Take Control of DNS Security

Visibility, Compliance, & Protection in One Platform

The Challenge of DNS Security

The Domain Name System (DNS) is the backbone of your digital infrastructure—but it's often the most overlooked. As organizations increasingly move to hybrid and multi-cloud environments, DNS management becomes increasingly complex with multiple DNS providers, undocumented records, and hidden zones from shadow IT, migrations, and acquisitions. Security teams face limited visibility, manual processes, and outdated tools that can't keep up with misconfigurations, unauthorized changes, or record drift.

Without automation and centralized oversight, enforcing consistent policies is nearly impossible—leaving organizations vulnerable to DNS-based attacks like spoofing, tunneling, and data exfiltration. This fragmented approach not only expands the attack surface but also delays detection and remediation, increasing both security and compliance risks.

What DNS Posture Management (DNSPM) Offers

- **Track DNS Inventory**
  Locate and manage DNS zones, domains, and records across providers with full context
- **Gain Powerful Visibility**
  Get a single pane view of DNS across multi-cloud and hybrid environments
- **Detect Misconfigurations**
  Identify vulnerable DNS records and configuration issues automatically
- **Monitor DNS Drift**
  Track unauthorized changes and ensure policy alignment
- **Protect Your Brand**
  Detect lookalike domains and defend against typosquatting and impersonation
- **Manage Certificates**
  Discover misconfigured, expired, or rogue TLS/SSL certificates across your domains
- **Deploy Quantum-Ready Security**
  Monitor certificate hygiene and prepare for PQC (Post-Quantum Cryptography) readiness
- **Maintain Continuous Compliance**
  Map DNS risks to 15+ frameworks (CIS, ISO, NIST, HIPAA, PCI-DSS, and more)

Why CheckRed?

CheckRed DNSPM delivers unified visibility and control across your entire DNS infrastructure. Whether you're running AWS Route 53, Akamai Edge DNS, Google Cloud DNS, Azure DNS, or legacy on-prem environments—CheckRed helps you discover, monitor, and secure every DNS asset from one platform.

DNSPM transforms your DNS security from fragmented and reactive to unified and proactive—eliminating guesswork, reducing risk, and enforcing continuous compliance.

How CheckRed Works

Inspect
Automatically discover DNS assets—no agent required

Detect
Uncover expired certificates, drift, risky CNAMEs, and shadow DNS zones

Prioritize
Score risks and prioritize the threats that matter the most

Remediate
Get step-by-step guidance and trigger automated workflows

Report
Benchmark DNS security posture and track improvements over time

DNS Security Challenges | CheckRed's Capabilities

Your Challenges	How CheckRed Helps
Incomplete visibility across providers	Unified DNS asset inventory across multi-cloud and hybrid environments
Manual auditing and drift detection	Continuous monitoring and alerting for DNS drift
Brand impersonation via lookalike domains	Lookalike and typosquatting detection
Expired/misconfigured TLS certificates	Automated certificate posture management
DNS misconfigurations and outdated records	Deep policy checks and remediation workflows
Compliance and audit complexity	Continuous compliance mapping and industry benchmarking

See More. Secure More. Stress Less.

CheckRed DNSPM is your partner in DNS visibility, risk mitigation, and policy enforcement.

Built to integrate seamlessly with your existing SIEM, SOAR, GRC, and ticketing tools, DNSPM keeps your DNS posture continuously protected—without slowing you down.

Request a Demo at **checkred.com/dns-demo/**