DNS Spy

PARANOID ABOUT YOUR DNS

Monitor, validate and verify your DNS configurations

dnsspy.io

INTRODUCTION

WHY DNS IS A BLIND SPOT FOR MANY MSPS

If you're running an MSP, you already know your clients depend on you to keep their infrastructure reliable and secure. But there's one part of that infrastructure that often goes unmonitored—until it breaks: **DNS**.

When DNS fails, websites vanish. Emails bounce. APIs stop talking. Your clients don't care whether the problem is upstream or inherited—they just know something is broken, and they're looking to you for answers.

The problem? Most MSPs don't have a scalable way to monitor DNS across dozens or hundreds of domains. There's no alert when someone changes a record. No history of what was changed—or who did it. And when something goes wrong, you're stuck troubleshooting blind.

This guide is here to change that. Whether you manage 10 domains or 1,000, we'll show you:

- What DNS issues matter most to your clients
- What you should be monitoring (and why)
- How to catch issues before they become outages
- How to scale DNS monitoring without adding overhead

Let's turn DNS from a silent risk into a managed asset you can confidently stand behind.

COMMON DNS MISTAKES MSPS INHERIT

THE MOST COMMON DNS MESSES MSPS INHERIT

When you onboard a new client, you're not just inheriting their systems—you're inheriting every risky shortcut, outdated record, and neglected zone they've accumulated over the years.

And DNS? It's usually a mess.

Here are the most common DNS issues we see MSPs inherit—and why they matter:

✕ Orphaned Records

DNS entries that point to decommissioned servers or expired services.

Impact: Creates unnecessary attack surface and client confusion when old endpoints appear "live."

✕ Misaligned Nameservers

Nameservers that aren't fully synchronized or show different record sets.

Impact: Clients experience inconsistent resolution depending on which server they hit.

✕ Unmonitored Changes

No alert when someone inside the client's org—or a third-party provider—changes a DNS record.

Impact: You don't find out until something breaks. Or worse: the client calls you first.

✕ Missing History

No audit trail of what changed, who changed it, or when.

Impact: You're flying blind when diagnosing issues or trying to prove it wasn't your fault.

✕ Neglected TTLs

Time-to-live values that are too short (overloading resolution) or too long (delaying propagation).

Impact: Sluggish updates or DNS storms during outages.

Pro Tip:

Even if DNS isn't "your responsibility," your client expects you to be the one who fixes it when it fails.

WHAT MSPS SHOULD MONITOR IN DNS

WHAT YOU SHOULD BE WATCHING IN EVERY CLIENT ZONE

You can't protect what you don't monitor—and with DNS, even small changes can create big problems. These are the core records and behaviors every MSP should be watching across client domains:

A Records

These are the backbone of web resolution.

Why monitor? Unexpected changes could signal misconfigurations, server migrations gone wrong, or even malicious redirection.

MX Records

These are the backbone of web resolution.

Why monitor? Unexpected changes could signal misconfigurations, server migrations gone wrong, or even malicious redirection.

CNAME Records

Point one domain to another.

Why monitor? Chained CNAMEs can break if any link goes stale. They're also a common place for dangling records.

NS Records

Define which nameservers are authoritative.

Why monitor? Incorrect or misaligned NS records can cause inconsistent resolution and lead to caching nightmares.

TTL Values

Dictate how long DNS records are cached.

Why monitor? Poorly chosen TTLs can delay record updates or cause update storms during changes.

Unexpected Changes

Whether from client staff, third-party vendors, or external threats—**you need to know when something changes.**

Real-time change alerts are your early warning system.

HOW TO MONITOR DNS EFFECTIVELY

MANUAL CHECKS AREN'T ENOUGH—HERE'S WHAT ACTUALLY WORKS

Some MSPs rely on periodic DNS spot-checks or trust that clients will notify them when something breaks. But DNS issues are rarely that cooperative.

To stay ahead of problems—and prove your value—you need a system that does three things well: **alert, log, and scale.

Real-Time Alerts

You need to know the moment a record changes, a nameserver goes out of sync, or a zone disappears entirely.

Waiting for users to report issues isn't proactive—it's reactive.

Historical Logging

Without a clear audit trail, it's impossible to diagnose recurring problems or defend your team when things go wrong.

Who changed the record? When? What was the value before? You should have those answers at a glance.

Scalability

What works for 5 domains doesn't work for 500.

You need tools that scale effortlessly—across dozens of clients and hundreds of zones—without adding operational overhead.

Avoid These Pitfalls

- Relying solely on DNS provider dashboards
- Monitoring only “important” zones
- No alerts for deletions or NS drift
- Assuming TTLs protect you from mistakes

The Right Approach

Use automated DNS monitoring that checks for:

- Record-level changes
- Sync mismatches
- Misconfigured zones
- Expired or dangling records
- RFC violations

All with centralized visibility—so you can stop fighting fires and start building client trust.

HOW DNS SPY HELPS

HOW DNS SPY MAKES DNS MONITORING SCALABLE, RELIABLE, AND MSP-FRIENDLY

At DNS Spy, we built our platform specifically for MSPs who manage dozens—or hundreds—of client domains. Our mission is to make DNS monitoring something you can trust, scale, and integrate seamlessly into your daily workflows.

Here's what DNS Spy brings to the table:

📈 Centralized Dashboard

View and manage all your monitored domains in one place. Instantly see what changed, where, and when—without jumping between providers or portals.

🔔 Instant Change Alerts

Be the first to know when a record changes, a zone is deleted, or a nameserver goes out of sync.

You can receive alerts via email—or integrate directly into your existing SIEM or incident response tools to empower your security team with DNS visibility.

🗒 Full DNS History

Every DNS record change is logged automatically—who changed what and when.

Perfect for client accountability, audit trails, and reducing time-to-resolution when issues arise.

RFC & Security Validation

Catch DNS misconfigurations and risky setups before they cause downtime or vulnerabilities.

We check every zone for compliance with DNS best practices and highlight records that could expose your clients.

API Access for Custom Workflows

Want to sync DNS change data with internal dashboards or automate reporting?

Our robust API gives you full access to change history, alerting, and monitoring controls—so DNS Spy fits right into your existing tooling.

Scales With You

Start with 50 domains. Add more in packs of 50 with no upper limit.

Whether you manage 5 clients or 500, DNS Spy grows with you—without adding operational burden.

Exportable Reports

Generate downloadable reports showing change history, misconfig alerts, and zone health.

Perfect for client updates, quarterly reviews, or internal reporting.

> DNS monitoring shouldn't be a manual process or a mystery. With DNS Spy, it becomes part of your MSP toolkit—scalable, reliable, and built for the real world.

CALL TO ACTION

START MONITORING SMARTER. SCALE WITH CONFIDENCE.

DNS is too important to leave unmonitored—and too complex to manage manually at scale.

With DNS Spy, you can:

- Catch DNS issues before your clients do
- Monitor hundreds of domains from one dashboard
- Prove your value with reports and change history
- Integrate alerts into your workflows or SIEM
- Scale with add-ons—no contracts, no gatekeeping

Whether you manage 5 domains or 5,000, DNS Spy gives you the visibility and control to protect your clients—and your reputation.

Get started with your first 50 domains today.

> Scale as your clients grow. Monitor smarter. Sleep better.

Get Started with DNS Spy →