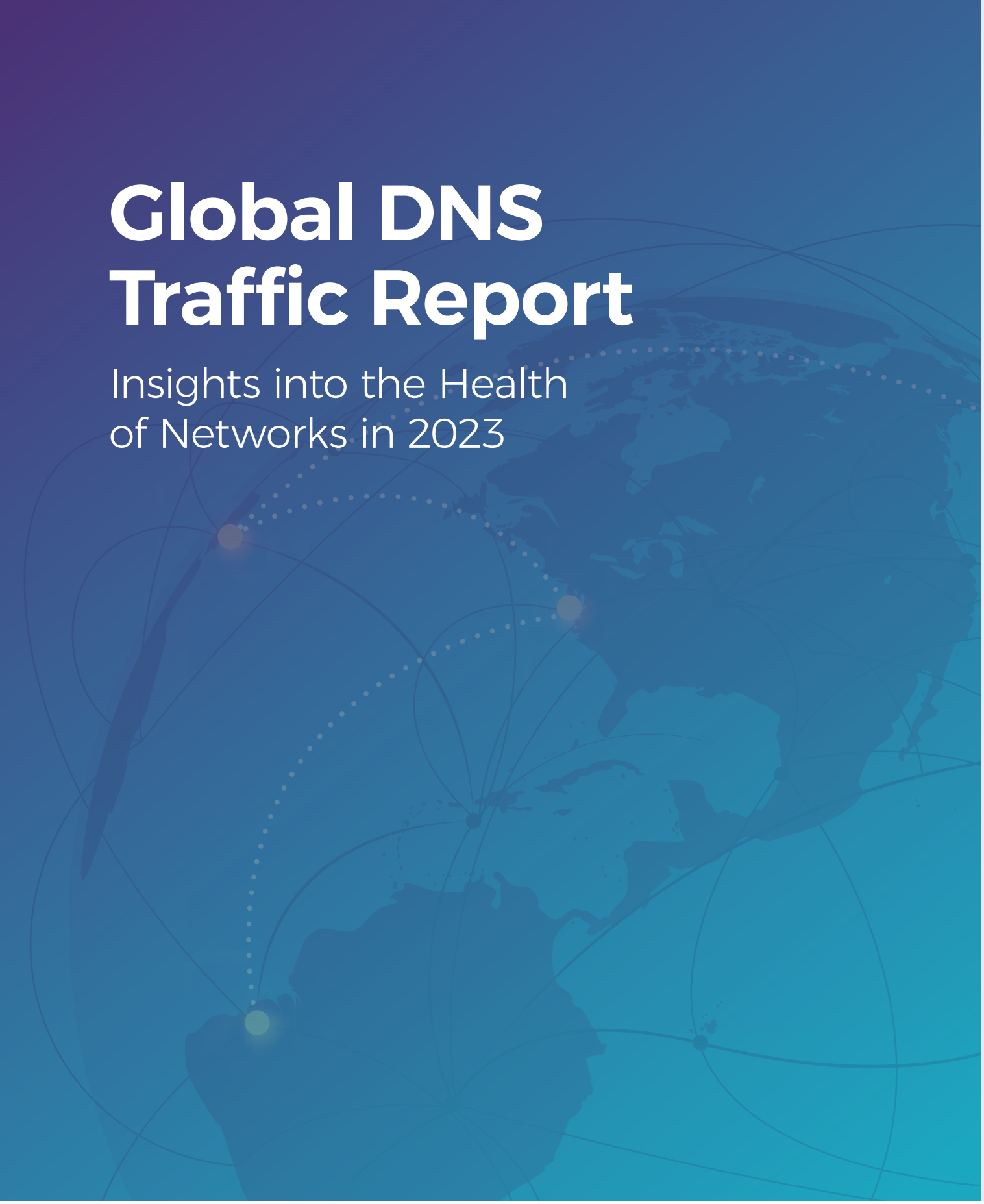
REPORT

Global DNS Traffic Report

Insights into the Health of Networks in 2023



NS1.

NS1.COM

As one of the largest authoritative DNS providers on the planet, NS1 resolves a significant percentage of the internet's total traffic. From the world's most notable brands to thousands of emerging startups, from applications to websites to online services, the requests resolved through NS1 Managed DNS reach every corner of the connected world.

