Authentic Web®

Empowering Enterprise Teams for DNS Security and Compliance

# Retail Companies are Failing DNS Security Framework Compliance

## *6 risk areas and the best practices to eliminate them*



> *"Retail is a top target for cyber criminals in part because their networks and data are exposed on the DNS. Our retail 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

# DNS Security and Compliance in the Retail Sector: Overview

## Purpose of this paper

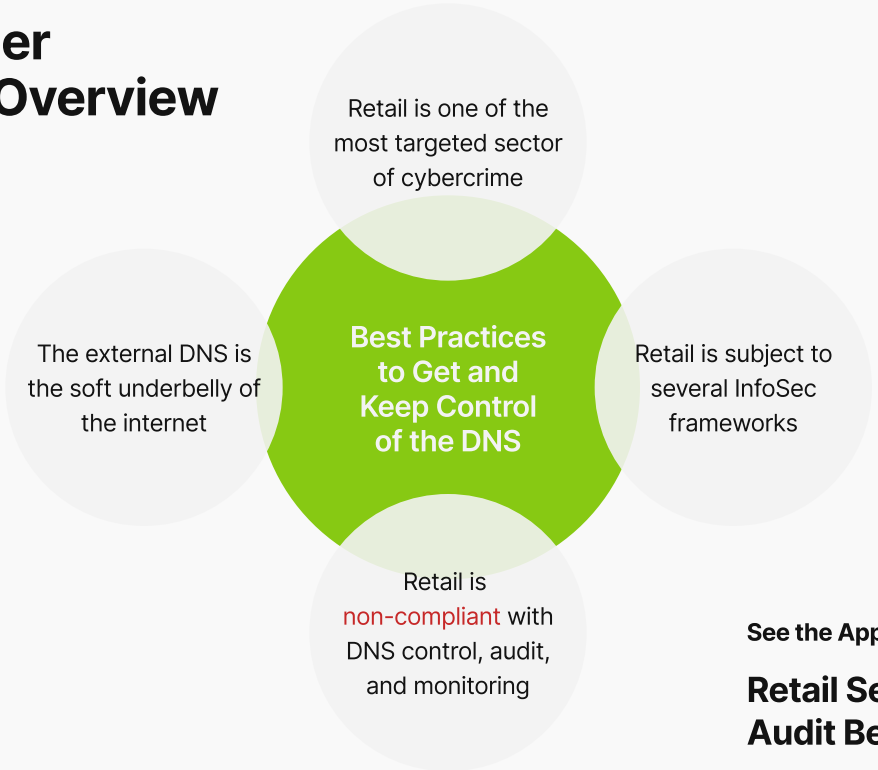
We examine **external DNS management** as a known, and under-addressed vulnerability among retail enterprises.

Our observations are:

01. The DNS is a principal attack vector, enabling cyber-attackers.
02. Compliance standards for external DNS management are inconsistently followed.
03. DNS management best practices can mitigate retail sector cyber-risk.

> *"Credit card data is the new currency for hackers and criminals, and retailers possess a lot of it. This makes the retail industry an almost irresistible target for cyber-attacks."*
>
> Global Cyber Executive Briefing - Retail, Deloitte.

## White Paper Contents Overview




**See the Appendix for an industry first:**

**Retail Sector DNS Security Audit Benchmark Report**

# The State of Threats and Compliance in Retail

Few sectors are as focused on IT security compliance as retail. It's a virtual goldmine of sensitive consumer data intersecting with payment authorities, supply chain partners, and other stakeholders.

## Retail ranks among the 5 most cyber-attacked sectors

Retail consistently ranks among the top five "most cyber-attacked" sectors with one ranking it the most cyber-attacked sector in 2019.

According to Fortinet, 24% of cyberattacks target retailers. "Given the wealth of payment information retailers have access to, it is no surprise that nearly a quarter, 24%, of all cyberattacks (target) retailers. Retailers often have varying levels of security, leaving them exposed to cyber criminals."

# IT security compliance standards in retail

Despite the many security framework standards followed by retail organizations, they remain a perennial target to cybercriminals, who are regularly succeeding in ransomware scams, data exfiltration, phishing exploits, and more.

We observe two reasons for this:

01. Most security frameworks do not explicitly call out domain and DNS governance, yet all include the requirement for full change controls over critical infrastructure. DNS networks are critical infrastructure.
02. Many senior security executives we've interviewed admit that they have operational gaps in applying framework standards specifically to domains and the DNS.

