DNS Security and Posture Management

Why DNS security posture has become a critical responsibility for MSPs and MSSPs protecting client environments.

May 2026 | v1.3

Jason Makevich, CISSP

Executive summary

DNS has moved from background infrastructure into a security, availability, and governance control MSPs need to manage with more intent.

For SMB clients, DNS affects email trust, website access, cloud applications, customer portals, APIs, certificates, brand protection, and service availability. A weak DNS record, abandoned subdomain, expired certificate, or unmanaged delegation can become a security incident, an outage, a phishing path, or a client trust problem.

That risk often falls back on the service provider. When something breaks or gets abused, clients expect their MSP to help explain what happened, what was exposed, what needs to change, and how similar risk will be reduced across the environment.

NIST's March 2026 update to SP 800-81 gives MSPs a stronger reason to act now. The updated guidance places DNS inside zero trust and defense-in-depth security risk management. It also covers protective DNS, DNSSEC, encrypted DNS, authoritative DNS hygiene, DNS logging, resolver control, and resilient deployment. For MSPs serving SMBs, that raises the bar for how DNS should be reviewed, governed, and reported. [1]

In this paper, "MSP" includes both MSPs and MSSPs. MSSPs provide managed security services, and the DNS posture issues covered here apply to both. The goal is to keep the paper clear and simple while addressing the providers responsible for helping clients secure and govern their environments.

If you support multiple clients, you support many domains, registrars, DNS providers, cloud services, SaaS apps, outside vendors, web agencies, and inherited technical decisions. Those environments were rarely built by one team using one standard. DNS posture gives providers a way to bring more order, visibility, and evidence to that client estate.

This paper explains what MSPs should know, what teams should review, and how DNS posture can fit into recurring service delivery. It also explains how CheckRed for MSPs helps bring DNS into a unified posture model across SaaS, cloud, identity, certificates, and compliance, without creating a separate DNS-only workflow for the MSP stack.

Why DNS needs MSP attention now

DNS is one of the paths users, apps, and attackers all rely on.

It routes users to websites, cloud apps, login pages, SaaS platforms, APIs, and customer-facing services. It supports email trust through SPF, DKIM, and DMARC. It connects to certificates, public brand trust, uptime, and incident response. DNS is also one of the areas where small configuration issues can create outsized risk.

For MSPs, the challenge is scale. Across a client base, DNS records can span multiple registrars, cloud platforms, web hosts, DNS providers, SaaS vendors, and outside agencies. Without a repeatable review process, DNS exposure can build up through normal business changes.

The other challenge is ownership. DNS changes are often made by different people for different reasons: launching a website, verifying a SaaS tool, configuring email security, connecting a cloud service, or giving a vendor access. Over time, those changes can outlast the project, vendor, employee, or system they were created for.

Examples MSPs see in the field

- A CNAME still points to an abandoned cloud service.
- A marketing vendor added records years ago and nobody owns them now.
- A delegated subdomain still points to a third-party provider.
- SPF, DKIM, or DMARC records no longer match the current email environment.
- A domain or certificate renewal process depends on one person.
- A registrar account still includes former employees or vendors.
  A browser or endpoint bypasses approved DNS controls through encrypted DNS settings.
- A client has multiple DNS providers after acquisitions, website rebuilds, or cloud migrations.

These are the normal result of years of change across SMB environments.

The risk is that DNS can keep working long enough for issues to go unnoticed. A stale record may not create a ticket. A weak delegation may not affect users today. An old vendor entry may not break anything. But those conditions can still create exposure that affects security, reliability, email trust, and incident response.

If a domain is hijacked, email authentication fails, a stale subdomain is abused, or a certificate issue affects a client-facing service, the MSP is likely going to help explain and fix it. DNS posture gives the provider a better way to find these issues before they become urgent.

For MSPs, DNS posture should be part of client onboarding, recurring review, QBR reporting, remediation planning, and compliance support. It helps show that security controls are being maintained across the real environment, including systems beyond those with dedicated tools.

