Technical Overview

MANAGED DNS

ORACLE® + Dyn

dyn.com ☎ 603 668 4998 @dyn

Technical Overview:
Managed DNS

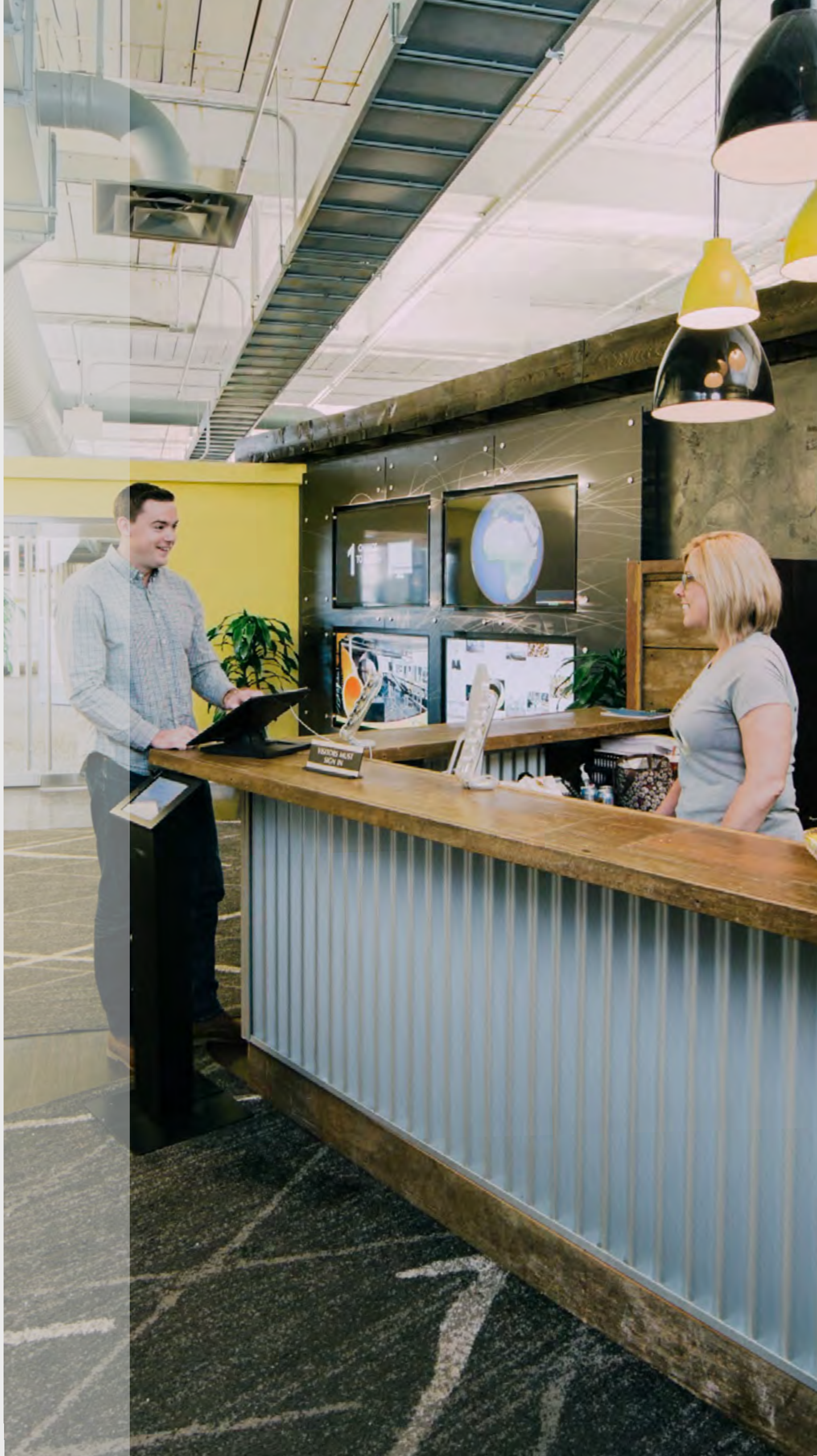
Oracle Dyn's Managed DNS provides the reliability, performance, and flexibility to connect users with websites, applications, and services at unmatched speeds. Managed DNS also helps shape online traffic to deliver an exceptional user experience for today's digital business.

