



# The 5 Dimensions of Diversity: A Winning Strategy for Securing your DNS

JULY 2009

## What is DNS?

The Domain Name System is the Internet's primary addressing mechanism, handling trillions of name resolutions on a daily basis. Hierarchical in nature, the DNS is the massively decentralized address book responsible for translating user-friendly strings of text into machine-friendly IP addresses.

## Abstract

DNS, the technology that underpins virtually everything an organization does online, is often a forgotten technology. While diversity is the cornerstone of any stable, secure system, nowhere is this more important than in mission critical DNS. Without DNS, websites would not be available and email would not work. Organizations should deploy a technological and topographical diversity strategy to improve security, ensure availability, reduce costs, and maximize revenue.

To execute this strategy, organizations should consider 5 key dimensions of diversity:

1. Diversity of DNS software and providers
2. Geographic diversity in DNS node architecture
3. A diverse physical infrastructure relying on multiple brands and suppliers
4. Multiple connectivity providers for each DNS node
5. Diversity in personnel and expertise

Organizations also need to carefully weigh the expense of building diversity into their internal architecture with more economical solutions like adding a second outside DNS provider or outsourcing the DNS function entirely to a Managed DNS provider with built-in diversity.

"The question is whether you don't put all your eggs in one basket, or you put all your eggs in one basket and guard the basket. In balance, I think that the risks of a monoculture in operating systems outweigh the advantages."  
(Schneier, Bruce)

"The whole organization can fall with a weakness or failure of one platform type... Not having diversity in place applies to everything from viruses to break-ins to denial of service to potentially even bad bugs and vendor failure." (Spafford, Eugene)

## The Strategic Need for Diversity

The alarming proliferation of professional, coordinated cyber attacks over the last few years has forced many companies to increase resources and focus on the security and stability of their online presence.

When so much revenue is reliant on a persistent, reliable Web presence, organizations simply cannot risk having a single point of failure on their networks.

The world's leading security thinkers, from Bruce Schneier<sup>1</sup> to Eugene Spafford<sup>2</sup>, agree: diversity is a crucial part of an effective security and stability policy.

Anybody who has ever run Windows Updater is aware of the dangers of platform homogeneity. In most organizations, having a single operating system deployed to all desktops means all desktops have to be taken offline for maintenance come patch day.

Desktop security, however, is nothing compared to an organization's web presence. No company serious about its online profile would consider running its web site from a single server or with a single Internet link. When every minute of downtime could easily equate to thousands of dollars of lost revenue or customers, the ROI case for investment in redundancy and overcapacity writes itself.

While most companies wisely invest in redundancy for data backup, uninterruptible power supplies, and Web servers, they forget about DNS. A chain, no matter how sturdy, is only as secure its weakest link. In many cases, DNS has become that weak link. Without 100% reliable DNS, it does not matter how scalable or redundantly provisioned a system is, because users may simply never get there.

For mission-critical systems, a diverse, redundant and robust DNS architecture should be as great a priority as any other aspect of your business.

(1) Computer World, "Q &A: Improved Security Requires IT Diversity," 4 Nov. 2009, <[http://www.computerworld.com/s/article/87470/Improved\\_Security\\_Through\\_IT\\_Diversity](http://www.computerworld.com/s/article/87470/Improved_Security_Through_IT_Diversity)>.

(2) Network World, "Security Expert Recommends 'Net Diversity,'" 30 May 2006, <<http://www.networkworld.com/news/2006/052206-purdue-spafford.html>>.

## Why Is DNS Important?

Companies think nothing of spending millions of dollars ensuring that their Web sites and email servers are stable and secure. Yet many still forget the importance of DNS, the technology that brings customers and partners to their Web sites and that sends the right email to the right mail server.

DNS is the Internet's phone directory. You wouldn't try to run a business from an unlisted phone number, but when your DNS infrastructure stops working, that's exactly what you're doing. Even though it is such a fundamental component of the Internet, DNS is often overlooked as a critical element that requires the same redundancy as other technical systems.

