Ebook:

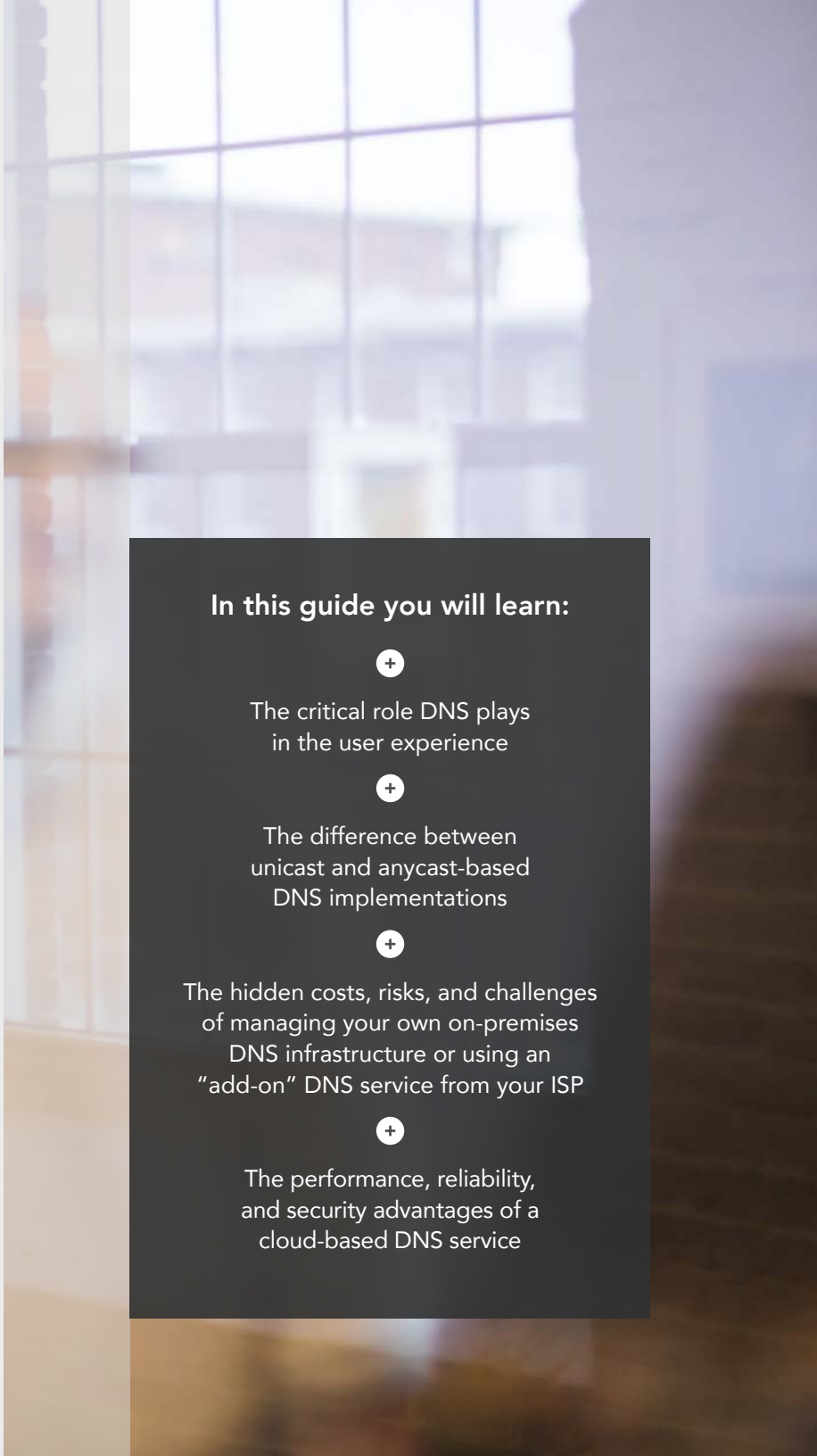
HOW CLOUD-BASED DNS IMPROVES DIGITAL PERFORMANCE AND RESILIENCE

ORACLE® + Dyn

dyn.com 603 668 4998 @dyn

High Availability DNS Reduces Downtime Risk and Improves End-User Experience

How Redundant DNS Services Provide Resilience and Improve Application Performance



