July 2023

Transform Security Effectiveness with

DNS DETECTION AND RESPONSE

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

INTRODUCTION: THE CHANGING THREAT LANDSCAPE REQUIRES A NEW APPROACH TO SECURITY

The threat landscape—which always has been complex—has evolved at breakneck speed. Short message service (SMS) phishing attacks ("smishing") are one example of threats that have increased in frequency recently. The Anti-Phishing Working Group (APWG) reports that phishing reached a record level in the third quarter of 2022. Look-alike domains are often used in phishing and spear-phishing attacks. In 2022, Chinese hackers used 42,000 imposter domains in a massive phishing attack campaign. Infoblox's research found that more than 1,600 domains contained a combination of corporate and multi-factor authentication (MFA) look-alike features. In these types of attacks and others, attackers often register domains several months in advance of being used. Therefore, there is a need for analytics and threat intelligence that proactively identify these emergent domains that could be used in future attacks.

Alongside security threats, the way we work has changed significantly, hastened by the pandemic. A look across the landscape shows a seismic shift.

Four factors will contribute to the need for enhanced security (Exhibit 1):

Hybrid work is now the norm. Despite some CEOs calling everyone back to the office, hybrid is the way forward. ZK Research forecasts that 90% of employees (more than 100 million in the United States and one billion worldwide) will work from home at least one day a week by 2025.

Cloud adoption is accelerating. ZK Research forecasts that the cloud market will grow from $200 billion in 2023 to $370 billion by 2028—a roughly 13% CAGR. Organizations are adopting a hybrid cloud scenario where they are moving some on-premises workloads to the cloud. In concert with that growth, the once-simple cloud model is evolving into multi-cloud and distributed cloud.

Internet of Things (IoT) deployments are increasing and will double by 2030. ZK Research forecasts that deployments will hit roughly 30 billion in seven years.

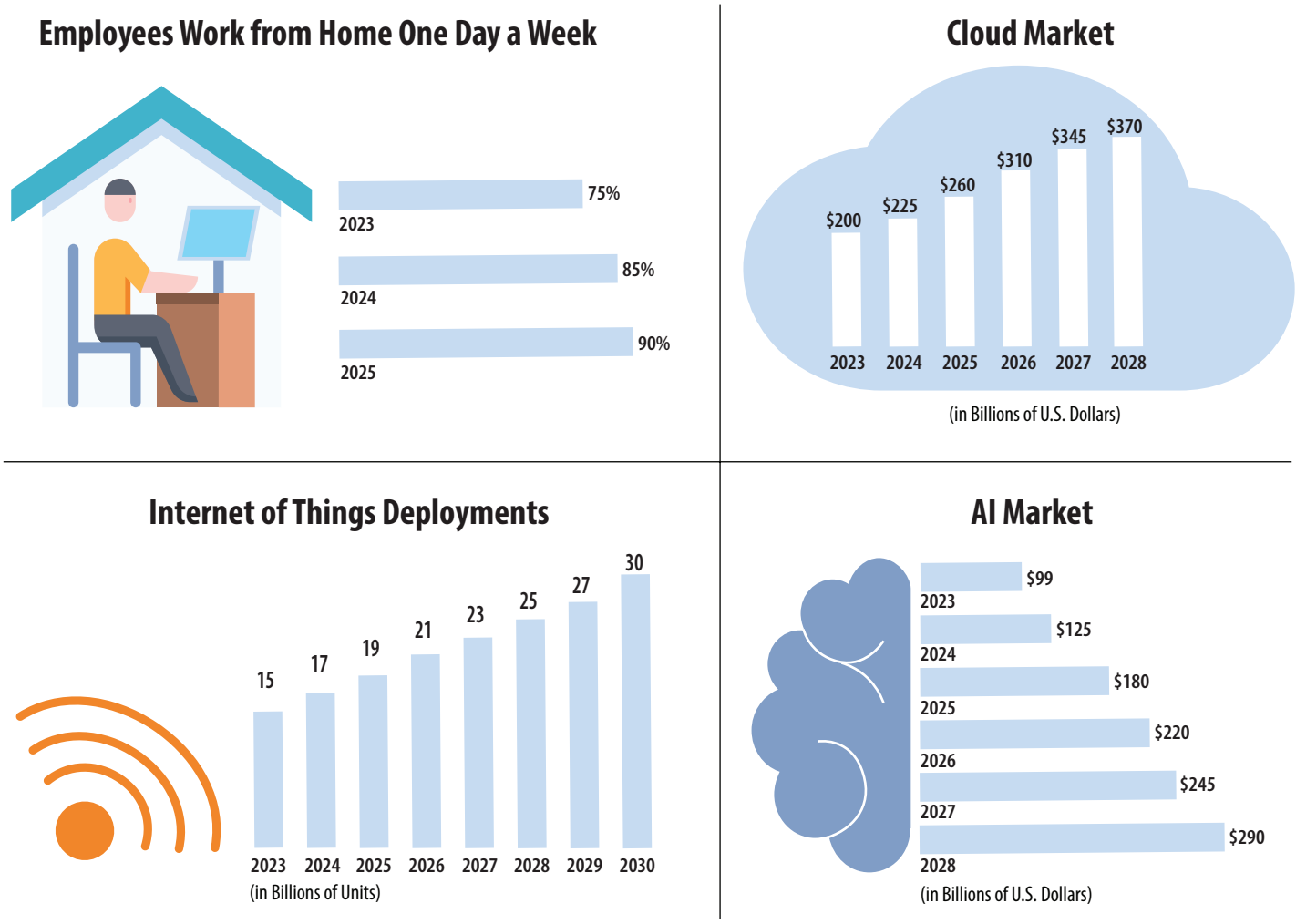
Artificial intelligence (AI) is going mainstream. The global AI market will hit just shy of $300 billion by 2028. But because it's so nascent and dynamic, the market size may end up being multiples of that forecast. Only time will tell. However, AI is not just about a slick front end and getting answers almost instantly; it's about the data that underlies it all. And there will be more data than ever in more places than ever.

