INFOBLOX

PREEMPTIVE SECURITY LEVERAGING THE POWER OF DNS

SUMMARY

Traditional reactive detect and respond methodologies to address cybersecurity needs are quickly becoming ineffective. Bad actors in growing numbers are weaponizing generative AI applications to dramatically improve the sophistication of cyberattacks for illicit ransomware gains. Furthermore, the use of emerging agentic AI frameworks by criminals to scale the speed and volume of threats is also troubling. Modern AI tools are fortifying cyber defense, but they represent a double-edged sword — also unlocking the ability for attackers to develop unique, single-use malware that renders reactive security solutions obsolete.

To address these challenges, a preemptive cybersecurity architecture to harden security is required. A design approach rooted in the Domain Name System is ideal. DNS serves as the underlying foundation of internet traffic and provides critical and deep visibility into emerging threats via IP address translation.

Based on Moor Insights & Strategy analysis, Infoblox appears well-positioned as a leader in protective DNS to provide a preemptive architecture that identifies threats and cyber-attacks before they occur. The company's approach is mature, built on investments in DNS-based security over three decades to provide a complete platform that addresses what is required for defense in the modern AI era.

THE POWER OF DNS

Modern network deployments are extraordinarily complex, all the more so because they employ disaggregated architectures. These often comprise unowned networks, including the internet and public mobile networks, enterprise networks both owned on-premises and in clouds, and private cellular networks deployed in operational technology environments. There are substantial benefits to this disaggregated approach, but it does create significant operational challenges, including visibility gaps, management that is often pinned to specific cloud service offerings, and the creation of a greater attack surface that is difficult to secure.

DNS-based security can provide an additional set of capabilities to help resolve these challenges. It can serve as the earliest point of prevention in an attack chain, given that

a DNS query is always triggered to a malicious domain. This occurs when a user clicks a link in a suspicious email or SMS message, or when a user scans a malicious QR code. Furthermore, when an attacker exploits a vulnerability to compromise an IT or OT system, or attempts to exfiltrate data, there is typically a DNS query to a command-and-control server that triggers a download of malware. Despite the use of modern AI-based tools by defenders to improve security controls, bad actors can also use them to facilitate prompt injections through DNS queries, whether automatically or via a user click.

The central role of DNS in these scenarios is why recent updates to the National Institute of Standards and Technology 800-81 cybersecurity framework identify DNS as an effective preemptive tool that should be considered within cybersecurity deployments. Growing adoption of DNS by public cloud providers to fortify security posture and control also reflects its value and strength in fortifying cyber defense. This is shown, for example, in Google's recent co-development efforts with Infoblox to provide Google Cloud's DNS Armor solution.

WHY INFOBLOX

We believe Infoblox continues to demonstrate leadership and depth in protective DNS security. Its threat intelligence telemetry tracks pre-attack activities, including bad actor infrastructure enablement. This is analogous to a pre-crime sensing capability popularized in science fiction yet translated to real-world cybersecurity. Through Infoblox Threat Intelligence, the company claims that it can root out over 80% of threats before an initial DNS query and provide over two months of preemptive protection before an attack — all with an 0.0002% false-positive rate. Additionally, in analyzing an average of 70 billion daily DNS events, Infoblox has been the first to expose many threat actors, including China-state sponsored Muddling Meerkat, which abused open resolvers with MX records to bypass traditional security measures, probe networks globally, and gain lateral movement.

The power of Infoblox's resolver capabilities also provides it with a foundation for deeper observability that has the power to fortify cyber defenses. The company possesses a demonstrated ability to enable complete visibility into every DNS connection from any device type — supporting a proven ability to detect attacks before they occur. Recent Infoblox innovations, including its Universal DDI Product Suite launched last year, Protection Before Impact, Security Workspace, Detection Mode, and Asset Insights integrations, combine to provide a complete platform-centric approach to

security across multiple domains. The company is also easing the friction associated with licensing its solutions, offering organizations a simplified procurement process that uses a token-based approach to deploy what is needed quickly and easily.

Stupp Bros. Finds Cybersecurity Strength with Infoblox

Founded more than 165 years ago, Stupp Bros. provides structural steel and professional services used in the engineering and construction of bridges, commercial facilities, and multi-family residential buildings throughout the United States. Over the past three decades, the company has modernized its operations through digital transformation for process optimization and scale. However, one of the most significant challenges that Stupp Bros. faces is the highly distributed nature of its employee base and the difficulty in issuing locked-down devices in the field.

To keep pace with the need to secure its endpoints, Stupp Bros. turned to Infoblox Threat Defense. In doing so, the company uses DNS security tools to proactively mitigate the risks of unsafe online behavior, automate web filtering, and significantly reduce the volume of virus alerts. Furthermore, Infoblox Threat Defense was initially stood up for the company in an astounding 15 minutes, pointing to its frictionless deployment capabilities and ability to easily integrate with Stupp Bros.' Microsoft Sentinel SIEM and SOAR platform for deep visibility and management across its entire digital estate.

Call to Action

Bad actors continue to improve the sophistication of their attacks, and reactive security tools used during this era of increased cyber threats are simply not enough to ensure the highest levels of protection. DNS continues to prove its value in this regard by providing preemptive security capabilities through the identification of potentially malicious domains that could become weaponized and used for illicit gain.

Moor Insights & Strategy believes that Infoblox has emerged as a leader in DNS security, supported by its battle-tested Threat Defense platform. Recent enhancements, including Protection Before Impact, Security Workspace, Detection Mode, and Asset Insights integrations, also provide organizations with a fortified and proactive security posture tool set to address today's dynamic threat landscape.

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR

Will Townsend, Vice President & Principal Analyst, Networking & Security Practices

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

This paper was commissioned by Infoblox. 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.