## Why is your DNS important

### Traffic Spikes Can Cripple Your DNS

Since the turn of the millenium, the Internet has become an increasingly hazardous place to do business, and managing a stable and secure network has become a key challenge for administrators.

From the early days of playground hackers, the Internet has seen a boom in the quantity and effectiveness of malware. The number of new malware signatures released by vendors each year is rapidly approaching two million.<sup>3</sup>

As the spread of malware has increased, so has its sophistication and impact. Large scale attacks now occur more frequently leading to denial of service attacks against targeted or infected Web sites. They can even be targeted against entire top-level domains (TLDs), making these sites or TLDs entirely unavailable.

Conficker, which caused large-scale disruption in early 2009, was one of the top 10 most prolific Internet worms ever, infecting millions of machines and causing chaos for many network operators. Planes were grounded and even networks belonging to governments and the armed forces were not immune.<sup>4</sup>

While a security vulnerability in some versions of Windows was primarily responsible for the worm's propagation, one of its attack vectors caused an indirect denial of service attack on some DNS services. In its later versions, Conficker attempted to update itself with new malicious payloads by downloading patches from up to 50,000 pseudorandom domain names spread across 110 different TLDs. Many of these were small ccTLDs unused to such heavy traffic and unprepared for the sudden spikes in DNS lookups and could have simply gone offline from the increased load.

(3)Symantec, "Internet Security Threat Report Volume XIV," April 2009, <<http://www.symantec.com/business/theme.jsp?themeid=threatreport>>.

(4)Telegraph.co.uk, "French fighter planes grounded by computer virus," 7 Feb. 2009, <<http://telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html>>

**“A major international incident such as the ongoing Conficker attack should remind network providers and ccTLDs alike that they do not exist in isolation from the rest of the Internet.”**

Traffic spikes can happen at any time, without warning, and they do not always have to be malicious in origin. Web sites running with any kind of bottleneck on their networks can and frequently do find themselves performing sluggishly or being knocked offline altogether after becoming the recipient of an unexpectedly popular link from a high-traffic site.

The phenomenon was once known as the Slashdot effect, after the popular technology web site, but nowadays there are hundreds of sites capable of generating this kind of impromptu and inadvertent denial-of-service attack – Twitter, Techcrunch, Facebook, Myspace, to name but a few.

This effect is also of concern to ccTLD operators. Witness the growing and unexpected popularity of URL-shortening services or other international services using country-code extensions – bit.ly and tr.im for examples – which have been embedded in services such as Twitter. For ccTLDs with open registration policies, the next such service could arrive in their namespace and become unmanageably popular in a very short space of time. A sudden rush of traffic to one of these domains could inadvertently cause a degradation of performance for all registrants, if the TLDs DNS is not properly provisioned. At best, it may cause an unexpected jump in costs that are not recoverable, or at worst, it may take both the site and TLD down and damage their reputations long term.

A major international incident such as the ongoing Conficker attack should remind network providers and ccTLDs alike that they do not exist in isolation from the rest of the Internet. Actions of a few malicious actors anywhere in the world could ultimately cause their customers or local users to experience problems accessing domestic web sites, or even government services. Only a highly diverse DNS resolution infrastructure costing tens of millions of dollars to deploy and maintain could provide anything close to an effective safeguard against such an eventuality.

Conficker did not directly target DNS, but its impact was felt in DNS regardless. The same could be said of any security threat, from large-scale distributed denial-of-service attacks all the way down to the background hum of daily spam deliveries. However, DNS resolution software and the platforms upon which it runs are frequently the targets of attacks and the subjects of serious vulnerabilities.

