BLUECAT™

Driving NetOps 2.0 with DNS Insights

2020 Networking Trends Report

February 2020

Executive Summary

Digital transformation has redefined the role of CIOs in the enterprise. With a new emphasis on driving business initiatives and revenue growth, CIOs need their NetOps team to power and enable the rapid changes to the network that support the business's evolving needs. For NetOps teams, meeting that challenge requires leveraging the data at their fingertips to optimize and secure the network.

In this report, we demonstrate how DNS information can be leveraged to provide the insights businesses need to support digital transformation.

Key findings

Optimize performance with insights from DNS

Visibility into DNS queries enable IT teams the opportunity to discover network and query performance degradation, identify root cause, and speed remediation. It allows organizations to gain meaningful insights into usage levels of applications and cloud services, to better understand user adoption and behaviors, and measure ROI.

Change KPIs of network performance

Legacy metrics such as uptime and latency are still relevant, but service delivery is a growing focus as IT departments move toward new business models. In this context, DNS data offers a wide range of meaningful business metrics that can assess the value of a NetOps team in delivering services.

Develop a cross-functional approach

DNS data often holds the context that threat hunters and security operators need for a smart, focused response to malicious activity. The ability to collect and analyze that data often originates with the network team, however. A collaborative, cross-departmental approach is required to truly reap the rewards of this valuable data set.

Leverage DNS data for security policies

Periodic analysis of DNS traffic (and internal DNS traffic in particular) can uncover significant threats to network security. That traffic should inform targeted security policies to lock down critical systems. Only by digging into the data and mapping it against business requirements can you discover how it can best serve network security in your particular context.

2020 Trends
Introduction

CIOs face increasing pressure to deliver revenue-generating services to their customers at a faster pace. Gartner's 2019 CIO Agenda report noted that **22 percent of survey respondents named revenue and business growth as their top priorities, placing them on the same level as "digital initiatives."** This statistic is a telling sign that technology and business outcomes are increasingly interdependent.

CIOs used to focus on providing a reliable technical infrastructure. Today, they are also asked to identify and deliver technology to drive business initiatives forward. Enabled by cloud, SD-WAN, and virtualization, CIOs are pushing their networks to do more.

Those same technologies are also driving the transformation of network operations (NetOps) teams to meet changing business needs. The advent of cloud services, DevOps, and edge computing is fueling the transition to a service-based IT model, where NetOps teams deliver core services and insights to users across the enterprise as it undergoes digital transformation.

2020 Trends
Introduction

As CIOs face pressure to aid business growth, information gleaned from the network can play a key role in advancing innovative approaches that drive operational outcomes. From cybersecurity to network optimization, NetOps teams should be driving this change, leveraging the data which flows through critical systems to spot misconfigurations, deliver improved customer service, and enhance the protection of mission critical data. With IT environments getting more complex, new approaches have to emerge to drive and support enterprise business initiatives and DNS presents an untapped opportunity to make that happen.

Hidden within DNS query information are meaningful signals and insights to accelerate business performance. Serving as the backbone for the internet, DNS serves as the gatekeeper for ensuring continuous communication between users, applications, and devices.

This results in DNS queries and logs being generated for everything from users accessing websites and SaaS-based applications to sending emails. The sheer volume of data provides unlimited potential for analysis by NetOps teams enabling them to tap into details to address vulnerabilities, network health and performance, and remediation.

This, combined with the growth in new services, cloud applications and fleets of IoT devices means a massive increase in DNS query data all of which can be mined to aid in business performance.

This report highlights the many ways CIOs and NetOps teams can use core infrastructure data like DNS to improve security, optimize performance, and uncover potential cost savings. Using examples drawn from the Domain Name System (DNS), we'll examine the operational challenges CIOs face as they try to deliver innovative and reliable network services in a rapidly changing environment.

The insights in this report are based on a representative sampling of over five billion DNS queries from BlueCat's extensive customer base in North America and Asia. Using thirty-days' worth of anonymized information, BlueCat's analysts performed a deep dive into key patterns and anomalies. Through this process, we uncovered many of the hidden keys to making businesses more agile, more secure, and more efficient.

NetOps Needs to Evolve

NetOps Needs to Evolve

Much has changed in the world of IT in the last 10-15 years. The promise of cloud computing—speed and scalability—has fundamentally altered life for CIOs and impacted everything from the data center to business delivery models.

The emphasis on enabling faster delivery of revenue-generating services has trickled down throughout the IT department, creating entire new technology disciplines such as DevOps to better support the business.

To keep pace with these developments, the focus and expectations of NetOps teams need to evolve. In some ways, the goals of networking professionals in this new world will still sound very familiar. **Nearly 34 percent of network professionals surveyed in a study by Sirkin Research cited improving network agility as being among their top priorities.**

Thirty-three percent cited reducing the cost of service providers, while 31 percent said it was reducing the Opex budget. To reach these goals in this new, fast-changing environment, NetOps needs to evolve and embrace a new role, one that enables development and security teams to be more effective.

NetOps
Needs to Evolve

Gartner calls this transformation NetOps 2.0—the adoption of DevOps's principles and techniques alongside automation and analytics to provide the agility and scalability demanded to support digital businesses. As with other critical IT infrastructure, enterprise DDI (DNS, DHCP and IPAM) is being revolutionized by these rapid changes in technology, process and architecture.

The adoption of cloud technologies enables organizations to rapidly acquire IP addresses, assign DNS records, and deploy subnetworks using cloud-native DNS services. But that speed comes at a cost—the fracturing of a unified, single source of truth for IP space, namespace and DNS record management. That in turn leads inefficiencies, visibility gaps, data conflicts, errors, outages and security vulnerabilities.

This reality can put pressure on networking teams to simply step aside to avoid impeding velocity and focus on maintaining visibility and control over the networks on the back end.

