TechOwl SHIELD

DATA SHEET

TechOwl SHIELD
Attack Surface Monitoring

Overview

TechOwl SHIELD is a comprehensive digital protection suite designed to safeguard brands and individuals from online threats. Leveraging advanced detection technologies and expert response teams, SHIELD monitors and mitigates risks such as impersonation, data leaks, brand abuse, and dark web exposure across digital platforms. From phishing takedowns to identity enforcement, Techowl SHIELD ensures robust defense in today's complex cyber landscape.

Notable Highlights

- Unlimited Takedowns
- All-in-One Platform
- Seamless Integration with SOC
- 27x7x365 days Support

Email Health Monitoring

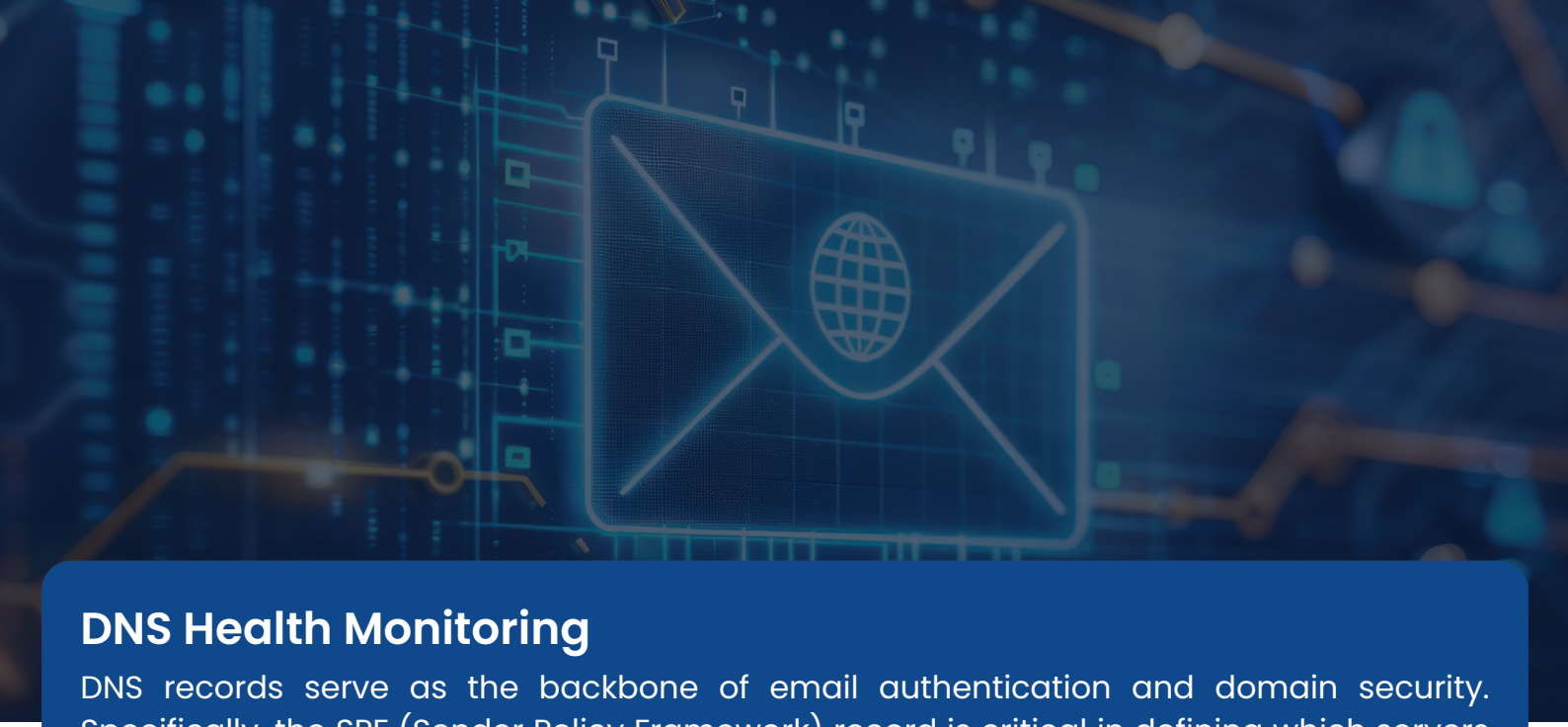
Email remains the attack vector for cybercriminals from spoofing and phishing to misconfigured servers that expose your organization to risk. A single vulnerability in your email infrastructure can open the door to massive data breaches or fraud.

