

Ebook:

THE #1 QUESTION YOU SHOULD ASK ANY POTENTIAL DNS VENDOR

ORACLE® + Dyn

🏠 dyn.com

☎ 603 668 4998

🐦 @dyn

Ebook: The #1 Question You Should Ask Any Potential DNS Vendor

Introduction

The DNS is an often-overlooked protocol. Historically, many companies believed they could either run their own DNS service in-house or simply use a bundled option provided by their hosting or CDN provider. However, with the rise in DDoS attacks and continued migration to the cloud, the mission-critical nature of the DNS has become quite apparent to companies around the world. As a result, many are searching for a managed DNS provider.

At the first glance, many of these competitors seem similar, but there is one question every prospective DNS buyer should ask of a vendor: did you build and do you operate your own network?

The way they answer that question should influence how you react to the rest of their pitch. If they say no, then they are simply providing you with theory -- solutions they hope will work. If they say yes, and, just like you, they did build and now operate their own network, then what follows are recommendations and best practices based on first hand experience running a DNS network that's trusted by the world's most-admired digital brands.

Like many vendors, Oracle + Dyn often talks about the impact the internet has on a company's network, and we provide tips and tricks on how to improve performance. We are qualified to make these suggestions because we run a massive network, which gives us great insight that we can share with our customers. In this Ebook, we'll look at three specific areas (at right), that we have found crucial to building and operating a network.

This guide will explain:



How we build a world class network

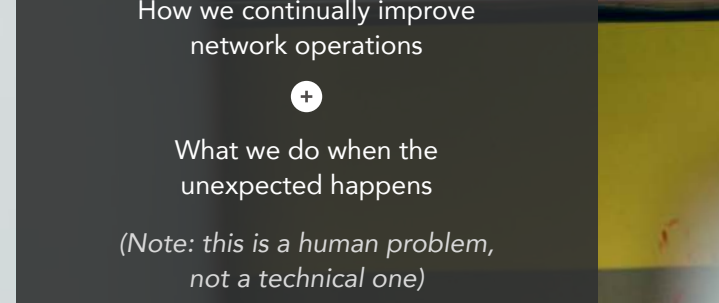
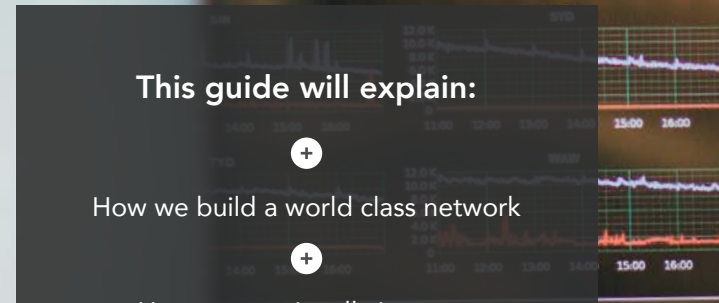


How we continually improve network operations



What we do when the unexpected happens

(Note: this is a human problem, not a technical one)



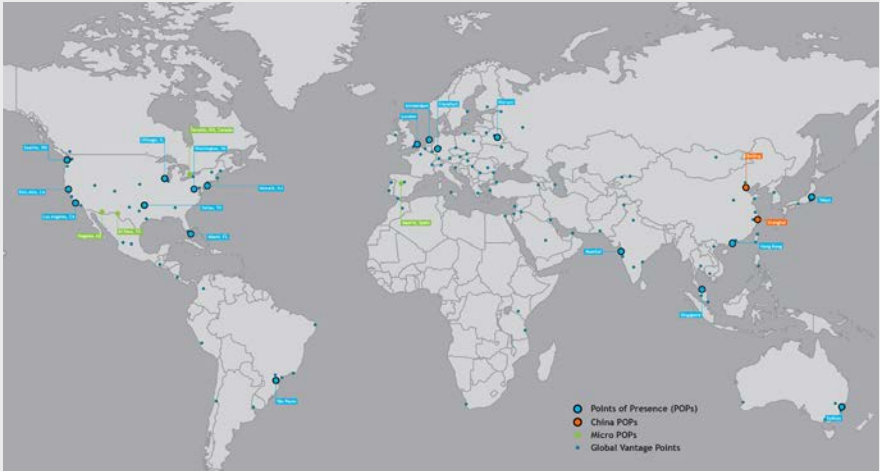
The latter two steps are crucial because operating a network is like repairing an airplane in mid-flight. Once you start you can't stop, and so you have to figure out how to deal with whatever is thrown at you. While this information can be useful for your own architecture planning, it should also instill confidence in Dyn as a vendor. For a key infrastructure component like DNS you do not simply want to have a vendor. A vendor takes the parachute and jumps when the plane looks like it will crash. You need a trusted partner that will be there by your side helping steer you to safety.