Unfortunately, the most likely outcome of this is the creation of a fragmented mess of systems and data. Disjointed approaches to DDI slow down the enterprise at a time when speed is at a premium by making the automation of changes even more difficult. Automation solves this challenge, but it can only be fully successful if it is enabled by a unified, consistent DNS, DHCP, and IP Address Management (DDI) infrastructure.

By deploying network automation tools and implementing a consistent and effective DDI infrastructure, NetOps teams will have the visibility needed to provide useful insights to their organization. Those insights range from data on performance, misconfiguration, the presence of shadow IT, abuse of cloud services, security breaches, and much more.

NetOps teams need to find ways to leverage the rich data their systems produce to optimize performance, improve reliability, and help ensure that all of the data that passes both internally and through hybrid networks is visible and secure.
As it turns out, DNS and the data it produces can provide several ways for NetOps teams to add value to their organization based on the unique visibility they have into the network.

NetOps 2.0 the adoption of DevOps's principles and techniques alongside automation and analytics.

Unlocking the potential of Cloud

Public cloud accounted for more than 50 million DNS queries analyzed as part of our study. This data provided some interesting insights into the patterns of public cloud usage across different industries and vendors.

According to the data, AWS remains the most widely used cloud provider, accounting for 71% of the public cloud queries BlueCat observed (Fig. 1). The next most popular was Microsoft Azure, representing 26%.

Even more interesting than the choice of cloud vendors is the data on how (or even whether) cloud is being used. Our data shows that 86% of all DNS traffic still comes from data centers, and only 14% came from public cloud services (Fig. 2).

Conventional wisdom has it that cloud adoption will continue to trend upward. At the same time, those predictions have been around for many years now. Our data seem to suggest that the pace of cloud adoption could be slower than most analysts predict.

We found that cloud adoption also varies quite a bit between different industries and verticals. Far and away, the leader in public cloud adoption was the education sector, with 23% of all DNS queries flowing through a public cloud provider.

This finding is likely due to the potential for cost savings for schools using the cloud as opposed to maintaining their own infrastructure.

Figure 1
Big 3 public cloud usage

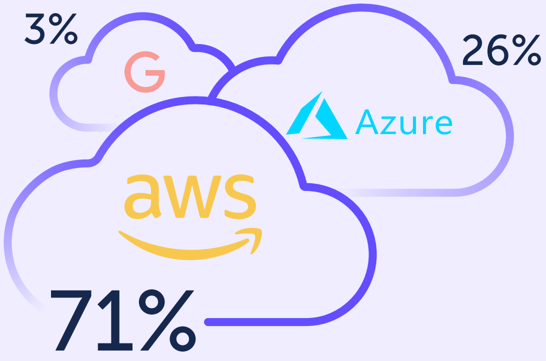
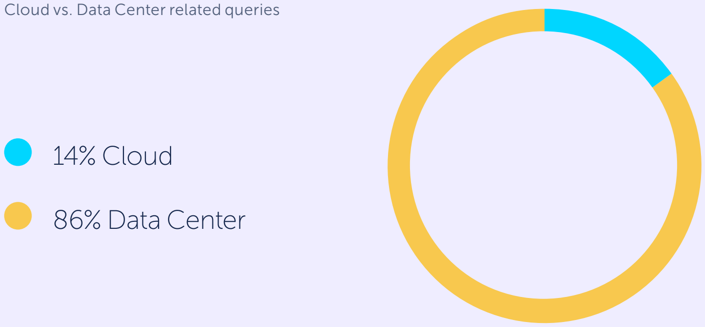


Figure 2
Cloud vs. Data Center related queries



Source: BlueCat 2020 Trends

Unlocking the potential of Cloud

The industry vertical showing the slowest rate of cloud usage is the government sector, which showed no public cloud use in the sample we examined. This is hardly surprising, given the compliance and security mandates which continue to stand in the way of cloud adoption by government agencies.

At the same time, these results could also be specific to the zones or subnetwork data analyzed in the study. The second smallest percentage of cloud usage belonged to retail, which showed only two percent.

From the standpoint of network optimization, having visibility into DNS queries can unlock opportunities for NetOps teams to provide insights that can improve efficiency.

For example, if a cloud service that an organization is paying for is not being used as heavily as expected due to employees leveraging another service, teams can realize cost savings by retiring the underutilized solution. By analyzing traffic patterns related to cloud application use, the networking team can unlock valuable data for the business.

Supercharging network performance with DNS insights

DNS data is an excellent source of intelligence for NetOps teams looking to uncover the causes of performance degradation.

In our analysis of DNS data, we discovered that organizations often fail to optimize query resolution paths for DNS. Queries for external services almost always get routed to a centralized DNS resolver before they are routed out to a service provider on the internet for authoritative resolution.

This extra step adds significant latency to each query and unnecessary load to internal networks. The result is a poor end-user experience as queries are routed to a "local" external service that may be half a world away in the company's primary data center.

A more efficient method is to route traffic straight to trusted service providers through direct internet access or "internet breakout". Our analysis shows that intelligent routing of DNS traffic can save significant time and money when compounded across a worldwide organization.

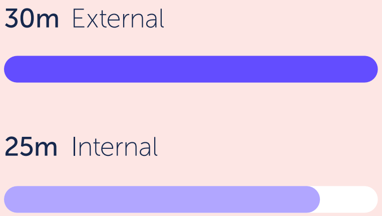
When one BlueCat customer discovered that 80% of all network traffic was bound for external trusted services (Fig. 3), they began routing it directly to the internet. As a result, they were able to optimally route network traffic, save on WAN costs, and provide a better user experience.

It isn't just query types that provide insights for network optimization. The responses to DNS queries also tell a revealing story about the health of a network.

