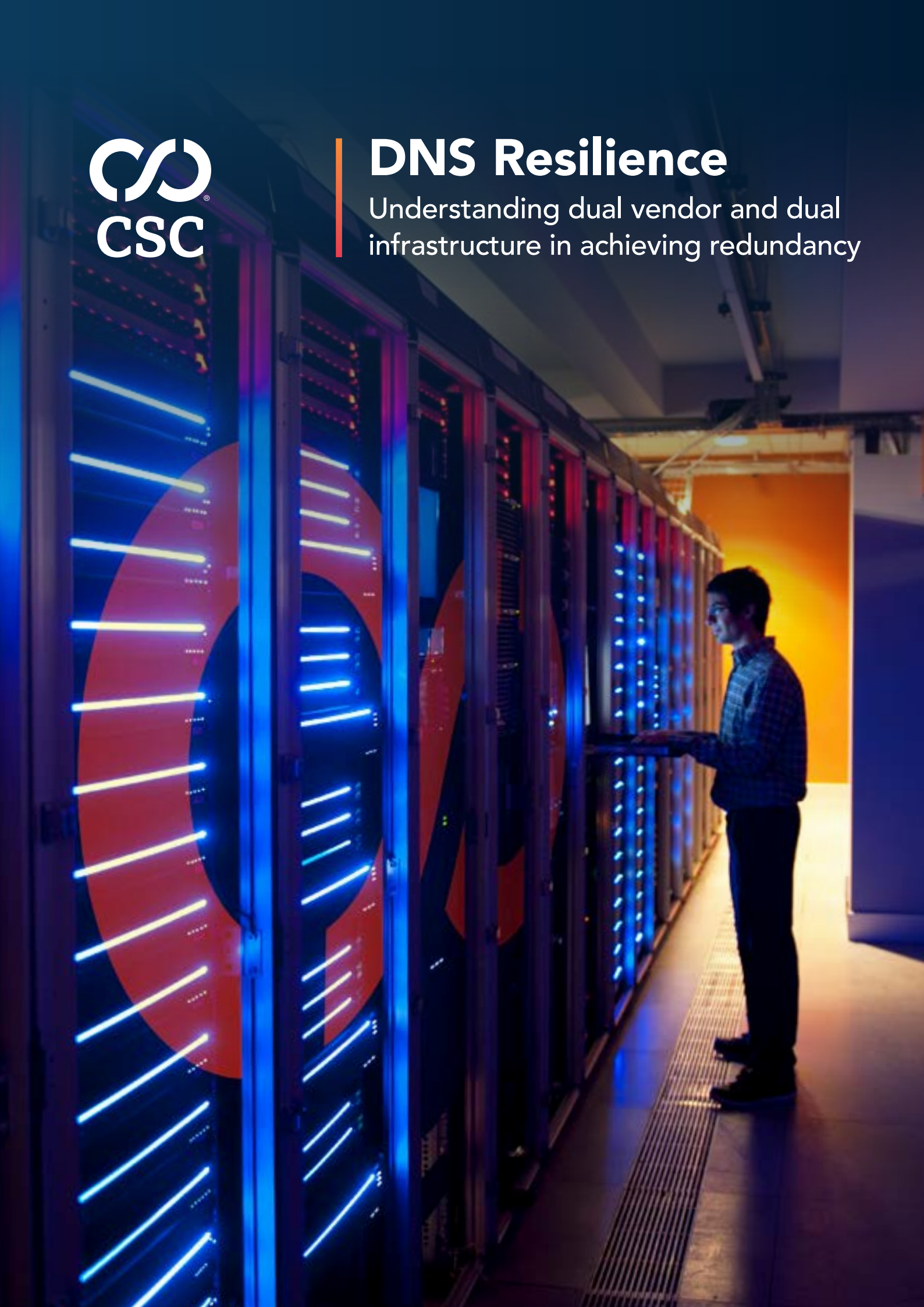




DNS Resilience

Understanding dual vendor and dual infrastructure in achieving redundancy



DNS Resilience

Understanding dual vendor and dual infrastructure in achieving redundancy

Many businesses frame the solution to domain name system (DNS) resilience as “dual vendor.” That sounds decisive, but it skips over the real question. The issue isn’t vendor count—it’s infrastructure resilience.

The core objective remains the same: Eliminate DNS as a single point of failure. And the right answer is two independent infrastructures.

Businesses can achieve this with either two vendors or a single vendor operating two fully independent environments. The vendor choice matters far less than the quality of the design, execution, and ongoing administration.

