White Paper

Enterprise DNS Security

By Jon Oltsik, Senior Principal Analyst

March 2018

This ESG White Paper was commissioned by Infoblox and is distributed under license from ESG.

Contents

Executive Summary 3
The State of Cybersecurity in 2018 3
DNS and Cybersecurity 5
DNS for Cybersecurity Advantage 5
Enterprise-Class Secure DNS 6
Enter Infoblox ActiveTrust Suite (Cloud and On-premises) 7
The Bigger Truth 8

Executive Summary

According to recent ESG research, 72% of organizations believe that cybersecurity operations have become significantly more difficult or somewhat more difficult over the past 2 years. Why the change? Cybersecurity professionals point to factors like an increasingly dangerous threat landscape, government/industry regulations, the volume of security alerts, and an upsurge in the amount of overall network traffic.[1] Additional ESG research also indicates that 51% of organizations have a problematic shortage of cybersecurity skills, exacerbating these challenges.[2]

What does this mean for enterprise organizations and what should they do to close the cybersecurity gap? This white paper concludes:

- **Enterprise organizations are under attack.** Large organizations face wave after wave of cyber-attacks from sophisticated adversaries. Often, these are targeted attacks using previously unseen methods, making them difficult to detect or prevent. Unfortunately, cyber-attacks often result in costly data breaches.

- **DNS can act as the first line of defense.** All network connections use the global DNS infrastructure to connect source systems to Internet destinations. This includes cyber-attacks where hackers use DNS to distribute malware, communicate with compromised systems, and exfiltrate data. DNS security solutions can be used as countermeasures to address this threat vector, preventing attacks that have breached the perimeter from succeeding, and helping organizations decrease their attack surface.

- **Enterprise DNS security offerings have specific requirements.** While there are many DNS security solutions to choose from, enterprises should look for specific features and functionality. Enterprise DNS security offerings should include strong detection/blocking capabilities, behavior analytics for detecting/blocking zero-day and sophisticated attacks that can't be detected using threat intelligence alone, a hybrid architecture that protects on-premises and mobile/roaming users, aggregated and curated threat intelligence feeds and analysis, central management, and tight integration into the network and security infrastructure on-premises for better visibility and context.

The State of Cybersecurity in 2018

According to ESG research, 63% of organizations plan to increase cybersecurity spending in 2018, and focus security investments in areas like network security, cloud security, and security analytics.[3] Why are CISOs increasing their cybersecurity investments? Unfortunately, organizations find themselves facing:

- **A continuous wave of publicly disclosed data breaches**. According to the privacy rights clearinghouse, there were a total of 612 publicly disclosed data breaches in 2017, exposing over 1.9 billion records. Some of the biggest data events included the Equifax breach (145 million records exposed), Verizon (14 million records exposed), America's JobLink (4.8 million records exposed), and Viacom (3 million records exposed). Organizations are investing in new types of threat prevention, detection, and response technologies to avoid becoming the next data breach headline. In some cases (i.e., Office of Personnel Management [OPM], Target, etc.), these attacks start with a compromise of business partners within the cyber supply chain. Infected partner systems have access to corporate networks, making them a perfect gateway for cyber-attacks and data breaches.

- **Targeted attacks.** Alarmingly, various security researchers report that 80% to 90% of all new malware is unique, designed to attack just one individual system. Furthermore, 50% to 60% of all web domains and IP addresses

