PORT1

CHECKRED For MSPs

DNS security and posture management for MSPs

A white paper for MSPs on DNS security and posture: what NIST's 2026 DNS guidance changed, the risks to review, and how to build DNS into your services.

November 2026 | Jason Makevich, CISSP

PORT1 brings enterprise-grade security and AI solutions to MSPs and MSSPs and sells only through them.

port1.ai/learn/downloads/dns-security-posture-management/

MSPs should run DNS as a recurring security and posture service: know every client domain and DNS provider, review access and risky records, govern resolvers and encrypted DNS, check certificates and email authentication alongside DNS, and report progress at every QBR. This paper explains why, what NIST changed in 2026, and how CheckRed for MSPs brings DNS posture into the same model as SaaS, cloud, identity, certificates, and compliance.

In this paper, "MSP" includes MSSPs, and the DNS posture issues covered here apply to both.

This white paper is for education and planning. For legal, regulatory, or contractual questions, work with qualified counsel and the right compliance advisors.

Why does DNS need more MSP attention now?

DNS needs more MSP attention because it affects email trust, website and app access, certificates, and uptime for every client, and three changes raise the stakes: NIST's new DNS deployment guide, shorter certificate lifetimes, and stricter email authentication enforcement.

Across a client base, DNS records span registrars, cloud platforms, web hosts, DNS providers, SaaS vendors, and outside agencies. Changes come from different people for different reasons: launching a website, verifying a SaaS tool, setting up email security, connecting a cloud service, or giving a vendor access. Over time, those records can outlive the project, vendor, employee, or system they were made for.

What MSPs see in the field

- A CNAME still points at an abandoned cloud service.
- A marketing vendor added records years ago, and nobody owns them now.
- A delegated subdomain still points at a third-party provider.
- SPF, DKIM and DMARC records no longer match the current email setup.
- Keeping domains and certificates current depends on one person.
- A registrar account still includes former employees or vendors.
- A browser or endpoint skips approved DNS controls by using its own encrypted DNS settings.
- A client has several DNS providers after acquisitions, website rebuilds, or cloud migrations.

These are the normal result of years of change across SMB environments. DNS can keep working long enough for issues to go unnoticed, since a stale record doesn't open a ticket and a weak delegation may not affect users today. Those conditions can still create exposure that affects security, reliability, email trust, and incident response.

Why now

- **NIST's new DNS guidance.** In March 2026, NIST published SP 800-81r3, which replaces its 2013 DNS deployment guide and treats DNS as a layer of security.
- **Shorter certificate lifetimes.** Under the CA/Browser Forum's Baseline Requirements, publicly trusted TLS certificates issued from March 15, 2026, can last at most 200 days, dropping to 100 days from March 15, 2027, and 47 days from March 15, 2029. Renewing more often means more chances for an expired certificate to take a site down.
- **Email authentication enforcement.** Google's email sender guidelines require SPF, DKIM, and DMARC from bulk senders, and its sender guidelines FAQ says Gmail started ramping up enforcement on non-compliant mail in November 2025. Weak DNS records now cause delivery problems as well as spoofing risk.

For MSPs, DNS posture belongs in client onboarding, recurring reviews, QBR reporting, remediation planning, and compliance support.

What changed in NIST's DNS security guidance in 2026?

In March 2026, NIST published SP 800-81r3, the Secure Domain Name System (DNS) Deployment Guide, replacing the 2013 version. It treats DNS as a layer of security within zero trust or defense-in-depth risk management, and it covers protective DNS, encrypted DNS, DNSSEC, DNS logging, and authoritative DNS hygiene.

For MSPs, five parts of the guide stand out.

DNS can act as a policy enforcement point

NIST describes using DNS as a policy enforcement point that blocks harmful traffic in real time. It defines protective DNS as a DNS service enhanced with security capabilities that analyze DNS queries and responses. For SMB environments built on cloud services, SaaS, remote users, and identity-driven access, that adds control before a user reaches a risky destination.

Authoritative DNS hygiene is a security task

NIST notes that threat actors can exploit misconfigurations and lapsed domain or name server registrations. The guide covers lame delegations, dangling CNAME records, and lookalike or typosquat domains, and it uses the term zone drift for secondary name servers that end up with incorrect zone data. These are the kinds of issues MSPs find across long-lived client environments.

Encrypted DNS needs governance

Encrypted DNS protects privacy, but unmanaged encrypted DNS can bypass approved resolvers, logging, and filtering. NIST recommends restricting stub resolvers to authorized encrypted DNS services wherever possible, and blocking unauthorized DNS over TLS (DoT), DNS over HTTPS (DoH), and DNS over QUIC (DoQ) traffic from the internal network.

