SOLUTION NOTE

TRANSFORM SECURITY EFFECTIVENESS WITH DNS DETECTION AND RESPONSE (DNSDR)

A proactive approach using DNS as part of your XDR framework

THE RAPIDLY EVOLVING THREAT LANDSCAPE

The cyber threat landscape is in a constant state of flux, with threats continuing to evolve at an unprecedented pace. As the digital transformation has permeated various industries, organizations find themselves grappling with an ever-expanding attack surface. This expansion ranges from the limitless realms of the cloud to the interconnected hybrid workforces, and extends to the burgeoning landscape of the Internet of Things. Each new touchpoint creates fresh pathways for malicious actors to exploit.

DNS frequently plays a pivotal role in the sequence of events which are part of a cyberattack, often referred to as the “attack chain”. Cyberattackers, along with the malicious software they deploy, frequently exploit DNS due to its critical function in network communications, employing dangerous techniques like domain shadowing and fast fluxing to conceal malicious domains and launch insidious attacks, unnoticed by defenders. Tactics and techniques like smishing that include very sophisticated look-alike domains and persistent low-profile infrastructure malware leveraging DNS beacons to establish C2 can easily escape detection of today’s modern security strategy.

Smishing involving lookalike domains and persistent low-profile infrastructure malware evade existing defenses

On an average, 200,000 new domains are created every day

There are now top-level domains that look like file extensions (ZIP, MOV), causing confusion for end users

Researchers flag around 80 million domains as malicious every six months

Digital initiatives make the problem worse:

- Multi-cloud adoption is accelerating at a fast pace, with over 73%[1] of surveyed enterprises adopting cloud platforms.
- IoT deployments are increasing and will double by 2030.
- AI is going mainstream and bad actors are using AI to design, scale and distribute sophisticated attacks quickly.

DNS FACTS & FIGURES

> *“Using secure DNS would reduce the ability for 92% of malware attacks both from command and control perspective, deploying malware on a given network.”*

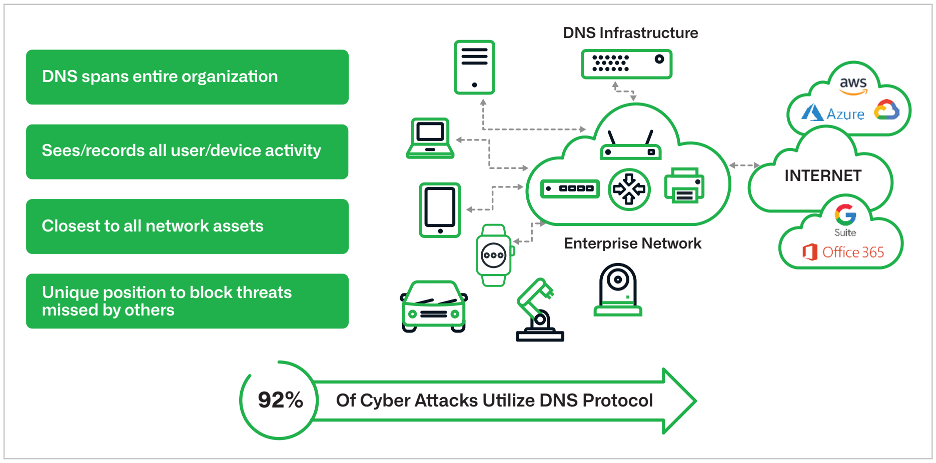
Anne Neuberger,
Director of the Cybersecurity Directorate,
National Security Agency (NSA)

[1] 20/20 Visibility Clarifies Network Security, Forrester, June 2022

This expansion of the attack surface increases the burden on security teams to maintain visibility and control of who and what is connected to their network. Armed with traditional security solutions that each only focus on a piece of the network, security teams face an impossible challenge of hunting threats and minimizing dwell time.

