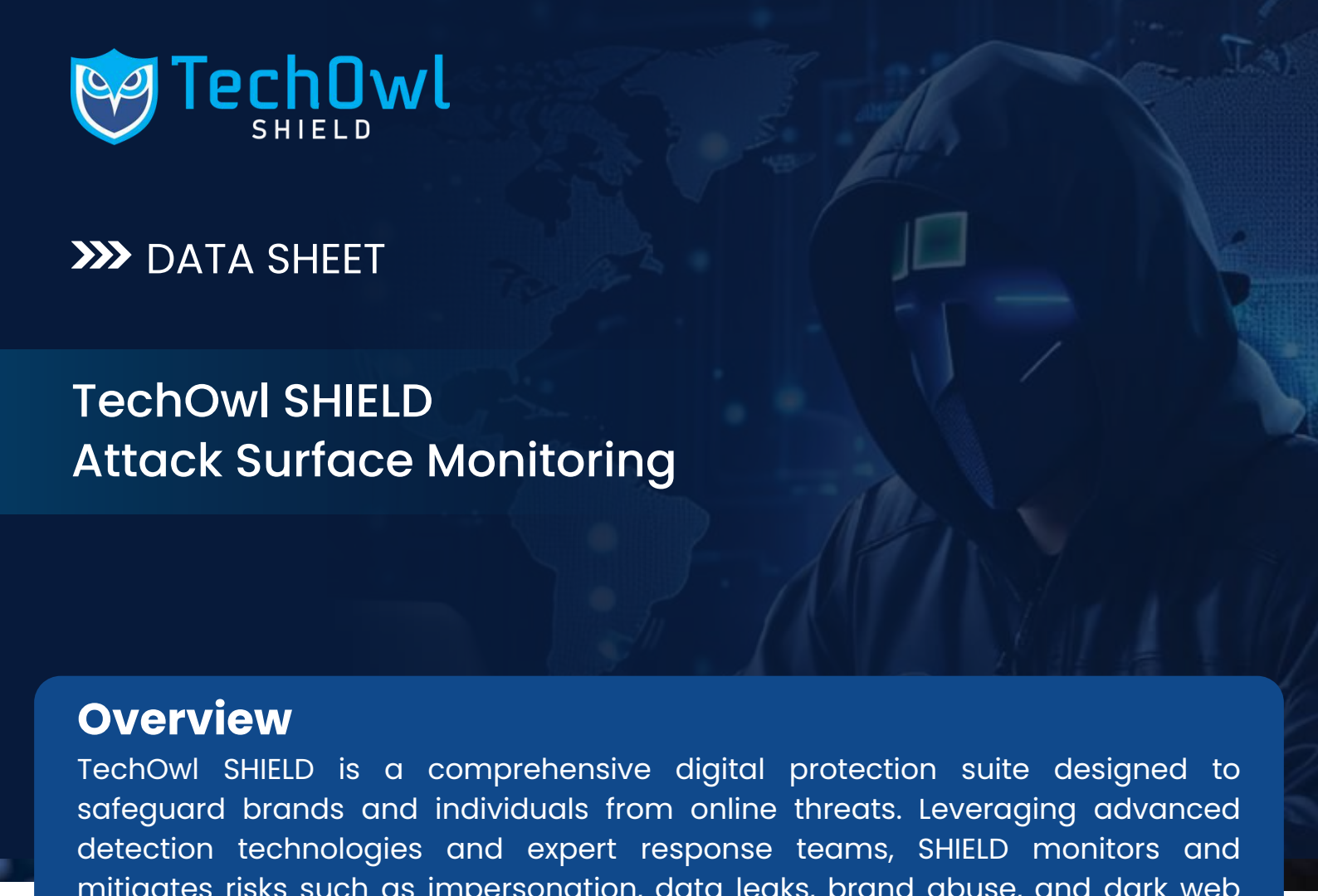
TechOwl SHIELD

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

Supply Chain Risk Monitoring

Vendors and third parties can unknowingly expose your organization to cyber risks. TechOwl SHIELD monitors both your systems and your extended supply chain 24x7, detecting credential leaks, malware infections, and other threats early. This continuous oversight helps you respond swiftly and minimize potential damage before it escalates.

Key Features

Third-Party Risk Visibility	Get alerts on vendor-side exposures that can impact you.
Continuous Ecosystem Monitoring	Monitor assets beyond your perimeter.
Early Threat Detection	Spot leaked credentials or infected systems before attackers exploit them.
Compliance Support	Align with RBI, SEBI, and other regulatory expectations for vendor risk management.

Use Case

An organization experienced a data leak caused by a third-party vendor breach. Although the compromise originated from the vendor's systems, TechOwl SHIELD's third-party monitoring swiftly identified the exposure. Thanks to SHIELD's real-time alerting, the threat was detected early, access was revoked immediately, and the risk was quickly contained. This incident underscores the importance of proactive third-party risk monitoring because with SHIELD, organizations can respond before damage spreads.

Credentials Leaks

In the modern digital supply chain, your organization's security posture is only as strong as your weakest vendor or third-party partner. Even if your internal systems are fully secure, a breach at one of your vendors could result in sensitive information such as employee credentials or access tokens being leaked onto the dark web. These credentials can then be exploited in targeted attacks, credential stuffing, or unauthorized access attempts, putting your systems and data at risk without any warning. The challenge is that these leaks often go undetected until damage has already occurred. Continuous monitoring of underground forums, breach dumps, and dark web sources is vital to detect any credentials tied to your organization that may have been exposed due to vendor-side incidents, enabling you to act before attackers do.

Associated Threats:

- Leakage of your organization's credentials due to third-party breaches
- Unauthorized access through stolen usernames and passwords
- Supply chain-based credential stuffing attacks
- Compliance risks due to vendor-side data handling lapses

How TechOwl SHIELD Helps:

TechOwl SHIELD scans dark web marketplaces, breach forums, and paste sites to detect if your credentials have been leaked as a result of vendor-side breaches. We map leaked records back to your organization and notify you with context including the likely source vendor, type of data leaked, and remediation actions. This ensures you're aware of supply chain exposures before attackers can exploit them.

Infected System

An infected system within your supply chain — whether it belongs to a vendor, service provider, or subsidiary — can become an unnoticed gateway for attackers to infiltrate your organization. Malware, remote access trojans (RATs), or command-and-control (C2) beacons operating on third-party systems can exploit trusted connections and integrations to bypass traditional security controls. Because these systems are often considered "safe" due to their approved access, malicious activity can go undetected for extended periods. The lack of visibility into the cybersecurity posture of vendors creates blind spots, allowing attackers to move laterally, steal data, or compromise your operations through the weakest external link. Monitoring supply chain risks is therefore critical to protecting your core environment from indirect threats.

Associated Threats:

- Malware communication from systems linked to your vendor's infrastructure
- Data exfiltration or surveillance via third-party systems
- Lateral movement through trusted network paths
- Risk to business continuity and client data

How TechOwl SHIELD Helps:

TechOwl SHIELD leverages global threat intelligence feeds to detect if any system within your supply chain is infected and communicating with known malicious infrastructure. When such infected endpoints are identified whether internal or external you receive actionable alerts, enabling you to isolate and address the risk before it reaches your core environment.