SERVFAIL responses, which indicate that the DNS infrastructure was unable to locate an appropriate server to resolve the query against, is often evidence of a DNS misconfiguration. These mistakes almost always add unacceptable latency to a query. One network in the data study showed that 4.6% of queries returning SERVFAIL notices, significantly impacting their end-user experience until the configuration issue was resolved.

In addition to these broader examples of misconfigurations showing up in DNS data, we found many network-specific cases where DNS data provided the key to identifying the root cause of network configuration errors and pointing the way to remediation.

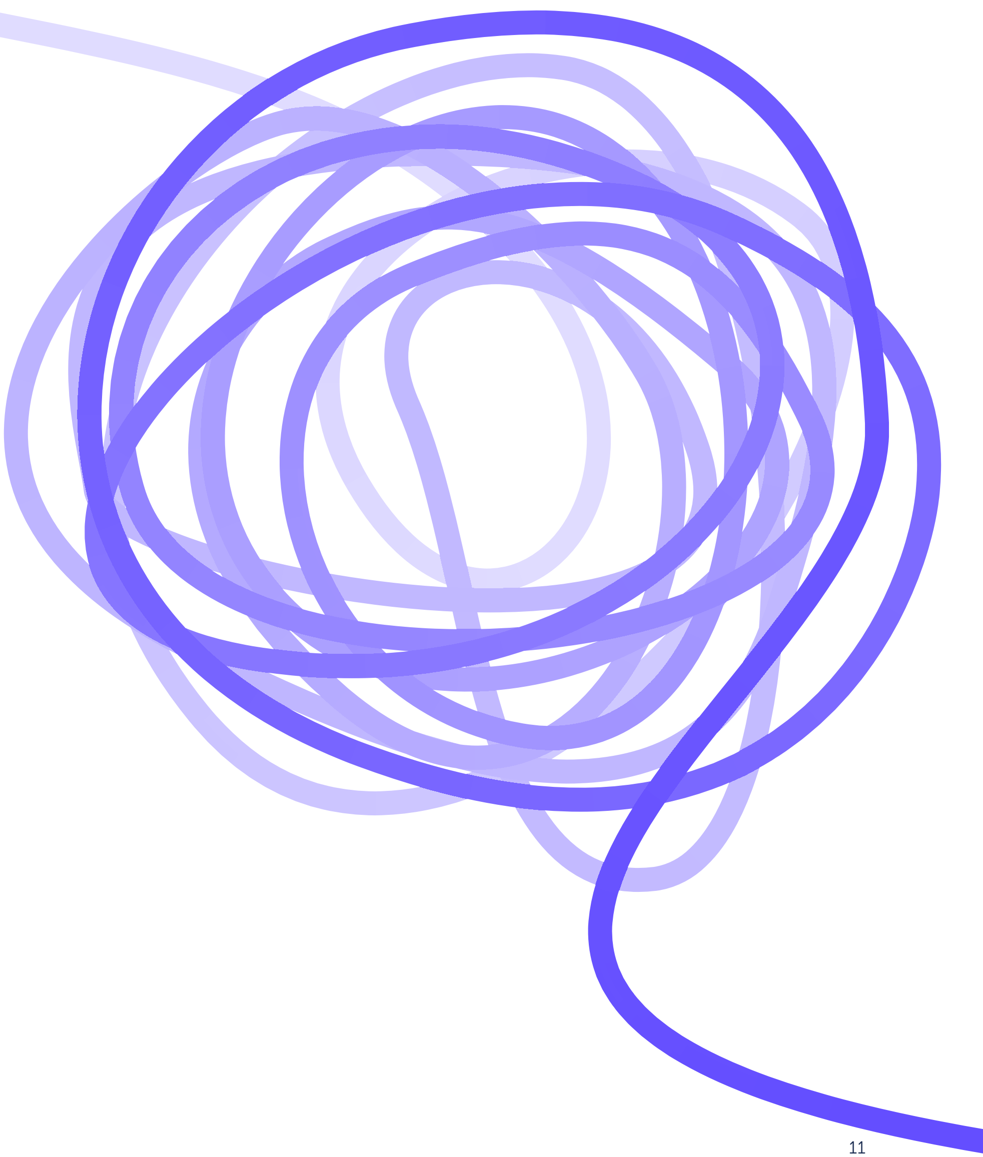
Figure 3
Internal vs. External Traffic Volume Latency



Source: BlueCat 2020 Trends

Finding the needle in the haystack

A BlueCat user noticed the declining performance of the company's virtual desktop infrastructure (VDI) when certain subnets with newer workstation images began to suffer from connectivity issues. Upon closer inspection, it was discovered the impacted subnets were experiencing high NXDOMAIN volumes, as well as a spike in anomalous PTR (reverse lookup) activity. The reverse lookups were all happening concurrently across the network.



After identifying the local firewall as the largest consumer of DNS on the network, the customer noticed that packets from the affected workstations included a large number of Link-Local Multicast Name Resolution (LLMNR) queries.

Further investigation revealed that a newer version of a workstation image had a firewall setting that enabled reverse name lookups on connection. The workstation image had LLMNR and NetBios enabled. The firewall would attempt to perform a reverse name lookup through a PTR query for every inbound connection.

Those queries failed because the clients were not consistently registering reverse records, resulting in an NXDOMAIN response. When the lookup failed, the client would send out an LLMNR broadcast to all other clients on the subnet. Those clients would then perform PTR queries on the same record, producing the same NXDOMAIN error. The resulting surge of lookups caused network performance to degrade.

Visibility into DNS activity allowed the network team to identify and address the issue. Just as importantly, they didn't chase any false leads—the DNS data showed them exactly what they needed to know and provided enough granularity to pinpoint the source of the problem.

