Recorded Future®

Recorded Future Solutions to Reduce Risk

In today's ever-evolving threat landscape, organizations must adopt a proactive approach to stay one step ahead of risks. Threat intelligence serves as the essential force multiplier for the modern security stack, empowering organizations to effectively mitigate cyber attacks by leveraging valuable insights to swiftly respond and take necessary actions.

Recorded Future has a comprehensive portfolio of solutions that help organizations reduce risk, no matter your IT & security stack, maturity journey, or industry.

Ransomware Mitigation

66% of organizations were hit by ransomware in the last year (Sophos), leading to business disruption, theft of sensitive data, and more. In addition, extortion amounts have increased as attackers focus more on quality than quantity.

Challenges

- Attack surface visibility
- Too many alerts
- Inability to easily track attackers

Recorded Future helps proactively defend against multiple initial access vectors for ransomware actors, such as exploitation of vulnerable technologies, stolen credentials, and first-stage malware.

Outcomes

- Proactive ransomware mitigation
- Operational and financial risk reduction

Increase Efficiency
Recorded Future clients report being
48% faster at identifying a new threat than before

Automate Security Workflows

Threat actors have an advantage, they only need to get it right once. Conversely, security teams have a lot on their plate and struggle to keep up with the changing threat landscape with tedious manual processes and not enough time or resources. In fact, only 33% of alerts received by SOC teams are investigated (Vectra).

Challenges

- Alert overload
- Lack of context
- Disjointed workflows

Respond to threats more efficiently by automating the collection and distribution of intelligence in an actionable format. Integrated into your security tools and workflows, Recorded Future correlates and enriches internal data with external insights to accelerate threat identification, prioritization, and remediation.

Outcomes

- Increase ROI of security tools
- Improve detection and response

Increase Capacity
Recorded Future clients realize a **32%** increase in their teams' capacity

Mitigate Supply Chain Risk

Third-party vendors are critical components for any business, helping to increase efficiency, spur innovation, and lower costs. However, each vendor introduces potential threats to your organization, and many third-party risk management practices take a static approach to assessing risk.

Challenges

- Static risk assessments
- Insight into product-specific risk
- Limited visibility to third- and fourth-parties
- Location-based risk monitoring

Recorded Future helps organizations reduce vendor risk by monitoring critical data sources for signs that an organization’s supply chain partners and software vendors have been compromised or are vulnerable. Real-time alerting and context enables effective decision-making to reduce supply chain risk.

Outcomes

- Reduce vendor risk
- Enable digital and physical business expansion
- Ensure compliance

Monitor Third Parties

Recorded Future clients report being able to monitor **35%** more third parties than before

Exposure Management

Using cloud-based resources is essential for driving business growth, but also puts your external attack surface in a constant state of change. This can lead to hundreds of exposed or poorly managed assets, greatly increasing the risk of a cyberattack.

Challenges

- Manual Scanning
- Limited prioritization and ease of remediation

Reducing your vulnerable attack surface, requires continually evaluating the accessibility, exposure, and exploitability of digital assets. Adding Recorded Future to your defensive strategy makes it possible to identify and inventory external assets, prioritize remediation efforts, and accelerate fixing risky exposures.

Outcomes

- Real-time attack surface discovery
- Secure business growth

Attack Surface Reduction

A Recorded Future client saw a **51%** reduction in their overall vulnerable attack surface within 6 months

Digital Risk Protection

Growing digital estates create challenges for organizations to secure their digital assets and data from external threats such as brand and executive impersonation, account takeovers, and data leakage.

Challenges

- Limited external visibility
- Complex triage and remediation

Leverage insights and contextual information from both open and closed sources to actively identify, analyze, and quickly mitigate potential external threats, such as brand impersonation or compromised employee credentials, that may impact your organization’s reputation and employee safety.

Outcomes

- Brand and digital asset protection
- Digital transformation acceleration
- Reduce risk of operational downtime and brand impairment

Understand Digital Footprint

85% of clients report having a better understanding of their digital footprint