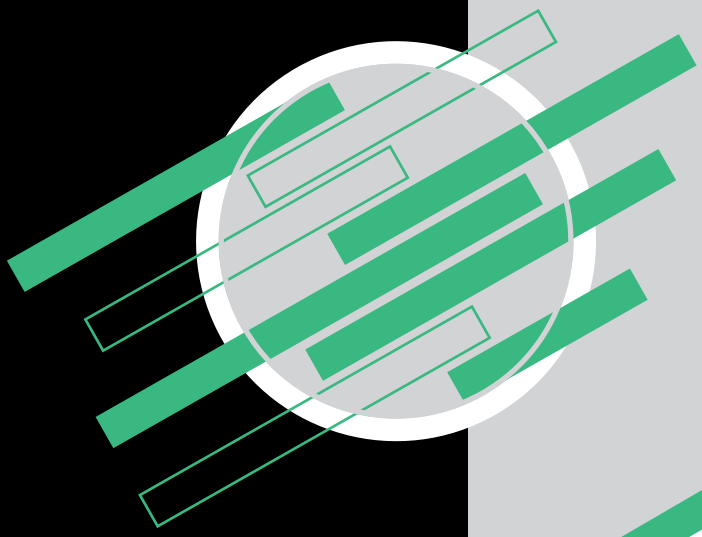
A Forrester Consulting
Thought Leadership Paper
Commissioned By Infoblox

July 2020

Accelerate Threat Resolution With DNS

Leverage DNS As A First-Level Security Control To Detect, Block, And Investigate Attacks



FORRESTER®

Table Of Contents

1 Executive Summary

2 DNS Is Critical To Addressing Top Security Priorities

6 S&R Teams Must Be A Jack-Of-All-Trades

8 Address ROI Needs And Threat Context

10 Key Recommendations

11 Appendix

Project Director:
Sarah Brinks,
Senior Market Impact Consultant

Contributing Research:
Forrester's Security & risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Threat investigations take too long.

74% of security operations teams spend more than 4 hours investigating a single threat incident.

More automation is needed.

58% of S&R leaders are using a mix of manual and automated incidence response processes — only 31% are almost completely automated.

Executive Summary

It has been stated in the press that customer data is more valuable in today's economy than oil.[1] If this is true, then protecting customer data must be a top priority for all businesses. This means all pathways to customer data must be secured, no matter where that data is stored. The domain name system (DNS) is a foundational network service that is critical to both connectivity and security, as it can provide a back door for data breaches. It should therefore not be overlooked as a first-level security control, especially in times of crisis and change, like the recent influx of home/remote workers.

In January 2020, Infoblox commissioned Forrester Consulting to evaluate the use of DNS in the detection of malicious attacks and the prevention of data loss. Forrester conducted an online survey with 203 respondents representative of top tier experts from organizations who typically lead the way in security best practices, serving as a good example for those striving to improve their own security posture. We surveyed US security and risk (S&R) leaders from firms with $1B or more in annual revenue from government, retail, education, healthcare, and financial services sectors. Half of the respondents hold the title of chief information security officer (CISO). These S&R experts use DNS as a vital component of their security strategy.

S&R leaders rely on DNS for three key priorities: 1) detecting and blocking threats as early as possible in the kill chain; 2) investigating and responding to threats; and 3) quickly identifying compromised devices.

KEY FINDINGS

- **DNS is a key starting point for threat investigation.** DNS queries and responses are one of the top three data sources that security teams use for threat hunting and investigations. Investigators rely on DNS because it detects malicious activity earlier in the kill chain than other security tools. It also gives S&R leaders much needed visibility into which devices are making requests to connect to malicious destinations — this visibility allows them to sever those connections and protect their entire infrastructure.
- **DNS fills gaps left by other security tools.** There is no perfect security tool that will fix all your problems, but it is important to have tools that fill in the gaps left open by other tools. Surveyed S&R leaders said the top benefit of using internal DNS, as a security control point to stop malicious attacks, is being able to catch threats which would otherwise not be caught by other security tools such as DNS tunneling/data exfiltration, domain generation algorithms (DGAs), and lookalike domain attacks.
- **Majority of S&R leaders want to improve ROI on security investments.** Fifty-six percent of S&R leaders listed improved ROI on security as the most helpful service to their organization. As more and more security tool investments were made in the last decade, S&R leaders want to see what ROI they can get with existing investments before approving budget for more tools and technologies.