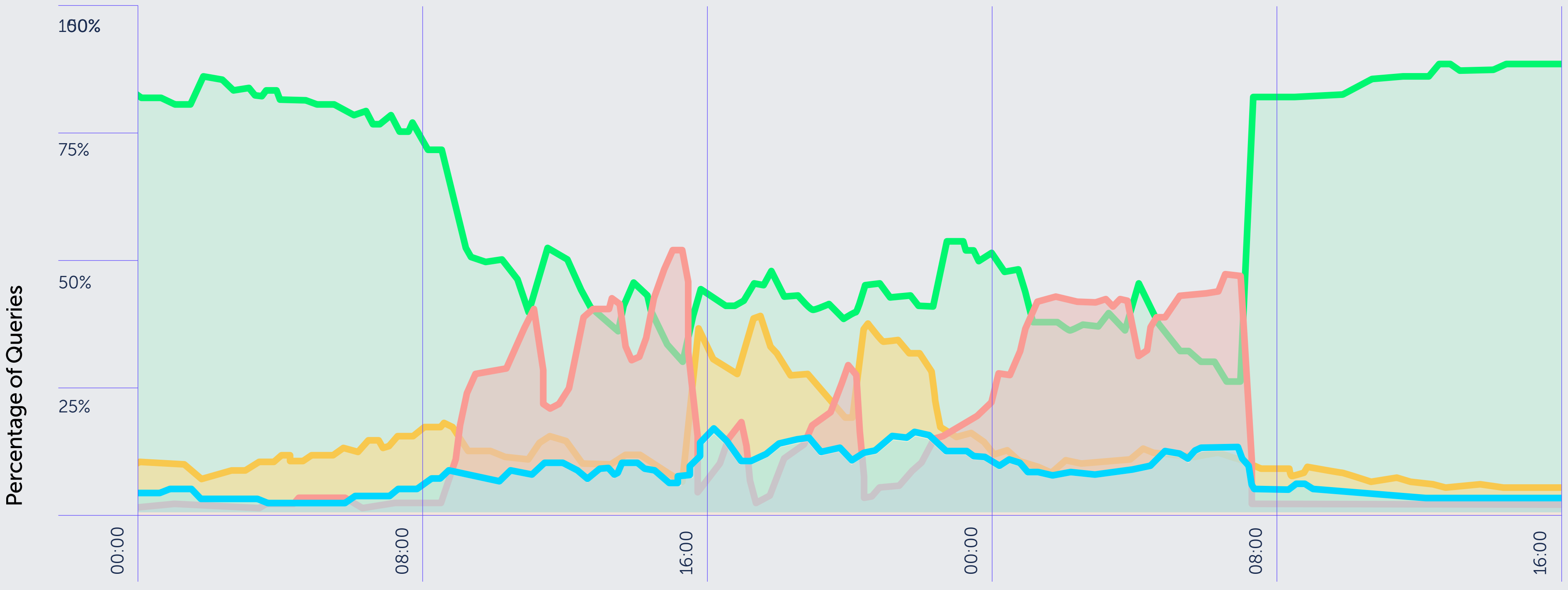


Figure 4
Query Resolution

Source: BlueCat 2020 Trends

Listen to the logs

The overall performance of DNS queries is also a leading indicator of network health. Since DNS resolution is typically the first step in any network communication, slow-performing queries can lead to slow-downs across the enterprise.

For one BlueCat customer in the financial sector, query latency can be the difference between a completed transaction and an abandoned shopping cart. By watching their DNS data, they were able to spot a performance blip where their resolvers went from a few milliseconds to over 200 seconds for a majority of their queries (Fig. 4).

Since this customer had a consolidated view of their systems, they were able to quickly spot a change that caused a misconfiguration of their DNS caching mechanism, roll it back, and restore normal function.

Rethinking NetOps KPIs

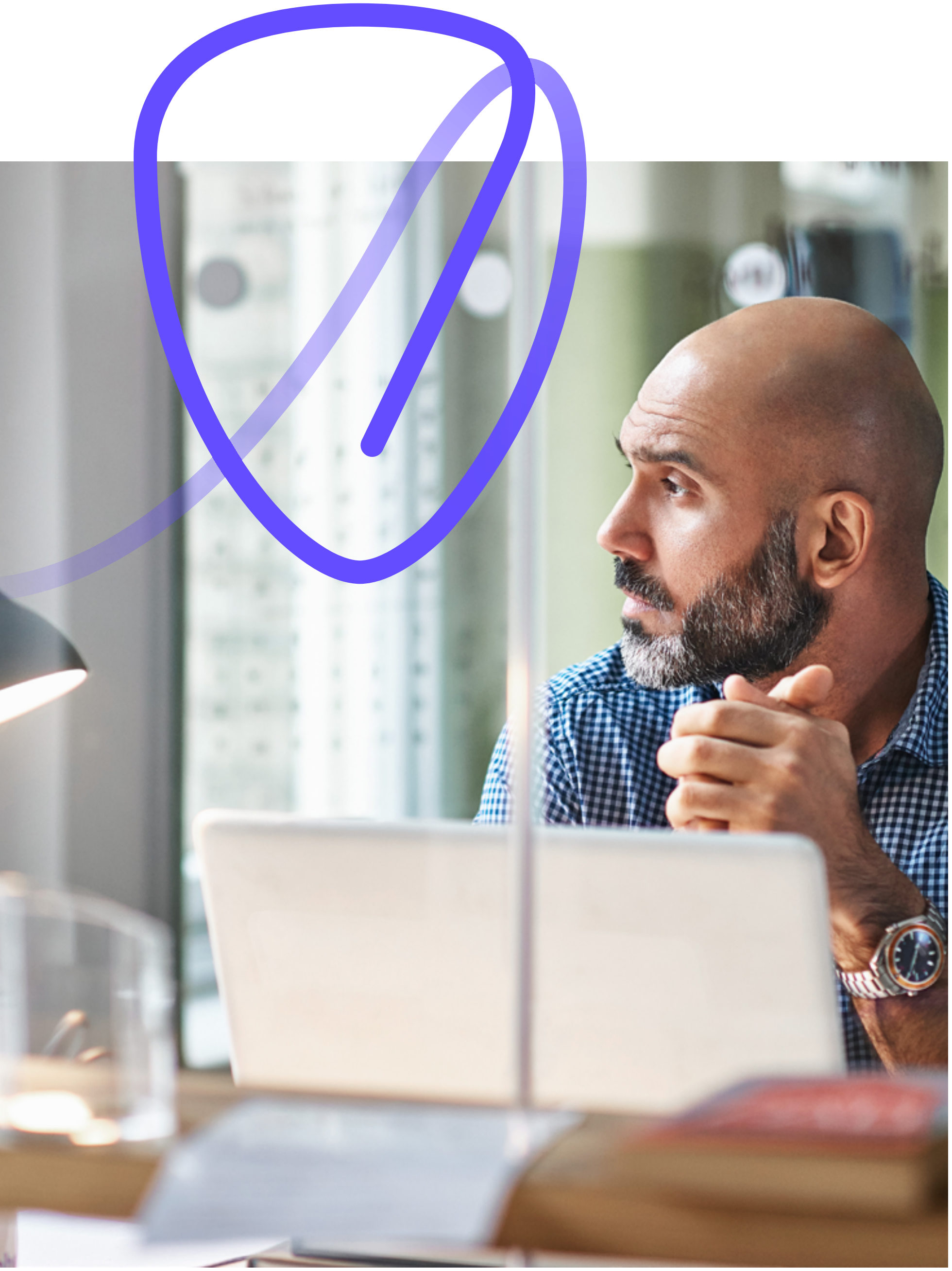
As the focus of network activity shifts to DevOps and the cloud, NetOps teams are rethinking how they measure success and contribute to business objectives. Legacy metrics such as uptime and latency are still relevant, but service delivery is a growing focus as IT departments move toward new business models.

