Logically
CYBER FIRST. FUTURE READY.

Dark Web Monitoring

Cybercriminals don't always break in—they log in.

Stolen credentials, impersonation domains, and hacker chatter on the dark web create a silent, growing risk for mid-market organizations. By the time you hear about it from law enforcement or a breach disclosure, it's too late.

Logically's Dark Web Monitoring delivers pre-breach awareness with real-time alerts and human-led threat analysis. It spots compromised credentials and impersonation activity tied to your organization—before attackers strike.

Integrated with SecureCare. Available standalone. Powered by Dark Web ID™.

WHAT YOU'LL GAIN

Actionable Insight. Real-World Intelligence. Faster Response.

- **Credential Compromise Alerts**
  Detects leaked usernames and passwords tied to your domains.
- **Threat Actor Intelligence**
  Surfaces dark web mentions tied to your people, systems, and infrastructure.
- **Proactive Dark Web Scanning**
  Crawls botnets, marketplaces, IRCs, and hidden services like Tor, I2P, Freenet.
- **Integrated Risk Reporting**
  Real-time alerts plus monthly executive reports for threat tracking and trend insight.
- **Human-Led Monitoring**
  Security analysts validate, prioritize, and triage alerts to cut through the noise.
- **Pre-Breach Awareness**
  Spot and stop credential threats before attackers exploit them.

KEY DIFFERENTIATORS

640,000+
botnets scanned daily

80,000+
compromised emails tracked per day

KEY DIFFERENTIATORS

76%
of users reuse passwords across accounts

60%
of SMBs close within 6 months of a major breach

WHO IT'S FOR

SMBs and mid-market orgs with phishing, identity, and insider threat exposure

Healthcare and financial services firms under compliance security

IT and InfoSec teams managing multiple accounts, tools, and identity platforms

Customers bundling Logically's MDR or SecureCare with proactive credential defense

WHAT'S INCLUDED

- 24/7/365 scanning across the dark web, forums, marketplaces, and hacker chatrooms
- Deep surveillance of Tor, I2P, Freenet—no risk to your systems
- Alerts for leaked credentials, spoofed domains, and active threat chatter
- Monthly threat reports with risk scores and context
- Healthcare-specific insight (PHI targeting, ransomware trends, insider threats)
- Fully cloud-based—no agents, no infrastructure, no complexity

RESULT

- Prevented unauthorized access to core financial systems
- Avoided costly disclosure and compliance penalties
- Gained visibility into credential risk across all users

USE CASE SNAPSHOT

A regional investment firm subject to SOC 2 and SEC oversight turned to Logically for help identifying silent identity risks before they triggered a compliance incident.

Logically's Dark Web Monitoring flagged multiple compromised employee credentials linked to third-party logins—including one with administrative access to a cloud-based trading platform. Within 48 hours, all accounts were secured, MFA was enforced across systems, and security awareness training was issued to impacted staff.

Logically. Cyber-First. Future Ready

www.logically.com hello@logically.com