DNS IS FRONT AND CENTER FOR RISK REDUCTION

A Strategic Solution with a Unique View


DNS spans entire organization
Sees/records all user/device activity
Closest to all network assets
Unique position to block threats missed by others
DNS Infrastructure
Enterprise Network
INTERNET
aws
Azure
Suite
Office 365
92%
Of Cyber Attacks Utilize DNS Protocol

Graphic 1: DNS is Front and Center for Risk Reduction

In the ever-evolving landscape of cybersecurity, reliance on outdated strategies can result in the theft of confidential information, damage to reputation and brand, and financial loss. Organizations need to adopt a proactive approach that acknowledges the dynamic nature of threats and places real-time protection at its core. This is where DNSDR comes into play.

FROM REACTIVE TO PROACTIVE: LEVERAGING DNSDR BENEFITS

For several decades cybersecurity defenders have been reactive. They spent much of their time responding to threats, scrambling after attackers who exploited vulnerabilities before they could be patched. This reactive approach left organizations perpetually vulnerable and dependent on luck and outdated tools. DNSDR revolutionizes threat detection by shining a bright spotlight on the often overlooked battleground for the domain name system.

DNSDR capabilities represent a paradigm shift to the combined strategies your information technology (IT), network operations center (NOC), and security operations center (SOC) teams use to defend your enterprise. Combining DNSDR with other Extended Detection and Response (XDR) products strengthens your defense-in-depth strategy and automates the response throughout your ecosystem. DNSDR benefits include reducing the risk of a data breach, the associated potential financial loss and damage to your brand.

THE NEED FOR SPEED IS REAL

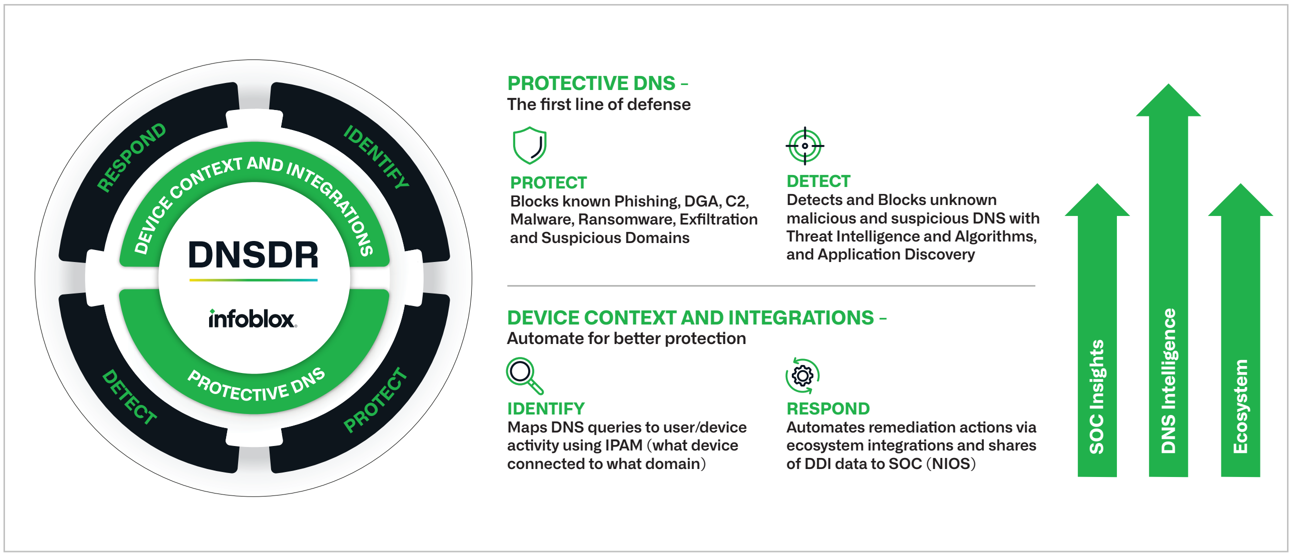
> *Defenders must move faster than attackers.*
>
> *In the context of cybersecurity, the goal is to execute decision-making processes faster than your attackers. This means that cyber defenders must identify the cyber attackers' infrastructure before they launch attacks.*
>
> *DNS threat intelligence, device/user context, automated response, and ecosystem integrations of Infoblox DNSDR complements the XDR framework and provides the agility and rapid decision-making you need to meet and defeat cyber threats."*

Anthony James
Vice President, Product Marketing
Infoblox, Inc.