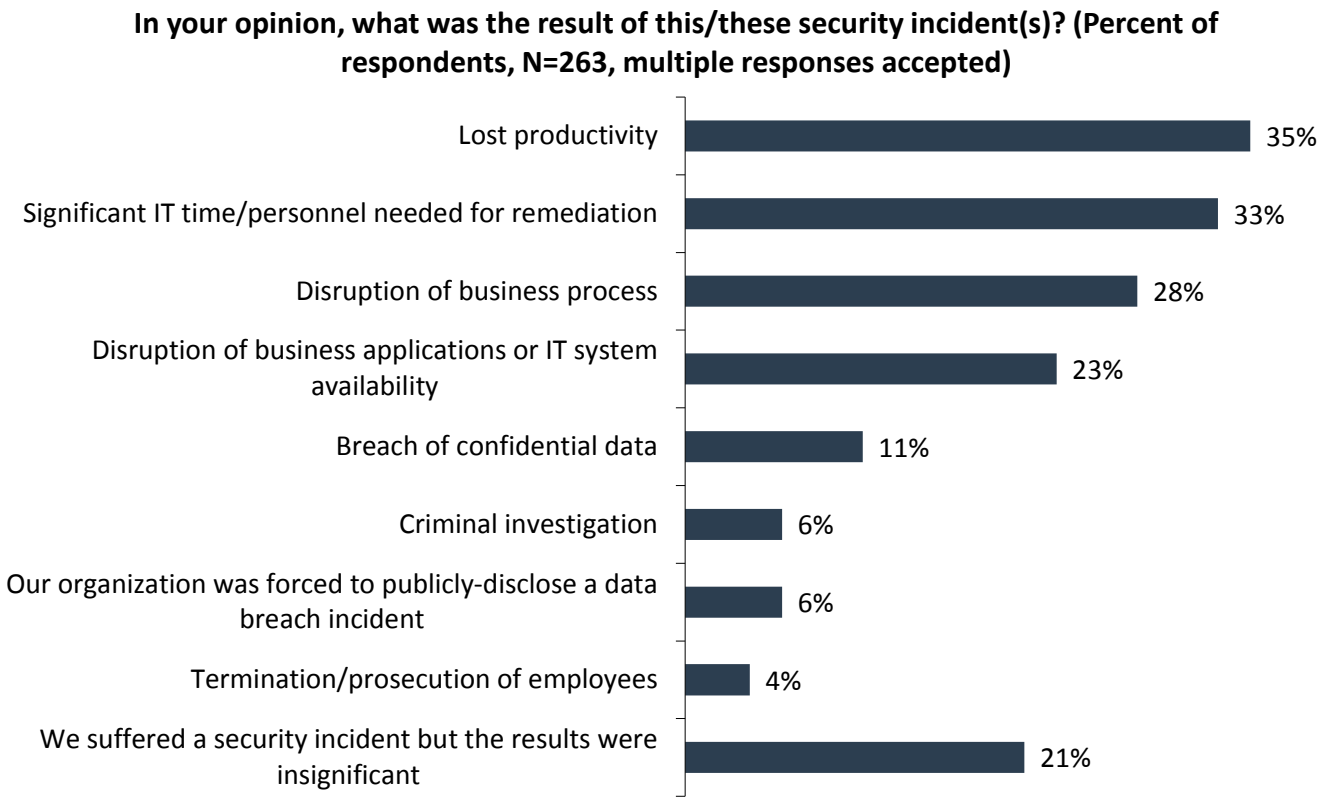
[1] Source: ESG Research Report, *Cybersecurity Operations and Analytics in Transition*, July 2017.
[2] Source: ESG Research Report, *2018 IT Spending Intentions Survey*, February 2018.
[3] Source: ESG Brief, *2018 Cybersecurity Spending Trends*, March 2018.

associated with malware distribution and/or command-and-control (C2) have a lifespan of an hour or less, making them difficult to detect or block using conventional security controls. Organizations are turning to new tools based upon artificial intelligence (AI) and machine learning to improve their chances of preventing or detecting the unique tactics, techniques, and procedures (TTPs) used for sophisticated targeted attacks.

- **Ransomware.** This type of threat was especially acute in industries like health care and transportation. The WannaCry ransomware spanned 150 countries and infected more than 300,000 machines. Other ransomware attacks of 2017 included BadRabbit and NotPetya, which were especially virulent in parts of Europe. According to cybersecurity ventures, ransomware damages were $7 billion in 2017, up from approximately $1 billion in 2016. To address the growing threat of ransomware, organizations are investing in host- and network-based threat detection tools and tightening system backup procedures.