**“A technologically homogenous system can be a single point of failure when a zero day threat emerges.”**

## A Vulnerable Victim Waiting for a Patch

No software is perfectly secure. Applying frequent patches has now become a fact of life. CERT, the Computer Emergency Response Team, currently publishes information about 2,000 new vulnerabilities in widely used software every quarter.<sup>5</sup> For organizations implementing sensible redundancy policies, patching can be a tiresome necessity.

With zero-day vulnerabilities, a vulnerability for which detailed information and possibly attack code exists but for which there is not yet an available patch, administrators unfortunately do not have the luxury of readily available patches. They have little choice but to just sit tight and wait for a vendor patch, hoping they do not come under attack in the meantime.

This underlines the importance of diversity of technology in critical systems like the DNS. A technologically homogenous system can be a single point of failure when a zero day threat emerges.

Organizations should be wary of single-platform DNS solutions. To be truly secure, DNS infrastructure should employ a multi-platform approach that enables vulnerable systems to be simply unplugged until patches become available. With such diversity built in, an attack on a vulnerability in BIND, the world’s leading DNS software, becomes irrelevant if the network is also running NSD, and vice versa. The risk of compromise is simply and cleanly eliminated.

Organizations can mitigate the risk of a zero-day attack only by adopting a diversity strategy and accepting the associated costs of managing a truly diverse architecture.

[5] CERT Statistics, <<http://www.cert.org/stats/>>.

## Security by Obscurity

Security by obscurity is an oft-derided way of presenting a system as secure purely because the details of its workings are kept private, an idea frequently championed by proponents of proprietary software. The concept was first challenged in 1883 with “Kerckhoffs’ principle”, which states that the defender should always assume the attacker has the same knowledge of the system.<sup>6</sup> Security by obscurity has been widely discredited by cryptographers ever since.

## The 5 Dimensions of DNS Diversity

Sound security strategy requires no single points of failure. When considering the importance of your DNS, diversity is critical to the design of your DNS architecture. To reap all the security and stability benefits of a comprehensive system, an organization would have to weave diversity into the fabric of its infrastructure at every layer, from the places it deploys its servers to the software it installs to the people it employs.

There are five key dimensions of diversification that are critical to maintaining the security of your DNS:

### 1. Diversity of DNS Software and Providers

Berkeley Internet Name Domain (BIND) is the industry standard software for domain name resolution services. In active service for over 20 years, BIND has survived the rapid expansion of the Internet and become more widely deployed than any other DNS software. As open-source software, unlike proprietary solutions, its code has been scrutinized, tested and battle-hardened by hundreds or thousands of programmers over the years.

But no software is invulnerable. Even if critical security problems are thankfully rare occurrences, maintenance patches can be routine in even the most bulletproof of software packages. BIND itself suffered from eight security vulnerabilities between 2007 and 2008. A DNS resolution network running only BIND would have required rolling patches on each occasion, with live unpatched servers running a risk of compromise during that process. The same applies to any piece of DNS software, whether open-source or proprietary.

An organization aiming to bolster stability through diversity would deploy both BIND and at least one other solution. NSD, for example, is an open-source alternative to BIND that was developed in the Netherlands specifically to enable diversity in DNS software and is currently considered reliable enough to run three of the Internet’s root name servers.

(6) Wikipedia, The Free Encyclopedia, “Security through obscurity,” 23 July 2009, <[http://en.wikipedia.org/w/index.php?title=Security\\_through\\_obscurity&oldid=303715786](http://en.wikipedia.org/w/index.php?title=Security_through_obscurity&oldid=303715786)>.

## Anycast

Anycast is a standardized method of providing load balancing on a global scale. Quite simply, Anycast allows many DNS resolution nodes to share the same IP address. End users are transparently routed to the optimal node, which usually means the geographically closest, increasing the speed of their transaction. Anycast enables massive redundancy, as requests invisibly fail over to a second/third/fourth node if the closest one is unavailable. When a user in Europe looks up a domain name, they may be routed to a node in London; if that node is for some reason unavailable or non-optimal, a node in New York can instantly handle their request.

