Authentic Web®

Empowering Enterprise Teams for DNS Security and Compliance

DNS Security in the Healthcare Sector

Why healthcare providers must improve security framework compliance in DNS management

1. Overview: DNS security and compliance in the Healthcare Sector
2. IT Security Frameworks and the DNS
3. How and why the DNS is at risk in Healthcare
4. Best practices to mitigate DNS security risk
5. Appendix: Healthcare Sector DNS Security Benchmark Audit

> "Healthcare is a top target for cyber criminals in part because its networks and data are exposed on the DNS. Our healthcare sector DNS security audit discovered non-compliance in IT controls across many InfoSec frameworks. This paper will help teams identify and remediate these security risks and compliance gaps."
>
> Peter LaMantia, CEO, Authentic Web Inc.

Control

Visibility

Compliance

To discuss this paper or learn about our DNS security audit, email info@authenticweb.com

Section One

Overview: DNS Security and Compliance in the Healthcare Sector

Purpose of this paper

We examine external DNS management as a known, and under-addressed vulnerability among healthcare providers. Our observations are:

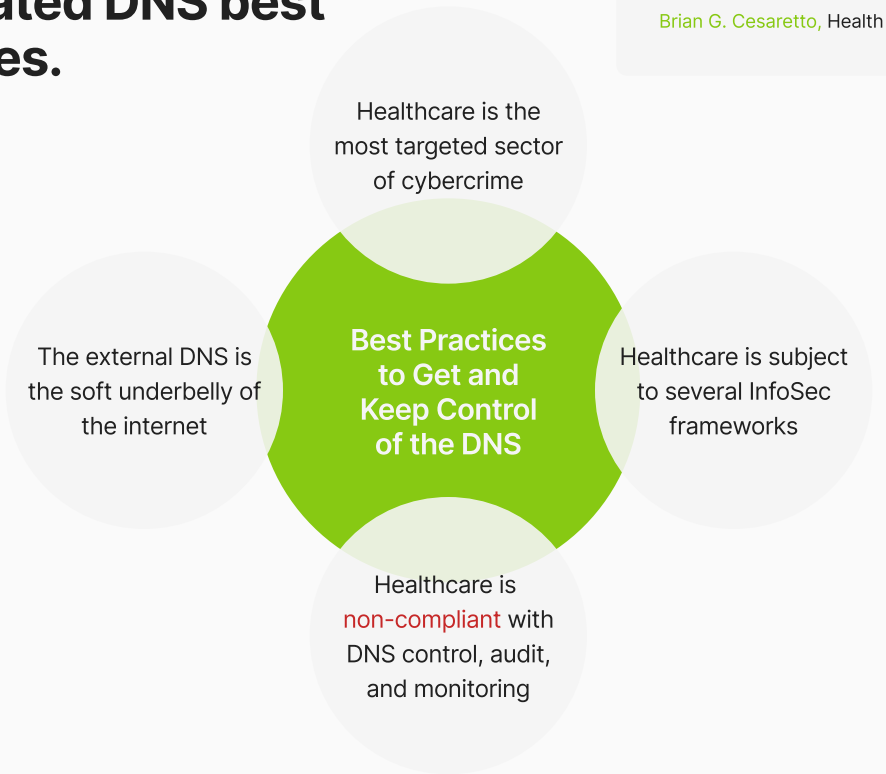
01. The DNS is a principal threat vector, enabling cyber-attackers in healthcare.
02. Compliance standards for external DNS management are inconsistently followed by healthcare providers.
03. DNS management best practices can mitigate healthcare cyber-risk.

Healthcare Law Specialists: Epstein Becker Green

The importance of the Domain Name System (DNS) to your organization's cybersecurity cannot be understated... A malicious party (can) exploit a weakness in DNS (and) re-route sensitive traffic, including Protected Health Information (PHI), Personally Identifiable Information (PII) and other valuable information from the intended recipient to (unauthorized sites.)

Brian G. Cesaretto, Health Law

The analysis follows four discussion areas and related DNS best practices.



