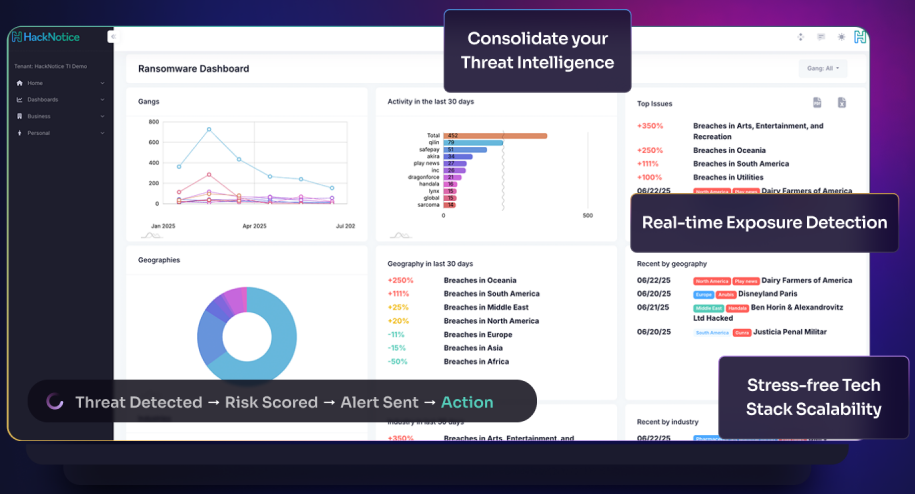
HackNotice

REAL TIME BREACHES & ATTACK DATA

Full-Spectrum Threat Intelligence For The Public Sector



Defend your workforce and public systems with continuous dark web intelligence tailored for government agencies and critical infrastructure.

Government agencies and public sector organizations face persistent threats from nation-state actors, cybercriminals, and hacktivists targeting exposed credentials, vulnerable infrastructure, and third-party service providers. As ransomware and data extortion attacks continue to disrupt public services, safeguarding citizen data and ensuring operational continuity is mission-critical.

HackNotice delivers real-time, actionable intelligence to help security teams detect threats early, reduce exposure, and accelerate incident response. Support compliance with federal cybersecurity mandates such as NIST and FISMA, while strengthening your resilience.

From securing employee credentials to protecting critical systems, HackNotice empowers public sector organizations with always-on visibility into emerging cyber risks.

Within days of onboarding, HackNotice will

- **Detect and monitor compromised dark web data and users infected with infostealer malware.**
- **Deliver continuous threat intelligence and real-time alerts on ransomware and supply chain breaches**
- **Strengthen your dark web hunting and incident response with search access to our extensive index.**

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

Protect Government Owned Accounts

Monitor for leaked government credentials from platforms and systems in active use, enabling rapid response to prevent account takeover (ATO), fraud, and unauthorized system access.

Monitoring Employee & Agency Assets

Identify exposed credentials and sensitive agency data found on the dark web or leak sites—reducing the risk of unauthorized access, espionage, and service disruption.

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.