DNS logging supports investigations

NIST says DNS logging should capture current and historical traffic to support digital forensics and incident response. It also describes sending query and response data, along with blocks and redirects, to security operations through tools like a SIEM or SOAR.

Tunneling needs detection

NIST recommends controls that detect and block unauthorized applications from tunneling data through DNS.

The update gives MSPs a credible outside reason to treat DNS as a recurring posture control, a security data source, and a governance layer across clients.

Why is DNS harder to manage across many clients?

DNS is harder for MSPs because they manage it across many clients at once, each with different registrars, DNS hosts, vendors, and histories, and DNS problems often come from normal client changes that leave records, delegations, access, or certificates behind.

Across a client base, DNS may include:

- Registrars outside the MSP's control
- DNS hosted in cloud platforms and with website providers
- Records created by marketing tools, payment platforms, CRMs, and email vendors
- Delegations to agencies or developers
- Old subdomains tied to retired systems
- More than one email security or email delivery vendor
- Unclear ownership of record changes
- Uneven MFA and access control on DNS provider accounts
- Unclear certificate ownership

A website gets rebuilt. A SaaS tool gets tested. A cloud resource gets retired. A vendor asks for a record during onboarding. A domain moves to a new registrar. Each change is ordinary, and each can leave something behind that needs review. When DNS review falls behind client change, exposure builds across every account, and for an MSP that turns into a scale problem.

DNS posture brings records, ownership, process, evidence, and recurring review into the same managed service model. It moves DNS from reactive cleanup into a repeatable way to review risk, assign remediation, and show clients what changed over time.

The tool problem

Many MSPs already juggle several security dashboards. One client needs Microsoft 365 posture review, another needs cloud posture, another needs SaaS access review, and another has compliance reporting needs. Each added system means more onboarding, access management, alert review, ticket routing, exception tracking, follow-up, reporting, training, and QBR prep.

The number of tools adds up, and so does the time it takes to turn scattered findings into something a client can act on. Engineers may know where to look, while service managers, vCISOs, account teams, and client leaders still need a clear view of what was found, what changed, and what's in progress.

DNS gets harder still when it lives outside the posture model, as a separate checklist, console, or engineering task. Tracked apart from SaaS, cloud, identity, certificates, and compliance, DNS findings are harder to explain as part of a client's overall risk, and progress is harder to show over time.

Start where MSPs already are

Microsoft 365 posture review is the familiar starting point for most MSPs. A client can have strong Microsoft 365 review and still have weak visibility into Google Workspace, cloud accounts, identity systems, certificates, other SaaS apps, and DNS. That creates an uneven service model, where some layers get recurring review and others depend on manual checks, tribal knowledge, or reactive support.

DNS makes that gap easy to see, since every client depends on domains, email records, public websites, and certificates. For the first step, see Microsoft 365 and Google Workspace posture for MSPs.

Which DNS risks should MSP teams understand?

The DNS risks MSP teams should understand are dangling records and subdomain takeover, lame delegations, stale records, lookalike domains, weak email authentication, unmanaged encrypted DNS, DNS tunneling, and certificate exposure tied to DNS.

Dangling DNS and subdomain takeover

A dangling record points at a resource that no longer exists or that the client no longer controls. If someone else claims that resource, they can serve their own content on the client's subdomain, which can support phishing, brand damage, and misuse of a trusted domain. How exploitable it is

depends on the provider and resource.

Lame delegations and weak ownership

NIST explains that an incorrect zone delegation, called a lame delegation, can make a child zone unreachable. Delegated subdomains are common in managed environments because agencies, SaaS vendors, developers, and outside providers ask for them. Review delegated zones, parent-zone and child-zone data, and who owns anything connected to a third party.

Stale records

Old CNAME, TXT, MX, verification, and vendor records often stay long after a service is retired, and they can create exposure or confusion. Check that DNS records match current services, current vendors, and current security requirements.

Lookalike domains and brand abuse

NIST notes that threat actors extensively use lookalike or typosquat domains to impersonate organizations. For clients, that means executive impersonation, customer phishing, and payment fraud, and a lapsed domain can let someone else receive the client's email.

Weak email authentication

SPF, DKIM, and DMARC are DNS-based controls for email trust, spoofing resistance, and deliverability. When they're missing, stale, or misaligned, clients face more phishing exposure and delivery problems. It's one of the easiest DNS posture entry points, because SMB leaders already understand business email risk.