In this context, DNS data offers a wide range of meaningful business metrics that can assess the value of a NetOps team in delivering services. Here are a few examples of meaningful network performance metrics which can be measured through DNS data:

- How quickly are failures identified and remediated
- How many network changes are automated
- How fast network services are updated
- How fast host records are provisioned

Taking host record provisioning as an example, a network which embraces automation should be able to provision a host record or an IP address in under two to three seconds. The ability to do these things quickly is not only a measure of network efficiency, but also of service quality. If it takes hours or days to provision a host record, employees are more likely to circumvent policies and turn to shadow IT.

Security's Second Chance



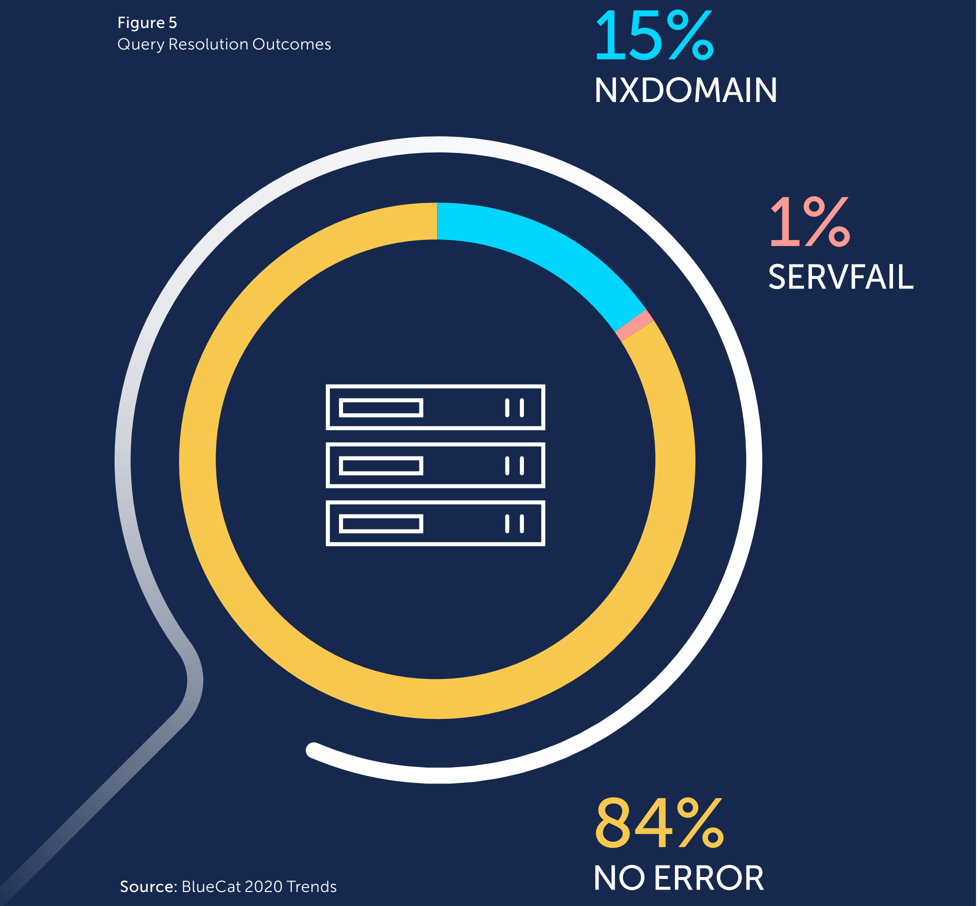
Security's Second Chance

DNS queries offer significant value for security teams, providing a comprehensive map of interactions between users, applications, data, and devices. When cybercriminals develop malware, they often focus on encrypting their web traffic and masking their malicious code. Almost all malware, however, uses DNS for command and control communication (C&C) as opposed to hard-coded IP addresses, making an analysis of DNS behavior an effective means of identifying attacks.

