



# DNS Posture Management

The Domain Name System (DNS) is a critical component of every organization's infrastructure, yet it often remains an overlooked vulnerability. Misconfigurations and hidden assets can lead to service disruptions, data breaches, and compliance failures, impacting both security and business continuity.

A proactive approach to monitoring, risk detection, and policy enforcement is crucial to prevent outages, mitigate threats, and ensure compliance with industry and security regulations.

## The challenge of DNS security










Organizations today face increasing complexity in managing their DNS posture because of evolving network architectures and hybrid and multicloud deployments that involve multiple DNS systems. Businesses struggle with maintaining visibility across distributed network environments where shadow IT, cloud migrations, and acquisitions create undocumented DNS zones and records that expand the attack surface. On the technical side, teams grapple with detecting and remediating misconfigurations, unauthorized zone transfers, and outdated record hygiene across disparate DNS platforms.

Without automated monitoring, security teams rely on manual processes that introduce human error and fail to enforce consistent security policies, leaving critical infrastructure vulnerable to DNS-based attacks, including DNS spoofing, tunneling, and data exfiltration. This fragmented approach creates significant compliance risks while increasing the mean time to detect and remediate issues as security teams lack comprehensive tools that integrate with existing security operations centers.

## How Akamai DNS Posture Management helps

Akamai DNS Posture Management is designed to address these challenges head-on by providing end-to-end visibility, automation, and risk mitigation for your DNS infrastructure. It provides a single pane of glass view by consolidating DNS zones, domains, subdomains, and records from all DNS providers, helping to eliminate visibility gaps and improve efficiency. This centralized approach simplifies the complexities of managing DNS security in multi-vendor environments, allowing organizations to monitor, secure, and optimize their DNS infrastructure from a single platform.

### Benefits for your business

-  **Track DNS inventory**  
Locate and manage DNS assets across providers with full asset context for improved oversight
-  **Gain powerful visibility**  
Get a single pane of glass view across your DNS environments, including AWS Route 53, Akamai Edge DNS, Google Cloud DNS, and more
-  **Detect misconfigurations**  
Quickly identify and address configuration-based vulnerabilities and unauthorized changes that may compromise security
-  **Monitor DNS drift**  
Track unauthorized or unexpected changes to DNS records, ensuring that DNS settings stay aligned with your organization's security policies and operational needs
-  **Integrate seamlessly**  
Headless API capabilities allow for integration into your favorite SIEM, SOAR, GRC, ITSM, and XDR platforms
-  **Protect your brand**  
Identify and manage phishing and impersonation threats with continuous monitoring for look-alike domains
-  **Maintain continuous compliance**  
Help meet compliance requirements of 15+ frameworks (CIS, NIST, ISO, HIPAA, PCI-DSS, and more)
-  **Manage certificates**  
Monitor and assess digital certificates to prevent security risks like expired, misconfigured, or rogue certificates
-  **Deploy quantum-ready security**  
Prepare for quantum threats with post-quantum cryptography (PQC) monitoring that helps ensure that your certificate infrastructure remains protected against future quantum attacks before they become a reality

# Transform complex DNS security into actionable intelligence

A powerful user interface (UI) with intuitive dashboards enables users to seamlessly search across all major DNS providers, visualizing relationships and potential threats (Figure 1). Alerts are prioritized by severity, which ensures that critical issues receive immediate attention. Real-time monitoring capabilities detect emerging risks, including DNS drift that could indicate configuration compromise, while also identifying look-alike and typosquatting domains that are targeting your brand.