The Current State of IT Security Threats and Compliance in Healthcare

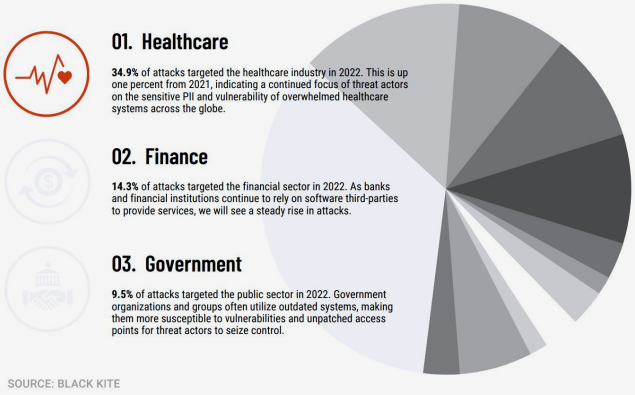
Few sectors are as focused on IT security compliance as healthcare. It's a nexus of sensitive patient data intersecting with payment authorities, insurance companies and other stakeholders.

Healthcare is the most attacked sector

Healthcare providers are collectively the most cyber-attacked sector in North America, recently surpassing Banking & Finance.

"...34.9% of cyberattacks occurred in health care, ..., making it the most attacked sector for the second year in a row—most likely due to the heavy regulations surrounding Personal Health Information (PHI) that have only attracted more attention from hackers. The report also highlighted a lack of budget, outdated software, and the ability to remotely share personal data between patients and hospital systems as avenues for hackers to gain access to sensitive data."

Dozens of other public reports corroborate the state of cyber compromises faced by the healthcare sector.



SOURCE: BLACK KITE

Section Two

IT Security Frameworks and the DNS

IT security compliance standards in healthcare

Healthcare has attracted numerous standards to help govern InfoSec compliance.

Despite the many security framework standards followed by healthcare providers, they remain a perennial target to cyber-criminals who are regularly succeeding in ransomware scams, data exfiltration, phishing exploits, and more.

What IT security frameworks apply to Domains and DNS management and what do they require for compliance?

Security frameworks and the DNS

Managing external domains and DNS controls are not prescriptively specified in all security frameworks, yet relevant themes affecting DNS management are clear. Frameworks including CIS18, SOC2, PCI, NIST, GDPR, and HITRUST CSF contain standards that relate to domains and DNS. Here are some important examples:

Information Security Framework Standard	Domain and DNS Applicability
01. **IT Controls and User Access Controls** Only authorized individuals and systems to have appropriately access to critical company assets and systems.	Domains and DNS are mission critical network assets/systems.
02. **Logging, Audits, Audit Management, Auditability** Track & report all activity related to interaction with company assets, networks, security information, monitoring, etc.	Domain and DNS change history and change reporting required.
03. **Domain and DNS change history and change reporting required.** Any material change to systems and assets must to go through a change management control process.	Change control workflow required to edit domain and DNS records.
04. **Monitoring for Vulnerabilities** All known cyber-attack vectors must be actively monitored and reported on.	Systems to identify and monitor DNS specific attack vectors.
05. **Backups Recovery/Availability of Critical Systems** Companies must be able to backup and restore key systems and information to ensure business continuity.	Secondary DNS and zone file backups are required.
06. **Network Security** No unauthorized/managed access to any company networking systems.	Includes external DNS and domains.

Conclusion

If healthcare providers don't apply InfoSec frameworks to their management of domain assets and DNS network they will fail compliance. More importantly, they'll greatly increase their exposure to known security threats that continue to play out in the sector.

Section Three

How and why the DNS is at risk in Healthcare

External DNS networks: The soft underbelly of IT security

External DNS management is widely acknowledged to be a principal source of cyber breaches and data loss in healthcare and other sectors. The DNS is a publicly accessible network that cyber criminals use to discover and exploit enterprise and customer data.

Despite DNS security risks, security compliance for DNS management is inconsistently covered by the eight most important security frameworks used in healthcare. References to external DNS management vary between frameworks from explicit (NIST, ISO, and CIS), to indirect (HIPAA, PCI DSS, GDPR and SOC II.)

IT'S ALWAYS THE DNS!

Enterprise DNS risk

A study conducted by Efficient IP and IDC shows the importance of the DNS to enterprise cybersecurity strategy with 73% of respondents stating that DNS security is critical. (Source: Efficient IP-IDC 2022)

(Additional references can be found in Resources at the end of this paper.)

What's happening in healthcare to make DNS the primary attack vector

DNS management among healthcare providers often fails to comply with standards-based best practices due to three important factors.