Build for Success

Global Distribution: The first step to building a world class network is to have geographic distribution. We have various points of presence (PoPs) all across the globe, primarily driven by customer demand (see below). These include 18 primary PoPs, and two in China, which are unique in that they are behind the Great Firewall of China and optimize in-country performance. Additionally, Dyn has micro-PoPs and traceroute collectors, which help us collect telemetry, which we feed back into our products to improve features like geolocation.

While distribution is beneficial to end user optimization, it also makes your infrastructure both globally and locally elastic. This allows you to add or remove capacity, which ensures a high level of redundancy allowing you to be responsive to real-time situations.

Elasticity affords you the ability to take sites down and repair them without obstructing the general flow of end-user traffic. We have built our infrastructure in a way that this action is replicable within each site so that we could withdraw an individual server or router and upgrade them without any impact being felt by customers.



The Dyn network (Managed DNS, Email Delivery, Recursive DNS) is deployed on top of a global IP network, consisting of 20 existing facilities and connectivity from a mix of Tier 1 Internet Service Providers (ISPs). The network has been split into two diverse constellations (A and B) to provide active/active failover between constellations in the event of catastrophic failure.

Within each constellation, we distribute traffic to multiple data centers, providing global active-active load balancing using the Anycast routing technique. This network allows Dyn to offer its customers a world-renowned level of service and reliability.

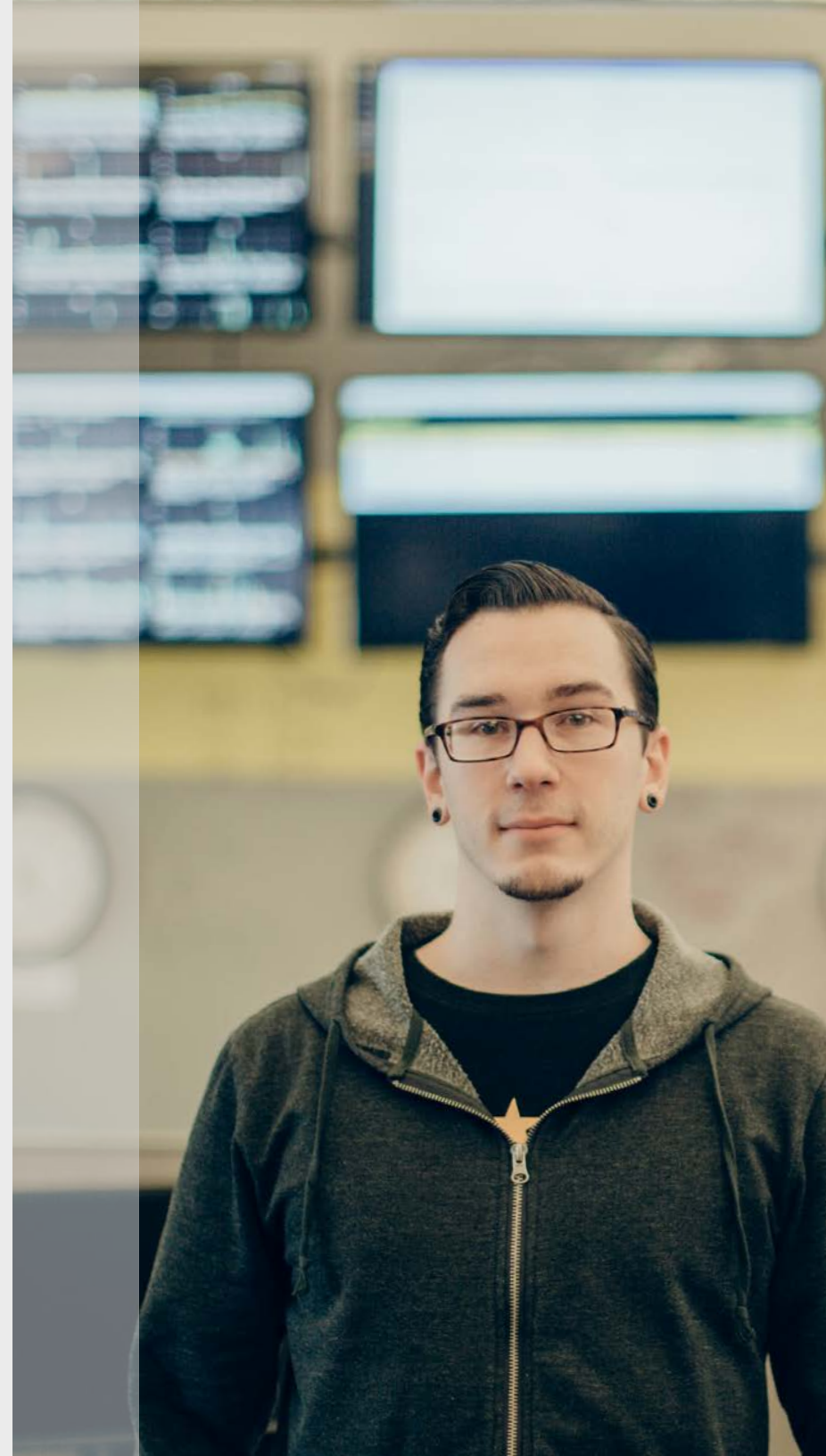
Data Center Operations: If you were to visit a Dyn data center, you would see the type of data center that would attract a child: very colorful. But those colors are not for play. They represent a data center that is color coded and properly planned. While this process takes more time upfront, it also means that each of our data centres around the world are similar.