This document provides an overview of the technical considerations and benefits of using Oracle Dyn's Managed DNS solution.

Overview

Corporate websites and online services are crucial elements of revenue acquisition, branding, and day-to-day operations for today's digital business. It is essential for companies to stay on top of ever-evolving technical challenges to ensure that their online gateways are high performing and always available for visitors from all parts of the world.

With increasing security risks such as distributed denial-of-service (DDoS) attacks and the need to maintain internet infrastructure without a moment of downtime, it's easy to understand why IT professionals with the highest standards for performance, security, and maintainability rely on Oracle Dyn's Managed DNS to ensure their network runs smoothly.



Network Design

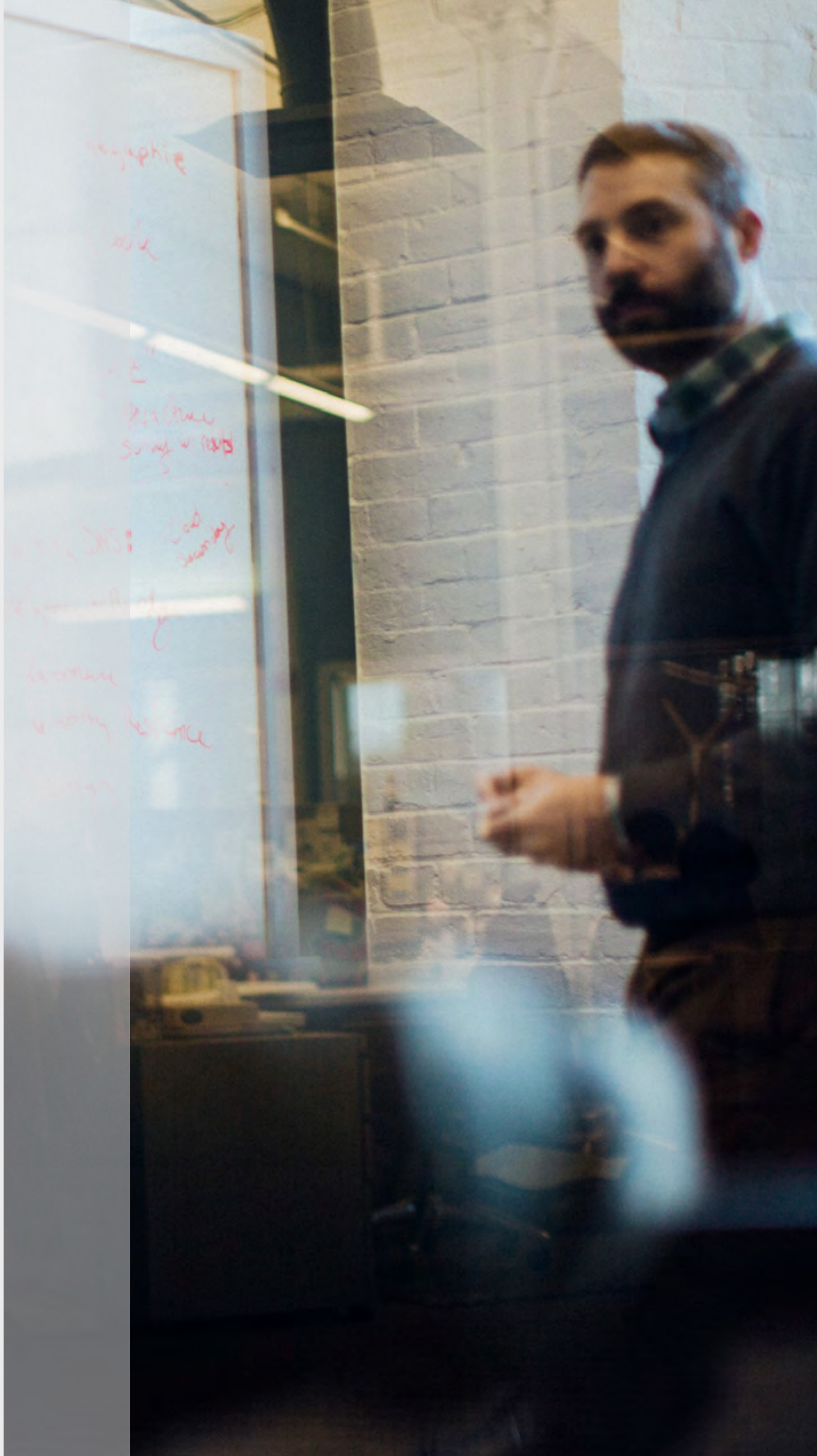
In order to help businesses deliver on promises of uptime, performance, and security, DNS providers have created world-class networks capable of supporting massive traffic throughout all regions of the world. When it comes to designing these networks, there are two primary approaches to DNS architecture: unicast and anycast.

