CYWARE™ | Datasheet

Operationalizing Digital Risk Protection

Executive Summary

In today's hyper-connected environment, your brand is constantly under fire. Attackers clone domains, impersonate executives, and trade stolen credentials on the dark web before internal security tools can react. Cyware Digital Risk Protection closes this visibility gap. By integrating intelligence-backed digital risk protection capabilities with Cyware Intelligence Suite, organizations gain a continuous external radar that doesn't just identify threats but initiates a structured, automated response to neutralize them.

The Challenge: External Blind Spots

Challenge	Business Impact
Brand Impersonation	Phishing domains and fake social profiles erode customer trust and cause financial loss.
Dark Web Exposure	Leaked credentials and breached PII are traded in underground forums, leading to account takeovers.
Manual Remediation	Security teams struggle with slow, manual takedown requests to registrars and hosting providers.

CYWARE™

Core Capabilities: Unified Digital Risk Protection

Cyware Digital Risk Protection, powered by SOCRadar(™), serves as the external intelligence layer, feeding high-fidelity, brand-specific data directly into the Cyware ecosystem for immediate action.

Dark Web Monitoring

Continuous surveillance of over 10,000 unique deep and dark web sources. Cyware Intelligence Suite detects leaked credentials, credit cards, and PII, providing early warning before these assets are weaponized against your internal systems.

Social Media Brand Abuse

Detect fake profiles and scam campaigns across platforms like LinkedIn and X (Twitter). Cyware Intelligence Suite provides visibility into rogue mobile apps and fraudulent "Official Support" accounts that target your customers.

Domain & Keyword Monitoring

- **Typosquatting Detection:** Identify lookalike domains and rogue infrastructure targeting your brand.
- **Custom Keyword Tracking:** Monitor for executive names and organizational keywords to surface targeted fraud and impersonation campaigns.

Managed Takedown Services

Stop playing "whack-a-mole" with attackers. SOCRadar provides an integrated, in-house managed takedown service to expedite the removal of malicious domains, impersonating social accounts, rogue app store listings, and exposed data repositories like GitHub or paste sites.

Unified Value:

The Cyware Advantage

Personalized Intelligence

Transform global threat feeds into organization-specific risk by tracking your brand and your executives.

Zero-Trust Extension

Extend your security perimeter to the dark web, turning detected leaks into proactive internal defense actions like forced password resets.

Assured Remediation

Escalate threats directly from the Cyware interface into the SOCRadar takedown process for transparent, end-to-end lifecycle tracking.

Operationalizing the Threat Lifecycle

The Cyware Intelligence Suite solution, with integrated DRP from SOCRadar, doesn't just close a ticket. When a phishing site is detected it will:

Detect
SOCRadar identifies the domain and captures technical evidence.
intent mapping

Action
Cyware triggers playbooks to block the IOCs across internal firewalls and EDR.

Neutralize
SOCRadar analysts coordinate with the hosting provider for a verified takedown.

About Cyware

Cyware is leading the industry in Agentic-powered Operational Threat Intelligence and Collective Defense, helping security teams transform threat intelligence from fragmented data points to actionable, real-time decisions. We unify threat intelligence management, intel sharing and collaboration, with orchestration and automation, eliminating silos and enabling organizations to outmaneuver adversaries faster and more effectively. From enterprises to government agencies and ISACs, Cyware empowers defenders to turn intelligence into impact.

cyware.com

sales@cyware.com

111 Town Square Place Suite 1203,
#4 Jersey City, NJ 07310