Intelligence about malicious domains or domains associated with non-business activities enables organizations to block traffic to certain websites. This can take the form of blocking malicious top-level domains or more granular action to block or monitor traffic to domains with a history of connection to malicious activity.

Looking at the DNS queries for this report, BlueCat found that a surprising 16% of DNS queries failed to resolve. DNS queries failing at this rate is significant and is likely the result of a combination of factors, such as application misconfigurations, stale internal DNS records, incorrect blocks by security controls, or typos made by users as they typed a web address in their browser.

Figure 5
Query Resolution Outcomes



Source: BlueCat 2020 Trends

Security's Second Chance

However, those failures could also indicate a potential security issue. Queries that fail for external domains are often indicators of malware trying to communicate with a C&C server that may have been taken offline or moved to a new location to avoid security controls. An example of malware leveraging DNS is a recent ransomware variant that tested for resolution failure as a way to remain undetected when triggered in a security sandbox solution. Security teams should pay close attention to any external queries that fail.

Examining DNS queries can easily uncover telltale signs of DNS tunneling, which attackers have used for years to sidestep security controls and exfiltrate data from secure networks. To do this, attackers can simply encode information into a DNS query destined for an external resolver, and then decode it there—creating a two-way communication stream that functions just like a VPN tunnel.

These efforts are easy to spot with the right tools in place. DNS tunneling looks unusual when compared to typical query names, which typically contain human-readable text. Such activity also triggers alarm bells because it is almost always high volume and high frequency, giving DNS data experts numerous ways to spot and block this traffic.

Combing through DNS data, we also found many queries directed to the long domain names, which are the hallmark of a domain generation algorithm (DGA). These threats are typically detected by looking for indicators such as a high level of entropy in the query text. Entropy scores are measures of randomness. The more random the query text is, the more likely it contains a domain created by a DGA to dodge detection by security tools. We found that entropy is often coupled with a very low frequency of queries being directed to the domain, which provides additional evidence of traffic attempting to fly under the radar to avoid detection.

Uncovering hidden threats

DNS query types can also be a telling sign of potential compromise. During BlueCat's analysis, we found many devices attempting to look up MX-type DNS records. Since MX records are only be used by mail servers, the presence of these requests could be another indication of DNS tunneling or data exfiltration.

Another potentially hazardous type of DNS query is the IXFR/AXFR query. These queries are typically used to perform zone transfers between primary and secondary (or master/slave) DNS servers. As a best practice, these types of queries should be restricted to authorized DNS servers via ACL. Any use of these queries outside that context may indicate a security threat such as DNS poisoning.

Our analysis also uncovered a variety of threats leveraging DNS., including Remote Access Trojans (RATs) like Koadic and banking malware such as Emotet. Performed properly, the examination of DNS logs or the use of DNS security tools offers organizations a second change at detecting threats that slipped by their other defenses.

Uncovering hidden threats

Threat Type	Description	Sightings
Remote Access Trojans	Remote Access Trojans (RATs) are malware programs that include a back door for administrative control over an infected computer.	**Koadic Trojan**—This is a post-exploitation toolkit that leverages built-in Windows functionality, delivering all the features expected from a modern RAT. Koadic was first released at DEF CON in 2017 and has since been leveraged in nation-state cyberespionage campaigns by various nation-state threat groups. **Minidionis Trojan**—A RAT discovered by researchers at Palo Alto Networks being leveraged in campaigns by the nation-state threat group CozyCar.
Banking Trojans	A Banking Trojan's purpose is to harvest online banking credentials and intercept banking transactions in real-time. This is typically done by hooking into a victim's browser to hijack active logged-in sessions to a bank website.	**Emotet** is a modular banking Trojan that often serves as a downloader or dropper of other banking Trojans. Emotet continues to be popular among attackers, with targets ranging from governments to financial institutions to the public.
Credential Stealer	Credential Stealer malware is a form of spyware that harvests a variety of credentials from a victim computer. These credentials include social media, banking, email, instant messaging, VPN, and FTP accounts.	**Pony Stealer**—Pony Stealer is a piece of spyware that can decrypt passwords for over 110 applications, including VPN, FTP, email, instant messaging, web browsers.
Crypto-Miner Malware	Crypto-Miner malware makes use of a victim's computing resources to mine cryptocurrency on behalf of malware controller to generate revenue in the form of crypto coins such as Bitcoin, Monero, or Ethereum.	**XMRig**—XMRig is a legitimate, open-source Monero CPU Miner. It has been abused for the past few years by cybercriminals who have included the XMRig code in their malware to make use of an infected computer's resources to generate Monero coins for financial gain.

Enabling a smart and focused response to cyber threats

The data we analyzed shows that improving security requires more than a simple "identify and block" response to threats. Understanding the root cause of a threat is often the key to effectively mitigating its effects. That usually requires digging deeper to find the network pathways exploited by malware, the spread of infected devices, and where data exfiltration requests are pointing.

DNS data often holds the context that threat hunters and security operators need for a smart, focused response. The ability to collect and analyze that data often originates with the network team, however. A collaborative, cross-departmental approach is required to truly reap the rewards of this valuable data set.

Most Frequented Domains

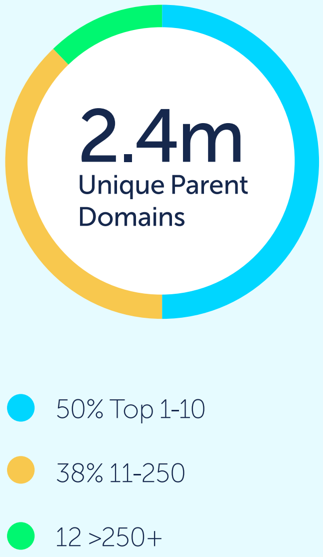
Most Frequented Domains

Our analysis uncovered interesting usage patterns that point toward both positive and negative implications for IT teams.