FORRESTER®

DNS Is Critical To Addressing Top Security Priorities

S&R leaders realize that maintaining customer trust is critical to their business and the fastest way to lose that trust is by losing and compromising their customers' data. Truly customer obsessed S&R leaders use every tool at their disposal to detect and block threats, investigate and respond to threats, and quickly identify compromised devices. In surveying 203 S&R leaders, we examined each priority:

DNS is a key threat control point.

69% of S&R leaders use DNS as a control point to defend against attacks.

DETECTION

- **Identifying compromised devices starts with DNS.** There is more risk in today's current network environment than there has been in recent memory. With the emergence of the COVID-19 pandemic, and subsequently, the general resetting of business as usual for all companies, gaps in security postures are opening. More employees are working from home with their own devices, i.e., connecting internet-of-things (IoT) devices without the proper security measures, etc. And security teams must be able to quickly identify and respond to devices when and if they become compromised. Insecure networks, devices, and internet access jeopardize customer data. DNS queries and response data are one of the top three tools which firms are using to quickly identify compromised devices. The top two tools are IP address management (IPAM) data (67%) and network device logs (62%).
- **The data exfiltration challenge continues.** Stopping data exfiltration has never been easy. In extreme cases, insider threats can exfiltrate data through DNS, though attackers are much more likely to upload stolen data out via HTTP/HTTPS or FTP. In the latter case, the target organization is lucky if the DNS request that precedes the exfiltration is on a published indicator of compromise (IOC) list.
- **S&R leaders gain deep insight into attacks from DNS investigations.** When an attack/infection occurs, investigators need tools that provide a holistic view of the extent and severity of the threat. DNS domain/address investigations are one of the top two tools that investigators use to determine who in their organization was infected after an attack/infection occurs. In fact, DNS and malware analysis are both reported as the top tools used in identifying what data and systems the attacker got access to. DNS is also helpful to investigators when determining how much information the attacker got access to.[2]

BLOCKING THREATS

- **DNS is a top-three security control point for defending against attacks.** DNS filters/firewalls were ranked just behind secure web gateways/proxy and intrusion detection/prevention systems that security teams use to defend against attacks. In fact, 66% of S&R leaders said DNS allows them to detect malware activity earlier in the kill chain, reducing the burden on their perimeter defenses.
- **Three in four S&R leaders use data loss prevention (DLP) solutions to protect data.** Over three-quarters of respondents are using DLP solutions to keep their customer data safe. The remaining 24% of S&R leaders use other solutions like next-gen firewalls, secure web gateways, and cloud access security brokers (CASB) to protect their data.

THREAT INVESTIGATION AND RESPONSE

Ninety-four percent of S&R leaders in our study said they have considered or do consider DNS as a starting point for their threat investigations. DNS plays a critical role in accelerating incidence response rates across all devices in the organization on the main network, in branch offices and mobile worker locations, and across IoT. An enterprisewide approach to sharing threat intelligence is seen as critical to over a third of S&R leaders, while another 45% agree it would benefit their business.

