Authentic Web®

Empowering Enterprise Teams for DNS Security and Compliance

Healthcare DNS Security and Compliance Benchmark Report 2026

An industry-wide assessment of external DNS security posture.

Powered by dns inspector™

Learn more at dnsinspector.io

Powered by DNS Inspector®, Authentic Web will publish follow-up healthcare and other industry sectors, chosen from our assessment of industries at risk, and report subscriber requests.

To receive new benchmark studies or related DNS security and compliance information, subscribe here.

Contents

Healthcare DNS Security and Compliance: Dashboard

Dashboard: HTTP/HTTPs totals exclude certain A Records.

Section One

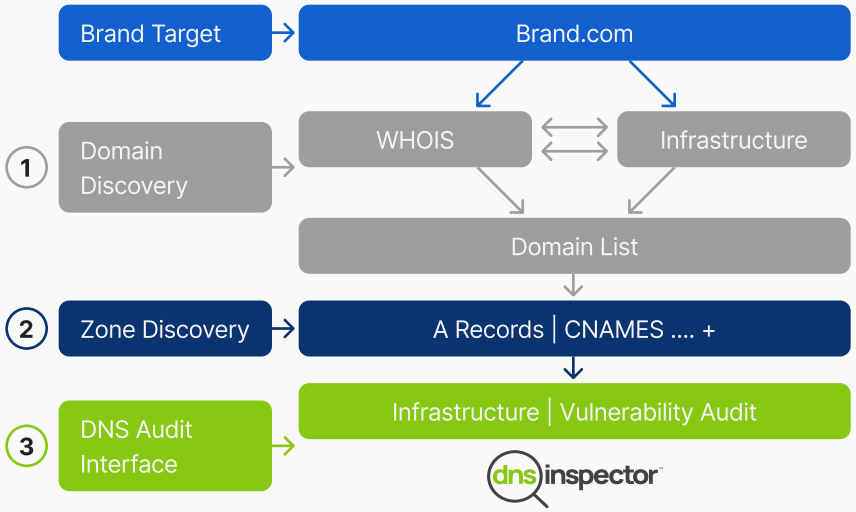
About This Report

This is the second benchmark for the healthcare industry following our last published report in 2024. The purpose of this report is to draw attention to enterprise security risks associated with external DNS networks. The DNS is the publicly available network that makes the internet work. Malicious actors also use it to identify endpoints and related vulnerabilities on the network. Failure to maintain good DNS hygiene, establish and enforce DNS security policies, and govern change management, makes enterprises non-compliant with security frameworks such as HIPPA, SOC2, and ISO., exposing enterprises to network and data vulnerabilities.

Effective infrastructure managers understand that strong DNS security and a strong compliance posture are the foundation for well-run infrastructure and systems operations.

Methodology

Authentic Web Inc. selected a representative sample of 25 medium to large healthcare providers across the United States. Using DNS Inspector domain and DNS discovery capabilities and cross-referencing WHOIS and IT infrastructure, we identified 9,337 domains used by the sample organizations. We further catalogued the zone files for each domain, capturing the ±32,500 resource records that underpin these companies' digital footprint, and scanned them for DNS network vulnerabilities.



Benchmark study parameters	
25	Medium to large healthcare providers
9,337	Domains across the organizations
32,543	Resource records associated with the domains' zone files

[1] Healthcare Providers Audited: 25 organizations with average revenue of $93B ranging from $240M up to $400B and average employees of 81,000 from 2,000 to a high of 440,000. The study included sub-sectors as well with 14 hospitals, five insurance companies, four pharmaceutical and two technology providers.

Section Two

Benchmark Study Scope

The following domain and DNS records were audited for this industry benchmark study.

Item	Number	Ratio	
Total Domains	9,337	373	Domains per entity
Analyzed	32,543	3.49	Records analyzed per domain
Total A Records	8,213	0.88	A Records per domain
Total CNAMES	2,716	0.29	CNAMES per domain
Total Redirects	2,081	0.22	Redirects per domain
SPF	5,030	0.54	SPF records for each domain
DMARC	4,829	0.52	DMARC records per domain
DNSSEC	337	0.04	DNSSEC records per domain

Domain Registrars

The domains found are with 85 domain registrars, five of which represent 95% of all domains audited.