What NIST changed in 2026

NIST SP 800-81r3, *Secure Domain Name System (DNS) Deployment Guide*, was published in March 2026 and supersedes the 2013 version of the guide. [1]

The update reflects a different security reality. DNS is now treated as part of modern security architecture, extending far beyond basic name resolution. NIST addresses how DNS supports zero trust, defense-in-depth, protective DNS, encrypted DNS, DNSSEC, dedicated DNS services, logging, authoritative DNS protections, and resilient deployment.

For MSPs, several parts are especially useful.

DNS can support zero trust and defense-in-depth

NIST describes DNS as part of zero trust and defense-in-depth security risk management. That's important for MSPs because many SMB environments are built around cloud services, SaaS, remote users, and identity-driven access. DNS can help support visibility and control before a user reaches a risky destination.

DNS can act as a policy enforcement point

DNS can help enforce policy before a connection is completed. Protective DNS can block or redirect traffic to malicious or unauthorized destinations, generate useful telemetry, and support incident response.

Authoritative DNS hygiene is now a security task

The updated guidance covers authoritative DNS risks such as dangling CNAMEs, lame delegations, look-alike domains, and zone drift. These are exactly the kinds of issues MSPs encounter across long-lived SMB environments.

Encrypted DNS needs governance

Encrypted DNS can improve privacy and protect DNS traffic, but it can also bypass approved resolvers, logging, filtering, and response workflows if it is unmanaged. MSPs need a plan for browsers, endpoints, mobile devices, and remote users.

DNS logging supports investigations

DNS query and response data can help security teams understand connections, identify malicious destinations, support digital forensics, and improve response workflows. NIST recommends integrating protective DNS with the wider security ecosystem.

The 2026 NIST update gives MSPs a credible external driver for taking DNS posture more seriously. DNS should be treated as a recurring posture control, security data source, and governance layer across client environments.

Why DNS is harder across managed client environments

A single business can struggle to maintain clean DNS. An MSP has to manage this across many clients, each with different vendors, platforms, histories, and levels of documentation.

Across a client base, DNS may include:

- Registrars outside MSP control
- DNS hosted in cloud platforms
- DNS hosted 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
- Multiple email security or email delivery vendors
- Unclear ownership of record changes
- Inconsistent MFA and access control for DNS providers
- Unclear certificate ownership and renewal processes

That variety creates delivery risk for the MSP. DNS issues can become tickets, incidents, outages, insurance questions, audit questions, and board-level escalations.

The hard part is that DNS problems often come from normal client activity. 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. None of those changes are unusual, but each one can leave behind records, delegations, access, or certificates that need review.

Microsoft's guidance on dangling DNS records is a useful example. Microsoft explains that dangling records can allow subdomain takeover when a DNS record points to a deprovisioned cloud resource. A hostile actor can redirect traffic meant for the organization's domain to attacker-controlled content, support phishing, harvest cookies, and potentially obtain a valid SSL certificate for the hijacked subdomain. [2]

This is highly relevant for MSPs because clients create and retire cloud resources all the time. When DNS review falls behind client change, exposure builds across the account. Across multiple clients, that becomes a scale problem, not just a technical issue.

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

The MSP operating challenge

Most MSPs already have too many security dashboards.

One client may require Microsoft 365 posture review. Another needs cloud posture. Another needs SaaS access review. Another has compliance reporting needs. DNS may sit in a registrar, cloud console, web host, CDN, email tool, or outside vendor portal.

Each additional system adds work:

- Onboarding
- Access management
- Alert review
- Ticket routing
- Exception tracking
- Remediation follow-up
- Reporting
- Staff training
- QBR preparation
- Client explanation

The issue is not only the number of tools. It is the amount of time required to turn scattered findings into something useful. Engineers may know where to look, but service managers, vCISOs, account teams, and client leadership still need a clear view of what was found, what changed, what needs attention, and what work is already in progress.

DNS becomes much harder to manage when it lives outside the posture model. It can become a separate checklist, separate console, or separate engineering task. That makes it harder to deliver consistently across clients, especially when each client has different DNS providers, cloud platforms, vendors, and documentation quality.

This also affects reporting. If DNS findings are tracked separately from SaaS, cloud, identity, certificates, and compliance, it becomes harder to explain overall risk in a way clients can understand. It also becomes harder to show progress over time.