It also leads to the more strategic question: Do we need two vendors, or do we need two infrastructures?

So, the real decision becomes choosing one of these options:

1 Two vendors with interoperable architectures in primary-secondary models

2 A single vendor with two independent infrastructures

The next step is to evaluate which option delivers on resilience with the least operational complexity and the highest long-term reliability. It’s also important to recognize that not all DNS providers interoperate seamlessly. Some cloud platforms—AWS and Google, for example—don’t support traditional primary-secondary DNS models, which limits pairing options.



Dual vendor

Two completely different DNS providers (e.g., CSC + AWS)

Pros

- ✓ True vendor diversity—isolates you from a single provider's outages, bugs, or business failures.
- ✓ Reduces systemic risk—if one provider has a global incident, the other remains unaffected.
- ✓ Stronger resilience story—easy to communicate to leadership and auditors.
- ✓ Potential performance gains—different networks may improve global resolution times.

Cons

- ✗ Operational complexity increases significantly—two portals, two APIs, two security models, two monitoring stacks.
- ✗ Change management becomes harder—every DNS change must be replicated, validated, and kept in sync.
- ✗ Not all providers interoperate—some cloud DNS platforms (AWS, Google) don't support traditional primary-secondary models.
- ✗ Higher cost—two contracts, two support agreements, two billing structures.
- ✗ Risk of configuration drift—the biggest cause of DNS failures in multivendor setups.
- ✗ Complex engineering required to use advanced features—Apex alias, geolocation, failover, etc.

Dual infrastructure

One vendor, but two fully isolated infrastructures (e.g., two separate clusters, regions, or accounts)

Pros

- ✓ Lower operational overhead—one vendor's tooling, APIs, and processes.
- ✓ Better risk mitigation—where there's a single point of contact for faster troubleshooting.
- ✓ Consistent feature set—same record types, same automation, same security controls.
- ✓ Easier to maintain configuration parity—reduces human error.
- ✓ Often cheaper—one vendor contract, scaled infrastructure.
- ✓ Still removes single points of failure—if designed correctly (separate regions, networks, control planes).
- ✓ Access to advanced features—Apex alias, geolocation, failover, etc., that sync seamlessly.

Cons

- ✗ Vendor lock in remains—if the vendor has a systemic issue, both infrastructures may be impacted.
- ✗ Resilience depends on vendor architecture—not all vendors truly isolate environments.
- ✗ Perception risk—some stakeholders equate “single vendor” with “single point of failure,” even when technically untrue.