This means when our remote hands (i.e. local engineers) show up and have to pull a cable, there is no ambiguity in what they are doing. This is an example of where architecture and process meet. If you build your infrastructure to be adaptable and redundant but then don't take the final step and create processes that make the actual execution of that possible then it is useless. That is why it is so important to build and run a network because they are two-sides to the same coin.

Measurement: The decisions you make on your infrastructure are only as good as the data you use to make them. That means what you measure is important and how you incorporate those results into your actual work flow is most important. We have tried to instill measurement and telemetry into our development culture and so we're measuring a lot of factors from Real User Monitoring (RUM) to how we fare against our competitors to fine-grained detail from deployed systems.

Speaking of development culture, continuous deployment and continuous integration are key to having an agile infrastructure that is both mature and stable and allows you to quickly respond to events and customer request. This mindset allow us to adapt to changing operational conditions as easily as we can deploy new features. This goes back to the previous section on elasticity. Our elastic edge platform is designed for mobile service loads and designed specifically to make anycast easy.

We put a lot of thought into building our infrastructure. So how do we plan for the unexpected?

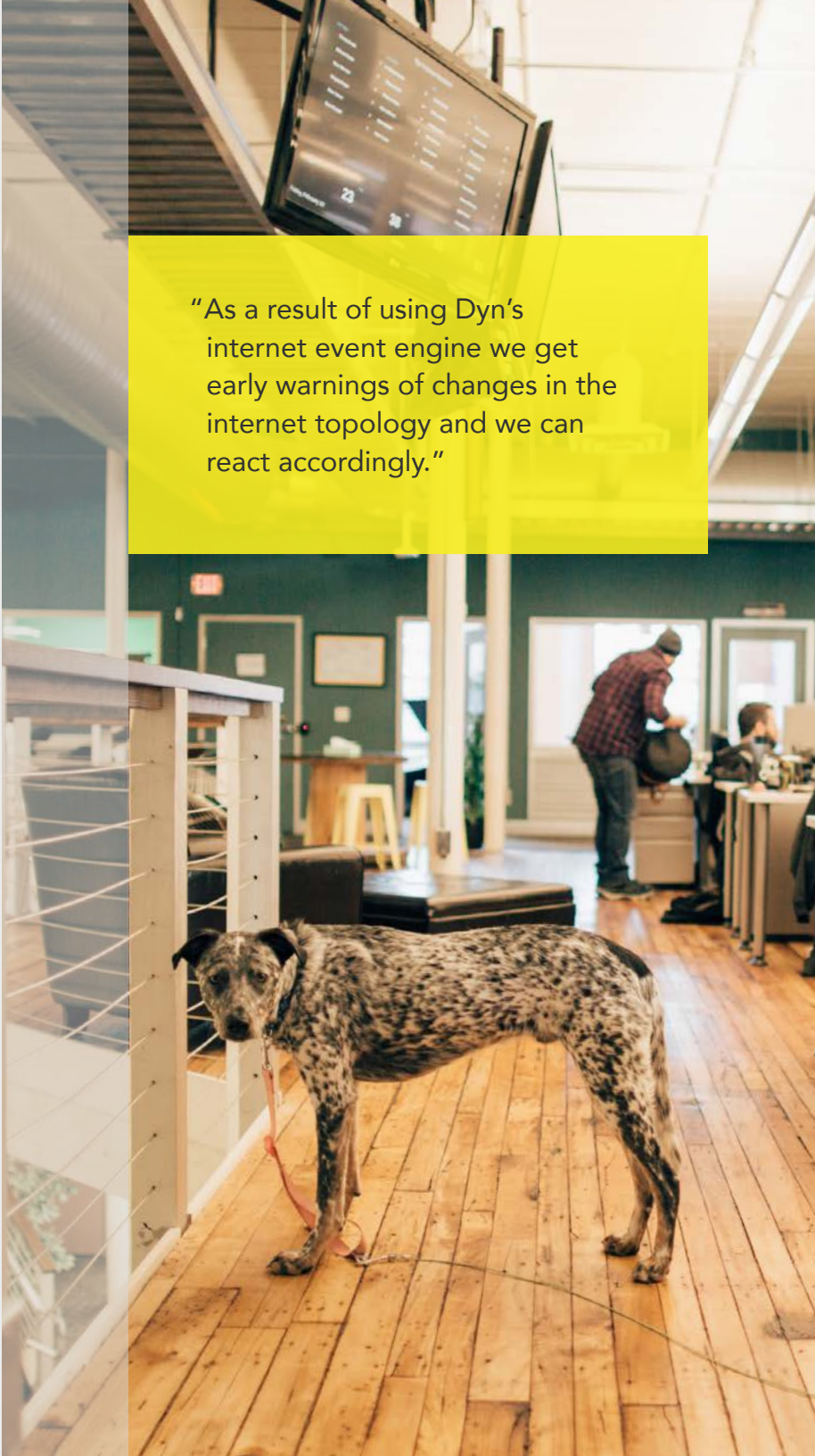


Continual Improvement

Eat our own dog food: Dyn has amassed what is arguably the most comprehensive dataset of internet “events”. This dataset is used to make policy- and real-time-based DNS traffic steering decisions, and can also be used to guide our network planning. This helps in a variety of ways like planning where we will build out our next edge site to guidance for transit and peering expansion. As a result of using Dyn’s internet event engine we get early warnings of changes in the internet topology and we can react accordingly.