In this guide you will learn:

- The critical role DNS plays in the user experience
- The difference between unicast and anycast-based DNS implementations
- The hidden costs, risks, and challenges of managing your own on-premises DNS infrastructure or using an "add-on" DNS service from your ISP
- The performance, reliability, and security advantages of a cloud-based DNS service

Introduction

DNS is the first link in your digital supply chain. Every user's first interaction with your website begins with a series of DNS queries. Poor DNS performance can lead to slow page loads, dissatisfied customers, damage to your brand, and lost business—so a "set it and forget it" approach to DNS simply doesn't work in the digital age.

That's why cloud-based, managed DNS services are now the norm for born-in-the-cloud companies—and increasingly for enterprise companies as well. They can enhance DNS performance, resiliency, and scalability, helping you ensure superior user experience worldwide. This paper reviews the features and benefits of a cloud-based DNS service.

DNS Overview

The Domain Name System (DNS) is a distributed internet database that maps human-readable names (like www.dyn.com) to IP addresses, enabling users to reach the correct website when entering a URL. Every user's first interaction with your website begins with a series of DNS lookups. When a user enters your company's URL, a DNS query is routed to the authoritative DNS name server that contains the address mappings for your company's Internet domain.

Getting There Is Half the Fun

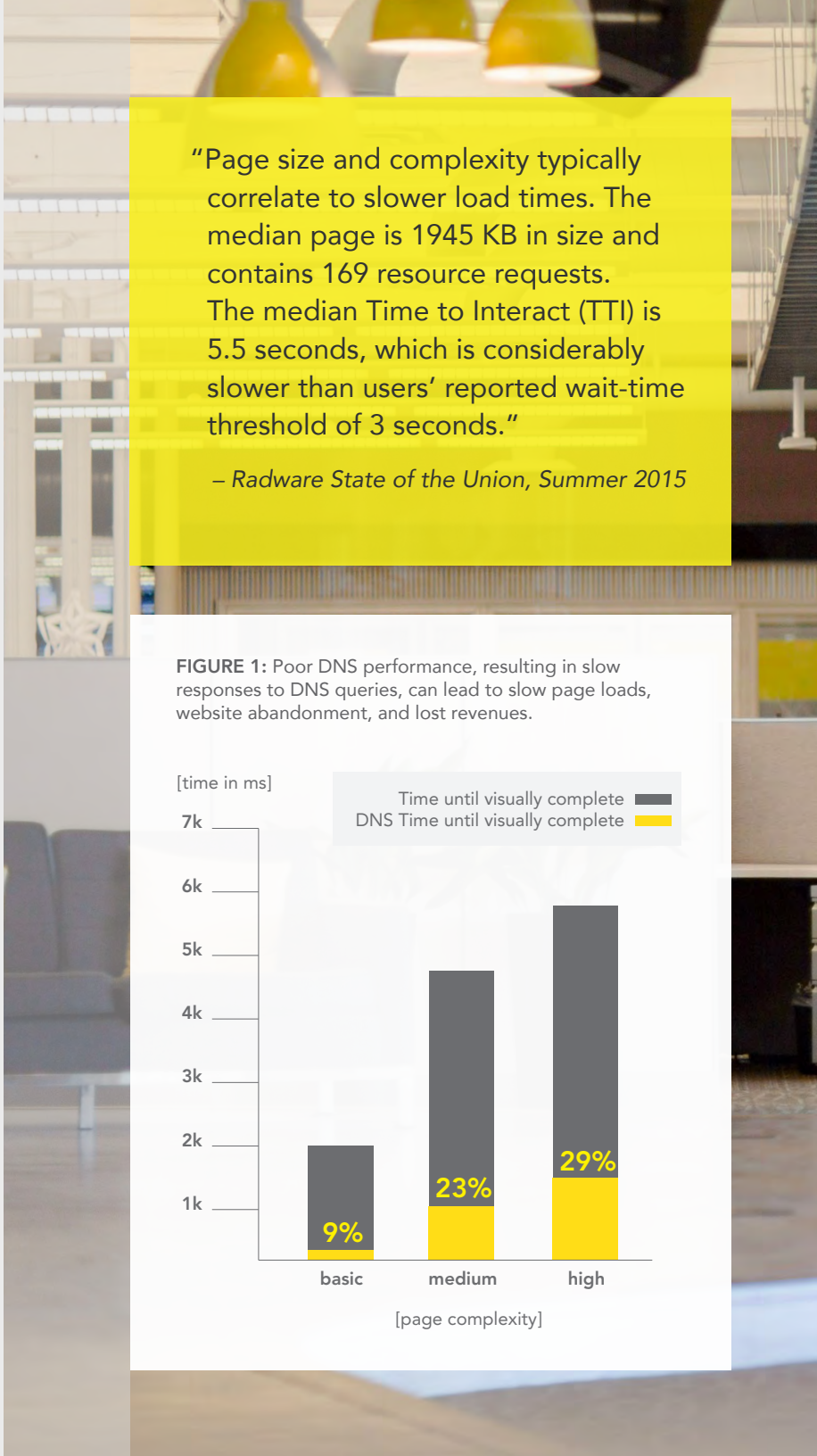
Your website and web application content is probably scattered across the Internet—some of it hosted in your data center, some of it distributed across content delivery networks (CDNs), and some of it with a cloud provider.