# Security frameworks and the DNS

Managing external domains and DNS controls are not prescriptively specified in all security frameworks, yet relevant themes pertaining to DNS management are clear. Frameworks including CIS18, SOC2, PCI, NIST, GDPR, and HITRUST CSF contain standards pertinent to domains and the DNS.

## Examples:

| Information Security Framework Standard | Domain and DNS Applicability |
|---|---|
| 01. **IT Controls and User Access Controls** Only authorized individuals and systems to have appropriate 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. **Change Management** Any material change to systems and assets needs to go through a change management control process. | Change workflow required to edit domain and DNS records. |
| 04. **Monitoring for Vulnerabilities** All known cyber-attack vectors need to be actively monitored, remediated and reported. | Systems to identify & monitor DNS specific attack vectors. |
| 05. **Backups Recovery/Availability of Critical Systems** Companies need to 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 & domains. |

## Conclusion

If retail organizations don't apply InfoSec Framework requirements to their management of domain assets and DNS network, they will fail compliance audits and greatly increase their exposure to known security threats that continue to play out in the sector.

# External DNS Networks: The Soft Underbelly of InfoSec

External DNS management is widely acknowledged to be a principal source of cyber-breaches and data loss in retail 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 retail. References to external DNS management vary between frameworks from explicit (NIST, ISO, and CIS), to indirect (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.

# Why the DNS is Retail's Primary Attack Vector

DNS management in retail fails to comply with standards-based best practices due to three important factors.

01. **Multiple Domain Registrars and Managed DNS Providers:** Retailers 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), IT security, operations, 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 typically 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 retail organizations. Examples include:

- ✓ Insecure redirect chain to the destination
- ✓ Orphaned A Records and Dangling 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 retailers' own domains.

# How and Why DNS Management is Non-Compliant in Retail

Vendor fragmentation in the domain and managed DNS space has created a lack of robust, compliant change management processes for this vulnerable area. Domain and DNS management is often the exception to retailers' security compliance in other IT and network areas.

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

05 Network asset or endpoint visibility and governance

## Retail Mergers & Acquisitions Make Matters Worse

Every time a retail organization buys a company, 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 retailers, compound the security risks as newly acquired DNS operations accumulate from previous acquisitions, without complete integration.

### Best practice solutions to DNS security risks from M&A

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

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

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

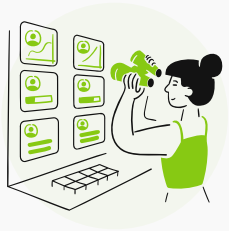
# Four Best Practice Recommendations

## How retail can eliminate external DNS security risks and 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 retailers are manual, costly, and rarely produce complete results.

**Retail organizations 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.

**Retailers 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 retail organizations follow these compliance measures in their domain and DNS management operations.

**While retailers 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.

**Retail organizations' DNS security posture demands constant, ongoing security framework compliance.**

# Summary


- Retail is one of the most cyber-attacked sectors in North America.
- Retail is subject to several InfoSec Frameworks, that require change controls, auditability and monitoring over domain and DNS networks.
- 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.
- Retail organizations 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 DNS service provider

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

  04 Establish a domain and DNS security inspection monitoring system

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


**Appendix:**

Our **Retail DNS Security Audit Benchmark Report** shows DNS security risks and compliance gaps.

