

Four Reasons To Outsource Your DNS

Your company's website is up. Servers are churning transactions. The network is pumping data. Life is good.

But everything in IT can change quickly. Today's slightly sluggish network could become tomorrow's downtime disaster. No matter what challenge may arise, you don't get extra time, staff, or budget to deal with it. Plus, since the whole company relies on IT, everyone notices when you're underwater.

Still, no one offers you condolences. When business users don't have what they need to run, you're held responsible. Marketers will be in your office in minutes. Business operations will prod you for a fix. End users will eat you alive. Plus, the CIO is watching it all go down.

What if you could deal with your problem du jour or, even better, work on projects that are more creative and strategic, and have peace of mind knowing that mission-critical processes are still going full throttle?

Managed DNS services can give you that confidence. With someone else managing your DNS, you can improve your own workflow since you will have the time to focus on what you do best (rather than having to put out DNS fires time and time again). Need a little convincing? Here are four reasons you should outsource your DNS services.

1) Better Network Performance

Say your company is expecting a boost in traffic during critical times—a new campaign or product launch, holiday shopping season, a breaking news story—are you ready for it? If not, a wanted boost can turn into a liability by weighing down the network, slowing load times and creating website latency. In a worse scenario, your network could become completely clogged, blocking all traffic from getting to your site—resulting in lost revenue, a tarnished brand, and eroded consumer confidence.

Managed DNS services, like Dyn, feature high-performing networks that not only ensure that users can get to your site but also that the site is highly responsive. Since information travels at half the speed of light (300,000km/second,) it ends up taking about 1 millisecond for every 200km that the data needs to travel. The further away your user is from your information, the longer the load time (e.g. information traveling from Newark, NJ, to Los Angeles, CA, has about 90ms of latency).

The median eCommerce page took 8.56 seconds to load for first-time visitors—14% slower than just three months before. **A long-standing best practice is to load a site in three seconds or less.**

"State of the Union: Ecommerce Page Speed & Web Performance," Radware,

WHITEPAPER

Providers place points of presence (PoPs) in major cities where fiber optic cables intersect to get data to your DNS servers faster. Your ISP likely has PoPs as well, but it won't have the same levels of DNS knowledge and expertise as a managed DNS provider, which will be better equipped to manage the unique issues relevant to DNS. Also, most self-hosted or ISP DNS networks are unicast which carries a number of limitations.

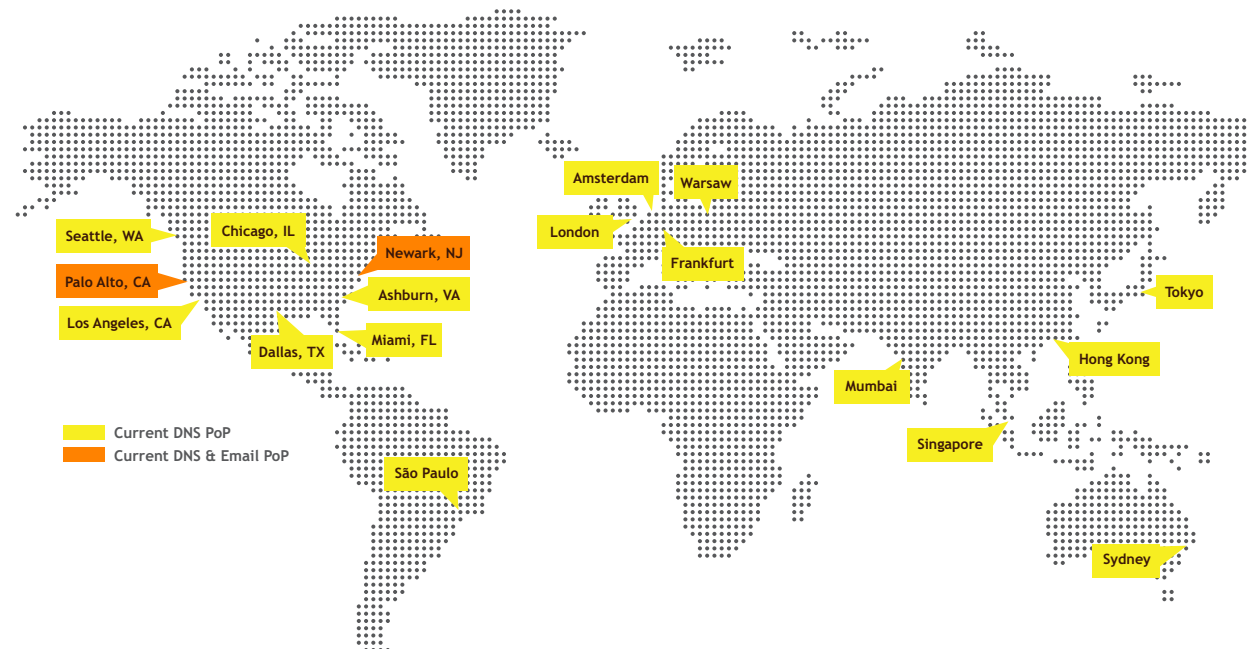
In a unicast network, a single PoP going down results in timeouts and slowing down DNS queries whereas in an anycast network, if there is a problem with one PoP, traffic can be rerouted to any of the other PoPs to avoid a disturbance. Additionally, there is no control over which datacenter queries will be directed, to which can result in poor performance especially if the query and the data center are on different parts of the world. Finally, adding additional unicast PoPs is difficult to do and they do not scale, unlike adding new PoPs to an anycast network which is more flexible.

