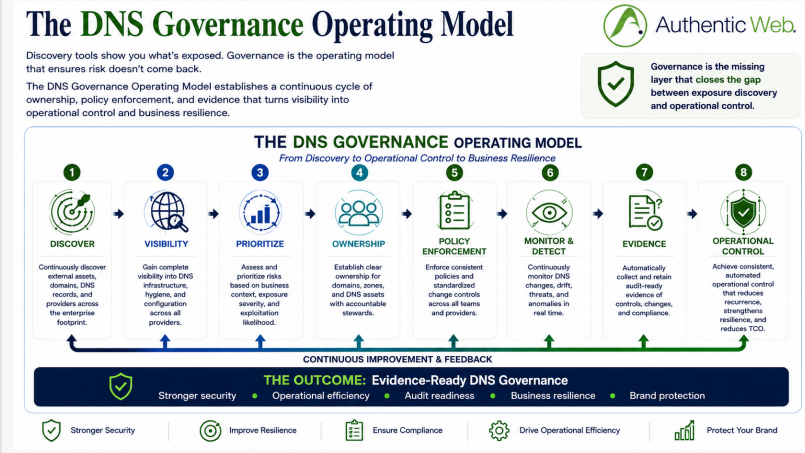
Healthcare DNS Benchmark Report Finds Persistent Gaps in Security and Operational Controls

Research across 25 healthcare organizations finds recurring DNS misconfigurations, ownership and control gaps, as well as DNS security blind spots



The DNS Governance Operating Model

TORONTO, ONTARIO, CANADA, September 24, 2026 / EINPresswire.com/ -- Authentic Web today released its 2026 Healthcare DNS Security and Compliance Benchmark Report, assessing external DNS security in large healthcare organizations.

The study analyzed 9,372 domains and more than 32,545 DNS records to discover dangling CNAMEs, orphaned IPs, insecure redirects, lame delegations, SPF and DMARC coverage, and DNSSEC. The study used publicly available DNS data, providing an external view of governance and exposure without accessing or testing internal systems.

The benchmark key findings:

- 38% of redirects are insecure, allowing interception or redirection of patient and staff traffic.
- 33% of CNAMEs are dangling, resolvable to decommissioned resources and eligible for takeover.
- 62% of A Records are orphaned or insecure, risking takeover, session compromise or MITM compromise.
- 20% of domains have lame delegations, exposing them to DNS hijacking.
- 46% of domains lack SPF and 44% lack DMARC, leaving them spoofable for phishing campaigns.

While some measures have improved since the 2024 study, the 2026 report points to a persistent control gap. Many organizations can identify DNS exposures but lack the ownership, change controls, workflow, policy enforcement, and audit evidence needed to keep them from

returning.

“The research points to a fundamental problem: organizations can often discover DNS risk without actually controlling DNS,” said Peter LaMantia, CEO of Authentic Web. “A vulnerability can be identified and remediated today, then recreated tomorrow because ownership, change control, visibility, and operational accountability are fragmented. The evolution of DNS management and security is therefore not simply better discovery. It is full governance.”

From DNS Discovery to Operational Control

DNS security cannot be treated as a periodic cycle of scanning and manual remediation. Authentic Web is introducing “The DNS Governance Operating Model”, a continuous operating cycle designed to move organizations from discovery to operational control.

The objective is to move from repeated finding and fixing to a durable control model: what exists, who owns it, which policies apply, whether controls are enforced, and what evidence is available for security, compliance, and audit teams.

DNS now spans infrastructure, security, cloud, DevOps, marketing, and business operations. Without clear ownership, change control, and policy enforcement, vulnerabilities can recur even with sophisticated discovery or external attack surface management tools.

A Growing Enterprise Governance Challenge

Healthcare organizations continue to face DNS exposures that can contribute to ransomware risk, DNS hijacking, phishing, service disruption, and loss of trust in critical digital services. For hospitals and health systems, DNS underpins patient portals, telehealth, email, clinical systems, vendor integrations, and public-facing services. As regulators and auditors increasingly expect evidence of control from HIPAA Security Rule risk analysis to NIST CSF 2.0's Govern function, point-in-time DNS scans and cleanup routines are insufficient.

The report highlights a broader enterprise issue: DNS security is a governance and operational control problem. Organizations require accountability across domains, DNS infrastructure, providers, teams, and change workflows, with evidence that controls are working.

The full report is available for download from Authentic Web.

Enterprise security, infrastructure, and domain management leaders can request a complimentary Domain & DNS Control Assessment from Authentic Web.

About Authentic Web Inc.
Authentic Web helps enterprise teams consolidate, control, and govern domains, DNS, and TLS certificates. Its DNAM platform, including the DNS Inspector service module, unifies discovery,

remediation, governance, and compliance evidence into a single system of operational control.

Paul Engels
Authentic Web Inc.
+1 416-583-3771
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/943985024

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.