# Resources

## DNS Security Related Whitepapers

### 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

# Retail DNS Security and Compliance Benchmark Report 2024

*An industry-wide assessment of external DNS security posture.*

Powered by dnsinspector™

Learn more at dnsinspector.io

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

# Contents



# Retail DNS Security and Compliance: Dashboard

Section One

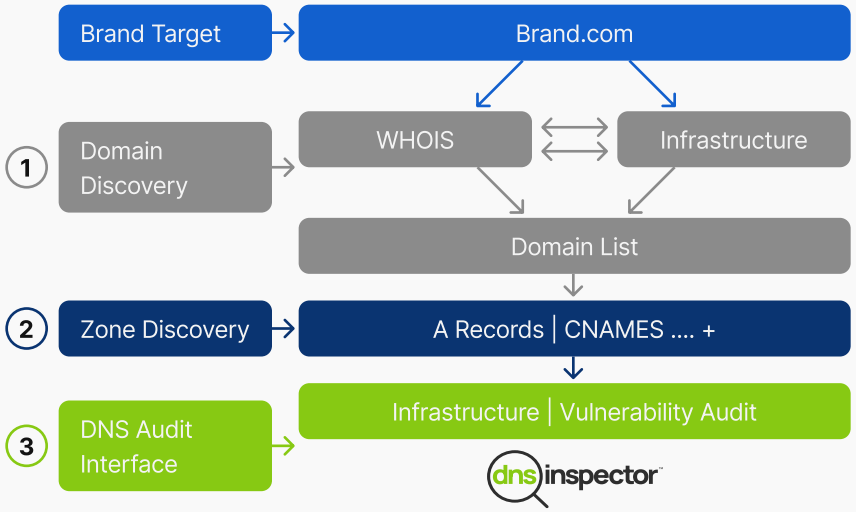
# About This Report

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

# Methodology

Authentic Web selected a representative sample of 25 medium to large retail brands[1] across the USA, Canada & the UK. Using DNS Inspector domain and DNS discovery capabilities and cross-referencing WHOIS and IT infrastructure, we identified over 20,531 domains used by the sample organizations. We further catalogued the zone files for each domain, capturing 79,531 resource records that underpin the digital footprint for these companies and scanned them for DNS network security vulnerabilities.




| Benchmark study parameters | |
|---|---|
| **25** | Medium & large retail brands |
| **20,484** | Domains owned by the brands |
| **79,531** | Resource records analyzed |

[1] Retail Brands Audited: 25 organizations with with average revenues of $24B ranging from $665M up to $245B.

Section Two

# Benchmark Study Scope

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

| Item | Number | Ratio | |
|---|---|---|---|
| Total Domains | 20,484 | 819 | Domains per entity |
| Total Records Analyzed | 79,531 | 3.88 | Records analyzed per domain |
| Total A Records | 24,440 | 1.19 | A Records per domain |
| Total CNAMES | 9,412 | 0.46 | CNAMES per domain |
| Total Redirects | 10,216 | 0.50 | Redirects per domain |
| SPF Records | 8,326 | 0.41 | SPF records per domain |
| DMARC Records | 6,434 | 0.31 | DMARC records per domain |
| DNSSEC Signatures | 223 | 0.01 | DNSSEC records per domain |

## Domain Registrars

The domains found use 297 unique domain registrars. The top 10 represent 61% of domains audited.

| Registrars | |
|---|---|
| Network Solutions | 4,568 |
| CSC | 2,355 |
| Directi Internet | 1,566 |
| MarkMonitor | 1,356 |
| Tucows/Enom | 1,138 |
| Key-Systems | 571 |
| Safenames | 394 |
| Com Laude | 379 |
| GoDaddy | 341 |
| NameCheap | 280 |
| Top 10 Total | 12,948 |
| Top 10 % | 63% |
| Total Domains | 20,484 |

## DNS Providers

The domains use 185 unique DNS providers the top 10 represent 78% of domains audited.

| DNS Providers | |
|---|---|
| RIPE | 3,040 |
| GoDaddy | 3,010 |
| Network Solutions | 2,710 |
| Cloudflare | 2,554 |
| Vercara | 1,982 |
| Amazon | 771 |
| APNIC | 712 |
| Google | 706 |
| NSONE | 571 |
| Microsoft | 543 |
| Top 10 Total | 16,599 |
| Top 10 % | 81% |
| Total Domains | 20,484 |

## Top-level Domains

The domains found are 88% legacy Top-level Domains and 73% of all domains audited are .com.

| Top-level Domains | |
|---|---|
| Legacy | 18,120 |
| % of Total | 88.5% |
| Country Code | 1,208 |
| % of Total | 5.9% |
| New | 1,158 |
| % of Total | 5.7% |
| Total Domains | 20,484 |

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**<br>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**<br>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**<br>n insecure redirect is indicated when one or more of the hops to a URL destination is unencrypted i.e., HTTP only. | 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**<br>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**<br>There are two gaps to understand.<br>1. The records do not conform to RFCs.<br>2. DMARC and SPF records are missing. | Where SPF or DMARC records don’t conforming to RFCs or where the records are missing, phishing attacks are enabled. |
| **DNSSEC Coverage Gaps**<br>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. |