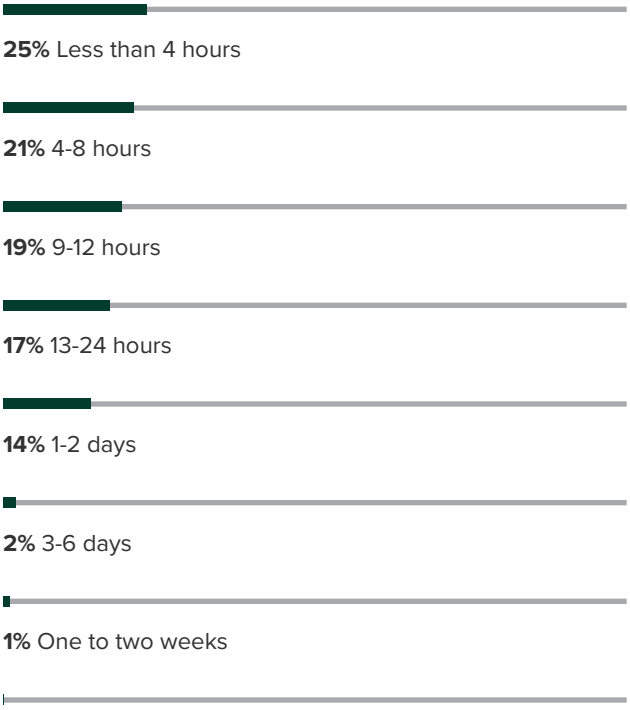
- **Even S&R leaders can only manage one to two investigations a day.** Nearly half (46%) of S&R leaders in our study found that it takes on average between 1 to 8 hours to investigate a threat. That averages out to roughly one or two complete investigations a day. Faster response times will require integrations and automatic data-sharing between tools that are both supported by skilled and trained staff and backed with precise processes (see Figure 1).
- **Automation is critical to improve incidence response rates.** Nearly 60% of senior S&R leaders have a mix of manual and automated incidence response processes. Only 31% of the surveyed S&R leaders said their incident response processes are almost completely automated. These leaders realize that any part of the process which can be automated should be automated, for the purpose of improving the speed and accuracy of incidence responses. Utilizing security orchestration, automation and response (SOAR) tools is how most respondents are automating their incidence response process; others are specifically selecting tools that include automation or are using their homegrown scripts. Homegrown scripts are most commonly used by the government sector. Thousands of scripts have been written over time to address various parts of the threat response process, which can become a burden to support over time.

DNS drives more effective investigations.

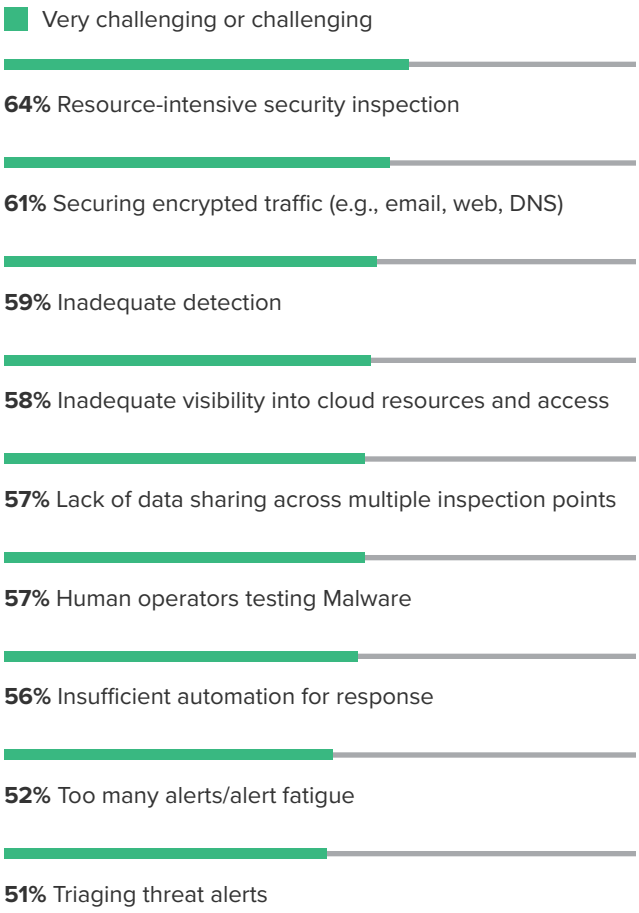
S&R leaders use DNS data throughout investigations for correlating network logs, determining exposure, and examining outbound resources.

Figure 1

"On average, approximately how long does it take your security operations team to investigate a threat?"



"How challenging are each of the following factors to your organization's threat prevention and investigations?"