Another approach that a managed DNS provider will use to deliver better network performance is to rely on anycast servers to route traffic to the most appropriate PoP. A good provider will be able to control their anycast routing system, monitoring and optimizing the routing between the query and your DNS server. Your ISP is probably equipped to monitor within its own network only, lacking external monitoring. This limited visibility increases the likelihood of an outage and makes one harder to find and fix when it does occur.

2) Improved Trust And Reliability

PoPs and anycast servers can shrink website latency and prevent full-on downtime. But what happens when there's a complete failure within the network?

Dyn's global PoP locations



WHITEPAPER

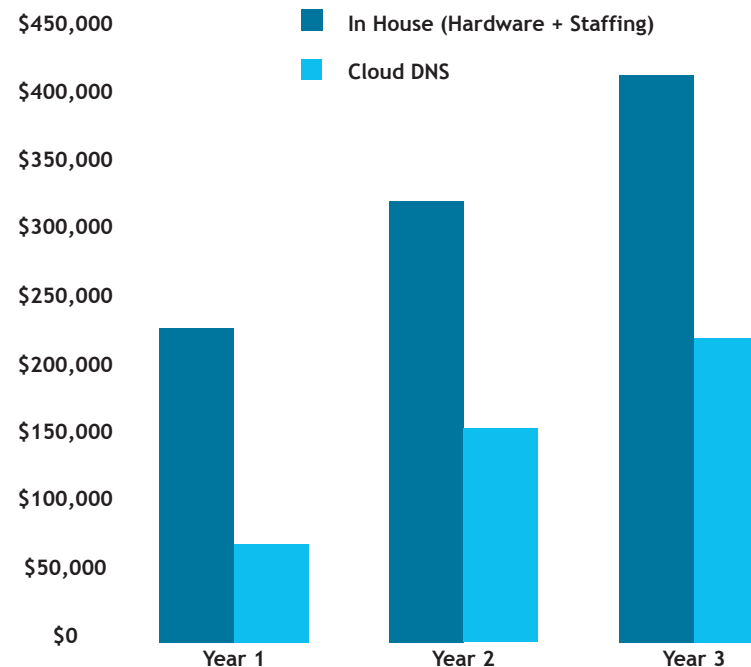
With thousands of miles of cables and systems around the country and world, some part of the infrastructure is bound to fail at some point.

Managed DNS services can provide failover protection, ensuring that your traffic gets to your site, even if the first-choice PoP infrastructure goes dark. In that case, your traffic is automatically rerouted to an online PoP, rather than hanging there, so that the query makes its way to your DNS server with undetectable disturbance. With managed DNS services, your web customers will be able to trust that your site will be available when they need it. This is a core feature of anycast routing and its resiliency and ability to route around problems. Unicast networks do not get this luxury.

But website reliability and trustworthiness can be threatened by a more than simple infrastructure failure. Attackers look for opportunities to launch DDoS and DNS amplification attacks, which intentionally overload networks to prevent your traffic from getting to you. Availability is only one issue in this scenario. No user wants to visit a website that has earned a reputation for being haunted by cache poisoning or registrar hijacking. A lack of DNS security can severely damage your reputation and shatter consumer trust.

