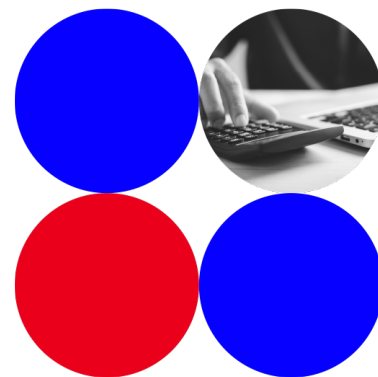


# Recorded Future's Predictable Pricing Scales with You

Packages built to grow as you mature your intelligence.



Cyber Operations				
Anticipate, prevent, and disrupt threats proactively. Hunt, detect, and respond autonomously.				
Feature	Description	Core	Professional	Elite
Monitor & Prioritize Threats & Vulnerabilities	Monitoring across open, technical, deep and dark web sources and generate detailed threat reports to keep stakeholders intelligence-led	✓	✓	✓
In-Depth Malware Insights	Analyze malware families, campaigns, and infrastructure along with a high-volume sandbox environment.	✓	✓	✓
Alert Triage & Threat Detection	Automatically enriches every Alert with threat actor context, campaign intelligence, and procedural IOC analysis.	✓	✓	✓
Intelligence-Driven Defense	Get ahead and stay ahead of threats with finished intelligence, automatic Watch Lists, and ready-to use detection rules.	✓	✓	✓
Autonomous Threat Hunts (NEW!)	Autonomously hunt threats across your entire security stack with built-in guidance for IoCs, malware, and threat actor TTPs, that dynamically updates to the changing threat priorities		✓	✓
Continuous Threat Monitoring (NEW!)	Monitor for future indicator activity and run simultaneous detections across multiple tools		✓	✓
Automated Threat Preventions (NEW!)	Deploy malicious indicators for blocking directly to security tools with an intelligence-led, risk rules and scoring based approach.		✓	✓
External Intelligence Ingestion (NEW!)	Unify threat analysis across Intelligence Graph® data, ISACs, and third-party feeds through multi-source ingestion and correlation		✓	✓
Digital Risk Protection				
Defend your brand, workforce & customers from threats outside your security perimeter				
Feature	Description	Core	Professional	Elite
Malicious Sites Monitoring	Detect phishing domains, typosquats, and fraudulent websites targeting your brand to enable rapid takedowns before customer impact.	✓	✓	✓
Code Repository Monitoring	Detect source code leaks, API keys, proprietary information, and sensitive company data in code repositories to prevent intellectual property theft and data exposure.	✓	✓	✓
Executive Impersonation Monitoring	Detect fake profiles impersonating executives or your brand on social media and professional networks to prevent social engineering and reputational damage.	✓	✓	✓
Dark Web Monitoring	Monitor underground forums, marketplaces, and ransomware sites for brand mentions and threat discussions to detect planned attacks before execution.	✓	✓	✓

Feature	Description	Core	Professional	Elite
Public Brand Monitoring	Track brand references across news sites, blogs, and the open web to detect emerging threats, fraud attempts, and unauthorized brand usage.	✓	✓	✓
Employee Credentials Monitoring	Detect compromised employee credentials from active infostealer malware logs to prevent account takeover.	✓	✓	✓
Digital Risk Hub (NEW!)	Unified hub and seamless workflows covering brand exposure across channels with reports demonstrating security outcomes	✓	✓	✓
External Asset Discovery	Continuously discover and analyze forgotten assets, shadow IT, subsidiaries, and third-party infrastructure tied to your organization		✓	✓
Prioritize external vulnerabilities	Proactively discover exploitable vulnerabilities, misconfigurations, and out-of-policy assets to help organizations reduce business risk		✓	✓

### Third-Party Risk

Detect third-party cyber threats before they disrupt business operations, expose data, or damage trust

Feature	Description	Core	Professional	Elite
Vendor-Specific Threat Exposure	Access on-demand profiles of third-party vendors to aid in vendor selection, re-evaluation, and investigation			✓
Accurate Risk Ratings	Evaluate vendor security posture with objective, evidence-based risk ratings.			✓
Continuous Risk Monitoring	Monitor vendors and receive Alerts for breach activity, credential leaks, and ransomware mentions.			✓
Vendor Action Plans	Select issues to share with third parties using the collaboration portal, and track remediation status.			✓
Third-Party Portfolio Risk	Visualize risk across your third- and fourth-party ecosystem including concentration risk.			✓

### Intelligence Platform

Intelligence foundation for complete protection

Feature	Description	Core	Professional	Elite
Intelligence Graph®	Source collection from over 1M sources including open web, deep web, dark web, technical sources, customer telemetry, malware intelligence, network data, and Insikt Group® Research.	✓	✓	✓
Recorded Future AI	Natural language conversations, intelligence summarization, report writing, and MCP support.	✓	✓	✓
Ecosystem Integrations	100+ integrations across SIEM, SOAR, EDR, IAM, and ticketing platforms.	✓	✓	✓
Collective Insights	Unattributable aggregated threat intelligence from the Recorded Future customer community.	✓	✓	✓

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,900 businesses and government organizations across more than 80 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at [recordedfuture.com](https://recordedfuture.com)