DNS Providers: Top 5
MarkMonitor Inc.
Corporation Service Company
Network Solutions, LLC
GoDaddy Inc.
Corsearch Domains LLC

DNS Providers

The domains found use 132 distinct DNS service providers, with ten representing 58% of all domains audited.

DNS Providers: Top 10
Aetna
Cloudflare
CIGNA
GoDaddy.com, LLC
Google
Mckesson
NSONE Inc
MarkMonitor
Worldnic
Ultradns

Top-level Domains

The domains found are concentrated in legacy top-level domains, with 59.5% of all domains found to be using .com.

Type	Domains	TLDs
Legacy Generic	8,973	7
Country Codes	215	25
New Generics	149	56
Total	9,337	88
.COM	5,551	59.5%

Section Three

DNS Vulnerabilities Explained

The following subset of DNS vulnerabilities represents the biggest risks to enterprise security, each capable of materially impacting affected businesses.

DNS is used in almost every cyberattack. Because DNS is a global public network, it exposes enterprise vulnerabilities to any party motivated to look at and execute an attack.

What are they?	How are they used in an attack?
Orphaned IPs A Records pointing to IPs which are not under the control of enterprise infrastructure and monitored by end-point vulnerability systems.	Loss of control of an IP on a shared web service such as AWS, creates a vector of attack where the IP can be taken over by a third party.
Dangling CNAMEs CNAMES pointing to a web resource or host which is not under the control of enterprise infrastructure and monitored by end-point vulnerability systems.	Allows the ability for the host name to be created by a third party where the CNAME is pointing enabling deployment of any type of attack.
Insecure Redirects An insecure redirect is represented where one or more of the hops to the destination is an unencrypted (HTTP only) hop in the chain.	Encryption gaps permit the execution of a Man-In-The-Middle exploit used to compromise audiences navigating from the origin to the destination.
Lame Delegations A situation where a domain does not have a Start of Authority Record (SOA) set up on the DNS which governs DNS create and edit control on a domain.	Permits the creation of an SOA record on the DNS service to assume full control over the DNS for that domain.
SPF and DMARC Coverage and Errors There are two gaps to understand. 1. The records do not conform to RFCs. 2. DMARC and SPF records are missing.	Where SPF or DMARC records are not conforming to RFCs or where the records are missing, phishing attacks are enabled.
DNSSEC Coverage Gaps DNSSEC is either not present or not configured correctly on domains. Some organizations resist DNSSEC implementation due to perceived risk of key rolls.	DNSSEC solves the risk of a recursive server being compromised by DNS cache poisoning which can result in exposure to Man-in-the-Middle attacks.

Section Four

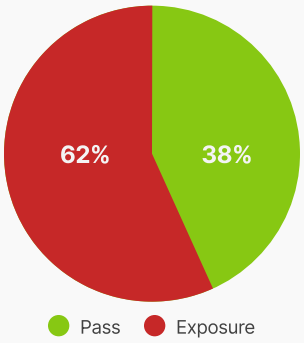
The Benchmark Vulnerability Metrics

DNS network conditions and security vulnerabilities audit

For each examination we are showing the results of the DNS Inspector audit.

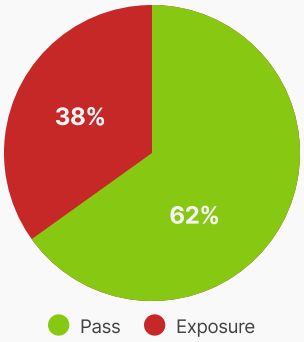
62% of A Records

The HTTP/HTTPS scan exposes potential security vulnerabilities, including orphaned IPs, insecure connections, and allowable use of deprecated TLS versions. Other connection responses may reflect legacy settings that need to be deprovisioned, while others may be acceptable as internal access only by design. This scan empowers infrastructure and infosec teams to investigate each record to classify risks as material or acceptable.



