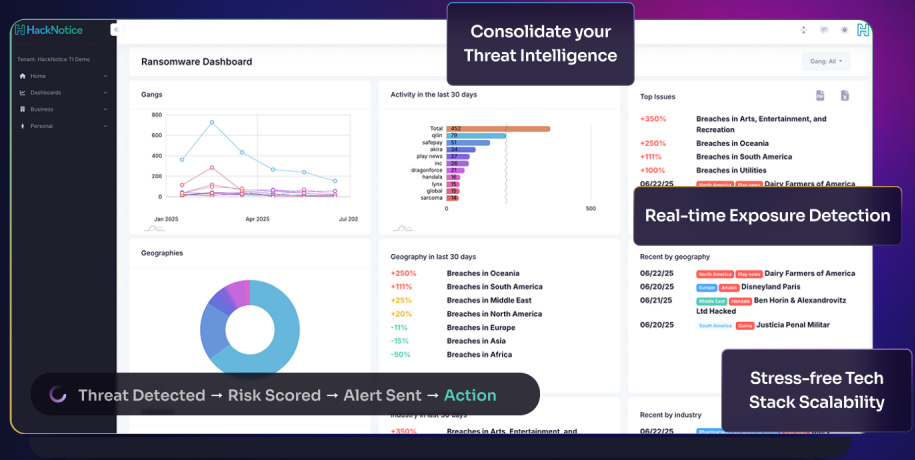


REAL TIME BREACHES & ATTACK DATA

Full-Spectrum Threat Intelligence For The Healthcare Industry



Defend your users, workforce, and patients with continuous dark web intelligence tailored for fast-moving healthcare businesses.

Healthcare organizations face constant threats from actors seeking to exploit exposed credentials, malware-infected systems, and vulnerable vendors. With the healthcare sector seeing a sharp rise in ransomware attacks and data extortion campaigns, protecting sensitive patient data and maintaining operational uptime is more critical than ever.

HackNotice provides real-time, actionable intelligence to help your security team detect risk early, reduce exposure, and respond swiftly to emerging threats.

From safeguarding PHI to protecting clinical systems, HackNotice strengthens your security posture with always-on threat detection tailored to the needs of modern healthcare organizations.

Within days of onboarding, HackNotice will

- ✓ Detect and monitor for compromised dark web attack data and users infected with infostealer malware.
- ✓ Provide continuous threat monitoring and real-time ransomware & data breach alerts for your supply chain.
- ✓ Analyze regional and global ransomware and data breach trends within the healthcare industry

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

Protect Patient Accounts

Monitor for patient credentials leaked from your platform or reused elsewhere, enabling rapid response to prevent account takeover (ATO), fraud, and unauthorized access.

Monitoring Employee & Staff Assets

Identify leaked admin credentials, sensitive healthcare data, and patient records exposed on the dark web or paste sites—preventing unauthorized access and IP theft.

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.