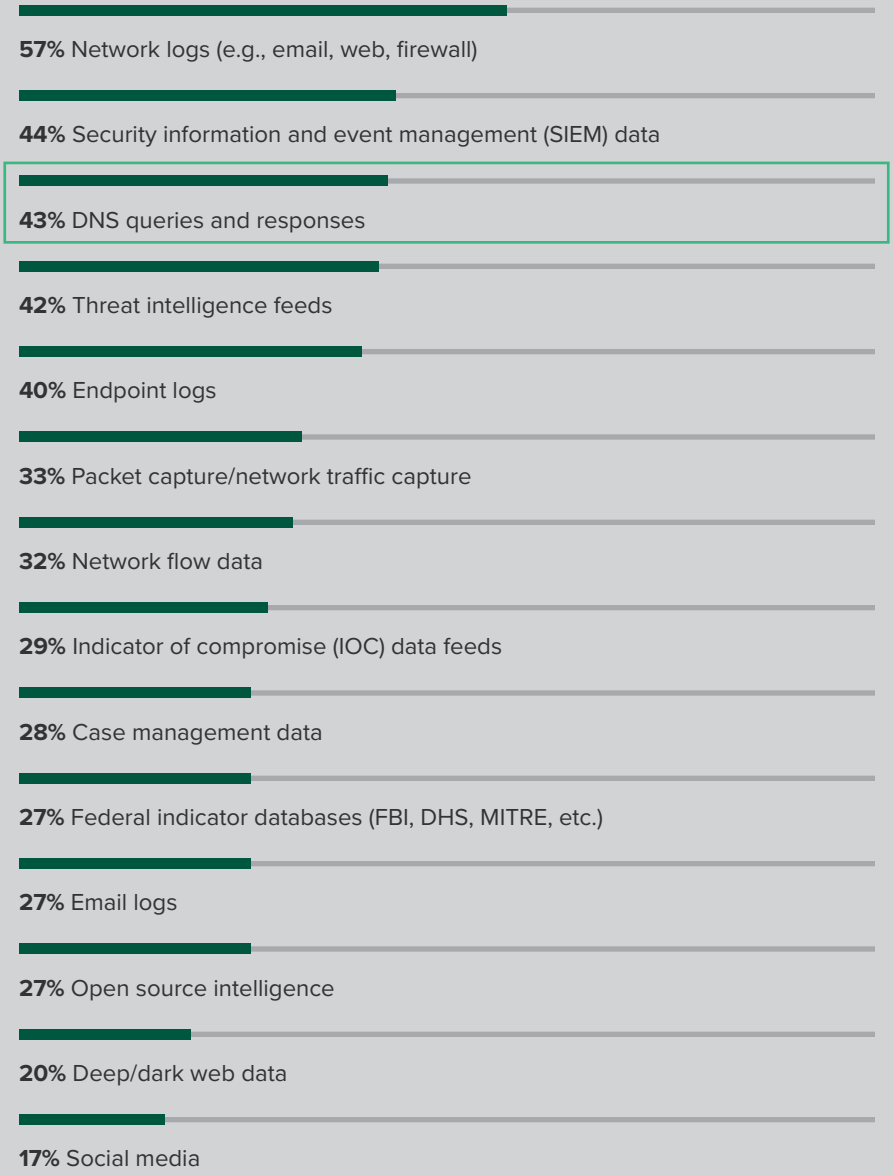


Base: 203 US security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, April 2020

› **DNS is a top investigation data source.** Forty-three percent of S&R leaders rely on DNS queries and responses to perform threat investigations. This means DNS is one of the top three data sources investigators rely on (at 43%) behind network logs (57%) and security information and event management (SIEM) data (44%) (see Figure 2). DNS is a key part of S&R leaders' security strategy by protecting firms from threats that other security tools might have missed and by allowing investigators to know which devices have requested connections to malicious destinations.

Figure 2

"Which of the following data sources do your security teams rely on to perform an investigation/threat hunt?"



Base: 203 US security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, April 2020

FORRESTER®

S&R Teams Must Be A Jack-Of-All-Trades

According to the Forrester Analytics Global Business Technographics® Security Survey, 2019, 43% of US respondents experienced one or more breaches that compromised sensitive data in the past 12 months.[3] Twenty-two percent of attacked firms said the attack was carried out through DNS. The high volume of threats from so many sources and attackers mean S&R leaders face many challenges:

- **S&R teams are overwhelmed by factors during investigations.** Without immediate and unimpeded access to all forensic resources, investigators are often left feeling that they have inadequate detection. They require clear visibility and access to private and public clouds. Additionally, threat investigators struggle with encrypted traffic through email, the web, and soon, DNS.
- **Fatigue has set in, and automation lags.** The volume of alerts that threat investigators address on a weekly and even daily basis can be daunting. Fifty-two percent of S&R leaders said too many alerts or alert fatigue is challenging. To add to that, 51% are challenged by triaging threat alerts. How do you address this fatigue? Automation is the direct answer, but even amongst the top S&R leaders we surveyed, 56% said they have insufficient automation for their threat responses.
- **Detecting and blocking bad destinations and malicious sites for mobile workers during a crisis.** When the COVID-19 pandemic began to hit the US in a significant way in March 2020, the North American workforce made a significant pivot to being home/mobile workers. Employees who had never had to work from home, suddenly had to find a way to work from home while still protecting sensitive customer data. Our survey was fielded mostly at the end of March when the pandemic was just in the beginning stages in the US. Even then, S&R leaders believed they were least effective at detecting and blocking threats for their mobile worker locations (see Figure 3). S&R leaders have been put to the test in 2020 as they have had to learn to secure mobile workers' devices and networks at a higher volume than they ever have in the past. Those S&R leaders, who can act fast and decisively, will win in the long run.

According to the Forrester Analytics Global Business Technographics Infrastructure Survey, 2019, enterprises can own over 500K tablets and more than 2M laptops, creating many points of potential infection and attack.

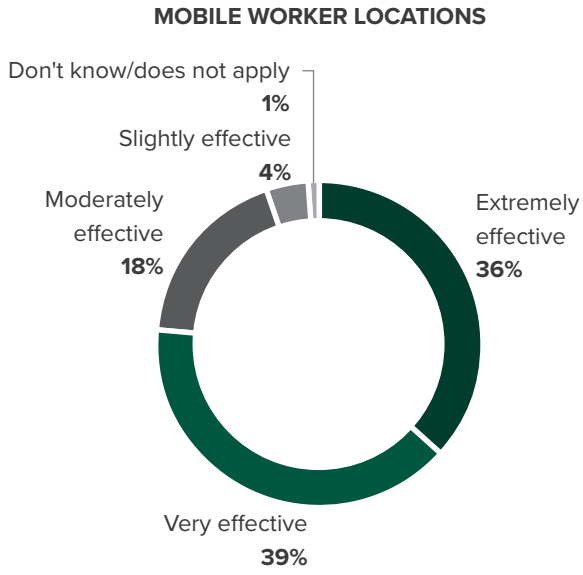
DNS is critical to catch threats.

66% of S&R leaders said DNS is able to catch those threats their other security tools cannot.

Figure 3

"How effective are you at detecting access to bad destinations and malicious sites at the following locations?"

"How effective are you at blocking access to bad destinations and malicious sites at the following locations?"



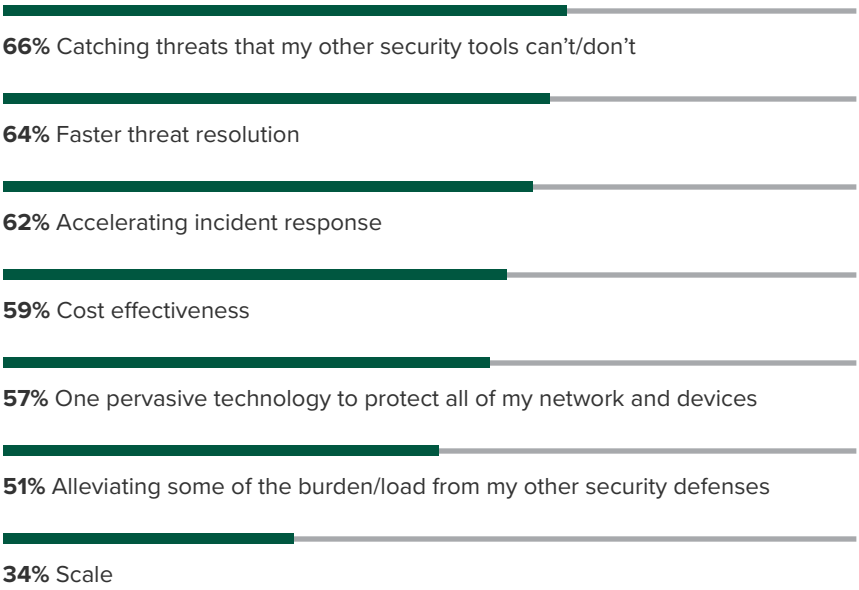
Base: 203 US security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, April 2020
Note: Percentages may not total 100 because of rounding.