All of the above trends are network centric in nature. The network is critical in ensuring these advanced technologies deliver the anticipated business value. However, in a world where every-

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

Exhibit 1: The Four Factors That Require a New Approach to Security



ZK Research 2023 Cloud Market Forecast; ZK Research 2023 Work-from-Home Forecast; ZK Research 2023 IoT Deployment Forecast; ZK Research 2023 AI Market Forecast

thing is connected, security must evolve as attack surfaces expand, breaches spread more quickly and security teams get overburdened.

In this report, we'll delve into precisely what companies can do to reduce threats, stop attacks earlier and protect their business everywhere by focusing on a burgeoning area: Domain Name System (DNS) detection and response (DNSDR). DNSDR can be thought of as an evolution of the extended detection and response (XDR) framework.

Over the years, the industry has started adopting the "detection and response" framework, beginning with endpoint detection and response (EDR), network detection and response (NDR), identity threat detection and response (ITDR), and XDR to combat cyber threats. DNS is a unique element that requires a similar detection and response approach because it detects threats that stay hidden from traditional detection and response systems.

Security teams can't keep up with the constant stream of data that's flying at them 24/7.

SECTION II: UNDERSTANDING THE SECURITY CHALLENGES IN A HYPERCONNECTED WORLD

Since the dawn of the computer age, security professionals have faced daily challenges similar to the ones we just outlined. But today's challenges are more complex than ever, so simplifying, streamlining or at the very least connecting systems is a requirement.

To illustrate that need, consider the distributed nature of security, which has caused a dramatic rise in the number of security tools an enterprise needs. A ZK Research survey found an average of 32 security vendors in enterprise-class companies. That's 32 different pieces of software to maintain and update, 32 different dashboards to monitor, 32 separate vendors to keep track of and 32 contracts to negotiate. That's a job in itself!

In addition to being buried by vendors, security teams can't keep up with the constant stream of data that's flying at them 24/7. Let's look at the facts, all based on ZK Research surveys and conversations with enterprises of varying sizes—from fewer than 500 employees to well over 20,000:

- Every hour, on average, 106 malware hits affect a typical enterprise.
- 90% of companies report that they've faced a breach (these varied in scope, but all resulted in some form of unauthorized access to data, applications, networks or devices), with 43% reporting a breach in the past year.
- It takes an enterprise an average of four months to find a breach.
- It costs a company $4 million to find the average breach and fix it.
- The financial impact of a breach on a company's reputation is incalculable.

Security teams can't possibly analyze the data fast enough to catch all the threats, which creates considerable risk for companies. With too much data, too many siloed systems and too much manual correlation, enterprises have significant blind spots. Imagine the damage one piece of malware can inflict if it penetrates a company's defenses and sits undetected for four months, wreaking havoc out of sight. Sadly, you don't have to imagine it.

Moreover, threat actors have gotten creative. They set up new domains several months in advance of using them in attacks. On average, there are 200,000 new domains created every day. Obviously, not all new domains are bad, but many are created by threat actors to wreak havoc.