NS1's position as the connection between users and online services offers a unique vantage point on the daily operations of the internet. Looking at the data flowing through NS1's servers, there's a lot to be learned about how we consume online applications, which technologies deliver internet traffic, and even how many queries never make it to their intended destination.

Early on, NS1 realized that specialized tools were needed to monitor and troubleshoot a network with the scale and complexity of a global player in authoritative DNS. To meet this challenge, NS1 developed Orb™, a network observability tool designed to capture and analyze relevant data on the network edge.

When we deployed Orb's powerful observability agents on NS1's Managed DNS infrastructure, it produced some fascinating insights about how the internet operates on a day-to-day basis. These query patterns produced some interesting trends that we thought the rest of the world would be interested in. NS1 customers can now leverage this data through DNS Insights, a feature of Managed DNS that helps to pinpoint the sources of misconfigurations that impact DNS performance.

This report is the first in an occasional series of insights we plan to share using data drawn from Orb and NS1 Managed DNS infrastructure. We hope it will be useful for network operators, analysts, and all those interested in how the internet works.

The insights in this blog are drawn from a 90-day pull of data from across the NS1 Managed DNS customer base in late 2022. That's over 7.54 trillion queries and 15.1 trillion packets - ***a consistent one million queries per second, 24/7/365.***

Geographically, 42% of the traffic we saw came from North America, 26% was from Europe, with the remainder scattered across Asia and the rest of the world.

IPv6 adoption still lagging behind projections

IPv6 was launched in **June 2012** to solve the challenge of IPv4 address scarcity while introducing advanced functionality designed for the internet of the future. Since that time, IPv6 adoption has been sluggish at best. Part of this is sheer organizational inertia, part of it is the complexity involved in making the change in certain industries, and part of it is that the use of IPv4 resources has been extended far longer than many predicted.

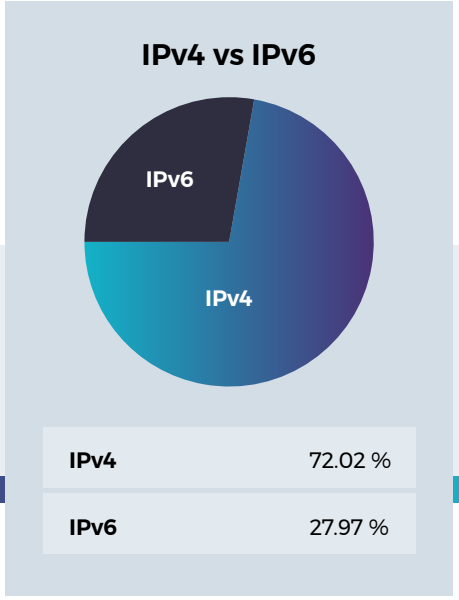
We attempted to examine IPv6 adoption using two different datasets. First, we examined the usage of IPv6 at the network layer between DNS resolvers and the NS1 authoritative DNS servers. Second, we looked at the percentage of inbound AAAA record requests to NS1's global infrastructure.

Network layer data

Our initial data pull from the network layer showed that just 27.97% of inbound queries came from infrastructure providers using the IPv6 protocol. This was a bit surprising to us - we had expected to see wider adoption of the IPv6 protocol among the large infrastructure providers that operate popular DNS resolvers.

IPv6 protocol adoption remains sluggish

Just 27.97% of inbound queries came from providers using IPv6



DNS layer data

We also took a look at the volume of A vs AAAA requests. Out of every 100 requests for either of these record types, 27 are for AAAA records and 73 for A records. Assuming that IPv6 capable hosts will be dual-stacked and request both A and AAAA records, then the percentage of IPv6 capable end systems would be approximately 37% (that is, 27 out of 73 single queries). This matches well with **similar IPv6 usage statistics** from Google, which also show usage hovering near 40%.

Even factoring in the complexities of definitively measuring IPv6 adoption and usage, the directional numbers indicate that the protocol still falls short of its true potential. This trend will likely continue unless large enterprises make it a priority. Realizing the operational benefits of IPv6 means taking it beyond test environments and forming concrete plans for a network-wide transition.

Dumpster dive: What response codes reveal about network performance

The vast majority of DNS queries are answered correctly, meaning the requestor was directed to the intended endpoint without issue. In our analysis, 86.2% of all incoming queries to our platform were resolved with a NOERROR response.