- **Using internal DNS as a security control point addresses key security challenges.** Sixty-six percent of S&R leaders said DNS is able to catch those threats their other security tools cannot. DNS also helps accelerate their incident response times, which makes their threat resolution faster. DNS assists an organization's deception technology, which can snare attackers when they first penetrate; that same technology can be leveraged to redirect hosts to special inspection zones when they request resources of unknown reputation. Over a third of firms said using internal DNS as a security control point can help them stop malicious attacks at scale (see Figure 4).
- **S&R leaders must address challenges that are specific to COVID-19.** Businesses have been forced into an unprecedented experiment with remote working that seemingly has no end. Until a vaccine is widely available, some portion of the workforce will always be remote.[4] Along with the much higher volume of mobile workers, S&R leaders must address also the additional challenges that COVID-19 has brought to the surface. Due to the reduction of onsite staff, many S&R leaders have needed to find automation solutions to fill staffing gaps and to continuously monitor cloud access and usage. Many firms lack the tools/software to fully enable their mobile workforce. Other firms, particularly those in rural locations, lack the internet bandwidth to meet their needs. Malicious attackers are ramping up phishing and social engineering attacks as well as taking advantage of vulnerabilities in collaboration tools — so don't let your guard down.[5]

FORRESTER®

Figure 4

"What benefits would you anticipate from using internal DNS as a security control point to stop malicious attacks?"

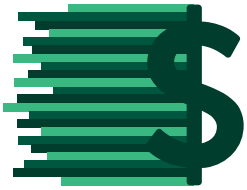


Base: 203 US security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, April 2020

Address ROI Needs And Threat Context

S&R leaders face challenges articulating which projects generate the most value for their organization. They often struggle to justify existing budgets as well. By leveraging partners who can measure performance and provide context to threats, leaders can better justify budgets and invest in best-in-market tools and technology. In this study, we found:

› **Even top S&R leaders are looking for additional services.** We targeted top S&R leaders for this study, but even top tier experts from organizations who typically lead the way in security best practices recognize that they can continue to improve. S&R leaders are keenly searching for a service that will improve their ROI on security. Saving money on their investigations means they can invest further in innovation, better technology, and hiring/training staff. Additionally, they are looking for continuous monitoring services that address their visibility challenges. They also want help automating common and repetitive security tasks, as this will lead to cost reduction. And, in considering the future, automation can only be a boon to securing a workforce that is just now beginning to settle into remote work, on either a permanent or semipermanent basis.

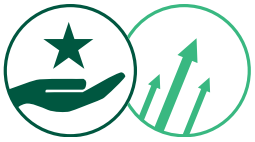


ROI is most important.

56% of S&R leaders listed improved ROI on security as the most helpful service to their organization.

FORRESTER®

- **S&R leaders seek more detailed context for threat identifiers.** S&R leaders in our study were clear, they ranked better threat intelligence as the most important resource to improving their organizations' overall security capabilities (see Figure 5). A key component of improving those capabilities is a better understanding of specific threat identifiers. Leaders expect their providers to understand the context of both the unique threats to their environment and the complexity of their business. By knowing what to look for, investigators can provide more effective breach responses, triage threats faster, and collaborate better across teams. Contextual information within alerts can make the difference between immediate and drawn out threat resolutions.
- **Mobile workers require increased threat intelligence.** In the midst of the coronavirus pandemic, many businesses are asking, or mandating, that office-based employees work from home. Millions of employees who have been logging in from workstations on corporate networks are now logging in from home or elsewhere on public networks. Stronger authentication, and VPNs, that used to be required for a subset of employees at any given time now become the point of entry for your entire workforce.[6] It is expected that many workers will remain at home for most of 2020 and some will never return to the office. Leading organizations are giving employees increased flexibility to work remotely. However, our study revealed it is hardest for even top-tier S&R leaders to detect and block bad destinations and malicious sites at mobile worker locations. Leaders must act fast to leverage DNS as a foundational threat intelligence device to accelerate incident response, discover and manage inventory, and optimize their security stacks for faster threat resolution.



Context drives effective response.

Half of S&R leaders see more/better context driving efficiencies in triage, breach response, and collaboration.

Figure 5

"What benefits would you anticipate from your organization having more/better context about specific threat identifiers?"