01. **Multiple Domain Registrars and Managed DNS Providers:** Healthcare providers often own hundreds of domains registered across multiple domain registrars and managed DNS provider services.
02. **Lack of Clear Ownership:** Internal ownership of domain assets and DNS is split across departments. This siloed approach includes network infrastructure, legal (IP), InfoSec, and product and marketing.
03. **Complex Environment - Decentralized Management:** Domain and DNS management is inherently complex, involving domains, zone file records and DNS security configurations, that are not centrally managed, governed for compliance, or monitored.

Exacerbating the above, the global DNS infrastructure is publicly accessible - and dangerously so. Unlike internal networks, the external DNS can be viewed, probed, and exploited by external parties.

> Awareness of DNS security is very strong: **73% say it is critical**

DNS security consequences

The smallest misconfigurations and errors can expose healthcare providers. Examples include:

- ✓ Insecure redirect domains
- ✓ Orphaned or missing CNAMES
- ✓ Missing or misconfigured DNS settings, like SPF, DMARC, DNSSEC, and DKIM

Malicious parties constantly scan for these gaps to execute various intrusion tactics such as man-in-the-middle exploits, domain hijacking, DNS cache poisoning, takeover of orphaned A Record and CNAME endpoints, and phishing scams using the healthcare provider's own domains.

How and why DNS management is non-compliant in healthcare

Vendor fragmentation in the domain and managed DNS space has created a lack of robust, compliant change management systems for this vulnerable area. Domain and DNS management is often the exception to otherwise compliant approaches in healthcare IT practices.

External DNS management often lacks these important compliance measures:

01 Role-based, permissioned access to DNS change management

02 Tamper-proof logging of change and auditable change reports

03 Correctly configured and monitored DNS security settings

04 Missing MFA or single sign-on access controls across all vendor systems

05 Lack of network asset or endpoint visibility and governance

Healthcare mergers & acquisitions make matters worse

Every time a healthcare enterprise acquires an entity, it also acquires the latent security issues in the target company's domain assets and DNS network. Domain and DNS security issues are notoriously difficult to identify. Due diligence rarely determines the full security posture of target domain and DNS assets.

Serial M&A events, the strategic aim of many large HCPs, compound the security risks as newly acquired DNS operations pile on to previous acquisitions, without complete integration.

Best practice solutions to DNS security risks from M&A

01 Always conduct a though (external) audit of target domain assets and DNS networks

02 Consolidate acquired assets to a single domain registrar and managed DNS service

03 Place all acquired assets under a unified, compliant, change management system

Section Four

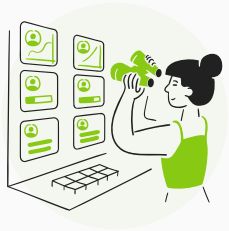
Four Best Practice Recommendations

How healthcare can eliminate external DNS security risks and close compliance gaps

Benchmark your DNS security posture with a domain and DNS security audit

Audits confirm that every organization has security gaps in their domain assets, corresponding zone files, and DNS security settings. Internal audits, self-conducted by healthcare providers, are manual, costly, and rarely produce complete results.

Healthcare providers believe their external DNS is compliant. It is not.



Consolidate domains and DNS to a single registrar and managed DNS service provider

Employing multiple domain registrars and managed DNS providers creates several security issues. Multiple, non-integrated administrative controls for each service make critical domain, DNS, and TLS certificate details less visible to stakeholders, and harder to manage.

Healthcare providers believe their domain assets and DNS are locked down. They are not.

Place domains, DNS, and TLS certificates under a standards-compliant change management system

ISO/IEC, NIST, and CIS demand role-based, permissioned access controls and a tamper-proof audit history of all access and change activity. Yet, few healthcare providers follow these compliance measures in their domain and DNS management operations.

While healthcare providers are standards-compliant in most of their network operations, in domain and DNS management, they are not.

Place domains and DNS assets under a DNS-specific security inspection and monitoring system

Companies must continually monitor DNS security. New vulnerabilities can surface at any time from internal staff and the ongoing efforts of unauthorized external parties.

Healthcare providers' DNS security posture demands constant, ongoing security framework compliance.

Summary

- ✓ Healthcare is the most cyber-attacked sector in North America.
- ✓ Healthcare is subject to several information security frameworks, that are often not applied to domain asset and DNS management.
- ✓ The external DNS remains an open vulnerability, perpetuating IT security risk.
- ✓ Current DNS practices fall short of compliance requirements included in SOC2, CIS, NIST, and ISO.
- ✓ Healthcare providers must do better. Four best practices are essential as a starting point:

  01 Conduct a domain and DNS security audit to benchmark your DNS security posture

  02 Consolidate domains and DNS to a single registrar and Managed DNS service provider

  03 Place domains, DNS, and TLS certificates under a compliant change management system

  04 Place domains and the DNS under a DNS-specific security inspection and monitoring system

These four actions can demonstrably reduce external DNS vulnerabilities and risks that currently help perpetuate successful cyber-attacks against the healthcare sector.