For example, a single web page can involve dozens of DNS lookups–and a page cannot load until all DNS requests are completed. In our internal testing, Dyn saw that, for complex webpages, DNS resolution comprises as much as 29 percent of initial page load time (See **Figure 1**). Architectural approaches like microservices are only increasing reliance on third-party functionality in modern sites and applications.

DNS is responsible for steering users to the appropriate content source. If your DNS name servers are unreachable because of hardware problems, configuration errors, or network issues, users may not be able to access the content on your site.

Time Is Money

DNS queries are subject to network transmission and propagation delays as they make their way across the internet traversing intermediary routers. Network latency impairs the user experience. The greater the roundtrip latency, the slower the response to the DNS query.



"Page size and complexity typically correlate to slower load times. The median page is 1945 KB in size and contains 169 resource requests. The median Time to Interact (TTI) is 5.5 seconds, which is considerably slower than users' reported wait-time threshold of 3 seconds."

– Radware State of the Union, Summer 2015

FIGURE 1: Poor DNS performance, resulting in slow responses to DNS queries, can lead to slow page loads, website abandonment, and lost revenues.

Unicast Addressing vs Anycast Addressing

Distributed DNS networks can be implemented using two distinct standards-based IP addressing schemes: unicast addressing or anycast addressing. The unicast approach is far simpler to implement, but the anycast approach offers significant performance and resiliency benefits.

Unicast addressing delivers unpredictable results and less consistent performance.

The DNS request may be answered by any Point of Presence (PoP) and potentially increasing latency.

With a unicast approach each of your company's DNS nameservers (or server clusters) is assigned a unique IP address which resolves to a single (thus uni) physical location. The recursive DNS nameserver (typically owned by the user's ISP) maintains a table of your domain's nameservers and their corresponding IP addresses. When a user enters your company's URL, the recursive server arbitrarily[1] performs a request to the IP address of one of your DNS nameservers which then returns the IP of the asset the user is trying to reach. You have no control over which of your nameservers the recursive server selects. A user in China could be served by a nameserver in North America. And a user in the U.S. could be served by a nameserver in Europe.

Anycast addressing optimizes DNS performance, enabling consistent user experiences across the globe.

The DNS request is answered by the closest Point of Presence (PoP) for the fastest possible DNS performance.