By deploying more than one DNS resolution solution, should either suffer from security issues, organizations can simply remove that software from production servers until the problem has been addressed.

The same cannot be said of systems using a single flavor of software, whether open source or proprietary.

Additionally, using only a single DNS provider will put an organization at similar risk should a catastrophic event occur. Considering a solution that provides for a secondary DNS provider ensures that even in the event of complete failure of the primary provider, DNS will continue to resolve.

## 2. Geographic Diversity in DNS Node Architecture

The Internet does not exist in isolation from the physical world.

An earthquake in California, a hurricane in Florida, a monsoon in Mumbai ... any of these natural disasters could easily take out that area's power, Internet and DNS resolution. This could result in an organization's Web presence and entire electronic communications system being unreachable worldwide if it has not built geographical diversity into its DNS.

Indeed, the DNS's master directory, the root server system that sits at the top of the addressing hierarchy, fundamentally embraces geographic diversity. The Internet has, logically, 13 root servers managed by 13 different organizations using 13 IP addresses. But in reality, the weight of the DNS resolution load is shared between servers deployed at over 180 locations worldwide using IP Anycast.

Organizations should consider an Anycast, geographically diverse DNS network as vitally important to the security and reliability of their online presence.

**“The popularity of one vendor’s brand of network routers, for example, makes its hardware and firmware a frequent target for attack.”**

### 3. A Diverse Physical Infrastructure relying on multiple brands and suppliers

Recalls of defective components, often in batches of hundreds of thousands or even millions, are a sadly common occurrence.

Hardware diversity not only mitigates the risk of falling victim to deliberate attacks against vulnerabilities in firmware, but also eliminates the potential single point of failure that comes with rolling out defective hardware.

The popularity of one vendor’s brand of network routers, for example, makes its hardware and firmware a frequent target for attack. With a diversity of hardware, those routers can simply be removed from the network until a fix is available; this simply isn’t possible with a homogeneous network.

Homogenous server hardware represents similar risks. However, a fully diverse infrastructure would also take into account the various components of those servers, from the CPU manufacturer to the brand of hard disk drives.

Such an infrastructure would also expect diversity right down to the level of the power leads that plug the servers into the walls, and the uninterruptible power supplies and backup generators that power them in emergencies.

“Each DNS node should be linked by multiple backbones, with no overlap between providers at different nodes”

## 4. Multiple Connectivity points to each DNS node

Multi-homing is a fact of life for many connected organizations. No serious network administrator would consider relying upon a single ISP for their Internet connectivity; the risk of excessive latency, outright downtime or corporate failure would be too much to bear. By balancing load between two Internet connections, or merely keeping a second or third connection on standby for failover purposes, administrators eliminate the single point of failure their connectivity provider represents.

A fully diverse DNS network would build this reasoning into its network on a global level. Each DNS node should be linked by multiple backbones, with no overlap between providers at different nodes. This ensures that, whether an ISP was hit by massive latency or a clear blackout, the network would be able to continue to resolve DNS traffic normally. A similar level of diversity would be considered when rolling out network operations centers (NOCs).

## 5. Diversity in personnel and expertise

A diverse technological platform requires diverse sets of knowledge and skills. Likewise, a lone employee solely responsible for any critical system is an obvious single point of failure. A decision to deploy a diversity of hardware or software would necessarily require a commensurate diversity in human expertise, while avoiding the pitfalls associated with giving the keys to the kingdom to a single individual.

“Unfortunately, DNS diversity adequate to mitigate or eliminate these risks requires a significant investment of millions of dollars.”

## Conclusion

Very few things in life or business offer 100% guarantees. However, it is ESSENTIAL to require 100% uptime in DNS, since DNS underpins everything from the acquisition of customers and revenue to the productivity improvements enabled by reliable communication.