Evaluating the Options

As mentioned earlier, the industry has adopted various detection and response approaches, such as the following:

EDR, which monitors end-user devices to record activities and events taking place on endpoints

NDR, which monitors communications within the network to detect threats that might otherwise remain hidden in unmanaged devices

ITDR, which detects threats to all service and privileged accounts on a company's network and cloud

XDR, a culmination of these approaches, which uses the EDR, NDR and ITDR capabilities to extend protection across endpoints, the network, cloud workloads, servers, email and more

These are competent tools in their specific domains. But that's the problem—none of the approaches has total visibility across the enterprise environment, which includes not just end-user devices but also network infrastructure, cloud resources, IoT/operational technology (OT) and remote users. Also, they don't track adversary infrastructure but use a malware-centric approach, which means they cannot preempt attacks and must find a compromise that has already happened. Therefore, there's a real need to do things differently.

One critical service—which is available in every network—does have enterprise-wide visibility as well as visibility into adversary infrastructure: DNS. DNSDR leverages DNS's unique view and position in enterprise networks, and it just makes sense.

As we noted earlier, DNSDR can find threats and eliminate them before they hit the enterprise network. In addition, DNSDR can close gaps in protection and help speed up mean time to repair (MTTR) for security operations (SecOps) teams by providing network and threat context and automation.

SECTION III: INTRODUCING DNS DETECTION AND RESPONSE

One of the most profound challenges SecOps faces when responding to security events is a lack of visibility into which devices or users have been affected by an attack. The team must manually cor-

WHAT IS DNS, AND HOW DOES IT WORK?

Everything that traverses the internet interacts with DNS. Whether it's emails, website traffic or malicious actors, it all has to go through DNS.

DNS translates domain names into IP addresses that computers use to identify and communicate with each other on the internet.

Typing a domain name into a web browser or sending an email triggers a request to a DNS server, which then finds the corresponding IP address for that domain name.

DNS is a critical component of the internet infrastructure, enabling the smooth functioning of various online services. It helps users access websites and other resources by displaying domain names that are easy to understand and remember, which simplifies the web navigation process.

relate an IP address to a network-connected device and the actual associated user. And the only way to do that is to pore over various logs or put in a request to IT—and it could take hours or even days to get the necessary data. Of course, this increases the time to respond to security events and burdens the already-strapped SecOps group. So, why keep doing the same thing the way you've always done it when it's just not working?

There's a completely new approach to detection and response that does what's needed: DNSDR. DNS spans the whole company and provides a rich set of telemetry. A DNS server is the first element of the infrastructure to encounter a request to connect with any internet destination.

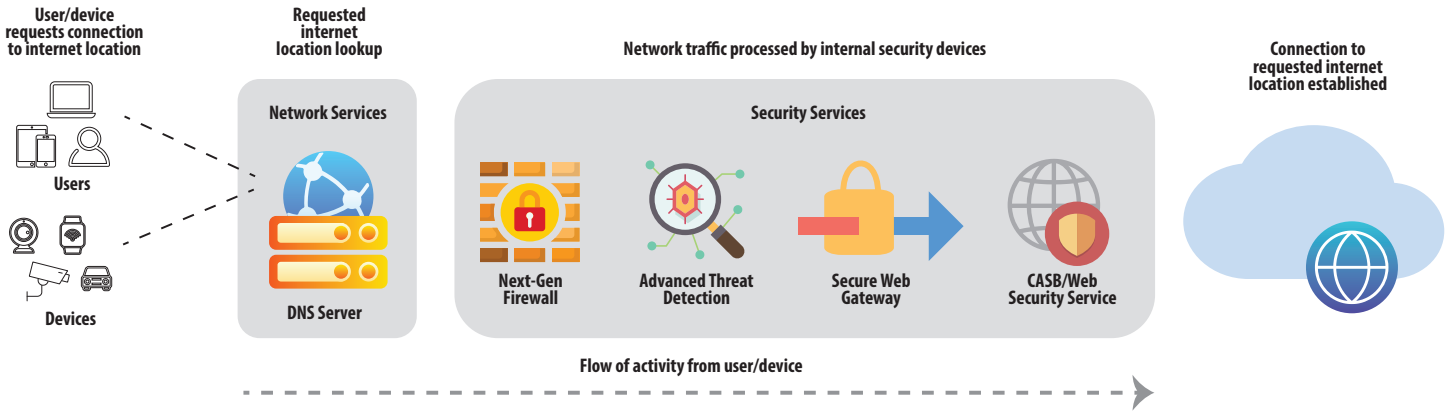
The Attack Sequence

Attackers are nothing if not methodical. They're organized and focused. And the typical attack sequence (Exhibit 2) follows a logical path:

1. Typically, the attacker creates a malicious payload, in what's called the weaponization stage, and delivers the payload to a target, often through a spear-phishing email.
2. When a user clicks on the link, the device requests a connection to the internet location, and the lookup is done via a DNS server.
3. Network security devices such as next-generation firewalls (NGFWs) and web gateways process the traffic, and then the connection is established.
4. Once the connection is established, the payload is downloaded and executed on the target device.