Additional Resources

DNS security-related white papers

A CISO Brief: Why your Enterprise is Exposed on the DNS

Lack of functional ownership over domain and external DNS security, combined with a lack of unified control systems to enforce DNS security policies are the top factors that expose your company and customers to external DNS vulnerabilities.

Download white paper →

M&A Guide to Assess and Consolidate Domain Assets and DNS Networks

Assessing and consolidating domains and DNS service providers are crucial “pre” and “post” M&A deal priorities. When you acquire a company, you are not only buying the assets, you are also buying the cyber security risk.

Download white paper →

Six DNS Problems in the Digital Enterprise

Recent audits of dozens of companies’ domain/DNS systems spanning over 20,000 domains reveal common security and compliance problems. Learn what the top six issues are and how to correct them in your organization.

Download white paper →

Contact us to discuss this paper or arrange a DNS security audit for your organization.,

info@authenticweb.com

authenticweb.com | dnsinspector.io

Appendix

Authentic Web®

Empowering Enterprise Teams for DNS Security and Compliance

Healthcare DNS Security and Compliance Benchmark Report 2024

An industry-wide assessment of external DNS security posture.

Powered by dns inspector™

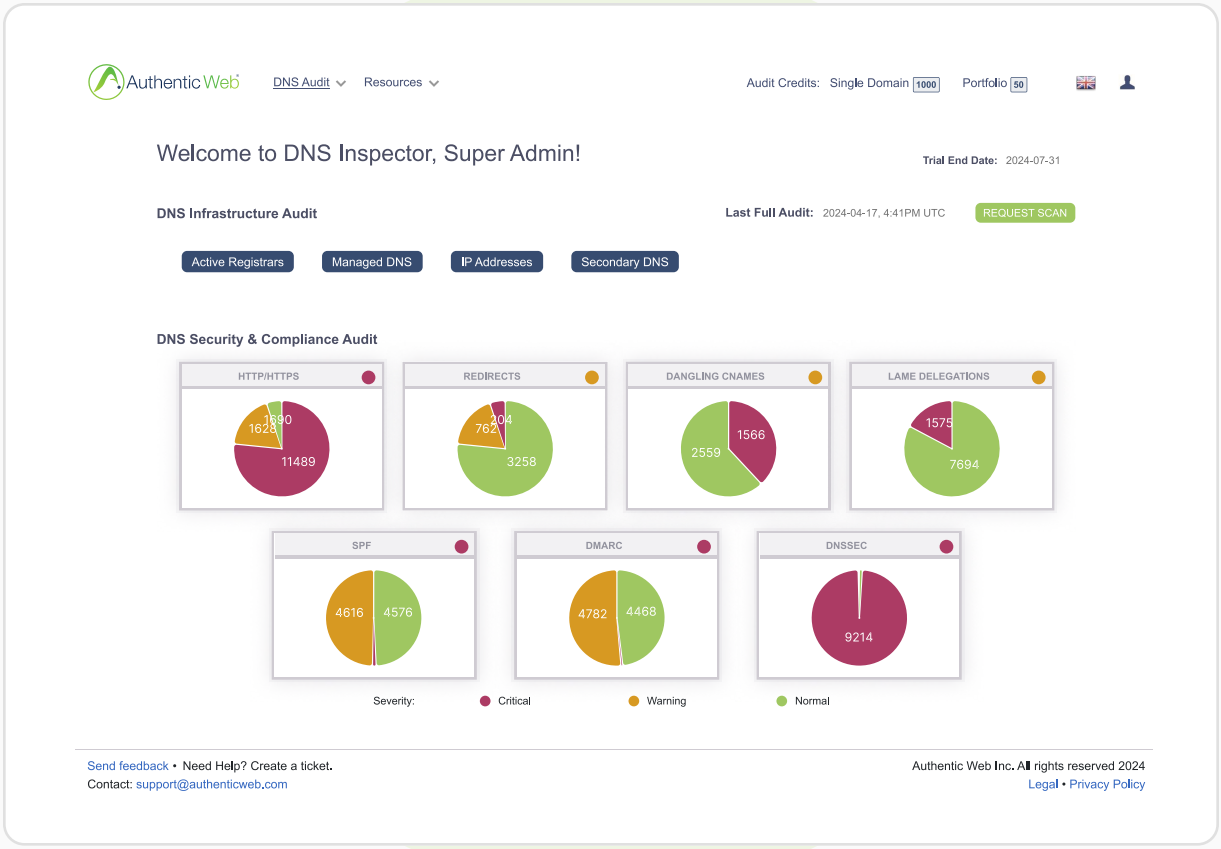
Learn more at dnsinspector.io

Powered by DNS Inspector, Authentic Web will publish follow-up benchmark studies on 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