DNS resilience decision tree

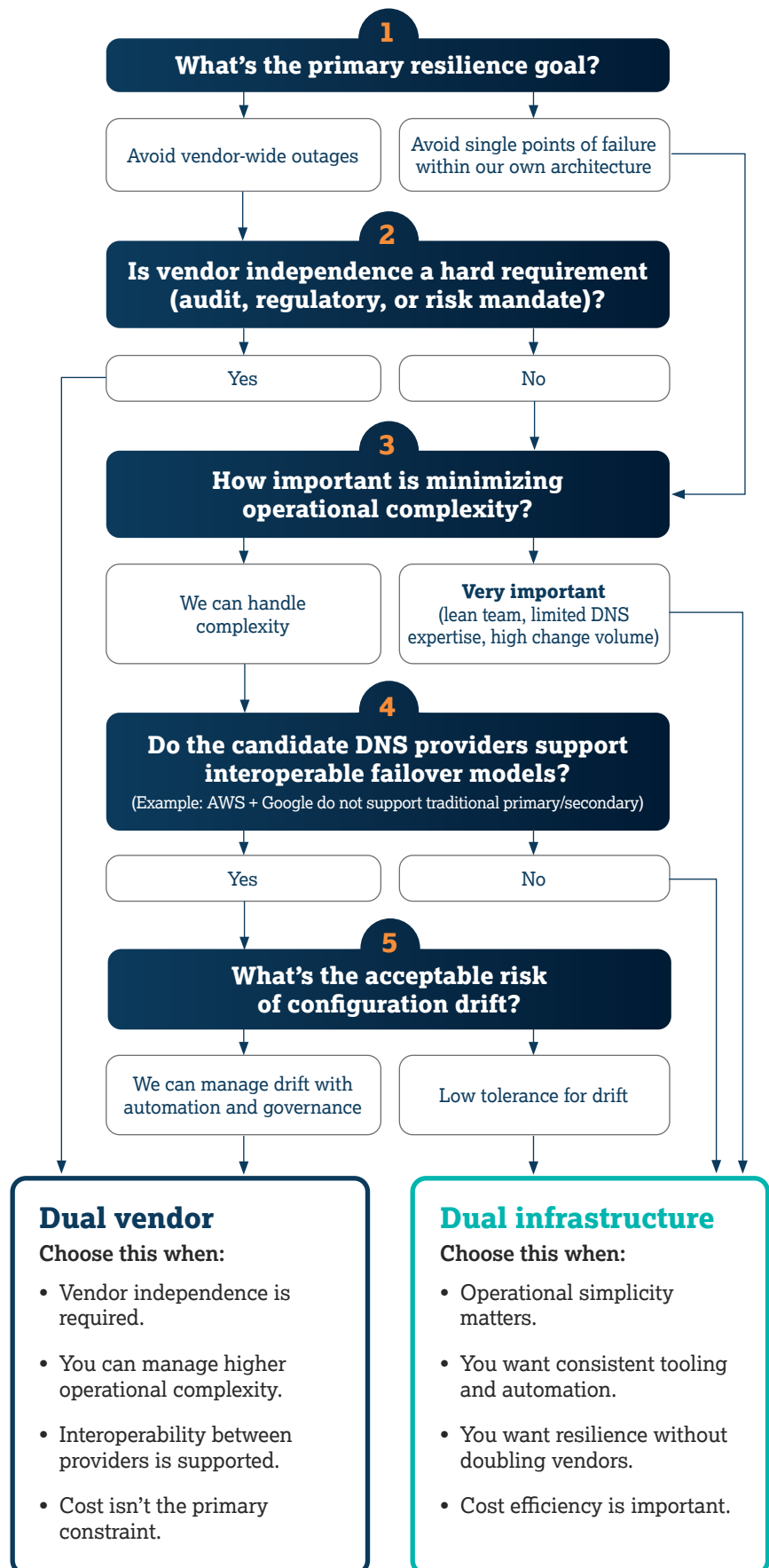
A dual vendor approach

offers the highest level of vendor independence, reducing reliance on any single provider. However, it introduces greater operational complexity, increased integration effort, and management overhead.

A dual infrastructure approach

provides strong resilience with lower complexity by creating redundancy within the same operating model. This option offers single-pane-of-glass oversight and is easier to manage than a dual vendor strategy, but it remains dependent on a single vendor's ecosystem.

The right choice depends on your priorities.



Whichever approach you need, we have the solutions.

CSC's dual vendor solution— with 100% uptime

CSC's enterprise-class DNS services are backed by an authoritative network that uses border gateway protocol (BGP) and IP AnyCast routing schemes to manage billions of global queries a day via 48 points of presence (POPs) across six continents. It has the longest credible 100% uptime in the industry. Plus, you can apply advanced features, such as DNSSEC, failover, geolocation, and weighted load balancing for additional security control.

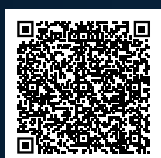
CSC's dual infrastructure solution— one user interface in active-active configuration

CSC's Ultimate DNS offers all the features an organization needs in enterprise DNS management, with the added redundancy of a second independent global DNS anycast network via one user interface in active-active configuration. Vendor risk is mitigated with truly isolated environments, as well as using different data centers and carriers. This ensures exceptional value and a single point of contact for managing your DNS network.





CSC is the trusted security and threat intelligence provider of choice for the Forbes Global 2000 and the 100 Best Global Brands (Interbrand®) with focus areas in domain security and management, along with digital brand and fraud protection. As global companies make significant investments in their security posture, our DomainSecSM platform can help them understand cybersecurity oversights that exist and help them secure their online digital assets and brands. By leveraging CSC's proprietary technology, companies can solidify their security posture to protect against cyber threat vectors targeting their online assets and brand reputation, helping them avoid devastating revenue loss. CSC also provides online brand protection—the combination of online brand monitoring and enforcement activities—with a multidimensional view of various threats outside the firewall targeting specific domains. Fraud protection services that combat phishing in the early stages of attack round out our solutions. Headquartered in Wilmington, Delaware, USA, since 1899, CSC has offices throughout the United States, Canada, Europe, and the Asia-Pacific region. CSC is a global company capable of doing business wherever our clients are—and we accomplish that by employing experts in every business we serve.



Get in touch

 cscdbs.com

CSC is a service company and does not provide legal or financial advice. The materials here are presented for information purposes only. Consult with your legal or financial advisor to determine how this information applies to you.