Unicast networks are characterized by a one-to-one relationship between an IP address and the authoritative nameserver it corresponds to. As a result, DNS requests for a given IP address will always resolve to a single location. When a visitor requests a domain within a unicast network, the response that their resolver receives typically includes each nameserver, in addition to the unique IP address for where each one is located.

It's then the job of the resolver to send requests to each nameserver to determine which provides the fastest response. Under normal circumstances, the majority of future queries will be sent to this location. Because this design is relatively easy to implement and maintain, most organizations that manage their DNS in-house utilize the unicast architecture.

Unfortunately, unicast networks have several drawbacks due to this one-to-one mapping of nameservers to IP addresses. These networks are susceptible to DDoS attacks as hackers are able to direct massive amounts of traffic from anywhere in the world to each nameserver. If there are multiple authoritative nameservers for a given domain, attacks can focus on overwhelming each location individually until all nameservers are unavailable.

Additionally, as nameservers map to unique IP addresses, there is no redundancy in place if one of the nameservers goes offline due to either system failure or routine maintenance. The result of any nameserver going offline for any amount of time will be dropped requests and timeouts, greatly increasing the latency and degrading the user experience of associated websites and services.



In contrast, anycast networks are characterized by a one-to-many relationship between IP addresses and their associated nameservers. This design causes the traffic to a single IP address to be distributed to different nameservers based on the origin of the requests. Most managed DNS providers run anycast networks due to the significant benefits in speed, reliability, maintainability, and security provided by this distributed nature.

When a resolver performs a query within an anycast network, the answer it receives includes each set of nameservers authoritative for that domain. The resolver then selects one of the sets to query, and the anycast network takes care of routing those requests to the closest nameserver within the set, measured in network hops.

By routing requests to the closest nameserver for each resolver, the resolution time can be greatly reduced, resulting in better overall performance for visitors on this network. This improvement is magnified on websites that include multiple DNS lookups when web pages include references to additional files and assets that need to be loaded before a page completes. It is not uncommon for a web page to consist of a couple hundred objects, with as many as 50-60 of those requiring separate DNS lookups.

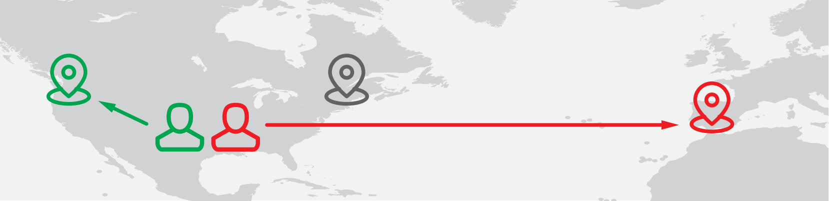
Reliability is significantly improved in anycast networks as high redundancy is achieved by distributing DNS service for each IP address across multiple nameservers. If a single nameserver goes down, that server will automatically be removed from the available routing options, and future traffic will continue to be routed to the remaining nameservers. Once service to the nameserver is restored, it can be activated on the network.

Another benefit of anycast is that the distributed nature of these networks makes it significantly more difficult to perform effective DDoS attacks. While unicast networks allow attackers to flood a single nameserver from anywhere in the world, anycast networks direct the traffic of attacking machines to their closest nameserver.

If the attack comes from several areas of the globe, the traffic will become diluted among various nameservers. If the attack originates from a single location, this traffic will become effectively localized to a single nameserver, leaving the rest of the network unaffected.

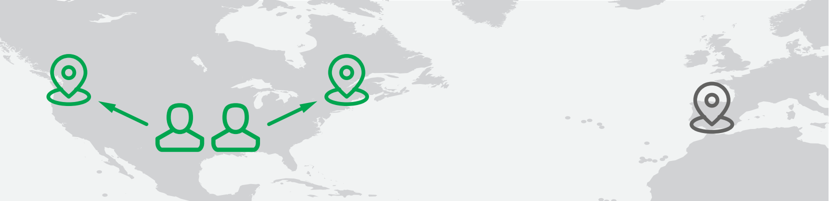
As this localized traffic hits the nameserver, managed DNS providers can mitigate the attack through techniques such as "black holing," effectively dropping the excess traffic to this location.