Section One

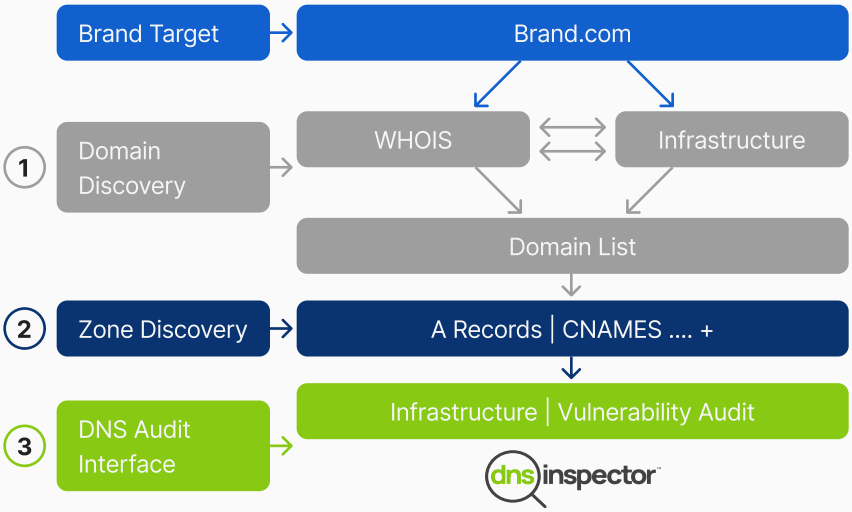
About This Report

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. It is also used by malicious actors to identify endpoints and related vulnerabilities that exist 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 a strong DNS security and compliance posture is the foundation for well-run infrastructure and systems operations.

Methodology

Authentic Web Inc. selected a representative sample of 25 medium to large healthcare providers[1] across the United States. Using DNS Inspector domain and DNS discovery capabilities and cross-referencing WHOIS and IT infrastructure, we identified 9,269 domains used by the sample organizations. We further catalogued the zone files for each domain, capturing the ±40,000 resource records that underpin the digital footprint for these companies and scanned them for DNS network vulnerabilities.



Benchmark study parameters	
25	Medium to large healthcare providers
9,269	Domains across the organizations
40,000	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	9,269	371	Domains per entity
Total Records Analyzed	40,789	6.24	Records analyzed per domain
Total A Records	14,807	1.6	A Records per domain
Total CNAMES	5,392	0.58	CNAMES per domain
Total Redirects	2,222	0.24	Redirects per domain
SPF	4,576	0.49	SPF records for each domain
DMARC	4,458	0.48	DMARC records per domain
DNSSEC	55	0.006	DNSSEC records per domain

Domain registrars

The domains found are with 91 domain registrars, five of which represent 93% of all domains audited.

Registrars
Network Solutions
MarkMonitor
CSC
GoDaddy
Corsearch

DNS providers

The domains found use 81 distinct DNS service providers, with five representing 72% of all domains audited.

DNS Providers
Cloudflare
AT&T
CIGNA
NSONE Inc
GoDaddy

Top-level domains

The domains found are concentrated in legacy Top-level Domains with 60% of all domains found to be using .com.

Type	Domains	TLDs
Legacy Generic	8,855	6
Country Codes	275T	25
New Generics	139	56
Total	9,269	87
com	5,555	59.9%

Section Three

DNS Vulnerabilities Explained

The following subset of DNS vulnerabilities represent the biggest risks to enterprise security, each capable of material impact to businesses affected.

