AKAMAI 产品简介

DNS Posture Management

域名系统 (DNS) 是每个企业基础架构的关键组成部分，但它往往也是被忽视的漏洞。配置错误和隐藏资产可能导致服务中断、数据泄露和合规审计失败，从而影响安全性和业务连续性。

以主动方式进行监控、风险检测和策略执行，对于预防中断、抵御威胁以及确保遵守行业和安全法规至关重要。

DNS 安全防护挑战

由于网络架构的不断演进以及混合云和多云部署涉及多个 DNS 系统，当今企业在管理 DNS 安全态势时面临的复杂性日益加剧。企业难以在分布式网络环境中维持全面的可见性，导致大量未经备案的 DNS 区域和记录产生，从而扩大了攻击面。在技术层面，团队需要应对各种挑战：检测并修复异构 DNS 平台上的错误配置、未经授权的区域转移和过时的记录维护。

如果没有自动监控，安全团队就要依赖手动流程，这种流程会引入人为错误，且无法实施一致的安全策略，从而让关键基础架构易受基于 DNS 的攻击，包括 DNS 欺骗、隧道和数据泄露。这种分散的方法带来了严重的合规风险，同时增加了检测和修复问题的平均时间，因为安全团队缺乏与现有安全运营中心整合的全面工具。

Akamai DNS Posture Management 如何提供帮助

Akamai DNS Posture Management 旨在通过为您的 DNS 基础架构提供端到端的监测、自动化和风险抵御来正面应对这些挑战。它通过整合来自所有 DNS 提供商的 DNS 区域、域、子域和记录，提供了单一管理平台视图，有助于消除监测能力差距，提高效率。这一集中式方法简化了在多供应商环境中管理 DNS 安全的复杂性，支持企业从单一平台监控、保护和优化其 DNS 基础架构。

为贵企业带来的好处

跟踪 DNS 清单
通过完整的资产背景信息，实现跨提供商的 DNS 资产查找与管理，从而提升监管效能

获得强大的监测能力
在您的 DNS 环境中获得单一管理平台视图，其中包括 AWS Route 53、Akamai Edge DNS、Google Cloud DNS 等

检测配置错误
快速识别并解决可能有损安全的基于配置的漏洞和未经授权的更改

监控 DNS 漂移
跟踪 DNS 记录的未经授权或意外的更改，确保 DNS 设置与企业的安全策略和运营需求保持一致

无缝集成
借助无界面 API 功能支持与各类安全管理平台无缝集成，包括您常用的 SIEM、SOAR、GRC、ITSM 和 XDR 平台

保护您的品牌
通过持续监控相似域名，识别和管理钓鱼和仿冒威胁

保持持续合规
助力满足超 15 个框架（CIS、NIST、ISO、HIPAA、PCI-DSS 等）的合规要求

管理证书
监控并评估数字证书，防止过期、错误配置或恶意证书等安全风险

部署量子级安全性
通过后量子密码学 (PQC) 监控准备好应对量子威胁，这有助于确保您的证书基础架构始终能防范未来的量子攻击，避免此类攻击成为现实

将复杂的 DNS 安全转化为切实可行的情报

借助强大的用户界面 (UI) 和直观的仪表板，用户能够在各主流 DNS 提供商之间进行无缝搜索，同时监测关系和潜在威胁（图 1）。告警按严重程度进行优先级排序，可确保关键问题得到即时响应。实时监控功能可以识别新出现的风险，包括可能预示配置遭篡改的 DNS 漂移现象，同时能检测出针对企业品牌的仿冒域名和误拼域名攻击。