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.

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.

About Managed DNS

The Oracle Dyn anycast network contains 18 globally dispersed points of presence (POPs), strategically located at the cross-sections of several of the world's top Tier 1 transit providers to create the best routing options possible for DNS queries to travel throughout the world. Oracle Dyn's Managed DNS solutions have leveraged this network to provide many of the world's most heavily trafficked websites with industry-leading uptime and unmatched performance since we first launched the anycast network in 2007.

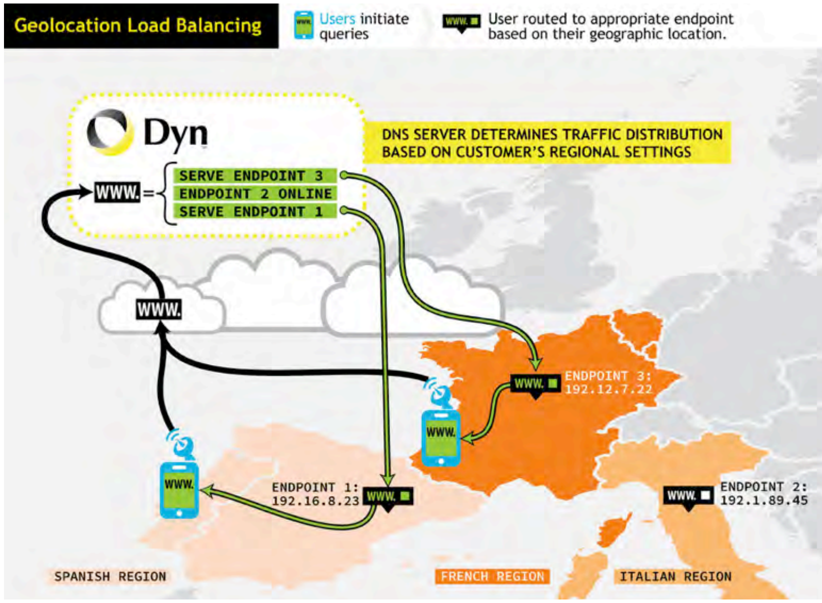
Within this network, customers are provided with a set of strategically diverse nameservers for delegation across uniquely routed BGP prefixes. By providing customers with unique nameservers, outages for a variety of reasons can be avoided. Outages due to peering, upstream ISP problems, or issues within a Dyn data center will be isolated to a single nameserver and its associated prefix.

About Traffic Director

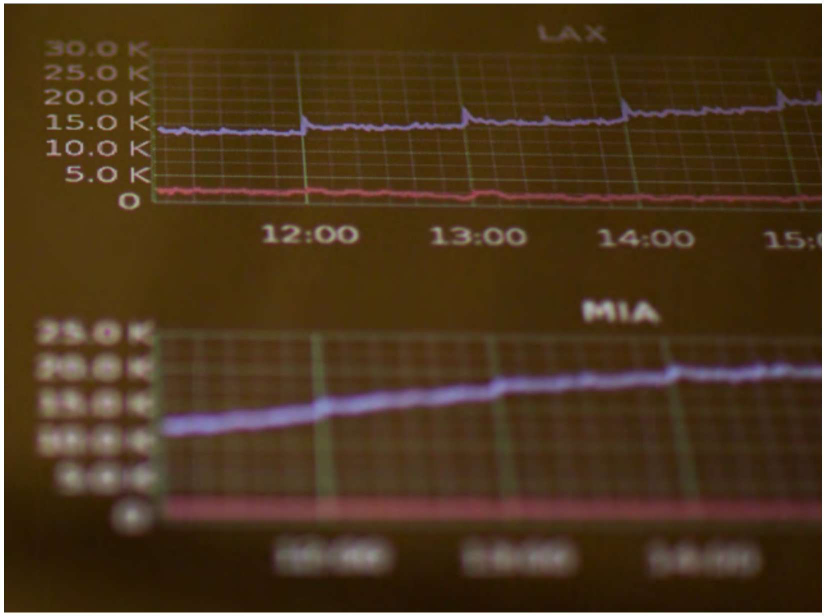
While the Oracle Dyn Managed DNS platform provides customers with the reliable foundation to ensure traffic is always routed to their website as quickly as possible, the Oracle Dyn Traffic Director adds the ability to granularly shape web traffic in order to best utilize company infrastructure and provide visitors with the best user experience possible.