Unmanaged encrypted DNS

If browsers, endpoints, or mobile devices use public encrypted DNS resolvers outside the approved path, the MSP can lose filtering, logging, and response visibility.

DNS tunneling and data exfiltration

DNS can be abused to tunnel data or command-and-control traffic. Make DNS telemetry available where it supports detection and investigation.

Certificate exposure

DNS and certificates are tied together through public trust, so a hijacked subdomain can serve malicious content that looks legitimate. Review certificates alongside DNS, especially for public domains, customer portals, login pages, and business-critical services.

Two more changes make certificate review a recurring job. With shorter certificate lifetimes, an untracked certificate is more likely to lapse. For post-quantum planning, NIST's IR 8547 says NIST will deprecate quantum-vulnerable public-key algorithms after 2030 and disallow them under its standards and guidelines after 2035.

What should MSPs do about DNS posture now?

MSPs should start with visibility and a repeatable review: inventory each client's DNS, review access and risky records, set resolver and encrypted DNS policy, check email authentication and certificates with DNS, set logging expectations, and build remediation and exceptions into onboarding and QBRs.

A 10-step DNS posture checklist

1. **Inventory the namespace.** Document client domains, subdomains, registrars, DNS hosts, delegated zones, public-facing services, and certificate dependencies. Ask which services, vendors, or websites the client has stopped using in the last few years, since leftover records often point at them.
2. **Review access and ownership.** Confirm who can access registrars, DNS providers, cloud DNS services, and vendor-managed zones. Remove stale users, require MFA where it's available, turn on registrar locks, and document who approves DNS changes.
3. **Check for stale or risky records.** Look for dangling CNAMEs, weak delegations, stale TXT records, secrets left in TXT records, abandoned subdomains, old vendor references, and records tied to retired services. Check CAA records, which name the certificate authorities allowed to issue for a domain.
4. **Review email authentication.** Confirm SPF, DKIM, DMARC, MX, and related records match the current email environment, including on domains that send no mail.
5. **Review DNS and certificates together.** Find expiring, misconfigured, unexpected, or weak certificates, and tie that work to DNS ownership and the public namespace.
6. **Define approved resolver policy.** Decide which recursive DNS services are approved and how endpoints, browsers, mobile devices, and remote users should use them.
7. **Govern encrypted DNS.** Support encrypted DNS where it fits, while keeping approved resolvers, logging, and policy enforcement in place.
8. **Set DNS logging expectations.** Decide which logs to keep, where they flow, how long they're kept, and how they support investigation, client reporting, and compliance evidence.
9. **Create a remediation and exception workflow.** Decide who reviews findings, who approves changes, how urgent issues get escalated, and how completed fixes are documented. Track risks the client accepts as exceptions, with an owner, business context, and a review date, so they stay visible instead of sitting in old tickets.

10. **Add DNS to recurring service delivery.** Build DNS review into onboarding, scheduled reviews, QBRs, compliance reviews, and client reporting.

What should MSP engineers review in a DNS deep dive?

MSP engineers should review resolver and protective DNS policy, authoritative DNS hygiene, encrypted DNS behavior on endpoints and browsers, DNSSEC signing and validation, certificates tied to DNS, and how DNS logs reach the team's response workflows.

Protective DNS and resolver control

- Approved recursive resolvers
- Remote and roaming user policy
- Endpoint and browser DNS behavior
- Unauthorized outbound DNS paths
- Failover and availability requirements
- Logging and retention
- Integration with ticketing, SIEM, XDR, or other response workflows

Protective DNS handles name resolution policy and threat blocking. Authoritative DNS, registrar access, stale records, delegations, and certificates still need their own review.

Authoritative DNS hygiene

- NS delegations and SOA values
- CNAME chains
- Stale TXT and MX records
- SPF, DKIM, and DMARC
- CAA records
- Registrar locks and MFA on registrar accounts
- Vendor access
- Dormant subdomains and references to retired services

Encrypted DNS governance

Check whether browsers, endpoints, mobile devices, and apps can override approved DNS policy. Where you can, use endpoint policy, browser configuration, mobile device management (MDM), and network controls to keep approved resolvers in place and block unauthorized encrypted DNS.

DNSSEC and integrity

NIST recommends deploying DNSSEC to protect the integrity of DNS data. DNSSEC helps validate the integrity and authenticity of DNS data, while encrypted DNS protects the connection between systems. Know:

- Which zones are signed
- Who coordinates DS records
- How key rollover is handled
- What happens when validation fails
- Which clients are good candidates for DNSSEC
- Who owns troubleshooting when DNSSEC affects availability

DNS and certificate posture

- Expiring certificates
- Certificates on old or unknown subdomains
- Weak keys or deprecated algorithms
- Unexpected certificate issuance
- Certificate ownership, and who renews each certificate
- Public-facing services tied to DNS records

CheckRed's Certificate Posture Management (Certificate PM) looks for certificates across domains and subdomains, and flags expired or misconfigured certificates, weak keys, deprecated algorithms, and rogue issuance.