For an organization to achieve the kind of security and reliability that enables such a guarantee, its DNS infrastructure must be designed with the 5 key dimensions of diversity in mind:

1. Diversity of DNS software and providers
2. Geographic diversity in DNS node architecture
3. A diverse physical infrastructure relying on multiple brands and suppliers
4. Multiple connectivity provides for each DNS node
5. Diversity in personnel and expertise

Unfortunately, DNS diversity adequate to mitigate or eliminate these risks requires a significant investment of millions of dollars. For most organizations, which do not focus on DNS as a core competency, the simpler, substantially more affordable alternative is to outsource their DNS operations to a Managed DNS provider. Managed DNS providers have existing systems that you can take advantage of, in either a primary or secondary capacity. These services can provide valuable insurance that your site and electronic communications will not go dark.

**“By outsourcing DNS resolution to a provider with a diverse, proven network, organizations can benefit from the security and stability of a large DNS network at a tiny fraction of the cost.”**

## Why Outsource your DNS?

DNS is a mission-critical technology, the enabler for almost everything an organization does online. But there are very few organizations that have made, or should make, DNS their core competency.

To achieve a DNS network that can ensure a 100% uptime guarantee would require a minimum investment of millions of dollars. Not only would building a large, diverse infrastructure require a major capital expenditure, it would require ongoing costs to maintain expertise, facilities, upgrades, and a ever-expanding network capacity.

This simply does not make sound business sense to most organizations. The simple answer is outsourcing.

By outsourcing DNS resolution to a provider with a diverse, proven network, organizations can benefit from the security and stability of a large DNS network at a tiny fraction of the cost of building and maintaining a similarly stable system themselves.

In cases where full-fledged outsourcing is not feasible or desired, organizations can also consider adding a secondary provider in parallel or as a backup to achieve true DNS diversity. With a secondary provider, an organization can continue to operate as its own primary DNS service, but benefiting from a backup always on standby should its own systems need routine maintenance or have a catastrophic failure.



## Afilias Managed DNS Benefits

### 100% Uptime Guarantee

#### Diversity

- Multi-layered, tiered design
- Multiple software, hardware, bandwidth providers

#### Transparency

- Web-based interface
- Advanced reporting suite with hundreds of report configurations as standard
- Bulk import functionality
- Domain folders & user groups for easy management of large portfolios

#### Security

- DNS diversity running Anycast networks
- Global locations
- Distributed Denial of Service (DDoS) protection and mitigation
- Enhanced security alert services

### 24/7/365 Customer Support

Afilias' Managed DNS Service provides a world-class service that guarantees 100% uptime for your site. Built on a diverse and trusted platform that supports the .INFO and .ORG top-level domains, Afilias' Managed DNS resolves billions of queries daily for over 15 million domain names, utilizing only a fraction of its capacity.

The "5 Dimensions of Diversity" form the heart of Afilias' DNS architecture, enabling 100% reliable operation on a globally distributed, multi-layered, secure infrastructure. Afilias' Anycast DNS network is deployed at multiple international locations. Unlike single-vendor or proprietary alternatives, Afilias runs on multiple software, hardware, and bandwidth providers, substantially mitigating the risks of falling victim to security vulnerabilities or patch problems.

Our Web management portal provides you with transparency into your network traffic and control to easily manage site portfolios large or small. Get the peace of mind of knowing that your DNS will always be up. Effortlessly manage traffic spikes and prevent unnecessary overage fees with our unique account management approach and overage protection.

Make your DNS make sense. Switch to Afilias Managed DNS Service today.

For more information please contact:

John Kane  
VP, Corporate Services  
Tel: 1.215.706.5700  
jkane@afilias.info

Or visit us online:  
[www.afilias.info/dns](http://www.afilias.info/dns)



**Afilias**<sup>SM</sup>  
MANAGED DNS SERVICE  
[www.afilias.info](http://www.afilias.info)