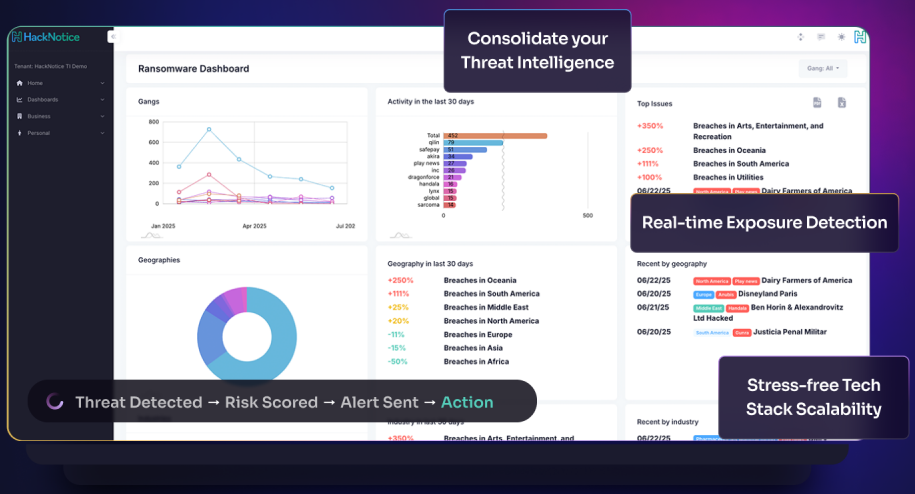
HackNotice

REAL TIME BREACHES & ATTACK DATA

Full-Spectrum Threat Intelligence For The Legal Industry



Safeguard client confidentiality and protect your firm's integrity with dark web intelligence and threat monitoring designed for law firms.

Law firms are high-value targets for threat actors seeking sensitive client data, case materials, and insider information. With growing attacks involving ransomware, data extortion, and credential theft, legal organizations face mounting pressure to secure confidential assets and maintain client trust.

HackNotice delivers real-time, actionable threat intelligence to help law firms detect exposure early, reduce risk, and respond swiftly to dark web threats. Our continuous monitoring of compromised credentials, leaked documents, and third-party risks strengthens your defense while supporting due diligence and compliance efforts.

For incidents requiring deeper analysis, our Dark Web Forensic Investigations team provides expert-led research to identify root causes, assess impact, and track adversarial activity across forums, marketplaces, and messaging platforms.

Within days of onboarding, HackNotice will

- **Detect and monitor compromised firm data, credentials tied to infostealer malware, and attack data.**
- **Provide continuous monitoring and real-time alerts on ransomware threats and supply chain breaches.**
- **Mitigate unauthorized access to legal platforms, client portals, and privileged data using leaked credentials.**

Proactively mitigate dark web and supply chain threats with AI-Powered Threat Intelligence

Protect Client & Firm Accounts

Monitor for compromised credentials used across case management systems, client portals, and email accounts—helping prevent account takeover (ATO), fraud, and unauthorized access.

Monitor Staff, Clients, and Case Exposure

Identify leaked attorney and client credentials, sensitive legal documents, and privileged communications on the dark web; ensuring fast, discreet action to reduce risk.

Mitigate Employee Account Take Over

Identify when employee credentials are stolen by infostealer malware, helping prevent Business Email Compromise (BEC), internal fraud, and unauthorized access to financial systems.

Supply Chain Threat Monitoring

Continuously track breaches, ransomware attacks, and trafficked data related to your third-party vendors and partners, enabling risk-based prioritization and remediation.

"We've been really happy with the service. Last month alone, **you provided us with 12 actionable alerts.**"

Empowering security teams with the intel they need to prevent compromise across their user base, workforce, and digital ecosystem—all in real time and at scale.