Managed DNS services provide risk mitigation for known and up-and-coming threats with the latest technologies—all overseen by security experts. These providers typically build out some of the largest infrastructures in the world to ensure that there is excess capacity to respond to any threat. Many self-hosted solutions have limited networks and bandwidth capacity.

The graph below shows the cumulative growth of the costs of in-house DNS versus outsourced DNS year over year which include operational and capital expenses versus outsourcing expenses respectively.²



WHITEPAPER

3) Low And Predictable Network

A well-managed DNS requires more than a high-performing, reliable network. DNS servers and clients are critical too, and to ensure optimal website responsiveness, businesses should place these servers close to their users—whether across the country or around the world. Few businesses have the resources to build and staff data centers everywhere their customers are. Businesses have traditionally looked to external data centers, renting space and infrastructure. Additionally, they still have to staff people to remotely manage the equipment.

When companies choose to self-host their DNS, they, typically choose to use only one or two data centers. This can save costs, but in the end can ultimately cost more than whatever was saved by having so few data centers. Having limited data centers is very risky and in the case of an outage, your website could be down for an unknown amount of time (especially if you only have one data center).

With managed DNS, you get all the benefits of a robust infrastructure and DNS expertise without the capital cost or additional training. There is no need to buy hardware, install software, or hire more IT personnel to manage and maintain the infrastructure. You can rest easy knowing that with managed DNS, you have a team of DNS experts dedicated to monitoring the service. If something happens in the middle of the night, they'll be on it and will most likely be able to fix it before you even wake up.

4) DNS Expertise

Celebrating the benefits of DNS expertise may seem over the top. After all, you've been running your DNS in conjunction with your ISP, perhaps for years. How confident are you that it's operating at its best? Many self-hosted or ISP DNS infrastructures are rarely ever touched unless something breaks. Plus, many ISPs only have 1 data center, meaning that if it goes down, so does your website. This can cause problems in performance or even downtime that could be otherwise avoided with a Managed DNS provider who regularly monitors the infrastructure.

Even true network expertise rarely translates to expertise in DNS, which has unique issues and extends beyond networks into server operating systems, software updates, load balancing, customer interfaces and physical and

LEARN MORE ABOUT DNS SECURITY
THREATS BY READING OUR WHITE PAPER
**5 DNS Security Risks That Should
Be Keeping You Up At Night**

DOWNLOAD AVAILABLE AT:

<http://bit.ly/laB9VyW>



WHITEPAPER

virtual servers. While you may have experience in all of it, do you really have the time to continually optimize your DNS? Advanced features such as failover, load balancing, or geolocation are concepts that take time to master—time that most people who aren’t solely focused on DNS in their companies aren’t able to spend.

DNS experts are passionate about what they do. DNS is their livelihood, and these professionals have more at stake when it comes to managing it. Website downtime will put you in the hot seat for a while because it’s a critical business function, but for a managed DNS provider, it’s the only business function that matters. There can only be uptime.

Dyn – DNS Experts At Your Service

Dyn has DNS experts ready to keep you online all the time with our managed DNS services specifically built for enterprises. Our professionals are driven by their work and care about the DNS community, actively participating in the Internet Architecture Board, DNS Security Extensions (DNSSEC) Industry Coalition, DNS Operations, Analysis, and Research Center (OARC), Internet Engineering Task Force (IETF) and Internet Corporation for Assigned Names and Numbers (ICANN).

Our services are packed with features, offer extreme system scalability, and 24x7 customer support from people you’ll like to talk to. We’ve been delivering industry-leading web speed and uptime for more than a decade.

You already have a tremendous amount of responsibility to keep your business operating at peak performance. Let the DNS experts at Dyn take care of what we do best, so you can focus on projects to move your business forward.



I E T F[®]



➔ Give us a call to learn more about outsourcing your DNS with Dyn.

1. "Forecast Overview: Public Cloud Services, Worldwide, 2011-2016, 4Q12 Update," Gartner, February 2012.
2. <http://www.cdnetworks.com/wp-content/uploads/2013/12/CDNetworks-CloudDNS-ROI-D5-EN.pdf>