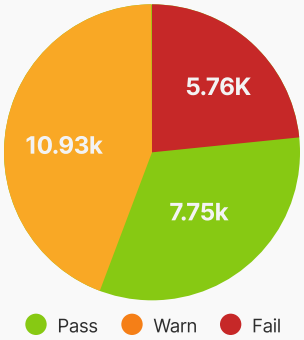
Section Four

# The Benchmark Vulnerability Metrics

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

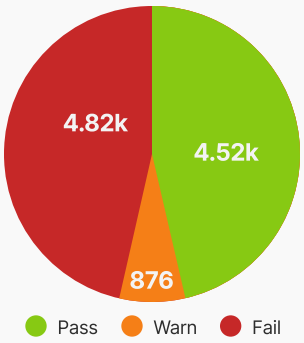
## 23.6% of A Records Fail

The HTTP/HTTPS scan identifies potential security vulnerabilities, including orphaned IPs, insecure connections, and the use of deprecated TLS versions. Other connection responses may be legacy setting in need of deprovisioning, or may be acceptable as internal only. This scan helps infrastructure and infosec teams to investigate each record to classify risks as material or not.



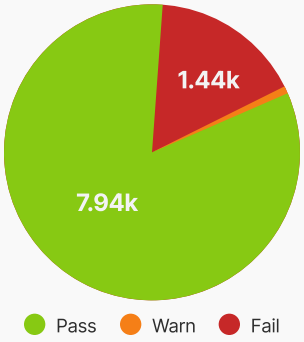

## 47.2% of Redirects Fail

The redirect scan identifies insecure 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 longer controls



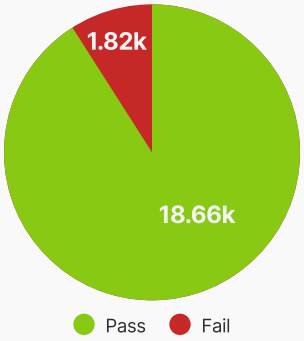

## 15.3% of CNAMES Fail

The CNAME scan identifies all CNAME destinations and Dangling CNAMEs in the domain portfolio. Like Orphaned IPs, Dangling CNAMES are vulnerable to compromise with minimal effort. Over time, IT teams 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 and/or phishing attacks using your own domains.



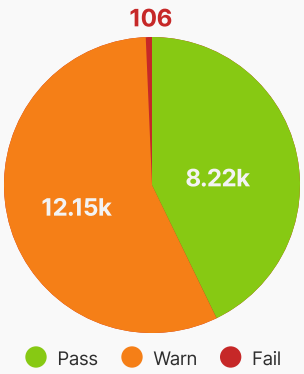
## 8.9% Lame Delegations

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. 9% is a very high number. This is clear evidence that legacy registrars and domain owners are failing to ensure their domains are secure, typically because they lack visibility.



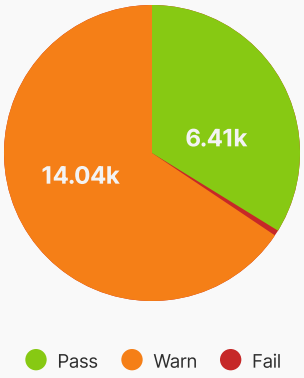

## 59.9% Sending Policy Framework (SPF)

59.4% of domains are not covered with SPF records or are non-compliant with the standards-based RFC. SPF records define the sending mail servers authorized to send mail using that domain. Missing or failed SPF settings expose the domain owner to phishing emails from their own domain. Since phishing is a prevalent threat, companies must ensure every domain owned has a valid SPF record.




## 68.7% Domain-Based Message Authentication, Reporting & Conformance (DMARC)

68.5% of domains are not covered by DMARC or are non-compliant with 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.




## 98.9% Domain Name System Security Extensions

98.9% of domains are not signed. DNSSEC uses cryptographic signatures to sign a domain's zone file. DNSSEC defends against recursive server DNS 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

- Retail is one of the most cyber-attacked sectors in North America.
- Retail is subject to several Information Security Frameworks.
- DNS control and monitoring falls short of compliance requirements if SOC2, CIS, NIST, and ISO. Source
- This Retail DNS Security Audit Benchmark Report provides evidence of the DNS security risks and compliance gaps that retail 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 to reduce costs and ensure 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 retail 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