Incidents like these are not random occurrences, as most organizations have suffered some type of cybersecurity breach over the past few years. These attacks can carry lots of negative results. Recent research from ESG and the Information Systems Security Association (ISSA) illustrates that security incidents result in lost productivity, significant time and resources needed for remediation, and disruption of business processes (see Figure 1).[4]

Figure 1. Results of Security Events Experienced



Source: Enterprise Strategy Group

As part of an exploit, hackers use various tactics, techniques, and procedures (TTPs) to send malicious code to user systems. Some use a technique called "water holing," where they plant malicious code behind a link in a trusted website. Some attackers use spearphishing emails to lure users to a realistic looking malicious website. Once infected, compromised systems

[4] Source: ESG/ISSA Research Report, *The Life and Times of Cybersecurity Professionals*, November 2017.

often receive further malware or instructions from a dynamic number of external C2 sites. Exploits, malware, and illicit network communication can be extremely difficult to prevent or detect.

DNS and Cybersecurity

The Domain Name System (DNS) is often referred to as the address book of the Internet as it translates numerical domain names into IP address destinations. As such, DNS has been a target with common cyber-attacks like DNS cache poisoning, DNS hijacking, and DNS spoofing. In each of these attacks, cyber-adversaries manipulate DNS services to direct unsuspecting users toward fabricated domains and websites in order to download malware and/or steal user credentials.

Over the past few years, cyber-adversaries have also used DNS to their advantage using domain generation algorithms (DGAs). DGAs are designed to bypass simple detection tools by generating massive numbers of random domain names, any one of which could be used as a C2 server to communicate with malware installed on compromised systems. DGAs became mainstream with the Conficker worm, first detected in 2008. Conficker.A generated 250 domain names per day while Conficker.C generated 50,000 domain names every day and then attempted to contact 500, giving an infected machine a 1% possibility of being updated every day if the malware controllers registered only one domain per day.

These types of DNS attacks are fairly well known but many cybersecurity professionals may not realize that hackers also leverage DNS for data exfiltration. In this type of attack, sensitive data is broken into chunks, often encrypted, and sent to a customized DNS server that unpacks, decrypts, and reassembles the data and then uses it for nefarious purposes like selling on the black market or other activities.

Recent Infoblox research suggests that DNS data exfiltration is far more common than most people believe—45% of survey respondents claimed that their organization has been a victim of DNS tunneling attacks in the past. This is especially alarming since network security technologies like firewalls and proxy servers are configured to allow free access of DNS traffic over TCP port 53. This means that DNS traffic is typically permitted network ingress/egress with little, if any, traffic inspection from existing perimeter security devices.

DNS for Cybersecurity Advantage

With all of the possible DNS risks, many organizations follow best practices by deploying hardened DNS servers, scanning DNS servers for software vulnerabilities, patching these vulnerabilities quickly, and monitoring DNS servers to detect anomalous behavior.

Beyond strong DNS security hygiene, however, a growing number of organizations now recognize that DNS can also be used as an active layer of defense in a defense-in-depth security strategy. This makes a lot of sense since DNS is part of every network connection—benign and malicious. As a result, DNS can be an essential component of cybersecurity for:

- Advanced prevention. DNS acts as a bridge between users, browsers, and web content. Instead of simply brokering these connections, secure DNS services can enforce security policies or block suspicious/malicious connections. For example, DNS services can be used to filter content like pornography, gambling, and hate sites for acceptable use policy enforcement. Leading DNS security services can also monitor the Internet to detect known malicious domains, IP addresses, and URLs, and then block connections in real time. Beyond malicious sites, DNS threat intelligence services can assign a risk score to newly observed domains (NODs) that often have short lifespans and thus may be used as C2 or malware distribution servers as part of targeted attacks. Organizations can then block connections to NODs based upon risk scores and policies. Finally, DNS services are very good at detecting and blocking anomalous voluminous requests that could indicate a compromised system using a DGA. Perhaps the best thing about secure DNS services is that they can help organizations bolster threat prevention without adding a lot of operational overhead and additional infrastructure. Basically they just use what they already have to improve security.

- Threat detection. As the middleman of every network connection, DNS can provide a wealth of information about the 300 million Internet domain names and 4 billion active IP addresses, and then correlate these entities to the TTPs used by cyber-criminals, hackers, and nation state actors. For example, when DNS security services detect a malicious

domain, historical DNS records can help uncover other domains and IP addresses used by cyber-criminals to launch similar types of attacks. In this way, DNS-based threat intelligence can help organizations not only block malicious domains today, but also understand and prepare for future targeted attacks. DNS threat intelligence can also be integrated with other open source and commercial threat intelligence feeds as well as analytics systems like EDR and SIEM, providing more holistic situational awareness. In addition to threat intelligence, behavioral analytics done on DNS queries going to the Internet can help detect the presence of data in what may otherwise look like legitimate DNS queries. Machine learning can help tune these analytics algorithms so that they become more effective over time.