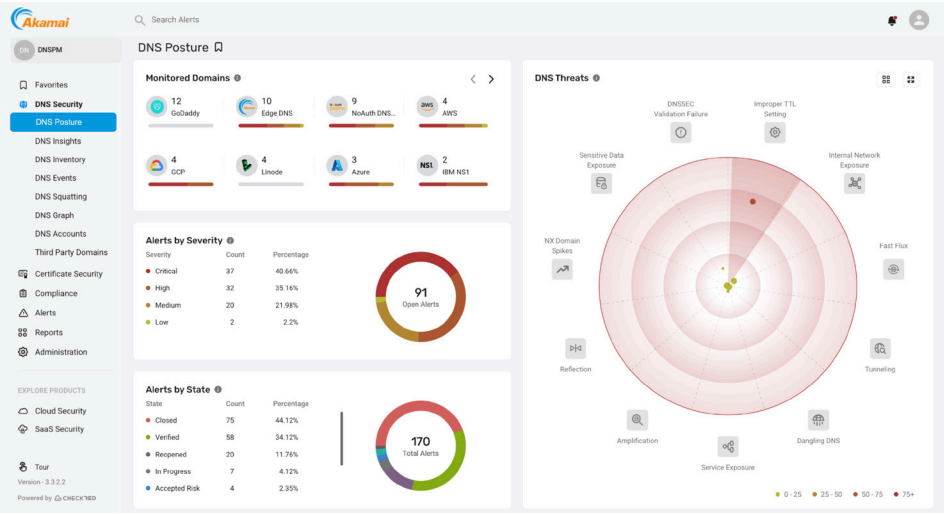

图 1：强大的仪表板可对 DNS 资产提供全面监测和控制，以检测并修复威胁和错误配置

此外，该 UI 还提供了有价值的行业基准测试功能，该功能根据类似公司的匿名数据提供了比较风险评分，帮助公司量化其相对于同行的 DNS 安全态势（图 2）。

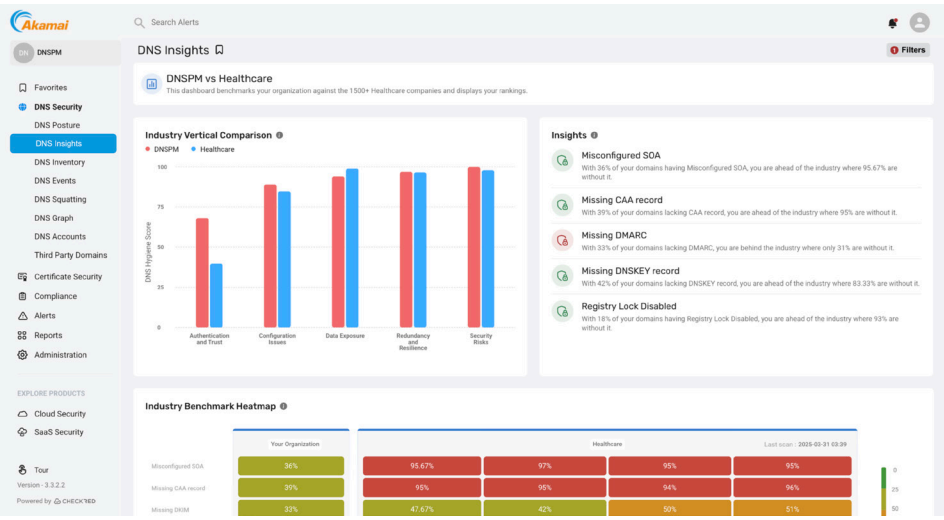

图 2：企业可根据同行的数据对其安全态势进行基准测试

主要功能

多提供商覆盖

- 与所有主流 DNS 提供商无缝集成，包括 Akamai Edge DNS、AWS Route 53、Azure DNS、Infoblox、Google Cloud DNS 等，以实现统一的安全策略和集中管控

跨环境的统一监测

- 为跨多个云服务提供商和本地基础架构的所有 DNS 资产（域、子域和记录）提供单一管理平台视图

深入的策略检查

- 在 DNS 基础架构中进行广泛的策略检查和配置，包括检测悬垂 CNAME 记录，以便及时发现漏洞，防止其遭到利用；应用可扩展规则，根据企业的独特策略和不断变化的合规要求量身定制 DNS 安全检查

主动风险检测和预防

- 无需在端点或服务器上进行安装，可实现快速部署、最大限度节省开销并及时发现漏洞

动态修复工作流程和报告

- 提供手动、半自动和全自动工作流程的分步修复指导，从而快速有效地轻松解决问题

合规性支持

- 通过持续的策略检查和全面的报告，帮助企业保持合规性（遵循互联网安全中心 [CIS] 基准要求），降低监管风险并持续维持客户信任

证书态势管理

- 识别配置错误或过期 TLS/SSL 证书，以降低风险，同时满足审计就绪要求

Akamai Managed Service（可选）

- 安全运营指挥中心专家积极监控您的 DNS 基础架构，针对漏洞提出主动建议，并针对检测到的威胁提供紧急支持

如需了解更多信息，请访问 akamai.com/zh 或联系您的 Akamai 销售团队。

扫码关注，获取最新云计算、云安全与CDN前沿资讯