The DNS is used in every cyberattack, almost without exception. Because the DNS is a global public network, it exposes enterprise vulnerabilities to any party motivated to look 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.
SFP 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

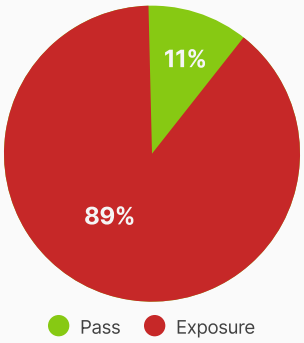
The Benchmark Vulnerability Metrics

DNS network conditions and security vulnerabilities audit

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

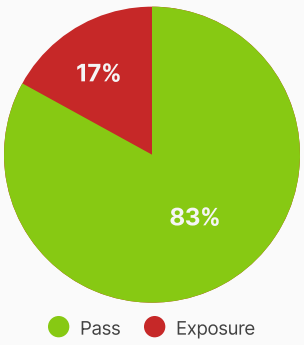
89% of A Records

The HTTP/HTTPS scan exposes potential security vulnerabilities, including orphaned IPs, insecure connections, and allowable use of deprecated TLS versions. Other connection responses may be legacy settings that need to be deprovisioned and 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.



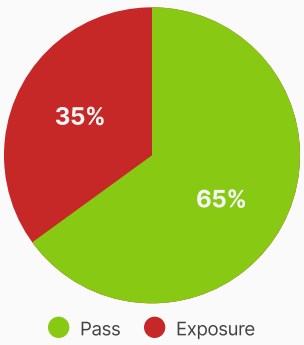
17% of Redirects

The redirect scan identifies unsecured redirects. All redirects must be set with 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 resources the company no long controls.



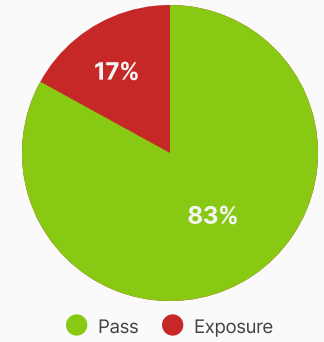
35% of CNAMES

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.



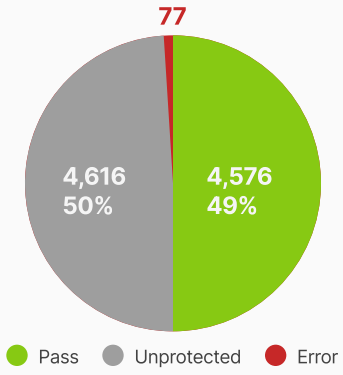
17% Lame Delegations

Failure to ensure a valid Start of Authority (SOA) record opens a vector of attack wherein parties can create an illegitimate SOA record on the DNS network where it is hosted. This enables the hijacking of the domain's DNS zone file. 17% is a very high number. This is clear evidence that legacy registrars and domain owners are failing to ensure their domains are secure.



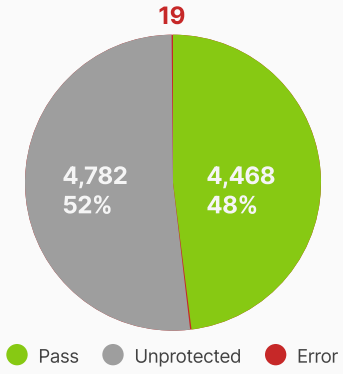
50% Sending Policy Framework (SPF)

50% of domains are not covered with SPF records and 77 or ±1% of the SPF records are non-compliant to 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.



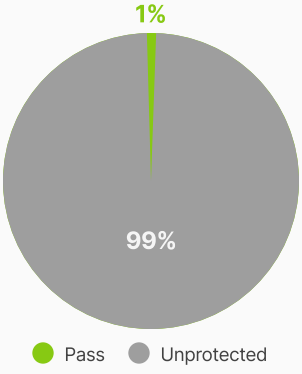
52% Domain-Based Message Authentication, Reporting & Conformance (DMARC)

52% of domains are not covered by DMARC records and 19 of the DMARC records are non-compliant to the RFC. DMARC records are used in conjunction with SPF records to ensure secure email communications. Without applying DMARC across the entire domain portfolio, phishing emails can be sent from your own domain.



99% Domain Name System Security Extensions (DNSSEC)

99% 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 in use by modern registrars and DNS provider systems is expected to increase adoption over time.



Section five

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 audit 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 on 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 Reduce total cost of ownership through consolidation and automation.

How does your healthcare company compare?

Authentic Web is offering to conduct a DNS Inspector security audit and review at no cost to qualified healthcare providers. To schedule an audit, email info@authenticweb.com with subject "**DNS Audit Request**" 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