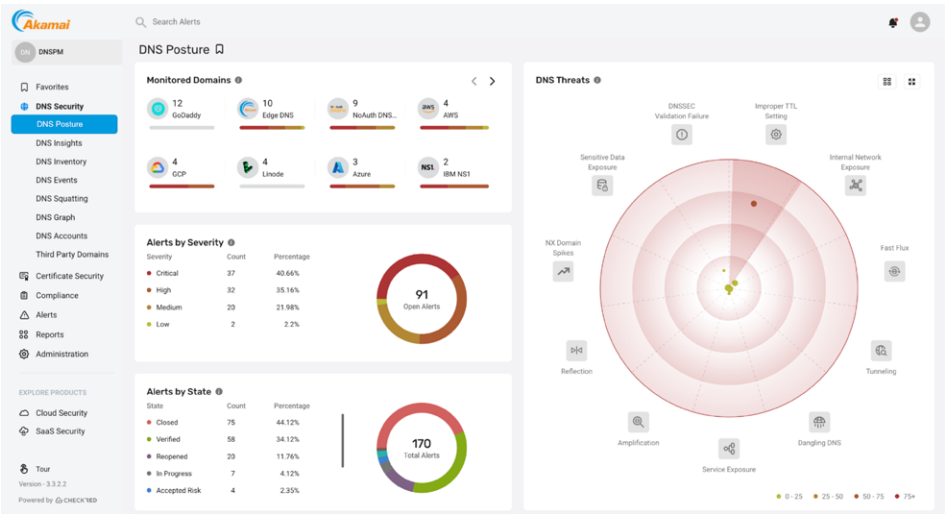


Fig. 1: Powerful dashboard provides complete visibility and control over DNS assets to detect and remediate threats and misconfigurations

The UI also provides a valuable industry benchmarking feature that provides comparative risk scoring against anonymized data from similar companies, helping companies quantify their DNS security posture against industry peers (Figure 2).

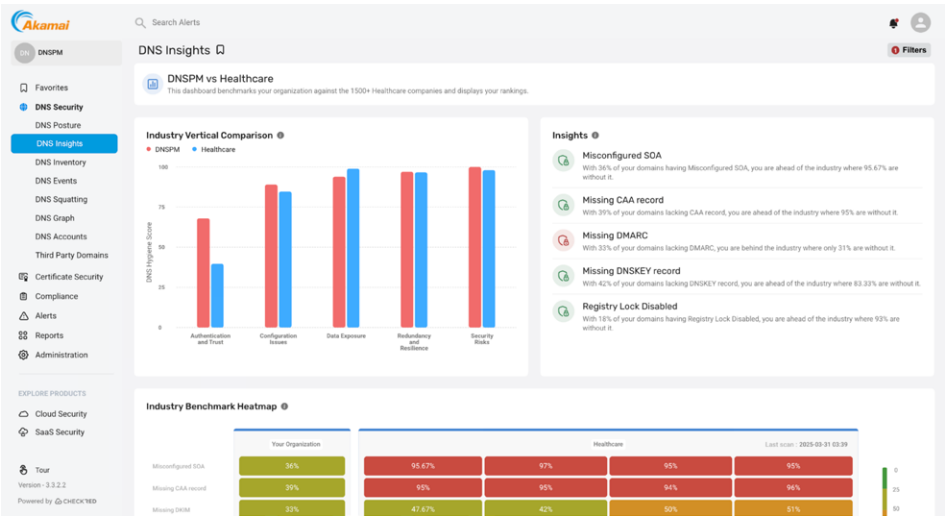


Fig. 2: Organizations can benchmark their security posture against industry peers



# Key capabilities

## Multi-provider coverage

- Integrates seamlessly across all major DNS providers — including Akamai Edge DNS, AWS Route 53, Azure DNS, Infoblox, Google Cloud DNS, and more — for consistent security and centralized control

## Unified visibility across environments

- Delivers a single pane of glass view for all DNS assets — domains, subdomains, and records — spanning multiple cloud providers and on-premises infrastructures

## Deep policy checks

- Conduct extensive policy checks and configurations across your DNS infrastructure — including detection of CNAME dangles — to uncover vulnerabilities before they can be exploited; apply extensible rules to tailor DNS security checks to your organization's unique policies and evolving compliance needs

## Proactive risk detection and prevention

- Requires no installation on endpoints or servers, offering rapid deployment, minimal overhead, and immediate insight into vulnerabilities

## Dynamic remediation workflows and reporting

- Provides step-by-step remediation guidance with manual, semi-automated, and fully automated workflows, making it easy to resolve issues quickly and effectively

## Compliance enablement

- Helps organizations maintain compliance (following the Center of Internet Security [CIS] benchmarks), reduce regulatory risk, and uphold customer trust through continuous policy checks and comprehensive reporting

## Certificate posture management

- Identify misconfigured or expired TLS/SSL certificates to reduce exposure and support audit readiness

## Akamai Managed Service (optional)

- Security Operations Command Center specialists actively monitor your DNS infrastructure to provide proactive recommendations for vulnerabilities and deliver emergency support for detected threats



To learn more, visit [akamai.com](https://akamai.com) or contact your Akamai sales team.