Key Features

DNS Health Monitoring	Validates DNS configurations including SPF, DKIM, and DMARC to prevent spoofing and ensure email authenticity.
SMTP Configuration Checks	Detects misconfigured or exposed SMTP servers that could be abused for spam, spoofing, or information leakage.
Phishing Email Detection	Identifies phishing attempts targeting your domain, employees, or clients , with real-time alerts and detailed analysis.

Use Case

An organization was facing repeated spoofed emails impersonating its leadership team. After deploying TechOwl SHIELD – Email Health, misconfigured SPF and missing DMARC records were identified and corrected. Real-time alerts enabled the team to intercept phishing attempts effectively. As a result, the organization's email reputation improved across service providers, enhancing both delivery rates and stakeholder trust.



DNS Health Monitoring

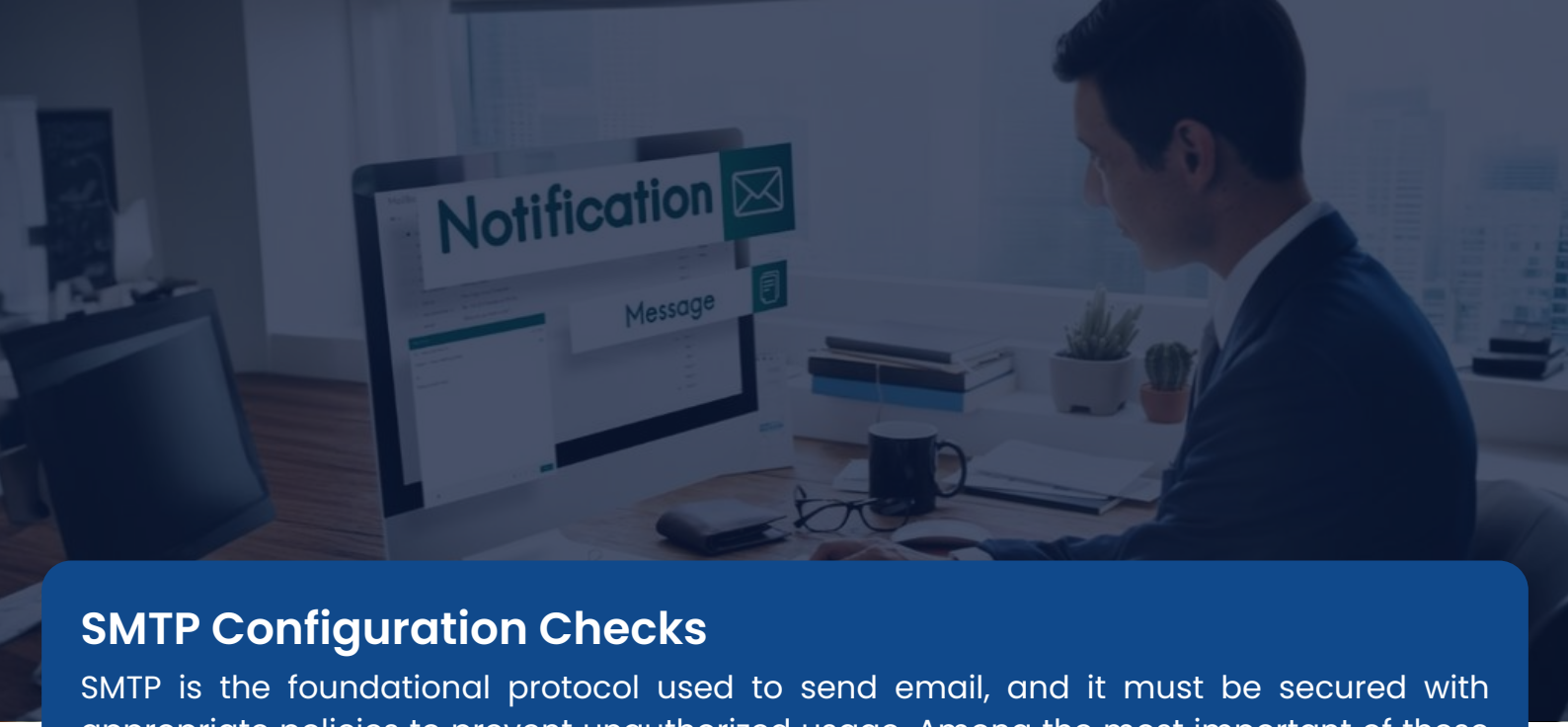
DNS records serve as the backbone of email authentication and domain security. Specifically, the SPF (Sender Policy Framework) record is critical in defining which servers are authorized to send email on behalf of your domain. If your SPF record is missing, overly permissive, or misconfigured, it leaves the door open for attackers to spoof your domain and send fraudulent emails that appear legitimate. Unfortunately, many businesses are unaware of these vulnerabilities until customers start receiving phishing emails claiming to be from their organization or legitimate communications begin landing in spam folders. Regular monitoring of your SPF settings via DNS analysis is essential not only to prevent impersonation but also to ensure the consistent and trustworthy delivery of your business communications.