DNSDR KEY CAPABILITIES

DNSDR encompasses several expanded and robust capabilities that help improve the resiliency and efficacy of your cyber defense ecosystem and deliver value.

DNS DETECTION AND RESPONSE



PROTECTIVE DNS –
The first line of defense

PROTECT
Blocks known Phishing, DGA, C2, Malware, Ransomware, Exfiltration and Suspicious Domains

DETECT
Detects and Blocks unknown malicious and suspicious DNS with Threat Intelligence and Algorithms, and Application Discovery

DEVICE CONTEXT AND INTEGRATIONS –
Automate for better protection

IDENTIFY
Maps DNS queries to user/device activity using IPAM (what device connected to what domain)

RESPOND
Automates remediation actions via ecosystem integrations and shares of DDI data to SOC (NIOS)

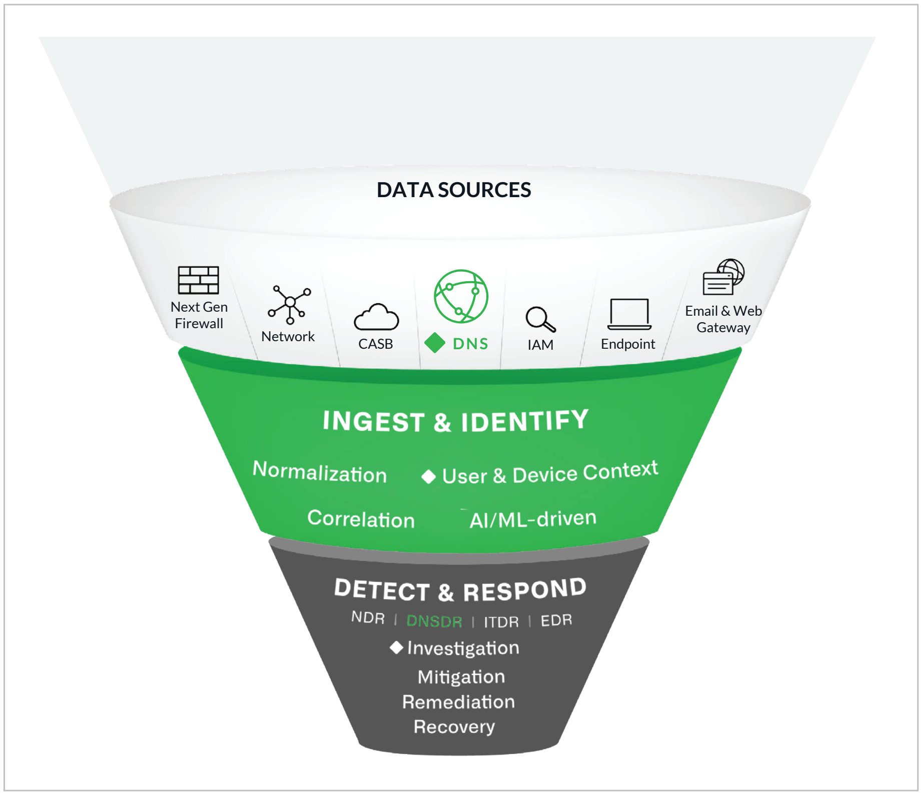
Graphic 2: INFOBLOX DNS Detection and Response

These are the five foundational aspects of DNSDR:

1. **Identify:** This maps DNS queries to user or device activity using IP Address Management (IPAM) and DNS-based application discovery. It helps in understanding the network landscape by identifying which users or devices are making which DNS queries. The benefit is that security operations teams can easily identify compromised assets in the network without having to go through multiple logs, enabling the benefit of faster triage and reducing MTTR.
2. **Protective DNS:** This is designed to block various types of cyber threats including phishing, ransomware, malware command and control (C&C), Domain Generation Algorithms (DGA), data exfiltration, and more. It also includes content filtering and DNSSEC to protect any system anywhere, including IoT and OT devices. The benefit is that protective DNS can help prevent malicious activities from affecting the network.
3. **Detect:** This detects and blocks unknown malicious DNS activities using DNS threat intelligence and AI/ML algorithms. It uses advanced techniques to identify potential threats that might not be caught by traditional security measures. The benefit is that proactive defense is now more strongly enabled against emerging threats.
4. **Respond:** This involves automated remediation via ecosystem integrations. It shares DDI data and triggers automatic response to events with Security Operations Center (SOC) tools. A quicker and more effective response to detected threats brings the benefit of potentially stopping the kill chain execution sooner, and reducing the risk and damage of a data breach.
5. **DNS Threat Intelligence:** Bringing together data science, DNS expertise and AI/ML capabilities, DNSDR uses **infrastructure centric threat intelligence** to identify attacker infrastructure and threat actors, as well as track them as they evolve. The benefit of blocking domains in “pre-crime” mode is that many attacks can be stopped before they are launched.

DNS WITHIN THE XDR ARCHITECTURE

At its core, XDR enhances security efficiency by consolidating control and visibility across various platforms, including endpoints, networks, and the cloud. This integration of data from disparate security solutions amplifies threat visibility, thereby accelerating the process of threat identification and response. This streamlined approach not only reduces the time taken to counteract an attack but also bolsters the overall security posture.



Graphic 3: INFOBLOX DNS Within XDR Architecture

DNSDR USE CASES BRING IMPORTANT BENEFITS

DNSDR, through its key use cases, offers a multitude of benefits across various domains. It plays a crucial role in mitigating the risk of cyber attacks that could potentially result in the loss of sensitive data, damage to brand reputation, and disruptions in revenue and operations. One of DNSDR's core capabilities is its ability to rapidly detect and interrupt a DNS-utilizing kill chain process, thereby averting potential harm. Additionally, DNSDR significantly cuts down the time and expenses involved in detecting, investigating, and comprehending new threats within the Security Operations Center (SOC). DNSDR use cases include:

1. **DNS as a Single Enterprise-Wide Control Point** to cover entire attack surface including on-premises, cloud, IoT/OT, remote workers and branch
2. **Block known bad traffic** using protective DNS capabilities to detect threats early and offload downstream security devices
3. **Monitor DNS for misuse** using streaming analytics for detecting data exfiltration and DGAs

> *"Planning a review of DNS threats and how to respond to them within a broader XDR framework should be a matter of 'when' rather than 'if'."*
>
> **HardenStanc**

> *"ZK Research believes that DNS security is the simplest and most effective starting point for any security strategy. As the leader in that area, Infoblox should be at the top of your list to unify networking and security and stop most malware before it becomes a problem."*
>
> **ZK Research**

4. **Identify attacker infrastructure** and block attacks pre-crime using infrastructure centric threat intelligence
5. **User and device attribution** to provide more than just the IP address of a compromised device, including device type, user name, network location and historical IPs
6. **Enrich security tools** with DNS data and automatically trigger response to events
7. **Digital brand protection** to identify lookalike domains and take down offending domains fast with domain mitigation service

LEARN MORE

To learn more about Infoblox DNSDR capabilities please visit our website. There are also available analyst reports[2,3] that covers DNSDR.

[2] https://www.hardenstance.com/wp-content/uploads/2023/07/HardenStance-Briefing-Wheres-DNS-in-the-XDR-Roadmap-FINAL.pdf

[3] https://insights.infoblox.com/resources-whitepaper/infoblox-whitepaper-transform-security-effectiveness-with-dns-detection-and-response

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

Version: 20240118v1