This is how malware typically inserts itself into an environment. After establishing a foothold, the attacker can now remote control the device via command and control, move laterally and finally carry out their intended goals such as data exfiltration.

Exhibit 2: The Steps in an Attack Sequence



ZK Research and Infoblox, 2023

DNSDR can detect threats and eliminate them before they hit other security devices.

The Case for DNSDR and Related Critical Capabilities

Protect and Detect

The attack sequence we just outlined makes a case for DNSDR. It sits at the nexus of the enterprise, so it can weed out problems before they affect vital infrastructure. Security teams should seriously consider moving to this protective DNS model that blends the DNS server with threat intelligence, a DNS-based AI engine and a DNS policy engine. According to a study from the National Security Agency's (NSA's) Cybersecurity Directorate in 2020, up to 92% of malware and command and control attacks can be identified via DNS. Protective DNS can actually disrupt this entire attack cycle at the first/initial step—when a user or device tries to connect to a malicious destination.

Using this concept of "shifting left" of protection, DNSDR can detect threats and eliminate them before they hit other security devices. It does this because it sees the destination the endpoint is trying to connect with, analyzes it and then suppresses the destination IP address—effectively blocking connections to malicious destinations.

Suspicious Domains

Another aspect to think about is the creation of domains by bad actors for use in future attacks such as large phishing campaigns. Hundreds of thousands of domains are created every day, and some of them could be used for future attacks. Identifying these "suspicious" domains requires tracking of this massive infrastructure and complex analytics to analyze billions of DNS queries.

Threat hunting in DNS can find all manner of issues by bringing together data science and DNS threat intelligence at scale, resulting in the identification of potentially problematic domains and pre-campaign blocking to stop attacks before they strike. For example, you can identify new domains and look-alike domains intended for malicious use during the weaponization phase and then categorize them as suspicious, using various parameters and metadata associated with those domains—several weeks or months before standard security solutions detect them as malicious.

In summary, DNSDR can protect companies against many attacks including the following:

- Look-alike domains
- Suspicious domains
- Employee-targeted attacks
- Domain generation algorithms (DGAs)
- Unauthorized data exfiltration

Identify and Respond

DNS is one of the many critical services every network needs, and it's often deployed on a purpose-built platform that includes other critical services such as Dynamic Host Configuration Protocol (DHCP) and IP address management (IPAM).

IPAM is a real-time database that records data about devices connected to the network. When combined with an enterprise-class DHCP solution, IPAM automatically captures the details of every

DDI can easily correlate DNS queries to a device with high accuracy.

device that has connected to the network when that device requests an IP address (via DHCP). IPAM tracks and updates each device whenever there are any changes, such as a user roaming from one network to another (which requires a new IP lease), keeping a history of each assigned IP address along with the times they were used on the device.

All of this information is then stored in the centralized IPAM database for everything connected to the network, and it becomes a real-time reflection of all devices.

In addition, you can integrate the DNS, DHCP and IPAM (DDI) system into authentication systems, collect network data and correlate with the integrated DNS server. These additional integrations provide a complete overview of any device on the network, such as the following:

- The device's media access control (MAC) address
- The device type and operating system
- The user's credentials logged into the system
- Network information, such as which access point or switch port is connected to the device
- A history of all of the IP addresses assigned over time

In addition, DDI can easily correlate DNS queries to a device with high accuracy.

So, why is this important for security? When there is a security event, IPAM data can be automatically included in the event information. Instead of a security alert containing only an IP address, the reporting can consist of additional information, such as the details highlighted above. This approach reduces the burden on SecOps because there's no need to find anything manually or to try to correlate multiple different types of data. Plus, the team can act faster, thereby reducing the impact of an attack and improving MTTR. So, it's clear that DNSDR works well with IPAM, which provides network context and device attribution for faster response times.

