PORT1

CHECKRED For MSPs

DNS, certificates and email authentication: what MSPs should check

What MSPs should check in client DNS, TLS certificates and email authentication: dangling records, shorter certificate lifetimes, SPF, DKIM and DMARC.

November 2026 | Jason Makevich, CISSP

MSPs should check three things across every client domain, including old and parked ones: DNS records that point at retired services or expose secrets, TLS certificates that are expiring, weak, or untracked, and email authentication records (SPF, DKIM, and DMARC). These records are often spread across registrars, cloud accounts, and hosting providers with nobody owning them end to end, and problems can lead to takeovers, spoofing, and outages.

Checking DNS records, zones, and domains for misconfigurations and takeover risks on an ongoing basis is called DNS posture management (DNSPM).

What should MSPs check in client DNS?

In client DNS, MSPs should inventory every domain and DNS host, clear out records that point at retired services, keep secrets out of TXT records, watch for lookalike domains, and track who changed what.

- **Inventory every domain.** Include old, campaign, and brand domains, where each one is registered and hosted, and who can change its records.
- **Clear out dangling records.** When a client retires a hosted app or marketing site and a DNS record still points at it, that leftover record is a subdomain takeover risk. How exploitable it is depends on the provider and resource, so present it as a risk to fix.
- **Keep secrets out of TXT records.** Anyone can read a TXT record, so API keys or credentials left there are exposed.
- **Watch for lookalike domains.** Attackers use typosquatted and lookalike domains that imitate a client's brand for phishing and wire fraud, and a lapsed domain can let someone else receive the client's email.
- **Track who changed what.** DNS changes through everyday admin work, so configuration drift needs watching between reviews.

What should MSPs check in TLS certificates?

MSPs should find every TLS certificate a client relies on, including ones nobody tracked, and check expiry dates, key strength, algorithms, and which certificate authority issued each one. Shorter certificate lifetimes make that more pressing.

Under the CA/Browser Forum's Baseline Requirements, a public TLS certificate issued on or after March 15, 2026 can be valid for at most 200 days. The maximum drops to 100 days for certificates issued from March 15, 2027, and to 47 days from March 15, 2029, under a schedule the Forum approved in Ballot SC081v3 in April 2025. Renewing more often means more chances for an expired certificate to take a site down.

Also check each domain's Certification Authority Authorization (CAA) record, which names the certificate authorities allowed to issue certificates for it (RFC 8659). Publicly trusted authorities must check it before issuing under the Baseline Requirements.

When should MSPs start on post-quantum readiness?

MSPs can start on post-quantum readiness now, with an inventory of which certificates rely on quantum-vulnerable algorithms like RSA and elliptic curve cryptography (ECC), since migration takes years. NIST published its first three post-quantum standards, FIPS 203, 204, and 205, in August 2024 and encouraged administrators to begin transitioning as soon as possible. Its final transition report, NIST IR 8547 (October 2026), says NIST will deprecate quantum-vulnerable public-key algorithms after 2030 and disallow them under its standards and guidelines after 2035.

Which email authentication records should every client domain have?

Every client domain that sends mail should have SPF, DKIM, and DMARC, and domains that send no mail, like old or parked ones, should still publish SPF and DMARC records that mark any mail using them as unauthorized.

- **SPF** (Sender Policy Framework) lets a domain authorize the hosts allowed to send mail using its name, and receivers check that authorization (RFC 7208). SPF allows at most 10 DNS-querying terms per check and returns an error past that, so records that pull in many services need pruning.
- **DKIM** (DomainKeys Identified Mail) lets a domain sign messages so receivers can verify them with a public key in the signer's DNS (RFC 6376).
- **DMARC** (Domain-Based Message Authentication, Reporting, and Conformance) passes only when SPF or DKIM passes for a domain aligned with the visible From domain. It lets the owner request reports and set a policy of none, quarantine, or reject, which receivers can honor but don't have to (RFC 9989, which replaced RFC 7489 in May 2026).

For non-sending domains, RFC 7208 calls an SPF record that authorizes no hosts well-established practice. We also recommend a DMARC policy of reject there, which RFC 9989 defines as the owner considering every failure a clear sign that use of the domain isn't valid.