Geolocation Load Balancing

While the Oracle Dyn network has been optimized to provide the fastest resolution times possible, there are times where the structure of the internet doesn't exactly align with a company's business model or content distribution needs. To address this, we provide geolocation load balancing to enable these companies to effectively configure Oracle Dyn's DNS network to their specific needs.



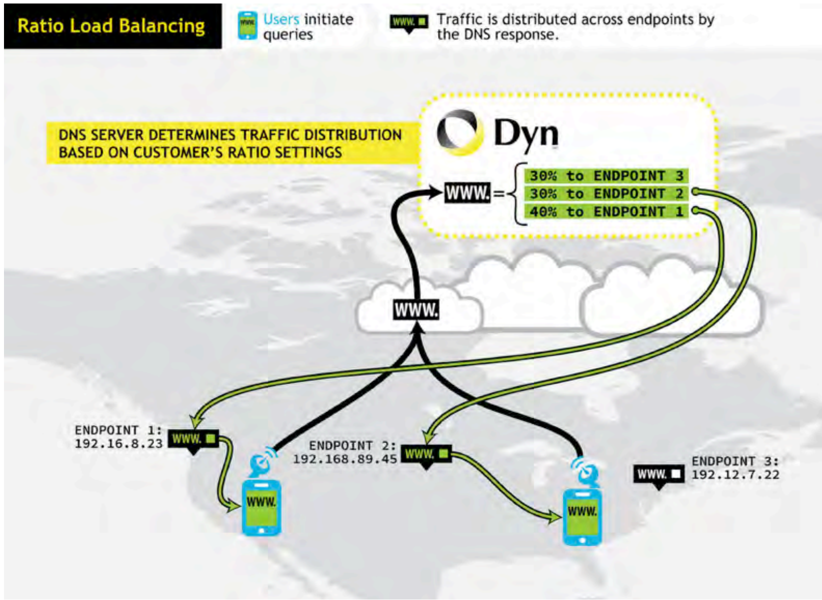
By grouping geographic regions into logical segments, customers can specify how DNS requests from each segment should be answered. Regions can be defined as granularly as the state and province level within the U.S. and Canada, and at the country level throughout the rest of the world. When a DNS request is made from a specific region, Traffic Director detects the IP address of the requesting server and provides the appropriate response for that region. Common use cases for geolocation load balancing include directing visitors to localized websites that include products or services available only in specific regions, or grouping countries together based on a commonlanguage (for example, Spanish is the official language of 21 countries, spread across three continents) and directing visitors to translated versions of a website.



Ratio Load Balancing

For situations where customers need to control the volume of traffic being sent to each of their endpoints, Oracle Dyn's Ratio Load Balancing provides the ability to assign a weight to each location in order to manage the frequency of requests from a defined region being sent to each endpoint. This weighting allows a company to create a rule that essentially says, "Send 50 percent of traffic originating from the U.S. west coast to data center A, 30 percent to data center B, and the remaining 20 percent to our content delivery network (CDN)."

By distributing the load to various endpoints, companies reduce the likelihood of overwhelming their data centers during traffic spikes, and ensure visitors to their websites experience the fastest page loads possible.



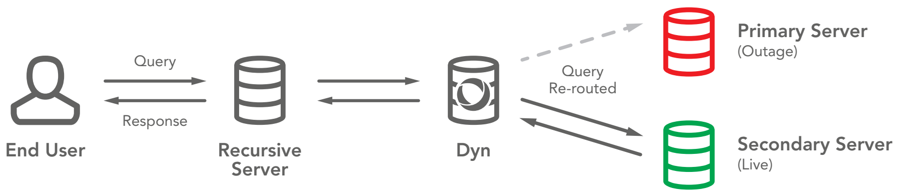
Active Failover

Even when traffic flow is distributed between multiple endpoints, there remains the possibility of issues occurring within a data center that could make it, and the servers that reside there, unavailable. When these issues occur, the traffic destined for the data center must be rerouted to a healthy endpoint to ensure customer experiences are unaffected.