With an anycast addressing scheme, all your DNS nameservers are broadcast from many locations around the globe from a each IP. When a user enters your URL, the recursive DNS nameserver resolves to the closest location of your DNS nameservers. The IP network automatically routes queries to the "closest" nameserver using BGP.[2]

1 Initially, this is arbitrary. Over time, recursives will store response information to make this less arbitrary directing queries to preferred nameservers. However the initial responses to the sub-optimal nameserver, as well as daily checks, would still be performed. This is known as Round Trip Time (RTT) banding (see: dyn.com/blog; May, 2012)

2 BGP directs the query to the DNS nameserver with the lowest hop count.

Distribution Is Key

You can extend DNS performance and resiliency by installing a network of geographically distributed name servers. By deploying multiple DNS name servers, you can eliminate single points of failure and ensure continuous service in the event of individual server problems or network outages. By distributing DNS name servers closer to users, you can reduce network transmission delays and router propagation delays, accelerate DNS responses, and improve the end-user experience.

Unicast Versus Anycast Addressing

Distributed DNS networks can be implemented using two distinct standards-based IP addressing schemes: unicast or anycast. The unicast approach is far simpler to implement, but anycast offers significant performance and resiliency advantages.

With a unicast approach, each of your company's DNS name servers is assigned a unique IP address. DNS maintains a table of your domain's name servers and corresponding IP addresses, as shown in Figure 2.

FIGURE 2: Unicast addressing delivers unpredictable results

When a user enters your URL, DNS arbitrarily returns the IP address of one of your DNS name servers. You have no control over which name server DNS selects. A user in China could be served by a name server in North America, and a user in the U.S. could be served by a name server in Asia.

With an anycast addressing scheme, all your DNS name servers share a common IP address, as shown in Figure 3. When a user enters your URL, DNS returns the collective anycast address for your DNS name servers. The IP network automatically routes queries to the geographically "closest" name server.

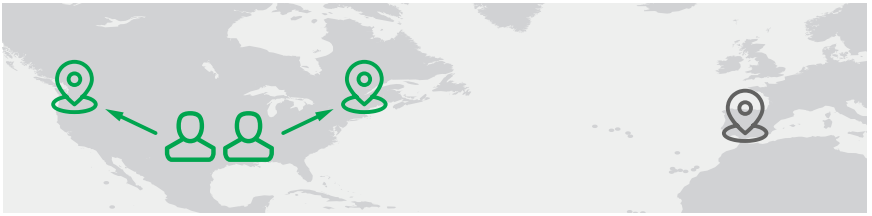


FIGURE 3: Anycast addressing optimizes DNS performance and enables consistent user experiences across the globe

Technically speaking, the BGP routing protocol employed in the IP network directs the user to the DNS name server with the lowest "hop" count. Each router along the path constitutes a hop and introduces delay. The use of anycast accelerates DNS resolution by minimizing the number of router hops between the user and the DNS name server.

The anycast approach offers a variety of performance, reliability, and security advantages:

- **Performance.** Anycast accelerates DNS resolution by automatically directing DNS queries to the "closest" DNS name server.
- **Reliability.** Anycast provides predictable and more efficient failover mechanisms. Anycast dynamically removes unreachable name servers from IP routing tables; and queries are deterministically directed to the "closest" active server.
- **Security.** Unicast exposes the IP addresses of individual servers. Attackers can initiate targeted DDoS attacks against specific physical servers or virtual machines. Anycast mitigates security threats by concealing the addresses of individual servers and automatically distributing attacks across collections of compute resources.

Are You Ready to Implement In-house?

Businesses that manage their own DNS infrastructure typically install one or more name servers in each corporate data center. Most employ unicast addressing schemes[1] and rely on a relatively small number of name servers (2 to 3 servers).

