NS1.

RESILIENCE QUIZ:

Does Your Network Infrastructure Mean Business?

Is Your Business at Risk?

Business runs online. Remote work, applications, transactions, and countless other mission critical activities rely on internet connectivity, regardless of your company's industry or size. But unless you are a technical specialist, you may not realize how vulnerable your network, and your business, may be.

Use the following questions to determine your company's risk level and assess network resilience.

NETWORK USAGE

1. **Do you process transactions online?** YES ○ NO ○
2. **Do you run applications online?** YES ○ NO ○
3. **Does your business rely on the internet for operational functionality?** YES ○ NO ○

RISK PROFILE

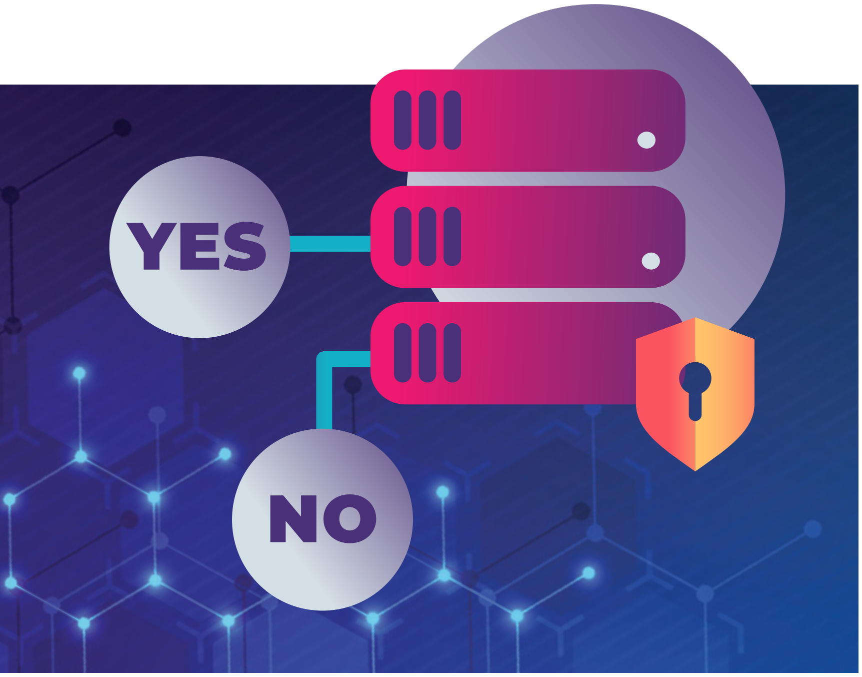
1. Do you pay for DNS service? YES ○ NO ○

2. Do you have a backup DNS server? YES ○ NO ○

3. Do your DNS servers have a common control panel for easy management? YES ○ NO ○

4. Are you prepared to mitigate the effects of a DDoS attack?? YES ○ NO ○

5. If you are under DDoS attack, can you continue to process transactions? YES ○ NO ○



Results

If you answered yes to any Network Usage questions and no to any Risk Profile questions, **you need to know more about network resilience and DNS** in order to protect your business from a network outage or attack.

What Is Resilience?

Resilience at its core means avoiding network outages, **making sure your business is available at any time to any customer from anywhere.** Your network needs to be vigilant, nimble, proactive, and able to deflect incoming threats so that disruption doesn't take root and your business processes don't experience painful downtime.

Because your network and application infrastructure are foundational to business technology as a whole, they must be secure, reliable (with a high percentage of uptime), and adaptable (able to detect, thwart, and reroute around threats) so failures don't disrupt the daily business of your organization.

This is true for companies of all sizes in all industries. Since most of your business interactions and transactions are likely being conducted on the internet, you need to be sure that this technology backbone is strong and always available.

FAST FACT

The average cost of **critical server outages** ranges from

$301,000 to $400,000 **PER HOUR.***

*ACCORDING TO STATISTA

DNS (Domain Name System) Websites are actually located at IP addresses rather than domain names. DNS allows users to type in a domain name to reach its associated IP address.*

* TechTerms.com

What Is DNS?

We are becoming more reliant on DNS than ever before, with myriad devices using the internet and DNS to communicate. DNS is now critical for both internal and external constituents—from the core to the edge. In fact, the internal environments at some companies are now as large and complex as external environments once were.

The expansion of DNS's role creates both opportunities and threats. DNS can be used as a proxy, allowing the router itself to be used as a server. If adequately protected, **DNS can also help ensure uptime in the face of DDoS attacks.**

But the more we use and rely on DNS, the higher the probability that we'll encounter errors and problems. Because of its increased usefulness, DNS is now also a prime target (or attack vector) for malicious entities. Problems with your DNS create a cascading chain of failures, so it's more critical than ever to make it bulletproof. **That's why a stable (and preferably redundant) DNS is so fundamentally important.**

What Is a DDoS Attack?

When your server is overwhelmed by a DDoS attack, there is no bandwidth for processing transactions. **The second server is a critical component** of the DDoS attack plan because traffic can be rerouted until the end of the siege. While this kind of attack is not an everyday threat, the damage can be severe enough to cost days of functionality in addition to any ransom demanded by the hackers.

DDoS (Distributed Denial of Service)
In a DDoS attack, a server or set of servers is bombarded with and overwhelmed by requests. Flooding a server in this way does not require authentication and can be accomplished with a "botnet," or a group of computers infected with malware.*

*TechTerms.com

FAST FACT

The average cost of a **DDoS attack** in the US is around

$218k.*

*ACCORDING TO A CORERO WHITEPAPER

How Does Business Size Impact Resilience?

SMALL OR GROWING COMPANY: A small or growing company must focus on driving revenue and growth. Risks that are low probability may not be addressed immediately. As the company matures and gains resources, hazards need to be managed because low probability isn't no probability, and the cost of downtime is simply too high.

MID-SIZED OR ENTERPRISE COMPANY: A mid-sized or enterprise company depends heavily on network availability for applications and business transactions. While the company may have the staff and resources to provide network support in-house, it often outsources DNS infrastructure management to avoid the associated hassle and expense.

The reality is that all companies that depend on internet connectivity need to consider resilience. A network outage can frustrate customers and users, impacting your reputation and your bottom line. **DNS redundancy protects your network so you can focus on growth and innovation instead of worrying about downtime.**

FAST FACT

34% of enterprises report costs in excess of

$1 MILLION

for an hour of downtime.*

*ACCORDING TO ITIC

Why Choose NS1.?

NS1's team has decades of experience in DNS network infrastructure. There's a lot of leverage in foundational network technology that allows you to take advantage of redundancy and add infrastructure so you can think less about the network and more about growing your business. **We can help you optimize application performance starting at the DNS layer.**

The convergence of applications and networks opens the door to a new ecosystem of products, architecture, and operating models that addresses today's challenging networking requirements. The current environment demands a set of requirements and a DNS-based delivery mechanism that more effectively ties together applications and elements.

This in turn creates resilient systems and simplified network management in dynamic, distributed environments. **Such a platform can also transform DNS from a cost center into a strategic tool to improve software reliability.**

NS1.

NS1's solution portfolio includes the application traffic intelligence and automation solutions you need to ensure the future of your business. Our solutions deliver scale, speed, and performance. Our track record of reliability and availability means we can help you move to a more modern network infrastructure with minimal disruption.

NS1.

AT INTERNET SCALE

Boosting Resilience for Stability and Success

READY TO LEARN MORE?

Read our eBook *Boosting Resilience for Stability and Success* to better understand risks to your network and how to protect against outages and attacks.