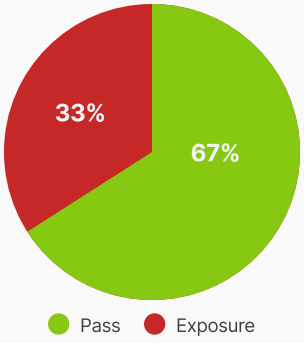
38% of Redirects

The redirect scan identifies unsecured redirects. All redirects must use certificates from the origin domain through to the destination URL. This ensures end-to-end encryption to protect users from MITM attacks. Other exposures may include an excessive number of hops to a destination or orphaned records pointing to a destination or orphaned records pointing to resources the company no longer controls.



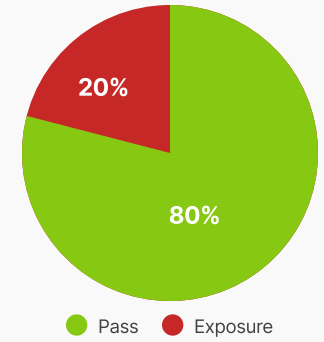
33% of CNAMES

The CNAME scan identifies Dangling CNAMEs in the domain portfolio. Like Orphaned IPs, Dangling CNAMES are vulnerable to compromise with minimal effort. Over time, IT teams will have configured CNAMES for specific purposes. When the purpose is no longer required, the destination is deprovisioned yet teams neglect to remove the CNAME, leaving it vulnerable to takeover.



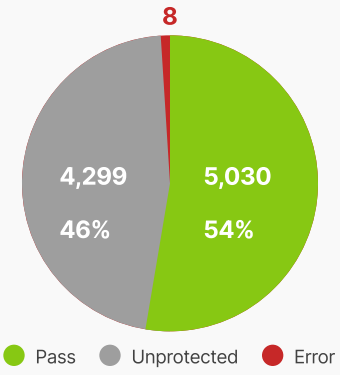
20% Lame Delegations

Failure to ensure a valid Start of Authority (SOA) record opens an attack vector that lets parties create an illegitimate SOA record on the DNS network where it is hosted. This enables the hijacking of the domain's DNS zone file. 20% is a very high number. This clearly shows that legacy registrars and domain owners are failing to keep their domains secure.



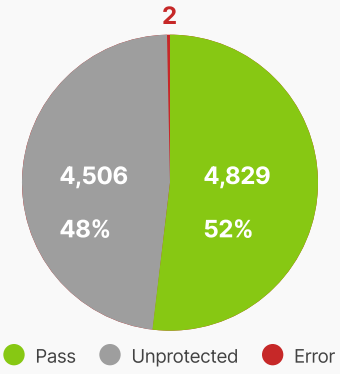
46% Sending Policy Framework (SPF)

46% of domains are not covered by SPF records. 8 of the SPF records are non-compliant with the standards-based RFC. SPF records define the sending mail servers authorized to send mail using that domain. This exposes the domain owner to phishing emails from their own domain. Since phishing is one of the most common attack vectors, companies must ensure every domain owned has a valid SPF record.



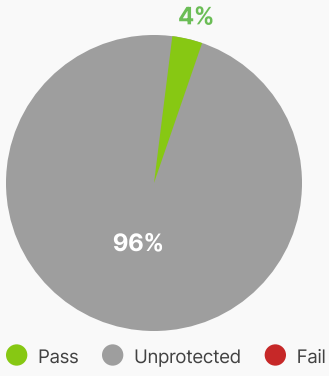
48% Domain-Based Message Authentication, Reporting & Conformance (DMARC)

48% of domains are not covered by DMARC records. 2 of the DMARC records are non-compliant with the RFC. DMARC records work with SPF records to help ensure secure email communications. Without applying DMARC across the entire domain portfolio, phishing emails can be sent from your own domain.



96% Domain Name System Security Extensions (DNSSEC)

96% of domains are not signed. DNSSEC uses cryptographic signatures to sign a domain's zone file. DNSSEC defends against recursive server cache poisoning, thereby preventing DNS-based MITM attacks. Automated signature key rolling, now used by modern registrars and DNS provider systems, will increase adoption over time.



Section Five

What Changed: 2024 vs. 2026

The following compares results from the 2024 Benchmark Study with those from this 2026 report.