Where it gets interesting is when queries aren't resolved in the normal way, or aren't resolved at all. Here's a breakdown of the main response codes we observed and some hypotheses on why we're seeing them.

	VALUE	PERCENT
NOERROR	6.5 tri	86.7 %
NXDOMAIN	744.9 bil	9.9 %
REFUSED	175.6 bil	2.3 %
SRVFAIL	76.4 bil	1.0 %
YXDOMAIN	2.0 bil	0.0 %
NOTIMP	10.6 mil	0.0 %
FORMERR	7.2 k	0.0 %

NXDOMAIN

Just under 10% of all DNS queries came back with an NXDOMAIN response, which is the internet equivalent of "address not found." In other words, it means the requested domain could not be resolved to an IP address. NXDOMAIN responses can happen for any number of reasons, including (but not limited to) fat finger errors in typing out an address, broken links, and random label/dictionary attack activity.

We found a significant variation in the prevalence of NXDOMAIN responses between different customers. On the lower end of the spectrum, some companies manage to keep NXDOMAIN responses to around 3% of their overall traffic. Yet we also saw quite a few companies whose NXDOMAIN traffic was a whopping 60% of their responses!

NXDOMAIN traffic is an often ignored - but incredibly useful - source of data about network health.

About 10% of DNS queries tracked came back with an NXDOMAIN response, but for some companies, it was a whopping 60% of their responses - worth digging into!

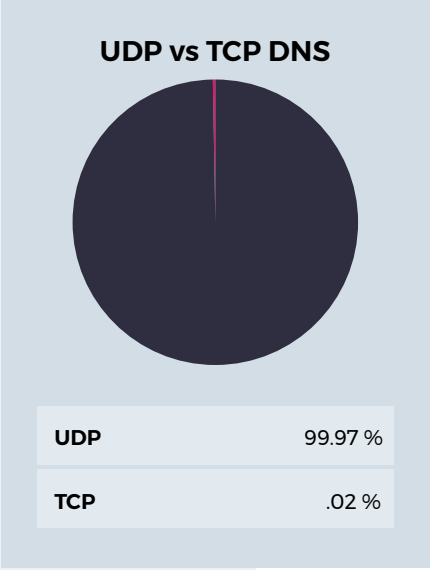
Some network teams consider the DNS queries that generate NXDOMAINs "garbage traffic." NS1 has a different perspective. NXDOMAINs can be an incredibly useful source of data about network health. Using the data at our fingertips, we work with customers to identify the root cause of NXDOMAIN responses to both improve the quality of their network architecture and lower the cost of delivering online services.

We've found that a surprising number of NXDOMAIN responses are caused by misconfigurations where internal domain names are inadvertently exposed. In extreme cases, these can expose sensitive information about devices and network architectures to the entire internet. More often than not, they simply result in inefficient use of network resources. Whatever the cause of NXDOMAIN responses, they are worth digging into.

Rare response codes

Our sample also returned data from a few of the more esoteric response codes:

- Around 0.027% of queries came back as **YXDOMAIN** - a domain that shouldn't exist, but does. Most often, this is the result of an overly long domain name that can't be parsed - usually connected to **feedback loops** created during a domain name forwarding process associated with the DNAME record type.
- About 0.00014% of queries got a NOTIMP response - usually an indication that the nameserver doesn't support the requested query type. Clearly NS1 sees a wide range of query types, so the fact that this anomalous behavior is so small testifies to the rarity of seeing something NS1 doesn't support.
- 0.00000010% returned FORMERR - an indicator of packet-related issues. Sometimes this means there's more than one query in the packet, or the query packet already contains a response. This response is a relative of YXDOMAIN, and sometimes associated with misconfigurations in DNS tunneling.



Faster is better: UDP beats out TCP usage

Not all DNS queries create connections in the same way. The User Datagram Protocol (UDP) is built for speed and efficiency, and is designed around a “best effort” model. The Transmission Control Protocol (TCP) is slower but also more reliable, building a stronger connection to ensure the validity of data.

TCP is primarily used for file/zone transfers, along with mail and text applications. UDP is used for services where the response is expected to fit within a single packet.