The better path is to include DNS in the same posture model MSPs use for SaaS, cloud, identity, certificates, and compliance. Teams need one way to find exposure, prioritize remediation, assign work, map findings to frameworks, and report progress.

The Microsoft 365 posture gap

Microsoft 365 posture tools helped many MSPs recognize the value of configuration review, drift detection, risky sharing review, OAuth exposure, MFA review, and recurring client reporting.

That awareness creates a good entry point for broader posture work.

A client may have strong Microsoft 365 posture review and still have weak visibility across Google Workspace, AWS, Azure, Google Cloud, DNS, identity systems, certificates, and other SaaS apps. For MSPs, this creates an uneven service model. Some layers receive recurring review, while others depend on manual checks, tribal knowledge, or reactive support.

DNS makes that gap easy to identify because every client uses DNS in some way. Even clients with simple environments still depend on domains, email records, public websites, certificates, and external services.

MSPs need a posture model that starts where the market already has awareness, then extends into the rest of the client environment.

DNS risks MSP teams should understand

Dangling DNS and subdomain takeover

Dangling DNS occurs when a record points to a resource that no longer exists or is no longer controlled by the client. Microsoft explains how dangling DNS records can create subdomain takeover risk. [2]

The business impact can include phishing, hostile content, brand damage, cookie harvesting, and misuse of trusted domains.

Lame delegations and weak ownership

A lame delegation occurs when delegation information points to name servers that do not properly serve the zone. Delegated subdomains are common in managed environments because agencies, SaaS vendors, developers, and outside providers often request them.

MSPs should review delegated zones, parent-zone data, child-zone data, and ownership for anything connected to third parties.

Zone drift and stale records

DNS records often remain long after a service is retired. Old CNAMEs, TXT records, MX records, verification records, and vendor records can create exposure or confusion.

MSPs should review whether DNS records reflect current services, current vendors, and current security requirements.

Look-alike domains and brand abuse

Attackers use look-alike or typo-based domains to impersonate trusted brands, support phishing campaigns, and increase user trust in malicious links.

For MSPs, this affects executive impersonation, customer phishing, payment fraud, and brand trust. It can also support advisory services for clients with strong public brands or regulated customer bases.

Weak email authentication

SPF, DKIM, and DMARC are DNS-based controls that affect email trust, spoofing resistance, and deliverability. When these records are missing, stale, or misaligned, clients may face higher phishing exposure and email reliability issues.

This is one of the most accessible DNS posture entry points because SMB leaders already understand business email risk.

Unmanaged encrypted DNS

Encrypted DNS can protect privacy, but it needs policy. If browsers, endpoints, or mobile devices use public encrypted DNS resolvers outside the approved path, the MSP may lose filtering, logging, and response visibility.

NIST recommends restricting unauthorized DNS use with public resolvers where feasible, including unauthorized DoT, DoH, and DoQ traffic. [1]

DNS tunneling and data exfiltration

DNS can be abused to tunnel data or command-and-control traffic. NIST recommends controls to detect and block unauthorized applications tunneling data within DNS packets.

MSPs can keep this focused by making DNS telemetry available where it supports detection and investigation.

Certificate exposure

DNS and certificates are connected through public trust. A hijacked subdomain can support malicious content that appears legitimate to users. Microsoft notes that hostile actors may use a hijacked subdomain to obtain a valid SSL certificate. [2]

Certificate posture should be reviewed with DNS posture, especially for public domains, customer portals, login pages, and business-critical services.

What MSPs should be doing now

DNS posture can begin with visibility and repeatable review.

Inventory client DNS assets

Document client domains, subdomains, registrars, DNS hosts, delegated zones, public-facing services, DNS ownership, and certificate dependencies.

Review access and ownership

Confirm who can access registrars, DNS providers, cloud DNS services, and vendor-managed zones. Remove stale users, require MFA, and document who approves DNS changes.

Check high-risk DNS records

Review dangling CNAMEs, weak delegations, stale TXT records, abandoned subdomains, old vendor references, SPF, DKIM, DMARC, CAA, MX records, and records tied to retired services.