- **Orchestrated response.** Enterprise organizations are actively orchestrating incident response and remediation processes to scale operations and bolster the productivity of security staff. DNS security services can help here by sharing indicators of compromise (IoCs) and indicators of attacks (IoAs) with security technologies like firewalls, network proxies, intrusion detection/prevention systems, endpoint security, NAC, and vulnerability scanners. When DNS security services detect a suspicious/malicious domain, this information can trigger the creation of new rules and signatures for blocking network traffic or start a scanning process to uncover vulnerable systems.

Enterprise-Class Secure DNS

CISOs looking to add secure DNS as a layer of defense will find numerous offerings and confusing choices. What should they look for? ESG believes that leading secure DNS should include (see Table 1):

- **Strong ability to detect and block malicious domains, URLs, and IP addresses in real time.** Leading DNS services will constantly crawl the Internet, seeking out malware distribution sites, C2 servers, DOMs, adware/spyware sites, questionable content, etc. This intelligence will be used to create signatures and domain reputation lists that can be utilized for actively blocking network connections. CISOs should assess the speed and accuracy of each provider's DNS threat detection capabilities. Some vendors will provide DNS firewalls for blocking malicious domains while others will rely on integration between DNS threat intelligence and the existing security infrastructure. Leading solutions will provide both.

- **Behavioral analytics for advanced detection/prevention.** In addition to signatures and reputation lists, DNS security should include behavioral analytics for examining DNS query properties (i.e., size, time, use of encryption, etc.) and detecting zero-day attack patterns in real-time. This is especially important for detecting and preventing the use of DNS as a data exfiltration vector.

- **A hybrid architecture.** Leading DNS security solutions will offer a hybrid architecture, combining on-premises appliances for large corporate facilities with cloud-delivered options to support cloud-first organizations, remote offices, and mobile workers. On-premises DNS security can tightly integrate into an organization's DNS and DHCP servers, offering closed-loop DNS security, unlocking valuable network context on criticality of infected devices and providing deep visibility. Alternatively, cloud-based DNS services can act as a scalable, turnkey alternative, delivering protection for distributed organizations with a large mobile workforce. These cloud-delivered services can also perform more advanced analytical capabilities and leverage larger threat intelligence data sets for advanced threat detection. In addition, cloud-delivered DNS security services alleviate the need for administrators to manage additional infrastructure, especially when they are overburdened with the systems they already have.

- **Central management.** Leading DNS security solutions will centralize management capabilities (i.e., policy management, configuration management, reporting, etc.) for all DNS traffic regardless of whether user systems sit behind a physical or virtual DNS security appliance or use cloud-based DNS security services.

- **Tight integration with the security infrastructure**. DNS security should integrate into security infrastructure technologies like SIEM, firewalls, proxies, vulnerability scanners, network access controls, and endpoint security software. This interoperability can be used to create orchestrated remediation workflows for advanced threat prevention. When a

new malicious domain is identified, DNS security solutions can share this intelligence with endpoint security software, firewalls, and proxies to block any further communications while simultaneously triggering a vulnerability scan.

- DNS threat research and intelligence. Since DNS is a part of all types of cyber-attacks, DNS security solutions should capture this behavior in the form of rich threat intelligence. Passive DNS is especially useful here, as it provides a historical record of all DNS transactions. Therefore, DNS threat intelligence should include details about malicious domains like the owner, location, and time-to-live (TTL) statistics. Leading DNS threat intelligence will also correlate malicious domains with one another based upon this information. In this way, organizations can group malicious domain activities used for cyber-crime, learn more about cyber-adversaries, and implement policies and controls to improve DNS threat prevention.