NS1’s data show that UDP is by far the most used protocol on the internet for DNS queries that flow from recursive to authoritative servers. 99.973% of DNS queries handled by NS1 used UDP, where only 0.027% used TCP.

Usage of brand-new HTTPS record type surging

Beyond the protocols used in DNS traffic, there are many different query types - each of which provides specific kinds of information to the requesting server.

HTTPS records, which are an efficient way to gather information on multiple data sources in a single information exchange, account for about 9.5% of the traffic in our data pull. The related “service binding” or SVCB records are less popular - only 0.001% of records in our data pull.

HTTPS is a relatively **new DNS record type** that NS1 was one of the first to support, and clearly it’s been a popular choice right out of the gate. The rapid adoption of this type is a clear indication of pent-up demand for new data transmission methodologies that go beyond the typical offerings of web servers.

It is worth noting that adoption of HTTPS is a bit lopsided - browsers and authoritative DNS providers are **enabling it** faster than companies can stand up support. In particular, default support for HTTPS queries in iOS 14 (and later) and macOS is probably driving traffic numbers. Many of those browser queries probably come back with NOERROR/NODATA responses and will continue to do so until word gets around.

DNS resolver usage: Who "runs" the internet?

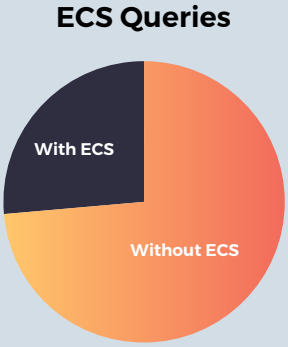
Which companies handle the most recursive DNS traffic? Which companies actually "run" the internet? We broke out usage of different recursive DNS resolvers to see what the market share numbers look like.

- **Google** is the clear front runner at a little over 30%. This includes traffic from 8.8.8.8 (clearly the most popular public resolver) and Google Cloud Platform, which some companies use as their authoritative DNS provider.
- At a little more than 16%, **AWS** comes in second. Unlike Google, AWS doesn't run a public resolver, so this is a more direct representation of organizations that are running DNS directly from the cloud. This number may also reflect the number of applications that query AWS zones for standard operations.
- **Cloudflare** (9.3%) is third on the list, representing a combination of its own DNS resolution service, its publicly available 1.1.1.1 resolver offering, and the Cloudflare CDN service.
- **Akamai** (5%) is fourth, primarily for its CDN offering, but there's also probably some of its DNS service as well.
- **Cisco's OpenDNS**, which includes Cisco Umbrella, came in fifth overall with 4.4% of the traffic in our data pull, putting it well behind Google and Cloudflare for public resolver traffic.
- Telecom giants appear next on the list, with **T-Mobile** (4%), **AT&T** (2.5%) and **Comcast** (2.1%), rounding out the top cohort. T-Mobile's global footprint, as well as its position as the backbone for a fair amount of interbank traffic, likely accounts for its prominent position against the other telecom companies.

We also broke out resolver usage by point of presence (PoP) and saw some interesting regional trends. Overall, European traffic runs through open public resolvers far more often than in other places. In our Marseille PoP, over 75% of traffic goes through Google, Cloudflare, or OpenDNS. In the Frankfurt PoP, it's over 65%. By comparison, those three resolvers only source 35% of traffic in the Atlanta PoP, and 41% of traffic in the Washington DC PoP.

Beyond the overall default to a privacy-centric approach in Europe, this also speaks to heavier reliance on ISP-based resolvers in the United States, many of which don't utilize third-party services. We've also found that many smaller ISPs in North Africa and the Middle East use Google Public DNS as a default service and connect to the closest NS1 point of presence in Europe.

What ECS tells us about the balance between performance and privacy



ECS Queries	
Queries without ECS	73 %
Queries with ECS	26 %

EDNS Client Subnet (ECS) is a DNS extension designed to find the most efficient routing for responses. It was originally created to help improve CDN performance. By transmitting only subnet-related information on top of the "traditional" DNS packet, ECS can significantly improve performance, particularly in cases where geographic targeting can make a tangible difference in response times.

The speed enabled by ECS responses can be offset by reduced data privacy in some cases. This is why some public resolvers like Cloudflare and Quad9 have **stopped supporting ECS** for recursive resolution (although Cloudflare's CDN still uses it for performance reasons).