Understanding traffic: Understanding our own traffic is imperative for us to be prepared for the unexpected. This goes well beyond simply knowing how much traffic we get on a regular basis, though that can be a good start. For example, if we know a site typically gets 5GB of traffic but we’re now seeing, at 1 o’clock in the morning, that it is getting 7GB of traffic that is good to know. But it is much more important for us to be able to investigate and discover the cause of that increase. Could this represent a precursor to a DDoS attack? Is this the side effects of a well-done marketing campaign? Has a new version of iOS been launched? We have seen all of these result in traffic spikes. Understanding the causes means we’re better prepared to handle the situation if, in fact, it ends up being unwanted traffic.

Adaptive service capacity: We just discussed the benefits of adding and removing capacity. Demand goes up and demand goes down. We need to adapt. As a result, we have a certain number of transit providers at each site. The practical reality of adding transit capacity is that happens over the course of weeks and months. But what if we need to add capacity in the next five minutes? If you haven’t architected your infrastructure in the right way, you might be in trouble. You need a better approach. Fortunately for Dyn, the combination of network diversity, geographic diversity and elastic compute capacity allows us to adjust our service capacity in real time. In fact, we can adjust traffic in the order of minutes and seconds. We do this quite regularly. If we see a large attack volume directed at a particular service, we can isolate traffic to particular service providers, making other sites unaffected by the load of unwanted traffic and thereby giving us a smaller edge on which to concentrate our mitigation efforts.



“As a result of using Dyn’s internet event engine we get early warnings of changes in the internet topology and we can react accordingly.”

Proactive security: Many times we think of external factors when it comes to security. And external factors are important. As we like to say, “our infrastructure welcomes visitors through a variety of doors, but we keep the windows locked.”