Item	2024	2026	Learnings
Scope			
Domains	9,269	9,337	Domains undermanagement has not increased
Records	40,789	32,543	In 2026, infrastructure teams have purged many orphaned A Records. This is a positive finding demonstrating that teams recognize the need to address these exposure risks.
Registrars	91 Total Top 5 = 93%	85 Total Top 5 = 95%	No material change.
DNS Providers	81 Total Top 5 = 72%	132 Total Top 10 = 58%	Significant change in the number and concentration. This is due to two factors. 1. High M&A activity without executing DNS consolidations. 2. Infrastructure teams are exploring new DNS providers.
Top-level Domains	60% = .COM	59.5% = .COM	No change in the makeup of top-level domains in use.
DNS Governance: Security and Compliance Findings			
Orphaned IPs Insecure Connections	89% Exposed	62% Exposed	These records represent Orphaned IPs or insecure connections. Companies have reduced the number of orphaned A Records overall.
Insecure Redirects	17% Exposed	38% Exposed	Insecure redirects represent a material risk and have worsened. Companies are failing to ensure end-to-end encryption on their redirects to destinations.
Dangling CNAMES	35% Exposed	33% Exposed	The exposure is consistent vs. 2024. CNAMES are left as legacy configurations, resulting in dangling CNAMES. Some of these records are validation records that require DNS hygiene to ID and remove.
Lame Delegations	17% Exposed	20% Exposed	Lame Delegations have worsened. This is likely due to DNS provider migrations that did not fully reset delegations and the adopted risk in M&A.
SPF Coverage	50% Exposed 1% Error Rate	46% Exposed 1% Error Rate	Domains without SPF coverage. | Error Rate We are seeing a marginal improvement; however, it remains high and exposes companies to phishing.
DMARC Coverage	52% Exposed <1% Error Rate	44% Exposed <1% Error Rate	Domains without DMARC coverage. | Error Rate We are seeing a marginal improvement; however, it remains high and exposes companies to phishing.
DNSSEC	99% Exposed 0% Error Rate	96% Exposed 0% Error Rate	Marginal improvement since 2024. This indicates that some teams are working on DNSSEC; however, the risk of DNS cache poisoning remains elevated.

Take Aways

Over the past two years, there is clear evidence that infrastructure teams are recognizing the need and have reduced their A Record exposure. However, other DNS risk exposures and DNS hygiene remain a significant challenge for these teams. Insecure redirects as a percentage of the whole have more than doubled. That is a big red flag.

Lame delegations have also increased, likely due to a lack of post M&A DNS consolidations. Modest improvements in SPF, DMARC, and DNSSEC coverage are a positive indicator of intent; however, infrastructure teams still struggle to make material risk-reduction improvements, likely because of manual processes and a lack of formal DNS governance, risk, and compliance programs to manage their DNS networks.

Bottom line

nfrastructure, compliance, and infosec teams cannot address DNS governance and security manually. Managing and securing DNS networks requires continuous security monitoring and DNS control systems.

Section Six

Summary

- → Healthcare is the most cyber-attacked sector in North America. Source →
- → Healthcare is subject to several Information Security Frameworks.
- → Current DNS practices fall short of compliance requirements included in SOC2, CIS, NIST, and ISO. Source →
- → This DNS Security Audit Benchmark Report provides evidence of the DNS security risks and compliance gaps that healthcare operators must address.

Best Practices

Achieve DNS management and security maturity.

01 Conduct a DNS security assessment to gain visibility and establish your company's security posture.
02 Consolidate domains to a single registrar and DNS provider with change control automation.
03 Implement ongoing DNS configuration, security inspections, and monitoring systems.

Benefits of action

These best practices will demonstrably reduce external DNS vulnerabilities and risks while delivering operating efficiency and compliance controls.

01 Keeps your company and customers safe in your branded spaces.
02 Complies with relevant security framework requirements on infrastructure controls.
03 Automates the practice and makes it **EASY** for teams to Get and Keep Control.
04 Reduces total cost of ownership through consolidation and automation.

How does your healthcare company compare?

Authentic Web is offering to conduct a DNS Inspector security assessment and review at no cost to qualified healthcare providers.

To schedule an assessment, email info@authenticweb.com with the subject **"DNS Assessment"** or visit dnsinspector.io to submit your request.

Powered by dnsinspector™

Learn more at dnsinspector.io

Find more white papers on DNS Security, Compliance and Best Practices on our website.

info@authenticweb.com
authenticweb.com | dnsinspector.io