider that offers a DNS Detection and Response (DNSDR) solution that marries a DNS approach to security that is an integral part of an overall extended detection and response (XDR) strategy. To this end, Infoblox claims that it can locate attacker infrastructure as it is created in near real-time, stop many threats before they materialize, and mitigate breaches faster with reduced mean time to resolution through DNS-tuned intelligence. This capability is

supported by the company's investment and development of unique threat research that marries data science and DNS expertise at scale to analyze suspicious domains, often months in advance of weaponization. Furthermore, Infoblox's threat intelligence platform supports robust threat intelligence data exchange (TIDE) and AI-driven analytics to speed evaluation and breach remediation.

FIGURE 1: INFOBLOX'S EXTENDED DETECTION AND RESPONSE



Source: Infoblox

Diving deeper, Infoblox's DNSDR solution, BloxOne Threat Defense, detects and prevents communication with malicious sites and domains that are controlled by attackers. It accomplishes this task using original DNS-centric threat intelligence and enforcement of response policies on suspected domains – leveraging contextual reporting, alerting, query monitoring, and logging of suspected endpoints. Additionally, Infoblox's tight integration between DNS and DHCP enables robust analytics capabilities. This includes facilitating the communication of detected security events, including user and device context, as well as infrastructure service and network device authentication, to compile actionable insights related to who, what, where, and when details.

BloxOne Threat Defense also integrates with other security ecosystem tools like NGFWs, SIEM/SOAR, Vuln scanners and IT services management (ITSM) platforms

such as ServiceNow. The end result is improved security efficacy and a high degree of automated response that has the potential to dramatically improve security defense outcomes.

Moor Insights & Strategy believes that Infoblox is raising the bar for proactive security defense. Its success is evidenced by 13,000 customer deployments including 70%+ of the Fortune 1000 over its 25-year history – with 25 million malicious and suspicious domains identified in the past year alone.

Call to Action

Bad actors are becoming more sophisticated, and an overwhelming majority of attacks leverage DNS schemes. However, DNS security can be deployed by enterprise network and security professionals to increase visibility, identify attacker infrastructure before weaponization and thwart attacks before they occur, all within zero-trust security frameworks.

Moor Insights & Strategy believes that DNSDR delivered through Infoblox is well positioned to deliver what enterprises require in a complete security solution. BloxOne Threat Defense detects and prevents communication with malicious sites and domains that are controlled by attackers, provides high fidelity threat intelligence and AI-powered analytics, and can be deployed at scale and managed easily on-premises and through multi-clouds with security ecosystem tool integration and a consolidated management console.

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR

Will Townsend, Vice President & Principal Analyst, Networking & Security Practices at Moor Insights & Strategy

PUBLISHER

Patrick Moorhead, Founder, President, & Chief Analyst at Moor Insights & Strategy

INQUIRIES

Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

DISCLOSURES

Infoblox commissioned this paper. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.