The Oracle Dyn Traffic Director provides this protection by constantly monitoring the health of all endpoints from three of our closest points of presence and adjusting the traffic pattern whenever an endpoint becomes unavailable. Customers are able to specify what constitutes an endpoint "failure" (such as two of three checks returning no response), and how traffic should be routed to either an IP address or a hostname whenever this condition is met.

Monitoring can be configured to use any of five protocols: HTTP, HTTPS, Ping, SMTP, and TCP. Each protocol offers an advanced set of parameters to include in the health check such as monitoring interval, number of retries, expected data in the response, path, port, host, and header. This flexibility makes it easy to replicate a request and response as seen from an end user's perspective, and not just whether an endpoint is "up" or "down."

In addition to protecting against unexpected outages, Traffic Director can be utilized to eliminate the need for planned downtime for endpoint maintenance. Often, performing necessary maintenance within a data center requires taking the websites and services that reside there offline for a period of time. With Traffic Director, these websites and services can be load balanced across many endpoints. When maintenance is performed, the data center will simply be removed from the pool of available endpoints, leaving Traffic Director to load balance all traffic between the remaining endpoints available in the pool. Once maintenance is complete, the data center can be added back into the pool, and Traffic Director will resume routing visitors to this endpoint.



Multiple-CDN Implementation

Oracle Dyn Traffic Director provides the flexibility to be fully integrated into any company's online infrastructure, seamlessly routing traffic between data centers, CDNs, and cloud-based services. This flexibility allows companies to expand their infrastructure as needed, adding new endpoints as they're acquired or by swapping out cloud services and CDNs whenever vendors are replaced. This is often referred to as "endpoint agnostic."

Oracle Dyn provides the ability to utilize CDNs from multiple providers, enabling astute companies to optimize their routing strategy by directing traffic from different parts of the world to the best performing CDNs within their region. In addition to gaining performance advantages through this strategy, these companies gain negotiating leverage over CDN providers as they're able to switch to a different CDN within a given region if it becomes financially beneficial to do so.

Companies that employ a multiple CDN strategy can temporarily route their traffic to a different CDN whenever their monthly usage approaches their limit with a given provider, potentially resulting in significant savings by avoiding overage charges.

Security

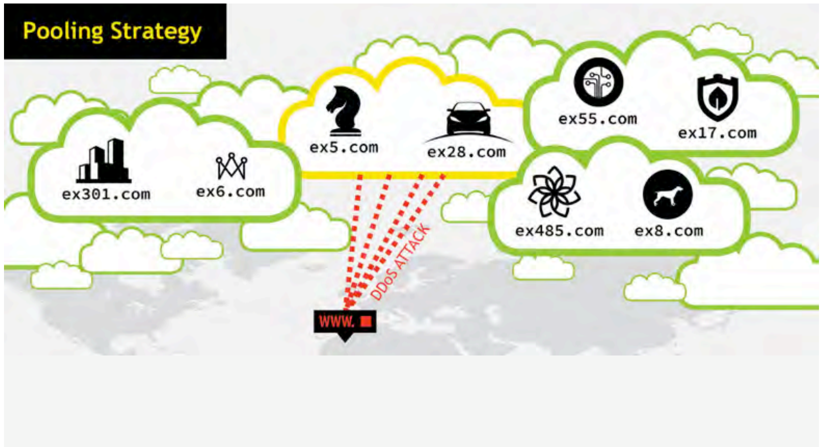
Given the extreme importance of company websites and online services, the security risks inherent on today's internet require companies to remain vigilant to ensure all aspects of their web infrastructure are protected.

One of the most common risks to websites is a distributed denial of service attack (DDoS). The goal of DDoS attacks is to overwhelm a network or service by sending massive amounts of traffic to DNS servers from computers that have been compromised by an attacker.

Oracle Dyn protects against DDoS attacks in a variety of ways, beginning with our globally distributed anycast network which confines local attacks to the closest nameserver and spreads distributed attacks across global points of presence, ensuring there are always sufficient nameservers available to respond to requests.

A policy of refusing to serve companies considered high risk due to the nature of their business (for example, gambling websites) further protects Oracle Dyn customers, as they are less likely to share a network with targeted websites.