Base: 203 US security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, April 2020

FORRESTER®

Key Recommendations

Forrester's in-depth survey of 203 US security and risk leaders about leveraging DNS as a foundational security control point yielded several important recommendations:

Share threat intelligence across the enterprise. The majority of enterprises surveyed by Forrester agree that an enterprisewide approach to sharing threat intelligence is a critical benefit for their business. Security and risk professionals need to distribute the threat intelligence used by their top tier forensics and security analysis teams across the enterprise to maximize the value of that intelligence at the point in time when it can be most effective.

Continue to accelerate incident response functions. Both 2018 and 2019 saw record numbers of high and critical vulnerabilities. Today, a security management team has a new high or critical vulnerability come online, on average, every 9 hours[7]. At the same time, attackers are automating the weaponization of just-published vulnerabilities, expanding the global threat surface, and gaining an opportunistic foothold in organizations. The pressure to respond to incidents, and the vulnerabilities that cause them, drives organizations to take the fastest route to the truth. And for many, DNS is that route.

Take control of asset discovery management. Modern asset management is one of the most difficult problems to solve, due in part to the ease in which new devices can be connected to corporate networks by employees, remote teams, and partners. Asset discovery continues to be a challenge. The integrated DNS solutions, DHCP and IPAM, can assist here, as they are the one type of control point that each device is guaranteed to interact with. Utilize IPAM data to identity compromised devices quickly. Lifecycle management of assets, from onboarding to disposal, is becoming its own discipline.

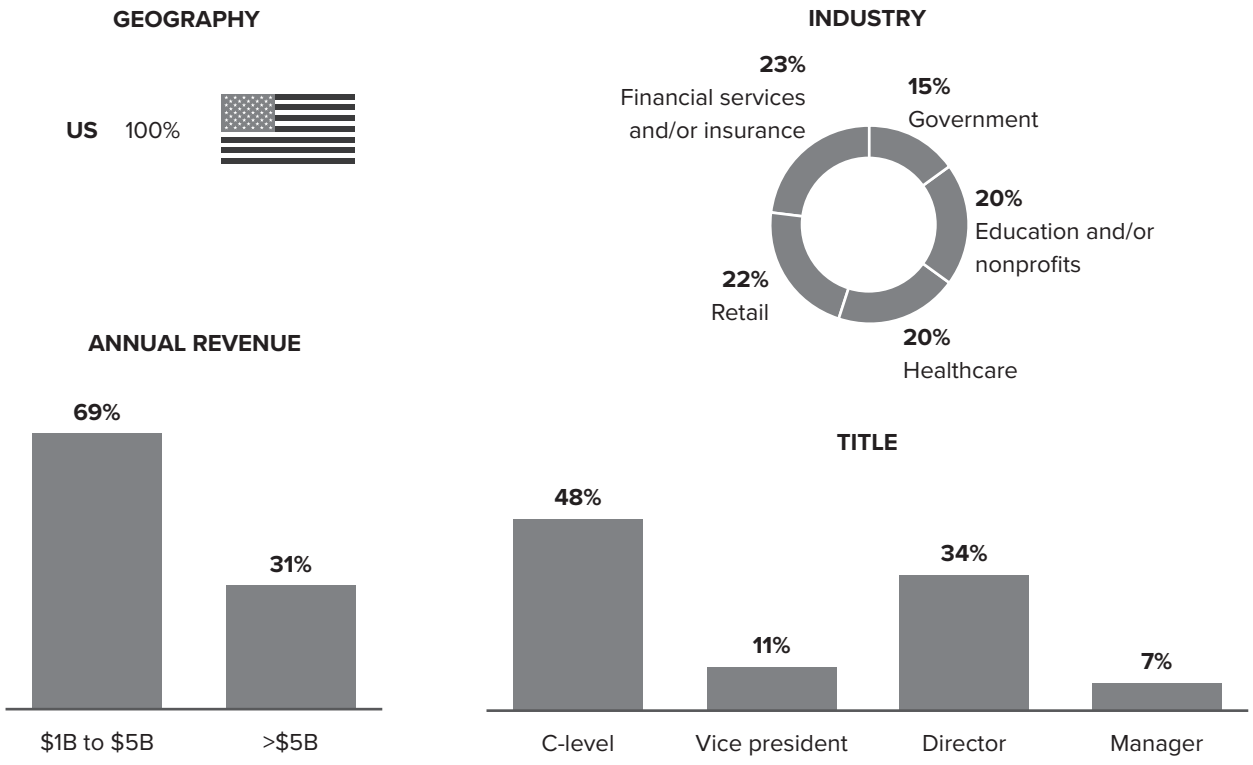
Tactically extend existing security infrastructure. The security stack architecture is changing; there is a move to deliver nearly all, or all, in some cases, security components from the cloud. Competition for the best security stack recipe is fierce, but it may be five years or more before the dominant design emerges. Cautious organizations can extend the lifetime of their existing security infrastructure through optimizations. Threat intelligence via DNS can play a major role here, in that "known bad" allows organizations to make cheap determinations faster and transfer only the most difficult inspections to the full stack, where sandboxing and human analysis have the final say.