The use of DNS over HTTPS (DoH) also has an impact on ECS usage. DoH-enabled resolvers typically don't support ECS, so queries originating from browsers with DoH automatically enabled (like Chrome and Firefox) will not have the ECS header added to their query by the resolver, leading to lower overall ECS usage numbers.

Overall, around 26% of queries run through NS1's systems in our data pull utilized the ECS extension. There's a lot of regional variation underneath that average; higher ECS usage often corresponds to use of Google's resolver services.

Looking at the data by PoP, Marseille leads the pack in ECS usage at just over 45% of all queries, which makes sense as it's also the #1 PoP for queries resolved by Google. Toronto (44%) and Hong Kong (40%) also show high ECS and Google resolver usage. On the other end of the spectrum, Seattle (8.2%), Miami (12%), and New York (13.2%) rank among the lowest PoPs for ECS usage. In general, ECS usage is lower in the United States (19.9% on average) than in Europe (27.6%) or Asia (27.6%).

When you correlate the public resolver data with the data about ECS usage, some interesting data points emerge. Canada ranked #2 in use of ECS but #9 in use of public resolvers, suggesting that Canadian ISPs are "all in" on ECS in ways that ISPs in other countries aren't. The opposite was true in data coming from our point of presence in Germany, which was #2 in resolver distribution but just #7 in ECS usage. Looking further into the data, this is probably non-ECS-enabled traffic from surrounding countries, as German ISP traffic at this location is primarily ECS-enabled.

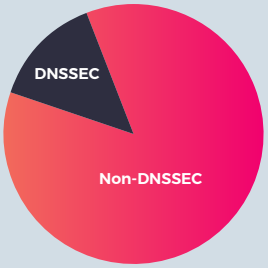
Security last: DNSSEC usage continues to lag

DNS Security Extensions (DNSSEC) use digital signatures and public key cryptography to authenticate DNS data. They've been a key component of internet security for a long time but are notoriously underutilized. Our dataset shows that DNSSEC adoption trends continue to lag well behind where they should be.

Our data captured queries where the resolver requested a DNSSEC-enabled answer and we responded with a signed answer.

Just 14% of the queries hitting NS1 infrastructure utilized DNSSEC signing.

DNSSEC Usage



Non-DNSSEC Queries	86 %
DNSSEC Queries	14 %

When we broke out the DNSSEC-enabled responses by ASN, we found significant variation by infrastructure provider. Google by its sheer size constituted the largest raw number of DNSSEC queries, but on a percentage basis only 5% of traffic we saw from Google was to a zone that had DNSSEC turned on. None of the major cloud providers or US-based ISPs saw more than 10% of our responses signed using DNSSEC. A few European ISPs and telecom providers broke the 50% barrier, but their overall number of queries was also rather low.

Delve deeper into your data with DNS Insights

DNS data is a powerful indicator of network health, resilience, and performance. In this report, we've shown just some of what we've learned from looking at traffic on NS1's own infrastructure. Now we're proud to make this same data (and more!) available to NS1 customers directly.

DNS Insights, a feature of NS1's **Managed DNS** offering, provides in-depth data feeds and dashboards to help network teams identify the root cause of misconfigurations, NXDOMAIN traffic, DDoS attack vectors, and more. With a dataset that's both larger and more in-depth than any other DNS provider, DNS Insights gives you the network intelligence you need to identify and mitigate a wide range of networking issues.

DNS Insights is powered by **Orb**, an open source observability tool developed at NS1. Orb delivers analysis and insights right on the network edge, and its "small data" approach dramatically lowers the cost of observability. With a few simple steps, you can deploy Orb in minutes - and even the hosted version (at orb.live) is free.

If you're an NS1 customer, ask your sales or customer success representative about DNS Insights, or try out Orb on your own at **orb.live**.

To learn more about DNS Insights, **contact us** or **visit our website.**

About NS1

With NS1's premium DNS and traffic steering solutions, enterprises do more with DNS by turning the workhorse of their network into an engine of innovation. Companies around the world depend on NS1 to keep their businesses online all the time, identify network performance anomalies, and lower the cost of delighting audiences. NS1 is headquartered in New York and has more than 850 customers across the globe, including Dropbox, Fox, Salesforce, LinkedIn, and eBay.