Table 1. Enterprise DNS Security Requirements

Requirement	Description	Benefit
Strong detection and blocking of malicious domains, URLs, hostnames and IP addresses	Ability to use reputation lists and signatures to identify and prevent connections to malicious domains	Decreased attack surface should block attacks and limit the number of incidents requiring investigations.
Behavioral analytics for advanced threat detection and blocking	Monitoring of DNS queries for size, time, use of encryption, etc., to detect and block anomalous behavior	Decreased attack surface should block attacks and limit the number of incidents requiring investigations. Can also provide threat intelligence.
Hybrid architecture	Support for on-premises appliances and SaaS services	Hybrid DNS security solution offering high-performance and full visibility for on-premises users along with support for cloud-first orgs, distributed locations, and remote users simplifies operations and lowers cost.
Central management	Policy management, configuration management, threat intelligence analytics, and reporting	Control and visibility for all policies and users can help eliminate human error and streamline operations
Tight integration with security infrastructure	Integration with SIEM, vulnerability management, NAC, etc.	Enables the ability to orchestrate incident response and remediation tasks.
DNS threat research and intelligence	Intelligence on cyber-adversary TTPs, relationships between malicious domains, etc.	Threat intelligence can help organizations anticipate cyber-attacks and add defenses for detecting/preventing new threats.

Enter Infoblox ActiveTrust Suite (Cloud and On-premises)

There are many DNS security solutions available, making it difficult for organizations to research, evaluate, and choose the one that best addresses their requirements. To cut through this confusion, security decision makers may want to look at ActiveTrust suite (on-premises and SaaS) from Infoblox, a company with a rich history in DDI (i.e., DNS, DHCP, and IP address management, or IPAM). ActiveTrust aligns well with the enterprise DNS security requirements outlined above because it offers:

- A DNS firewall designed to detect and block connections to suspicious/malicious web domains. The DNS firewall accomplishes this by using a combination of signatures, reputation lists, and behavioral analytics. In this way, ActiveTrust suite not only blocks connections to malware distribution sites and C2 servers, but is also designed to detect and block data exfiltration over DNS.
- A threat intelligence exchange platform. ActiveTrust suite is supplemented by Infoblox's threat intelligence data exchange (TIDE), which provides curated threat intelligence data directly from the Infoblox research team. TIDE can also aggregate additional internal and external threat intelligence, distribute threat data to the customer's existing security infrastructure, and expedite threat investigation through triage and context. ActiveTrust is further enhanced by Infoblox Dossier, a central tool for rapidly investigating and prioritizing threats.
- Behavioral analytics for data exfiltration detection. In 2015, Infoblox added behavioral analytics to DNS queries in real time to detect and actively block data exfiltration attempts using DNS as a communications pathway. In this way, Active Trust provides an advanced prevention layer, blocking DNS tunneling—a growing tactic for exfiltrating sensitive data.
- A hybrid architecture with central management. ActiveTrust can be deployed on-premises using a physical or virtual appliance, as a SaaS offering (ActiveTrust Cloud), or with a combination of both. When deployed as a hybrid solution, ActiveTrust suite supports a centralized management plane for common policy management, configuration management, and reporting.
- Integration with Infoblox DDI and a security partner ecosystem. ActiveTrust can work as a closed-loop security system with Infoblox DNS servers, DHCP servers, and IPAM to mitigate risk, improve security efficacy, and streamline operations. Furthermore, Infoblox supports open standards like STIX/TAXII, rest APIs, and third-party protocols to integrate into the security infrastructure tools like SIEM (Splunk), vulnerability management (Qualys, Rapid7), network access control (Cisco), and EDR tools (Carbon Black). In this way, ActiveTrust can help increase ROI on the existing security infrastructure.

The Bigger Truth

To address pervasive threats more effectively, ESG sees a growing trend where organizations are deploying advanced prevention solutions. These tools employ artificial intelligence and/or software-defined technologies, and are designed for ease of use and a decrease in the attack surface. The goals here are simple—improve security without requiring vast additional resources or operational overhead.

With this definition, DNS security can be considered advanced prevention as it is designed to detect and block suspicious/malicious network connections. The best DNS security solutions will go even farther, offering behavioral analytics for zero-day attacks and data exfiltration prevention, threat intelligence, hybrid architecture, central management, and strong interoperability with the security infrastructure.

Infoblox ActiveTrust is one DNS security offering that addresses enterprise needs. As such, CISOs should research and evaluate ActiveTrust suite to see how it can help them mitigate risk, improve security efficacy, and streamline security operations.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188