Continue to defend, in depth. The internet is encrypted now; network analytics and visibility (NAV) vendors informally report to Forrester that they're seeing between 72% and 95% encrypted traffic in corporate networks. For many organizations, only metadata like DNS requests remain as visible cues for real-time analysis. Security and risk professions will continue to embrace the tried and true DNS firewalling and filtering techniques as a first line of defense against malware, phishing, and ransomware. Attackers know this and have been curating algorithms to generate pseudo-random domain names for the C2 operations, leading to an arms race that only AI will be able to fight in real time.

Appendix A: Methodology

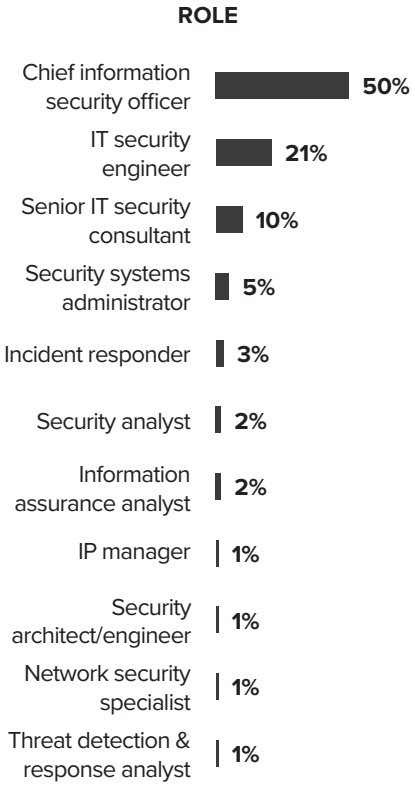
In this study, Forrester conducted an online survey of 203 US security decision makers from financial services, healthcare, education, retail, and government firms to evaluate how they were using DNS in their threat investigations. Respondents were offered an incentive as a thank you for time spent on the survey. The study began in April 2020 and was completed in April 2020.

Appendix B: Demographics/Data



Base: 203 US security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, April 2020
Note: Percentages may not total 100 because of rounding.

FORRESTER®



RESPONSIBILITY

	Security & risk assessment strategy	Threat intelligence strategy
Primary	79%	79%
Share responsibility	17%	18%
Provide input & execute	3%	3%

Base: 203 US security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, April 2020
Note: Percentages may not total 100 because of rounding.

Appendix C

ENDNOTES

[1] Source: Dan Gallagher, "Data Really Is the New Oil," The Wallstreet Journal, March 9, 2019.

[2] Source: Forrester Analytics Global Business Technographics Infrastructure Survey, 2019.

[3] Source: Forrester Analytics Global Business Technographics Security Survey, 2019.

[4] Source: "Collection: Learn To Support A Remote Workforce Permanently," Forrester (https://www.forrester.com/fn/37Kn3Q4mpMBdAxFZhMFbf1).

[5] Source: "Address The Security And Privacy Challenges Of Working From Home," Forrester (https://www.forrester.com/fn/21NX5awkIkxYASgFFz0Ejx).

[6] Source: Sean Ryan, "A Spike In Home Workers Raises MFA Resilience Questions," Forrester Blogs, March 17, 2020, https://go.forrester.com/blogs/a-spike-in-home-workers-raises-mfa-resilience-questions/.

[7] Source: National Institute of Standards and Technology, CVSS Severity Distribution Over Time (https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time).

FORRESTER®