Associated Threats:

- Email spoofing and impersonation
- Legitimate emails landing in spam folders
- Increased exposure to phishing and fraud
- Risk of domain being blacklisted

How TechOwl SHIELD Helps:

TechOwl SHIELD regularly checks your domain's SPF record configuration through DNS analysis. We identify syntax errors, missing includes, or overly permissive entries that weaken protection. With our alerts and recommendations, your team can maintain strong SPF settings to preserve email trustworthiness and stop unauthorized senders.



SMTP Configuration Checks

SMTP is the foundational protocol used to send email, and it must be secured with appropriate policies to prevent unauthorized usage. Among the most important of these is DMARC (Domain-based Message Authentication, Reporting, and Conformance), which works alongside SPF and DKIM to instruct receiving servers on how to handle unauthenticated messages. A poorly configured or missing DMARC policy exposes your domain to impersonation, phishing attacks, and delivery issues. Moreover, without DMARC reports, you lack visibility into how your domain is being used or misused across the email ecosystem. Monitoring SMTP configurations with a focus on DMARC helps secure your domain, improve email deliverability, and ensure that your brand remains protected from spoofing attempts.

Associated Threats:

- Email spoofing due to lack of DMARC enforcement
- Loss of control over who sends on your behalf
- Missed insights into attempted impersonation
- Deliverability issues without sender alignment

How TechOwl SHIELD Helps:

TechOwl SHIELD monitors your domain's DMARC policy via SMTP inspection. We alert you if no DMARC policy is present, if it's too lenient (none/quarantine), or if reports indicate misuse. Our insights help you move toward a strict policy (p=reject) and ensure your domain is protected from being exploited by attackers.

Phishing Email Detection

Phishing attacks are one of the most common and damaging threats facing organizations today, and your brand is a prime target. Attackers routinely impersonate trusted companies using forged domains, logos, and email formats to deceive recipients into revealing personal data or clicking malicious links. These phishing emails often originate outside your network, making them difficult to detect with traditional perimeter security. The fallout from such campaigns includes credential theft, malware infections, reputational damage, and customer distrust even if your own systems were never breached. That's why it's critical to proactively monitor the internet, dark web, and threat intelligence feeds for phishing emails that misuse your brand or domain, and take action to disrupt these campaigns before they cause real harm.

Associated Threats:

- Domain impersonation and spoofing
- Stolen credentials and financial fraud
- Malware or ransomware distribution
- Reputational damage and customer distrust

How TechOwl SHIELD Helps:

TechOwl SHIELD scans the web, dark web, and threat intelligence feeds to detect phishing campaigns targeting your brand. We track impersonating domains, lookalike email addresses, and malicious senders — and help initiate takedown actions. This proactive protection ensures your brand image and customers remain safe from email-based deception.