Oracle Dyn's segmentation strategy makes the job of monitoring the global network easier as customers are divided into pools across a number of IP addresses and delegation points in order to isolate them from one another. This isolation allows for quicker detection and response to DDoS attacks, and it enables the Network Operations Center (NOC) team to apply additional techniques for mitigation targeted at the affected customer – not the entire service platform. For customers who require complete isolation, private pools provide the maximum level of protection, ensuring other customers never affect them and any issues that arise can be easily identified and mitigated.



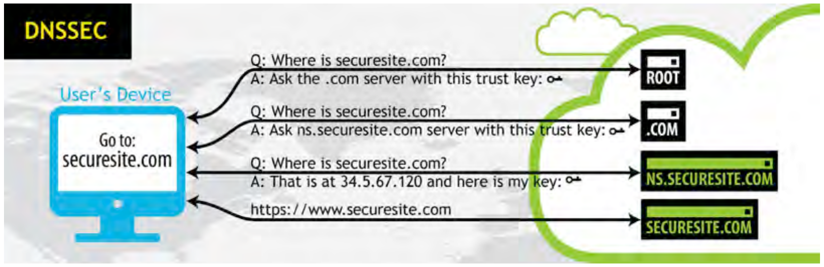
Another potential risk to company websites is the threat of "cache poisoning" or "man-in-the-middle" attacks. These attacks occur when hackers corrupt the response data returned from a DNS query so that visitors get routed to an IP address provided by the attacker. This IP address will typically display a site that looks exactly like the site the victim intended to visit. As a result, the victim may unknowingly enter sensitive information (such as banking credentials) or otherwise interact with the site in an unsafe manner.

Oracle Dyn customers are protected against these attacks through our support of the DNS Security Extensions (DNSSEC) protocol. DNSSEC protects DNS responses by digitally signing each response to ensure it's valid. Each step of the query resolution chain is signed when DNSSEC is implemented, enabling recursive DNS servers to identify whether or not responses are legitimate while discarding any that have been corrupted.

Automation

Oracle Dyn's Managed DNS solution can be configured to ensure any company's online services remain fast and fully available at all times, but there are times where manually configuring these services is undesirable or even impossible. For these times, our customers benefit from our fully documented platform API, available in either RESTful or SOAP formats, allowing for access via any programming language with samples provided for several of these languages: PHP, Perl, Java, C#, Ruby on Rails, and so forth.

Common API scenarios include signaling a failover event to the Oracle Dyn Traffic Director if internal monitoring systems detect suboptimal data center performance, automating updates of system information when performing routine maintenance, and failing over to Traffic Director as a Secondary DNS solution whenever there are issues with a primary DNS platform.


DNSSEC
User's Device
Go to: securesite.com
Q: Where is securesite.com?
A: Ask the .com server with this trust key:
ROOT
Q: Where is securesite.com?
A: Ask ns.securesite.com server with this trust key:
.COM
Q: Where is securesite.com?
A: That is at 34.5.67.120 and here is my key:
NS.SECURESITE.COM
https://www.securesite.com
SECURESITE.COM

Ensuring Customer Success

Ultimately, Oracle Dyn's success is fully dependent on the success of our customers. In order to ensure customer websites and online services are always available and responsive, we provide additional layers of protection in the form of expert monitoring, training, and support.

Our Network Operations Center (NOC) is staffed by infrastructure experts tasked with monitoring the network 24/7. The NOC's primary goal is to ensure an optimal user experience for all customers, detecting any network spikes or anomalies, and responding immediately to mitigate potential issues.

Upon purchasing Oracle Dyn's Managed DNS, every new customer is provided a one-on-one, web-based onboarding experience, provided by an Implementation Services team member. The goal of this team

is to ensure all new customers successfully transition to the Managed DNS portal, migrating any existing zones and instilling confidence by fielding any remaining questions regarding Oracle Dyn's products, services, or APIs.