Define resolver policy

Decide which recursive DNS services are approved and how endpoints, browsers, mobile devices, and remote users should use them.

Govern encrypted DNS

Support encrypted DNS where appropriate while preserving approved resolver use, logging, filtering, and response workflows.

Connect DNS and certificate review

Review expiring, misconfigured, weak, or unexpected certificates alongside public DNS records and subdomain ownership.

Set logging expectations

Define which DNS logs should be retained, where they should flow, how long they should be kept, and how they support investigation, client reporting, and compliance evidence.

Create a remediation workflow

Decide how DNS findings become assigned work. Define who reviews findings, who approves changes, how urgent issues are escalated, and how completed remediation is documented. DNS posture only becomes useful when the team has a clear path from finding to fix.

Track exceptions and business decisions

Some DNS risks may not be fixed immediately because of vendor dependencies, legacy systems, client decisions, or timing constraints. Track those exceptions with ownership, business context, and review dates so they do not disappear into tribal knowledge or old tickets.

Add DNS to recurring service delivery

Include DNS in onboarding, scheduled reviews, QBRs, compliance reviews, remediation tracking, and client reporting.

Technical Deep Dive for MSP Teams

Protective DNS and resolver control

Protective DNS can block or redirect traffic to malicious or unauthorized destinations and provide useful telemetry for detection and response. NIST describes protective DNS as DNS service enhanced with security capabilities that analyze DNS queries and responses and take action to reduce threat exposure. [1]

MSP teams should review:

- 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 helps with name resolution policy and threat blocking. Additional review is still needed for authoritative DNS, registrar access, stale records, delegations, and certificate posture.

Authoritative DNS hygiene

Authoritative DNS review should include:

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

NIST defines DNS hygiene as managing and monitoring DNS configurations to remove vulnerabilities such as lame delegations and dangling CNAME records, remove records no longer in use, and monitor for look-alike domains. [1]

Encrypted DNS governance

DoT, DoH, and DoQ can improve privacy and protect DNS traffic. They also affect visibility and enforcement if unmanaged.

MSP teams should review whether browsers, endpoints, mobile devices, and applications can override approved DNS policy. Where feasible, use endpoint policy, browser configuration, MDM, and network controls to preserve approved resolvers and restrict unauthorized encrypted DNS.

DNSSEC and integrity controls

DNSSEC helps validate the integrity and authenticity of DNS data. Encrypted DNS protects the channel between systems, while DNSSEC protects DNS data integrity.

MSP teams should understand:

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

Logging and investigations

DNS data can support detection, investigation, and response. It can help identify malicious destinations, policy violations, tunneling behavior, and affected endpoints.

MSPs should connect DNS findings to the workflows teams already use. That may include ticketing, SIEM, XDR, SOAR, PSA, GRC, compliance reporting, and QBR preparation.

DNS and certificate posture

DNS records and certificates should be reviewed together because both affect public trust and service availability.

MSP teams should review:

- Expiring certificates
- Certificates on old or unknown subdomains
- Weak keys or deprecated algorithms
- Unexpected certificate issuance
- Certificate ownership
- Renewal processes
- Public-facing services tied to DNS records

CheckRed's Certificate Posture Management page highlights certificate visibility across domains and subdomains, detection of expired or misconfigured certificates, weak keys, deprecated algorithms, rogue issuance, and remediation workflows. [6]

Compliance, reporting, and recurring services

DNS posture becomes more valuable when it supports recurring service delivery.

For MSPs, the strongest client value often comes from making DNS posture visible, reviewable, and reportable:

- Where DNS exposure exists
- Which records are stale or risky
- Which delegations need review
- Which certificates need attention
- Which findings connect to compliance requirements
- Which remediations were completed
- Which exceptions remain open
- What has improved since the last review

This is especially useful for clients in regulated or audit-sensitive industries, including healthcare, financial services, legal services, government contractors, and other SMBs with customer, insurance, or contractual requirements.

