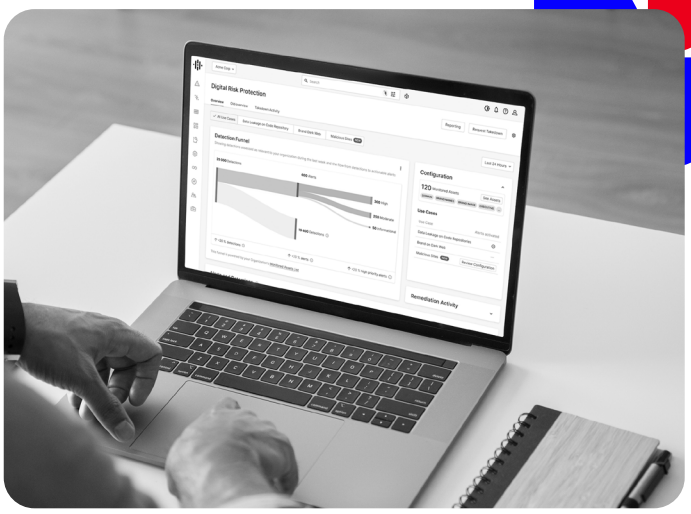
Recorded Future® | DATA SHEET

Digital Risk Protection

Defend your brand, workforce, and customers from threats outside your security perimeter



External threats target your most exposed attack surface

Your brand appears across domains, social media, code repositories, app stores, and the dark web. This creates your most exposed attack surface. Attackers exploit this exposure using AI and other sophisticated techniques to generate convincing phishing sites and synthetic identities at scale, contributing to over $12.5 billion in annual fraud losses, with impersonation scams among the top categories.

Traditional security tools often can't see beyond your network perimeter, leaving these threats undetected. Effective defense requires continuous monitoring across the full external landscape, intelligent prioritization that helps teams act on what matters most, and reporting that proves security outcomes to leadership.

Comprehensive Protection Across Several Use Cases

1. **Malicious Site Monitoring:** Phishing domains, typosquats, and fraudulent websites.
2. **Impersonation Monitoring:** Fake executive profiles and brand impersonation on social media and professional networking platforms.
3. **Code Repository Monitoring:** Source code, proprietary information, and sensitive data in code repositories.
4. **Dark Web Brand Monitoring:** Threats discussed on underground forums, marketplaces, and ransomware sites.
5. **Public Brand Monitoring:** Brand references and potential threats across the open web.
6. **Employee Credential Monitoring:** Compromised employee credentials from infostealer malware.
7. **Customer Credential Monitoring:** Available as an add-on to extend protection to your customer base.

Why Digital Risk Protection?

Recorded Future Digital Risk Protection (DRP) monitors nearly everywhere your brand appears, alerts intelligently on threats that require action, and provides one unified workflow from detection through takedown. Built on the Intelligence Graph®, DRP delivers the comprehensive coverage, actionable intelligence, and executive reporting needed to better protect your brand and avoid financial loss.

Top Benefits

- **Manage everything in one workflow:** Unified hub for asset management, Alert configuration, threat triage, and takedown coordination provides seamless end-to-end workflow.
- **See your complete brand exposure across every channel:** Coverage across domains, social media, app stores, code repositories, and dark web ensures reduced blind spots in digital footprint monitoring.
- **Receive alerts that signal real threats:** Intelligent alerting surfaces threats your team should act on, with clear prioritization and context.
- **Triage at the speed of attack:** Complete evidence and context in one view enables response in minutes instead of hours.
- **Prove security impact to leadership:** Reports showing detections, actions taken, and trends demonstrate security value to leadership.
- **Prevent account takeover and fraud:** Direct access to active infostealer malware logs enables response within hours of credential theft.

Level Up Your Digital Risk Protection Program with Recorded Future

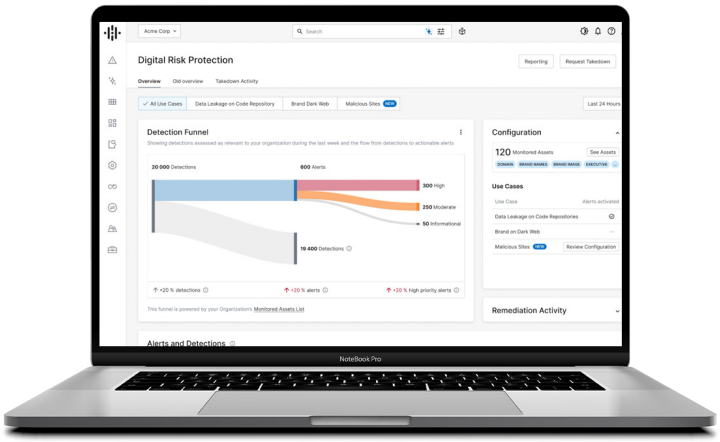
The Challenge	Our Advantage
Alert overload vs incomplete coverage Monitoring everything often means drowning in noise.	• Six clear Alert categories help teams cut through noise • Monitor all threats continuously while receiving Alerts only on risks that need response • Smart asset discovery ensures comprehensive coverage • Control what becomes an Alert with configurable settings for each use case
Slow triage, fast attacks Investigation can take hours while threats spread in minutes.	• Investigate and respond from one workspace with all evidence and actions in one place • Every Alert includes full evidence, risk logic, and recommended actions • One-click takedown coordination accelerates response
Can't prove security value Unable to demonstrate ROI or justify investment to leadership.	• Automated monthly, quarterly, and annual reports show detections, actions taken, and threats stopped • Managed services available to accelerate resolution and maximize impact • Manage brand and identity threats in one platform

Who it's For and How it Works

Digital Risk Protection serves teams responsible for protecting brand reputation, customer trust, and organizational assets from external threats. Whether in security, trust & safety, risk management, fraud prevention, or brand protection, teams get comprehensive coverage, intelligent alerting, and unified workflows to defend your digital footprint.

- **Monitor continuously:** Track domains, social media, app stores, code repositories, marketplaces, and dark web across surface, deep, and dark web sources
- **Detect intelligently:** Only actionable threats become Alerts across six use cases
- **Act efficiently:** Automated workflows from detection through takedown coordination

Your brand is your most exposed attack surface. Recorded Future Digital Risk Protection provides the continuous monitoring, intelligent alerting, and unified workflows needed to protect it across every channel where threats emerge.



> "We have improved brand protection by at least 100%... as we automate more coverage, we have saved hundreds of labor hours per quarter and improved efficiency."
>
> *Joe Azzouggagh, Manager of Trust and Safety, Ruby*