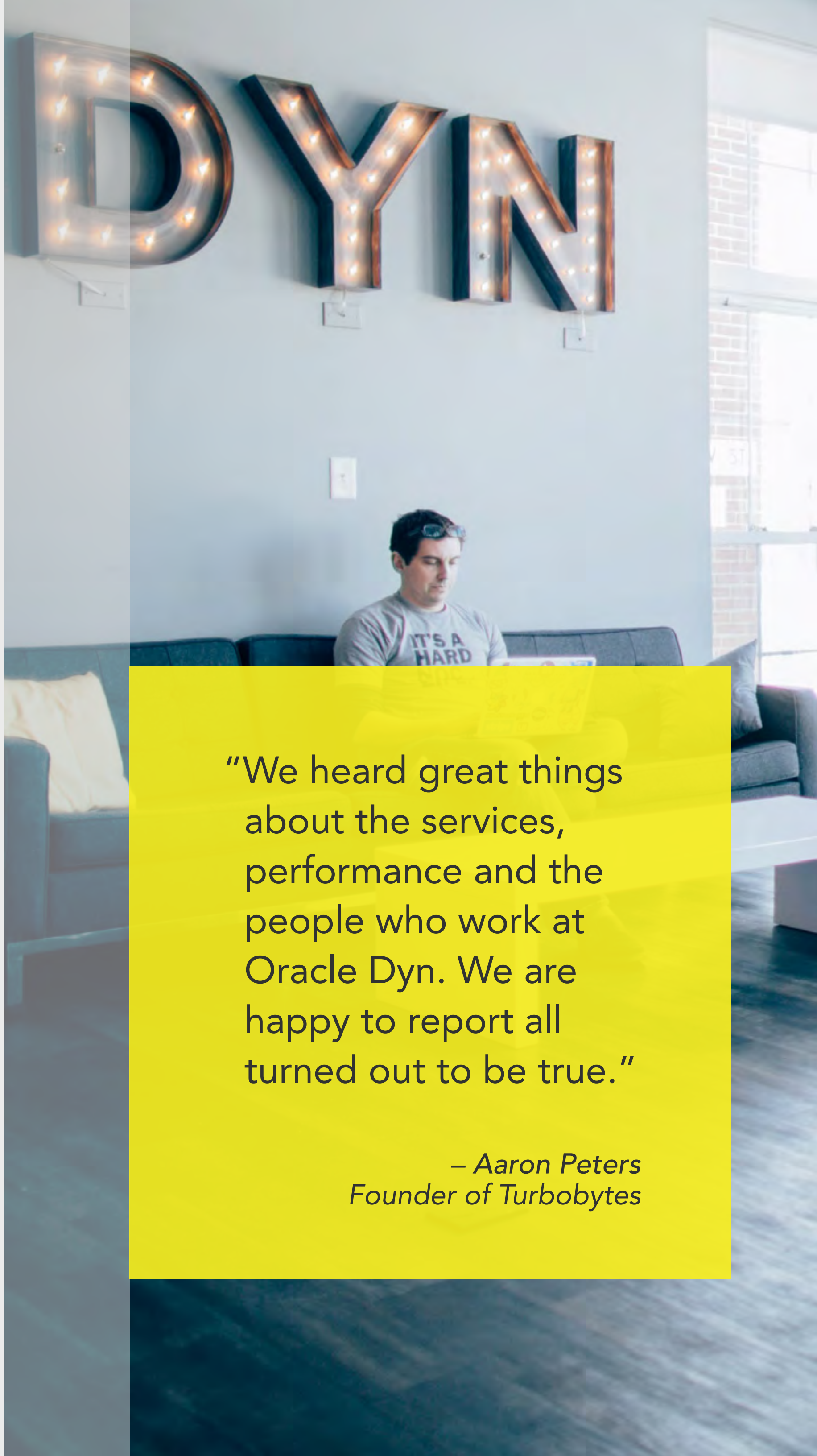
For customers who require further implementation assistance, we offer QuickStart, an onboarding service that digs deeper into customer requirements and walks through processes such as bulk zone transfers, advanced feature and security setup, troubleshooting, and best practices consulting. The goal is to ensure Oracle Dyn's services are properly implemented into the customer's infrastructure as quickly as possible.

Finally, Oracle Dyn customers are provided the best DNS technical support in the industry by our support team. Offered at three levels, customers are able to select the most appropriate level of service for their needs. All of our Managed DNS customers are provided phone and email support 24 hours a day/5 days a week with the option to add 24/7 support. Additional options include weekly check-ins and a dedicated technical account manager.

Conclusion

As websites and online services continue to play a critical role in the success of companies big and small, IT professionals need to ensure these services remain available and performing at optimal speed. Oracle Dyn Managed DNS provides the reliability, security, performance, and support needed to exceed our customers' web infrastructure requirements today and in the future.

Learn more – Visit: dyn.com/dns/managed-dns



"We heard great things about the services, performance and the people who work at Oracle Dyn. We are happy to report all turned out to be true."

– Aaron Peters
Founder of Turbobytes

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