You can optimize DNS performance and resiliency by implementing a global anycast network. However, engineering, deploying, and operating a large-scale DNS implementation is a resource-intensive and time-consuming proposition, beyond the financial means of most corporate IT organizations. (See sidebar)

Implementing a global anycast network in-house is also fraught with challenges and risks:

- Enabling anycast across public networks can be difficult or impossible—most network service providers do not support anycast addressing for commercial customers
- Deploying DNS name servers in your corporate data centers is inherently risky; if your corporate data network goes down, you lose DNS services as well
- You will need to implement new security solutions to mitigate DoS/DDoS threats and you may need to hire security experts to help
- Designing, building, and managing a global DNS network steals resources from other critical IT projects

1 In a 2014 emedia survey, fewer than 30 percent of organizations managing their own DNS infrastructure indicated they use anycast addressing.

Global DNS networks are costly and complex

Designing, installing, and managing a large-scale DNS network takes time, money, and resources.

Upfront Expenses

- Design the network
- Identify colocation facilities for
- Areas outside corporate data centers
- Establish peering and transit relationships with network service providers
- Hire incremental staff with DNS and security expertise
- Purchase and install server hardware
- Procure and configure DNS software
- Acquire and implement security solutions

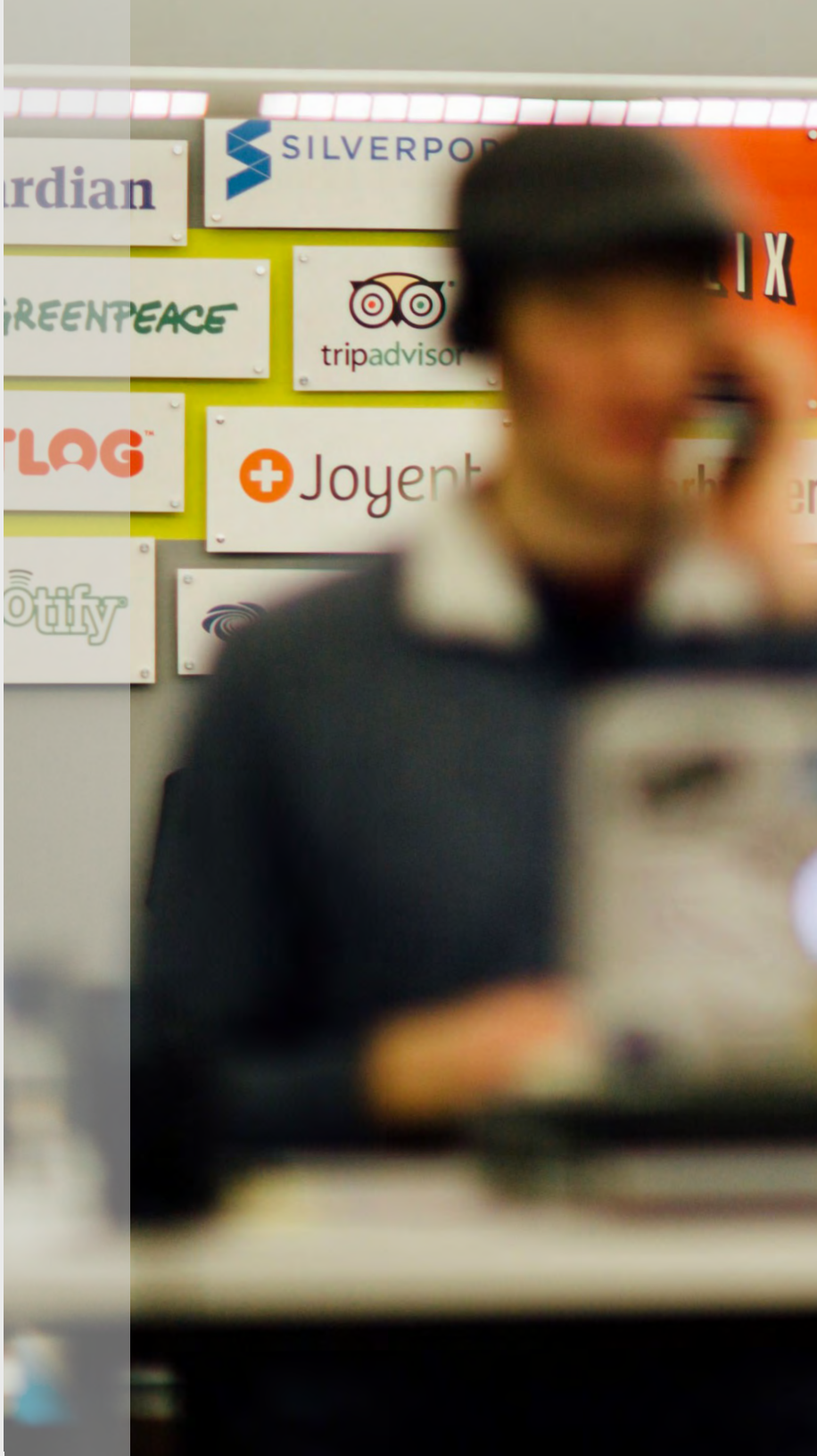
Recurring OpEx

- Ongoing network administration
- Recurring rack space, power and maintenance costs

Cloud-based Services Optimize DNS Performance

You can improve results, contain costs, and make better use of valuable IT personnel by leveraging a cloud-based DNS service. The top managed DNS service providers have the global DNS infrastructure and deep DNS expertise to ensure your success.

- **Global Performance and Scalability.** DNS service providers operate large-scale anycast networks with multiple points of presence (PoP) around the globe. They accelerate DNS resolution by automatically steering queries to the closest PoP, ensuring consistent user experiences around the world. On-demand bandwidth accommodates surges in traffic during periods of peak load.
- **High Availability.** DNS service providers run highly resilient networks with no single point of failure. They operate out of geographically distributed, high-availability data centers on separate power grids, flood plains, and fault lines. They can also deploy fully redundant servers and install connections to multiple ISPs to ensure uninterrupted service in the event of equipment failures or network outages.