Internal security is also crucial. This means you need to police your own infrastructure, make sure all software patches are update and listen to your security vendors’ recommendations. Additionally, we do regular phishing tests of our employees, as well as practicing careful management of access tokens and crypto assets.

Of course, prioritizing internal security is a result of proper training and, once again, making it a big part of your culture. Culture plays a pivotal role in the third step to running a world class network.

When enough just isn’t enough

While we’ve built something that is world class and built it so it can be adaptive, then made adaptations as we’ve learned more, we know that there are still situations that would challenge the most experienced operators.

A Resilience Culture: We have talked a lot about our ability to manage capacity. The flip side of that is managing demand. We over-build our infrastructure to support flash crowds and intentional high traffic loads from our customers. We want our customers to have more traffic. Their success is our success.

Not all traffic is good traffic however. Many times we get unwanted traffic and we must be able to sift through this to determine what to do next. We can receive this unwanted traffic for a variety of reasons including direct attacks on our customers, direct attacks on us and collateral damage from attacks on other victims.

While the reason for the unwanted traffic varies, one thing remains consistent: DDoS attacks are on the rise. The increased frequency of these attacks means we can’t treat any as a one-off occurrence. Yet despite the increased



frequency we must shield our customers from the effects of these attacks. To do this we must have a resilient infrastructure and the right tools in place. But perhaps more importantly we must build a culture with our team that gets excited about dealing with crisis on a daily basis.

It is the human element of dealing with a crisis that is often overlooked. Anyone can buy transit. If you don't know how to manage those things in a time of crisis and you don't realize there will always be a crisis - no matter how much transit you buy - then you still lose.

What you can't buy off the shelf is culture. How do you make it so that people enjoy coming to work every day knowing they're going to face attack traffic and complicated analysis that requires them to think on their feet? How do you make that culture sustainable and scalable?

We have built a culture of crisis management, modeled on other industries - military, healthcare, civil defense, etc. We learn from these because defending Internet infrastructure has many aspects in common, despite the differences in intelligence gathering, tools and techniques, including: chain of command, management of communications, continuity over time and diagnosis, response, review. Really the main point is to always work toward avoiding panic.

This is what you're buying when you buy from a premium DNS provider. Yes, the cheaper providers have points on a map. But they don't have the people. Of course, people need tools. We build our defense in layers. We have measurement points and traffic control points from the application deployed on the edge to the provider edge to the provider network. We can influence traffic behavior in our upstream network using traffic mitigation devices. We have multiple networks that we can rate-limit, we can black hole traffic, block and classify. We do this every way we can, starting on the outside of the onion and continuing as we peel back layers:

- provider networks (mitigation services, RTBH)
- our provider edge
- our service edge
- our compute platform edge
- our service container edge

This is not done manually. It is done through automation and coordination. We have experts at the server and network levels. We organize people into shifts, even if the incident seems small at first. We want to prevent burn out later in the day should the situation escalate. Our crisis culture is about a set of disciplines, tools and culture that allows us to mitigate attacks every day.

Know How vs. Know Why: David Isenberg, formerly of Bell Labs, wrote an essay that discussed the differences between the culture of an internet company and that of a telco. He said the culture of an internet company was "know why" while a telco was "know how."

On the Internet you can never predict what will happen next in infrastructure terms, you can never know what you will need to do to defend against the next challenge on your services. There is no manual for how to defend against attacks you haven't seen yet. This is very different from the telco space where employees are encouraged to read from a binder that was built over 100 years. On the internet things are changing every 100 days.

This attitude leads to a spirit of exploring. The 2 a.m. shift on the NOC is usually not the most glamorous as not much is going on. Most times people do it for as long as they can stand and then they move on. At Dyn, we've given our team a ton of personal empowerment. We encourage them to understand and investigate. At first they are not experts and their ideas may be wrong. But

they should always have ideas and we bounce them off each other and people learn. This has led to great retention. Like your actual infrastructure you have to make your people adaptable and part of the solution. Spending money on equipment and capacity will only get you so far. Having the right people in the right culture during a crisis is worth every penny.