As of November 2026, Google's email sender guidelines require bulk senders to set up SPF, DKIM, and DMARC (a policy of none is enough), with the From domain aligned to SPF or DKIM. Its sender guidelines FAQ counts anyone sending close to 5,000 or more messages a day to personal Gmail accounts as a bulk sender, permanently, and says enforcement ramped up in November 2025. Yahoo announced in December 2023 that bulk senders must authenticate with SPF and DKIM and publish a DMARC policy, enforced from February 2024. Weak setups now cause delivery problems as well as spoofing risk.

Should MSPs check DDoS protection too?

MSPs should check distributed denial-of-service (DDoS) protection for clients that already have it, to confirm it will actually engage, with traffic routed through the provider and every internet-facing asset covered. CheckRed's DDoS posture management (DDoSPM) runs outside-in readiness checks on IP prefixes and routing across providers like Akamai Prolexic, AWS Shield, Azure DDoS Protection, and Cloudflare, rating each check pass, warning, or fail. For small clients without a DDoS provider, start with DNS, certificates, and email.

How does CheckRed help MSPs check DNS, certificates and email?

CheckRed's DNSPM gives an MSP one view of each client's DNS across providers, with certificate, post-quantum, and email modules in the same family.

- **DNSPM:** discovers zones, records, and subdomains across providers including Amazon Route 53, Azure DNS, Google Cloud DNS, Cloudflare, and GoDaddy, tracks who changed what, and watches for lookalike domains. Its checks cover sensitive data in TXT records, dangling DNS, name collisions, reflection and amplification exposure, tunneling, fast flux, and subdomain takeover.
- **Certificate Posture Management (Certificate PM):** finds certificates no one tracked across domains, subdomains, clouds, and certificate authorities, and flags expiring, rogue, or misconfigured certificates, weak keys, deprecated algorithms, and certificates from unsanctioned authorities.
- **Post-Quantum Cryptography (PQC) Monitoring:** shows which certificates rely on quantum-vulnerable algorithms and which to upgrade first. Its scope is certificates, so cryptography inside applications and devices needs its own inventory.
- **Email Posture Management (Email PM):** checks SPF, DKIM, DMARC, and Brand Indicators for Message Identification (BIMI) records across a client's domains, and flags missing or misconfigured records, weak or unenforced DMARC, unauthorized senders, and drift.

CheckRed's DNSPM page lists guided remediation, plus exception management workflows that use compensating controls. DNS often sits with a registrar, host, or app provider, so the MSP coordinates each fix with its owner.

See what CheckRed checks and what MSPs should check in SaaS apps beyond Microsoft 365. CheckRed also maps DNS findings to frameworks for compliance readiness work with clients.

For NIST's 2026 DNS guidance, see the white paper.

Download: DNS security and posture management for MSPs ›

PORT1 brings enterprise-grade security and AI solutions to MSPs and MSSPs and sells only through them. Book a CheckRed demo to see CheckRed for MSPs in action, or Talk to PORT1.

Sources

- 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.
- CA/Browser Forum: Ballot SC081v3, Introduce Schedule of Reducing Validity and Data Reuse Periods, April 2025. Accessed November 8, 2026.
- RFC 8659: DNS Certification Authority Authorization (CAA) Resource Record, IETF, November 2019. Accessed November 8, 2026.
- NIST: NIST Releases First 3 Finalized Post-Quantum Encryption Standards, August 13, 2024. Accessed November 8, 2026.
- NIST IR 8547: Transition to Post-Quantum Cryptography Standards, final, October 2026. Accessed November 8, 2026.
- RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, IETF, April 2014. Accessed November 8, 2026.
- RFC 6376: DomainKeys Identified Mail (DKIM) Signatures, IETF, September 2011. Accessed November 8, 2026.
- RFC 9989: Domain-Based Message Authentication, Reporting, and Conformance (DMARC), IETF, May 2026. Accessed November 8, 2026.
- Google: Email sender guidelines, Gmail Help. Accessed November 8, 2026.
- Google: Email sender guidelines FAQ, Gmail Help. Accessed November 8, 2026.
- Yahoo: An Update on Enforcing Email Standards, Postmaster @ Yahoo, December 20, 2023. Accessed November 14, 2026.