Logging and investigations

DNS data helps identify malicious destinations, policy violations, tunneling, and affected endpoints. Connect DNS data to the workflows the team already uses, like ticketing, SIEM, XDR, SOAR, GRC, compliance reporting, and QBR prep.

How does DNS posture support compliance and recurring services?

DNS posture supports compliance and recurring services by making DNS exposure visible, reviewable, and reportable: findings mapped to each client's frameworks, fixes and open exceptions tracked over time, and progress shown at every QBR.

The strongest client value comes from showing:

- Where DNS exposure exists

- Which records are stale or risky, and which delegations need review
- Which certificates need attention
- Which findings connect to compliance requirements
- Which fixes were completed, and which exceptions remain open
- What has improved since the last review

That's especially useful for clients in regulated or audit-sensitive industries, like healthcare, financial services, legal services, and government contracting, and for SMBs with customer, insurance, or contractual requirements. CheckRed maps DNS findings to compliance frameworks as part of continuous compliance, alongside its SaaS and cloud findings. More on that is in continuous compliance for MSPs.

DNS posture can support:

- Client onboarding reviews
- Domain, delegation, and registrar access reviews
- Email authentication and certificate reviews
- DNS drift monitoring
- Exception tracking and compliance evidence
- QBR reporting and remediation guidance
- vCISO and advisory services

Security teams can do the technical work. Business owners need the evidence, the priorities, and the progress reports.

Where does CheckRed for MSPs fit?

CheckRed for MSPs brings DNS posture into the same multi-tenant platform MSPs use for SaaS, cloud, identity, certificates, and compliance, so DNS findings get prioritized, guided to a fix, mapped to frameworks, and reported the same way as everything else.

CheckRed's DNS posture management (DNSPM) gives one view of a client's DNS across providers: Amazon Route 53, Azure DNS, Google Cloud DNS, Cloudflare, GoDaddy, Akamai Edge DNS, Infoblox, legacy on-premises DNS, and more. CheckRed's DNSPM page lists:

- Automated discovery of zones, records, and subdomains
- Misconfiguration detection, including takeover risks
- Drift monitoring that shows who changed what, and where
- Fake domain monitoring for typosquatting and lookalike domains
- Continuous compliance mapping for DNS findings

- Certificate PM, for expired, misconfigured, or rogue certificates, weak keys, and deprecated algorithms
- Post-Quantum Cryptography (PQC) Monitoring, for certificates that rely on quantum-vulnerable algorithms
- Prioritized alerts and guided remediation

Email Posture Management (Email PM) checks SPF, DKIM, DMARC, and BIMI across a client's domains, and it's part of the same family.

DNSPM checks DNS records and domains, and it works alongside the protective DNS, resolver, and filtering tools that decide which lookups users can make. Those controls stay with the tools you already run, and so do encrypted DNS policy, DNSSEC operations, and DNS query logging. Ask PORT1 before tying any of them to CheckRed.

That helps MSPs answer the questions clients expect them to own:

- Which domains and DNS providers are in use?
- Which records are stale or risky?
- Which subdomains could be abused?
- Which DNS issues affect email trust or certificates?
- Which issues affect audit readiness?
- Which findings need fixing first, and which remain open?

PORT1 brings enterprise-grade security and AI solutions to MSPs and MSSPs and sells only through them. Partners get PORTER, PORT1's partner platform.

For the full DNS review, see what MSPs should check in client DNS, certificates and email authentication, and for the apps, clouds, providers, and frameworks CheckRed names, see what CheckRed checks.

Bring DNS into your posture service. Book a CheckRed demo or Talk to PORT1.

Sources

- NIST SP 800-81r3: Secure Domain Name System (DNS) Deployment Guide, March 2026. Accessed November 8, 2026.
- CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.3.1, October 4, 2026. Accessed November 8, 2026.
- NIST IR 8547: Transition to Post-Quantum Cryptography Standards, October 2026. Accessed November 8, 2026.
- Google, Email sender guidelines. Accessed November 8, 2026.
- Google, Email sender guidelines FAQ. Accessed November 8, 2026.
- RFC 8659: DNS Certification Authority Authorization (CAA) Resource Record, November 2019. Accessed November 8, 2026.