- **Strong Security.** DNS service providers take a multilayered approach to security, employing a variety of measures to establish trust and defend against threats. They retain dedicated security experts who closely monitor industry trends and proactively update security systems and practices to thwart malicious attacks and mitigate risks.
- **Easy-to-use APIs.** Most DNS service providers offer development tools and APIs to help you streamline integration with external applications and automate routine DNS configuration tasks.
- **Expertise and Support.** DNS service providers employ full-time DNS and network security experts, and offer 24/7 technical support to help keep your website running smoothly around the clock.



Conclusion – Now Is the Time to Make the Move to Cloud

Creating a highly scalable, reliable, and efficient DNS infrastructure takes time, money, and expertise. You can accelerate your success and contain costs with a cloud-based service. Cloud-based DNS also exposes myriad opportunities to leverage the DNS infrastructure for global load balancing and traffic steering across hybrid environments. You'll gain a variety of functional and financial benefits, including:

- **Increased DNS performance and reliability.** Enjoy all the scalability and resiliency advantages of a global anycast network.
- **Better business results**. Greater DNS performance translates directly to better user experience, improved customer satisfaction, and increased revenues.
- **No ramp-up or build-out costs.** Avoid all the expenses and risks associated with designing and deploying a worldwide DNS network – DNS expertise is hard to find.
- **Reduced network management expenses.** Minimize ongoing operational expenditures, because the provider manages the DNS infrastructure.

Rethink DNS.

Oracle Dyn is global business unit (GBU) focused on critical cloud infrastructure. Dyn is a pioneer in DNS and a leader in cloud-based infrastructure that connects users with digital content and experiences across a global internet. Dyn's solution is powered by a global network that drives 40 billion traffic optimization decisions daily for more than 3,500 enterprise customers, including preeminent digital brands such as Netflix, Twitter, LinkedIn and CNBC. Adding Dyn's best-in-class DNS and email services extend the Oracle cloud computing platform and provides enterprise customers with a one-stop shop for infrastructure as a service (IaaS) and platform as a service (PaaS).

ORACLE® + Dyn

dyn.com 603 668 4998 @dyn