Of the queries analyzed, 2.4 million unique parent domains were queried. Half of the total queries were to the top 10 domains, while 38% were to the top 11-250 domains. Many of the most popular domains will sound familiar: Microsoft (160 million), Google (139 million), and Apple (116 million). These domains are the most prevalent due to updates and communication traffic for network devices and Windows.

Ten of the top 25 domains were internal, such as instant messaging servers, Active Directory services, and company intranets.

Figure 6
% of Queries by Top Domain Range



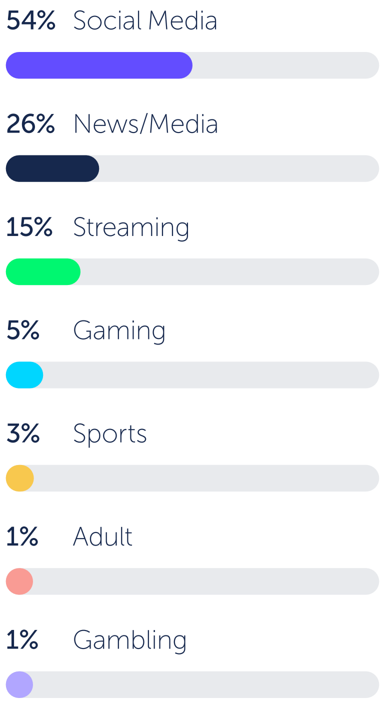
Source: BlueCat 2020 Trends

Where are your employees going online?

Surprisingly, only 3% of all queries were for non-business activity related websites. Where are those employees going online?

The answer depends on the vertical. Overall, roughly 54% of these domains were for social media sites. More than a quarter went to news sites, and just over 12% went to streaming sites.

Figure 7
Breakout of non-business related websites



Broken down by vertical, our analysis showed some key differences. The education sector saw the most use of social media, accounting for 61% of non-business activity. It also had the highest usage of non-business sites, accounting for 5% of overall traffic. For the financial sector, the largest percentage of non-business related queries belonged to news sites, which accounted for approximately 57%; social media accounted for about 14%. In the retail industry, the categories of the most queried non-business sites were news (45%) and social media (36%), respectively.

When it comes to social media across industries, Facebook is the most visited site, comprising 39% of social media queries. Snapchat was next with 32%. Instagram and Twitter tied for third with 8%.

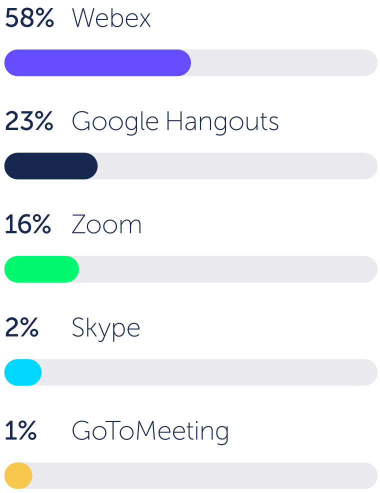
Given the relatively small percentage of queries to social media domains, the challenge of worker engagement may be overstated. The consistency of social media queries across industries also indicates that employers who stray from the mean should be concerned.

The expanding use of collaboration tools

Our analysis also sheds light on the most widely used business collaboration tools. WebEx is the most popular web conferencing application (58%), followed by Google Hangout (23%). As the population of remote workers continues to grow, it is safe to assume that the popularity of these applications will grow as well.

The different sectors also had different usage rates of cloud-hosted email and instant messenger applications. The government sector does not appear to be heavily leveraging IM or cloud email such as Yahoo! or Gmail, whereas the retail industry has higher usage rates of both. Education has the highest usage of cloud-hosted email. The differences in use may be tied to the security policies and threat landscape of particular industries.

Figure 8
Collaboration Tool Usage



Source: BlueCat 2020 Trends

Day in the Life

Day in the Life

For a closer look at usage patterns, we tried organizing DNS data by type of user. To observe a day in the life of a corporate device, researchers selected two random IPs from the logs for different 24- hour periods. Based on analysis of the DNS queries generated for those devices, two different personas were identified:

1 Sales Executive

2 Network Engineer

To get a look at how these devices were used, we have provided a more in-depth analysis that includes high-level metrics on query count, classification of the queries, and more.

Day in the Life
User generated queries

15% Sales Executive

7% Senior Network Engineer

Queries resulting from personal related browsing including (news, streaming, social media, and sports) and internal resources initiated by user.

Total # of Sales Executive queries: 2,811

Total # of Senior Network Engineer queries: 7,346

Application Usage

Understanding application usage via DNS query details provides insights into:

- Anomalous activity and emulation (malware beaconing, DNS tunneling, and more)
- Detection of rogue OS
- Non-OS related queries
- Utilization of non-approved applications
- User profiling based on social engineering and application usage
- Activity patterns of application investments
- Inventory of apps and device

Day in the Life
Machine generated queries

85% Sales Executive
93% Senior Network Engineer

Queries resulting from internal network configuration, application syncing, ad trackers, CDN, e-mail/IM updates, security updates initiated by machine

Total # of Sales Executive queries: 2,811

Total # of Senior Network Engineer queries: 7,346

Device Information

Device type: Windows-based/Mac-based

Understanding device information combined with DNS query details enables insights into:

- The eco-system communicating with the device and frequency
- Identification of new devices/types
- Activity patterns over time
- Inappropriate activity based on type
- Device misconfigurations

Spotlight

What DNS data says about the IoT devices in your home

With every person on earth now outnumbered by an estimated 6.58 devices, have you ever wondered what all those connected thermostats, TVs, refrigerators, and virtual assistants are actually doing on your home network?

