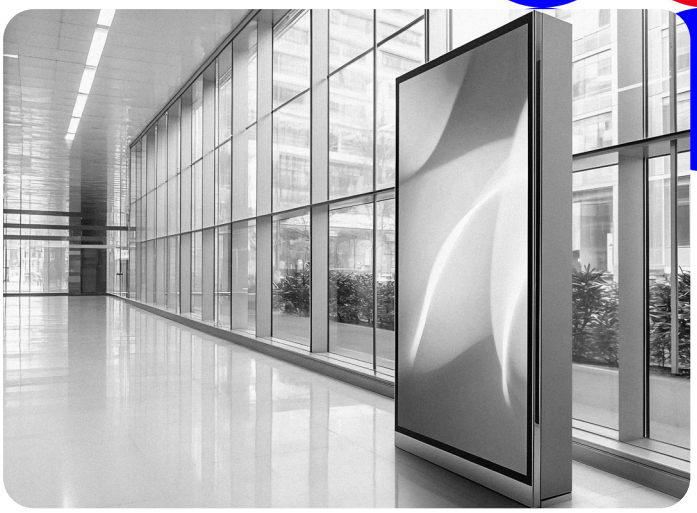
Recorded Future® | DATA SHEET

Brand Intelligence

Proactively Protect Your Brand From External Threats



Challenge

Phishing campaigns, data leaks, executive impersonation, and other forms of brand attacks pose immediate risk to your company, all while operating entirely outside your network. To mitigate these threats to your company, executives, employees, and customers, you need to monitor and find malicious entities in real time — and then act quickly to take them down.

Solution

Recorded Future's comprehensive Brand Intelligence and takedown services use a unique collection approach that aggregates data from an unrivaled breadth of open, dark, and technical sources, providing full visibility into brand threats like phishing campaigns, data leaks, and executive impersonation.

Real-time alerting enables you to instantly discover leaked credentials, typosquat domains, code leaks, discussion of your brand on dark web markets, and more. Immediately initiate takedowns directly within Recorded Future after identifying fraudulent domains or stolen assets that could pose a risk to your brand.

Benefits

- Access comprehensive, real-time intelligence and Alerts across dark web, social media, and closed forums to detect and stop brand attacks before they cause damage.
- Identify and take down attacks targeting your company, executives, employees, and customers.
- Focus resources on the most pressing threats through automated risk scoring and deep context, enabling faster response to impersonation, phishing attempts, and more.
- Monitor emerging threats across your attack surface and rapidly initiate takedowns of typosquats and brand abuse to protect your reputation and your customers from fraud.

Use Cases

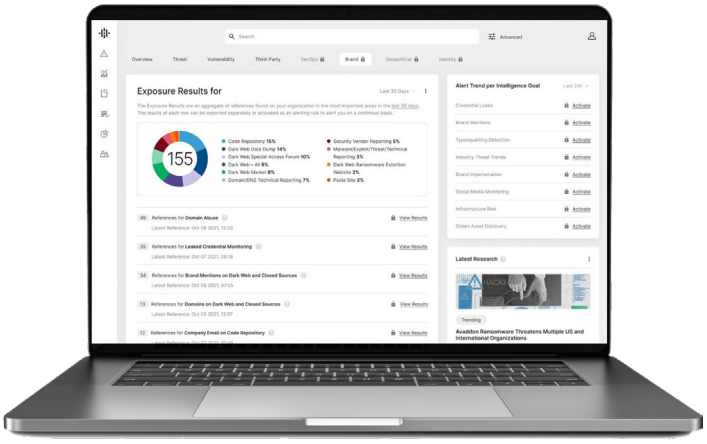
- Domain Abuse Detection
- Data & Credential Leakage Monitoring
- Dark Web Monitoring
- Brand Attack Mitigation
- Executive Impersonation Detection
- Digital Asset Monitoring
- Industry Threat Monitoring

33%
Average savings on brand abuse mitigation efforts using Recorded Future

$371,263
in savings due to business and brand risk reduction impact annually using Recorded Future

Results

Comprehensive source coverage	Monitor your brand across millions of open web, dark web, and technical sources in all languages including DNS records, social media, messaging platforms, paste sites, mobile app stores, and more.
Real-time alerting	Get instant notifications with context and recommended actions on brand threats including stolen assets, brand mentions, credential leaks, typosquat domains, and infrastructure risk.
Risk prioritization	Focus on critical threats using automated risk scoring and contextual insights for each detected incident.
Brand impersonation detection	Detect infringing content including unauthorized logo usage and fake mobile apps, which are often linked to phishing or account-harvesting attacks.
Domain abuse defense	Automatically identify and monitor newly registered domains that could impersonate your brand through typosquatting or similar domain techniques.
Data and credential leak monitoring	Monitor dark web forums, paste sites, and code repositories for exposed employee credentials, PII, source code, and sensitive company data to prevent unauthorized access.
Brand attack monitoring	Track malicious brand mentions across the open web, dark web, social media, and closed underground forums.
Executive impersonation detection	Monitor professional networking websites like LinkedIn to detect fake executive profiles.
Industry threat insights	Proactively track emerging threats targeting your industry and peer organizations.
Takedown services	Initiate rapid takedowns of fraudulent domains, phishing sites, and other brand abuse incidents.



See Brand Intelligence in action

Request a demo to learn how you can make fast, effective, data-driven decisions with Recorded Future.

"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 **(UserEvidence)**

"Having the ability to monitor for typosquat domains has protected us so much. We've had so many site impersonations that we had to act on. Recorded Future has enabled us to detect about six typosquatting domains per year—something we could never do before."

Judy Mayoral
Cybersecurity Manager, Hughes Federal Credit Union
(Case Study)