In addition, all this context and event data can be shared automatically with the rest of the security ecosystem stack in an enterprise network to accomplish the following:

- Help with faster analysis in a security information and event management (SIEM)/security orchestration, automation and response (SOAR) tool
- Trigger additional response actions such as vulnerability scans or IT ticketing

In summary, these are some of the benefits of DNSDR:

- Stopping attacks earlier and blocking malware at the earliest connection point
- Protecting businesses everywhere, including hybrid, multi-cloud environments as well as IoT and OT
- Application discovery and usage that can help create and enforce policies
- Seeing attacks that others miss as well as the ability to close gaps in protection
- Offloading traffic from downstream devices
- Quick and easy user and device attribution for faster threat response

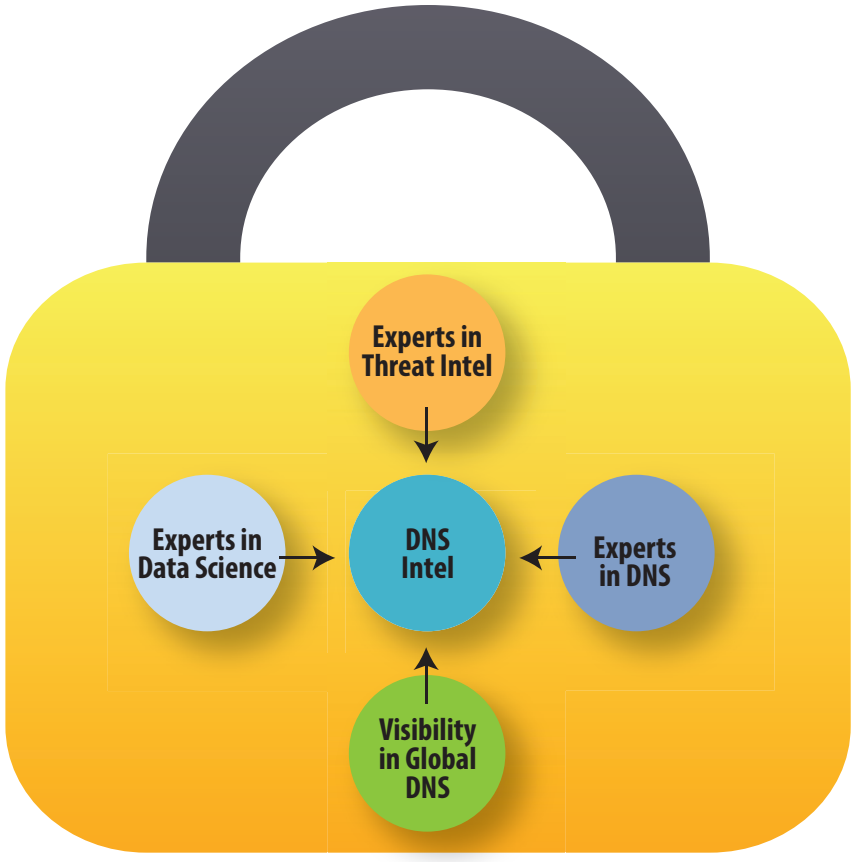
- Automation of remediation via ecosystem integrations
- Transforming security effectiveness

SECTION IV: INFOBLOX BRINGS NETWORKING AND SECURITY TOGETHER

Infoblox was founded in 1999 and continually supports more than 13,000 customers, including 92 of the Fortune 100—companies such as Hershey's, the Texas Rangers and the Port of Antwerp—as well as emerging innovators across 154 countries, enabling them to build safer, more resilient environments. The company delivers a simplified cloud-enabled networking and security platform that provides improved performance and protection.

Infoblox's broad ecosystem of partnerships creates seamless security workflows. Its close partnerships with companies such as Splunk, Microsoft, ThreatQuotient and AWS mean that Infoblox integrates deeply across cloud orchestration and security partners. Consequently, customers can continue to use existing solutions and improve their ongoing return on investment. Exhibit 3 high-

Exhibit 3: DNS Intelligence Requires Security and Network Data



ZK Research and Infoblox, 2023

lights how Infoblox's DNS intelligence is composed of DNS information as well as threat information, data science and global visibility.

SECTION V: CONCLUSION AND RECOMMENDATIONS

ZK Research sees DNSDR as a solution for keeping malware where it should be—at bay and outside your company infrastructure. It also reduces MTTR when there is a security event. We believe that DNSDR will grow quickly in the coming years. If you're in the market for a solution, consider the following points as you compare different offerings:

- Ensure the solution can spot look-alike domains, suspicious domains, employee-targeted attacks and unauthorized data exfiltration.
- Make sure it works in concert with IPAM for faster remediation.
- Ensure the provider has a raft of case studies and use cases so you can compare your needs with those of existing customers.
- Look for a solution from a company with a broad ecosystem of partners. An isolated solution likely won't work with your existing technologies and certainly won't grow with you as your needs change.

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.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314