CheckRed's continuous compliance page positions the platform around compliance monitoring across SaaS, cloud, and DNS environments, including framework mapping, compliance gap detection, and audit-ready reporting. [5]

For MSPs, DNS posture can support:

- Client onboarding reviews
- Domain and delegation reviews
- Registrar access reviews
- Email authentication checks
- Certificate reviews
- DNS drift monitoring
- Exception tracking
- Compliance evidence
- QBR reporting
- Remediation guidance
- vCISO and advisory services

Security teams can do the technical work. Business owners need the evidence, prioritization, and progress reporting.

What MSPs Should Do Next

A DNS posture checklist for MSPs

Inventory the namespace

Document client domains, subdomains, DNS hosts, registrars, delegated zones, and public-facing services.

Review access and ownership

Confirm who can access registrars, DNS providers, cloud DNS services, and vendor-managed zones. Remove stale users and require MFA where available.

Check for stale or risky records

Look for dangling CNAMEs, stale TXT records, abandoned subdomains, weak delegations, old vendor references, exposed information, and records tied to retired services.

Review email authentication

Confirm SPF, DKIM, DMARC, MX, and related DNS records reflect the current email environment.

Review DNS and certificate posture together

Identify expiring, misconfigured, unexpected, or weak certificates and connect that work to DNS ownership and public namespace review.

Define approved recursive DNS policy

Decide which resolvers are approved and how endpoints, browsers, mobile devices, and remote users should be configured.

Govern encrypted DNS

Support encrypted DNS where appropriate while preserving approved resolver use, logging, and security policy enforcement.

Set DNS logging expectations

Decide what logs should be retained, where they should flow, and how they support detection, investigation, client reporting, and compliance evidence.

Add DNS posture to onboarding and QBRs

Build DNS review into recurring service delivery so it becomes part of how the MSP manages client risk over time.

Use a unified posture model

Include DNS posture in the same service model as SaaS, cloud, identity, certificates, and compliance.

Where CheckRed for MSPs Fits

DNS posture is a strong control area on its own. It becomes more useful when it is connected to the rest of the client environment.

CheckRed for MSPs gives providers a unified posture control layer across SaaS, cloud, DNS, identity, certificates, and compliance. DNS posture becomes part of the same operating model MSPs use to review risk, prioritize remediation, map findings to compliance frameworks, and report progress to clients.

CheckRed's DNSPM capabilities include unified visibility across DNS environments, automated asset discovery, misconfiguration detection, drift monitoring, fake domain and look-alike threat monitoring, Certificate Posture Management, PQC monitoring, prioritized alerts, guided remediation, custom reporting, and third-party integrations. [3]

The broader CheckRed platform also includes SaaS, cloud, DNS, certificate, and compliance posture capabilities. [4]

This 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?
- Which DNS issues affect certificates?
- Which issues affect audit readiness?
- Which findings need remediation first?
- Which issues remain open?

Instead of managing DNS posture in a separate DNS-only workflow, MSPs can connect it to SaaS, cloud, identity, certificates, and compliance posture.

PORT1 helps MSPs and MSSPs understand where CheckRed fits, how to package it, how to position it, and how to support client needs. At PORT1, we help our partners with marketing and sales, along with technical design, implementation, and support.

Learn more about CheckRed for MSPs:
https://port1.io/checkred

Explore CheckRed DNS Posture Management:
https://checkred.com/platform/dnspm

References

[1] Rose, S., Liu, C., and Gibson, R. *NIST SP 800-81r3: Secure Domain Name System (DNS) Deployment Guide*. National Institute of Standards and Technology, March 2026. https://csrc.nist.gov/pubs/sp/800/81/r3/final

[2] Microsoft Learn. *Prevent dangling DNS entries and avoid subdomain takeover*. Last updated January 12, 2026. https://learn.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover

[3] CheckRed. *DNS Posture Management*. Accessed May 2026. https://checkred.com/platform/dnspm/

[4] CheckRed. *Unified Cloud, SaaS & DNS Security Platform*. Accessed May 2026. https://checkred.com/platform/

[5] CheckRed. *Continuous Compliance*. Accessed May 2026. https://checkred.com/platform/continuous-compliance/

[6] CheckRed. *Certificate Posture Management*. Accessed May 2026. https://checkred.com/platform/certificate-pm/