As part of our analysis we thought we would see what exactly happens with home IoT devices over a 24hr period while you are away and what we found was interesting.

Home network behave a lot like devices on a corporate network. Aside from the domains they query, most IoT devices ask for updates and provide information on a very predictable timeframe.

For example:

Samsung Smart TV,
4,762 total queries over a 24 hr period to 217 unique domains

Google Home,
2,997 total queries over 24 hr period to 25 unique domains

Pioneer receiver,
1,754 total queries over 24 hr period to 9 unique domains

Highlights

- Home network devices are very predictable.
- The DNS query success rate is extremely high...
- ...Except when it purposely isn't.
- Netflix is extremely chatty.
- Google never stops talking.

The predictability of DNS traffic from IoT devices shows just how valuable DNS data can be in fortifying security defenses.

If the smart TV suddenly queries a domain outside of the standard handful of usual suspects, you should unplug it immediately. If your Pioneer receiver starts resolving 100% of its queries—including those against the deliberately false ones—you have a security problem.

Read more

Adaptive, Dynamic, Intelligent

Adaptive, Dynamic, Intelligent.

Managing enterprise networks has never been more complicated. Old school approaches will not work—today's organizations need a strategy that can adapt to meet the needs caused by that complexity instead of collapsing under it. **Automation is the order of the day.**

By automating and centralizing their DNS infrastructure, enterprises can remove the pains associated with complexity and create a dynamic DNS infrastructure that can respond to their needs. The pressure to use technology to deliver products and services faster and more effectively has put a premium on NetOps having the ability to quickly push out changes that will empower the business to improve their speed to market.

These capabilities combined with insights found in DNS and fueled from integrations with existing technology investments can improve scalability, enhance security, and ensure availability. In a world of rapid technology adoption, multiple clouds, and Internet of Things (IoT), today's enterprises need to ensure their approach to DNS enables them to reach the level of scalability they want, and the insights they need to improve decision making at the speed of business.

Tips from BlueCat DNS Experts

Supporting digital transformation means transforming how NetOps teams operate.

By focusing on delivering relevant, output-driven insights and embracing automation and scalability, businesses will be able to more effectively meet the demands placed on their networks by new digital initiatives.

This evolution requires changing everything from performance metrics to the level of collaboration between NetOps and other teams.

To achieve real NetOps transformation and synergy with DevOps teams, CIOs and network teams must:

Tips for IT Leaders	Tips for IT Practitioners
Implement culture hacks to accelerate the shift towards NetOps 2.0.	Translate business impacts into network requirements to gain insights from DNS.
Develop a hybrid IT workload placement strategy to maximize business value.	Break down monolithic network architectures to drive higher levels of automation and support for cloud deployments.
Invest in network agility by focusing automation on new network buildouts and non-change activities first.	Break down monolithic network architectures to drive higher levels of automation and support for cloud deployments.
Focus on metrics that drive quality service delivery using DNS data, in addition to uptime.	Align stakeholders around a published catalog of network services for DevOps teams.
Align personnel, processes, and incentives with a cross-discipline approach for DevOps/NetOps/SecOps.	Develop skills in network abstraction and scripting such as Python and Ruby.
Favor vendors that have open APIs to quickly meet integration needs for monitoring security, and network performance.	Accelerate provisioning and service delivery with Ansible, Chef, Git, Jenkins, Jinja, and Puppet.
Invest in skills development for NetOps teams with focused training on automation and analytics.	Build skills in public cloud networking such as AWS and Azure with associated APIs.
Analyze external domains and patterns used on the network over the last six-months to establish a baseline.	Develop a culture that leverages DNS data to enable security teams with meaningful context to stop emerging threats.
Act on DNS alerts and insights with security policies that block malicious activity.	Adopt or build the back-end infrastructure needed to collect comprehensive DNS logs.
Establish a recurring cadence to analyze and act on outlier patterns and anomalous activity.	Create a baseline for network traffic patterns to identify and anomalies in network performance and aid in root cause investigations.

Conclusion
Fuel digital transformation with insights from DNS

Conclusion
Fuel digital transformation with insights from DNS

DNS is often overlooked as mere network infrastructure. It's just supposed to work in the background, humming along without interruption. In the absence of a problem, most CIOs barely acknowledge its existence.

Yet as the data and insights in this report show, DNS can also uncover significant cost savings, provide early warnings against cyber threats, and unlock insights that benefit business operations.

DNS is especially important in the context of today's changing networks. Virtualization, software-defined networking, cloud, and other new technologies are creating a more distributed networking landscape. When DevOps and cloud teams are at the forefront of innovation, NetOps teams are struggling to maintain visibility and control on the back end.

Since it underlies every action across the enterprise, DNS is a key point of leverage for network administrators as they look to find their place in this new IT landscape. Using the right metrics and the right technology, NetOps teams can make DNS the common thread between security and DevOps teams, maintaining the pace of service delivery and moving business operations forward.

Every CIO should be thinking about how DNS can bring value to their business. Whether digital transformation is already happening or a future state, DNS and the data it produces will play a critical role in the success of any strategic IT initiative.

About BlueCat

At BlueCat, we deliver the flexible, scalable DNS solutions which today's NetOps teams need to stay relevant in a changing IT landscape. We see DNS as a critical thread that connects distributed, hybrid networks to the secure, automated, reliable core infrastructure CIOs want to deliver.

With this DNS service layer in place, CIOs and administrators can leverage the rich insights from DNS data to improve security and optimize network performance. This report is just the tip of the iceberg—DNS data reveals different insights for every network.

Contact BlueCat today to find out what DNS data can tell you about your network.

Disclaimer: The insights and observations contained in the report are representative of DNS data analyzed by BlueCat analysts.

bluecatnetworks.com