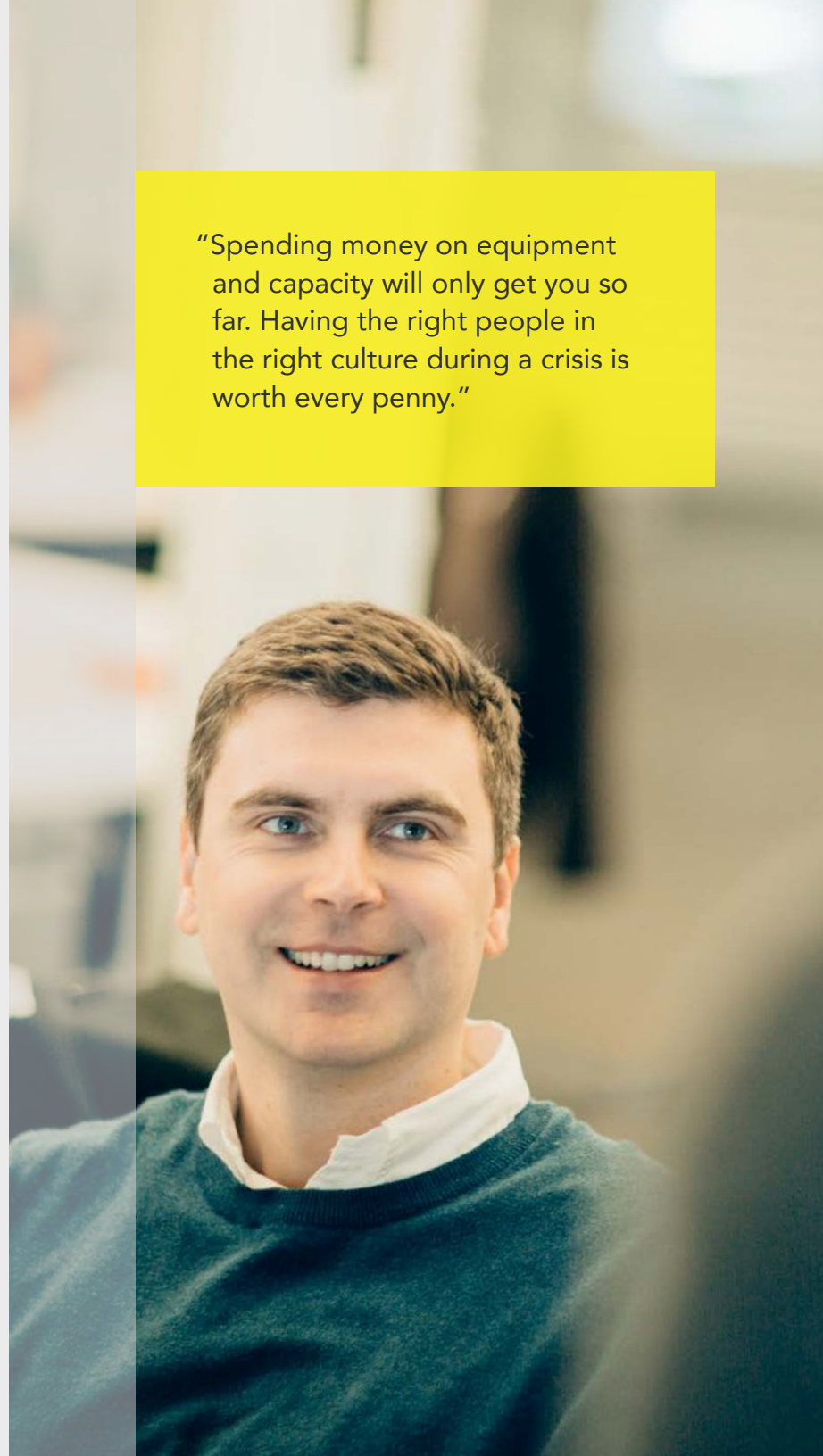
Conclusion

Not all DNS providers are created equal. When teaming with a premium managed DNS provider, you are not only buying infrastructure, you're gaining access to the team behind it - a team that operates its own network and is battle tested. In your time of need, this can be the difference between success and failure.

Dyn and **Spiceworks** recently conducted an Internet Disruption research study, tracking the experience and opinions of more than 200 IT professionals in the US, Canada and the UK. The research finds that 89% of companies surveyed experienced some form of internet disruption over the last twelve months.

Learn more – Read: [Internet Disruption Report.](#)

“Spending money on equipment and capacity will only get you so far. Having the right people in the right culture during a crisis is worth every penny.”



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).

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. 1012

ORACLE® + Dyn

🏠 dyn.com

☎ 603 668 4998

🐦 @dyn