RAPID7

SERVICE BRIEF

MANAGED DIGITAL RISK PROTECTION

Proactively protect your digital assets from external threats across the clear, deep, and dark web.

Rapid7's Managed Digital Risk Protection (DRP) gives organizations the power to anticipate and disrupt threats before they escalate into business-impacting events. Our team of specialized analysts provides continuous monitoring across the clear, deep, and dark web, surfacing the earliest warning signs of an attack across stolen credentials, leaked data, phishing domains, ransomware exposures, and criminal chatter. By cutting through the noise and delivering only verified, actionable intelligence, we help you understand where your organization is most at risk and move quickly to neutralize threats. With Rapid7 Managed DRP, you gain confidence that your external attack surface is being watched around the clock, so you can stay ahead of adversaries and focus on what matters most: driving your business forward.

Key Customer Benefits

1. **Spot threats before they strike:** Catch the earliest signs of a cyberattack, such as leaked or for-sale credentials, phishing domains and websites, or criminal chatter, to prevent breaches before they escalate.
2. **Get certainty around ransomware exposure:** Monitor ransomware leak sites and dark web activity to know exactly when and how your organization's data has been compromised.
3. **Eliminate threats quickly and effectively:** Rapidly remediate issues and coordinate takedowns of malicious infrastructure to minimize exposure and reduce attacker opportunities.
4. **Act with confidence guided by experts:** Rely on Rapid7's threat analysts to deliver verified and actionable intelligence that filters out noise and accelerates your response.

CHALLENGES OF THREAT DETECTION ACROSS THE EXTERNAL ATTACK SURFACE

Difficult to navigate the entirety of the clear, deep, and dark web - particularly restricted forums and channels	Challenging to effectively act on insights and operationalize ecosystem to eliminate external threats quickly
Lacking specialized skill sets to triage external threat alerts and access details to determine severity and priority	Disparate, point solutions amplify noise and false-positive alerts for already-constrained teams

Pinpoint threats at the beginning of the kill chain to prevent an attack

With Managed DRP, customers gain broad and deep external attack surface monitoring with experts who know how to navigate restricted channels and exclusive dark web forums. Our expert analysts extend your team and reliably identify real threat signals and enable your team to anticipate and cut off attacks before they can have a broader impact for your organization.

Organizations use Managed DRP to stay ahead of attackers and reduce business risk in critical ways:

Credential & Data Leakage: Detect exposed logins and sensitive information posted online.

Phishing & Brand Abuse: Identify phishing domains, lookalike sites, and brand misuse.

Ransomware Exposure: Monitor leak sites to know when your data has been compromised.

Dark Web Monitoring: Access restricted forums and marketplaces for early threat signals.

Malicious Infrastructure Takedown: Remove rogue domains and attacker assets quickly.

VIP Protection: Safeguard executives from impersonation, doxxing, and targeted attacks.