Recorded Future® | DATA SHEET

Recorded Future Malware Intelligence

Transform threat hunting from reactive to proactive

Challenge

Traditional threat hunting falls behind with malware threats hiding for an average of 10 days

- **44%** of CISOs reported missing data breaches with existing security tools[1]
- **10 days** average dwell time for threats in 2024
- **93%** of malware hides in data-in-transit
- Manual malware analysis is resource-intensive and requires specialized expertise
- Threat actors constantly evolve TTPs to evade detection
- Traditional sandboxes provide limited behavioral visibility

Solution

Intelligence-Native Malware Defense: From Isolated Detection to Automated Prevention

Recorded Future's Malware Intelligence connects every sample to our Intelligence Graph's 15+ years of threat data, allowing you to understand malware lineage, predict its evolution, and automatically generate protections—providing complete context and automated defenses in seconds rather than days.

Powered by the World's Largest Intelligence Graph

- Intelligence Graph correlation **with 1.5M+ unique malware samples analyzed daily**
- **90,000+** actively monitored command and control servers
- Recorded Future's **Intelligence Graph** with 200B+ nodes built over 15 years

1.5M+
unique malware samples analyzed daily

90,000+
actively monitored command and control servers

200B+
nodes built over 15 years

[1] https://www.darkreading.com/cloud-security/cisos-throwing-cash-tools-detect-breaches

Key Capabilities

NEW Malware Hunting

- AI-powered malware analysis with natural language querying
- Deep dive into static and dynamic behaviors without complex queries
- Analyze trends and changes in malware over time

NEW Auto YARA Rules

- Instantly generate detection rules for new and emerging malware
- Validate rules against known good filesets to prevent false positives
- Apply at scale across file systems, email, and downloaded binaries

NEW Malware Alerts

- Transform threat hunts from reactive to proactive with real-time alerts
- Create, manage, and refine custom detection rules through intuitive interface
- Spot emerging threats before they become problems

ENHANCED Sandbox

- Detect, observe, and detonate malware in a controlled environment
- Get full sandbox report details in the dashboard
- Understand malware impacts through direct observation

ENHANCED Data

- Access the world's largest structured malware dataset
- Gain context from Intelligence Graph enrichment
- See relationships across the threat landscape

ENHANCED APIs

- Connect all systems and workflows
- Run searches via natural language
- Integrate alerts into existing security tools

Business Impact

Contain and respond to threats faster

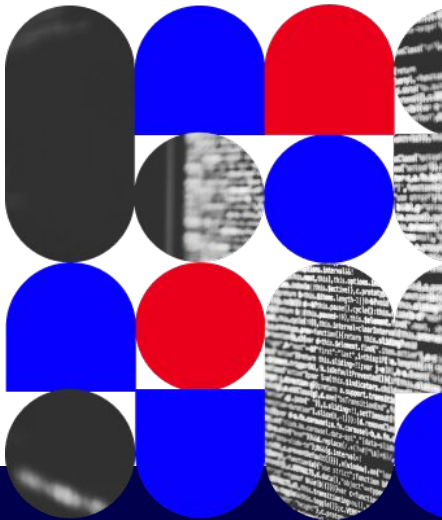
- Reduce 10-day dwell times to potentially hours or minutes
- Find and flag new variants before they impact your systems
- Speed up research and analysis workflows

Scale threat hunting through automation

- Empower your security team to punch above its weight
- Eliminate hours of manual rule-writing with Auto YARA
- Enable junior analysts with natural language querying

Shift from tactical hunting to strategic analysis

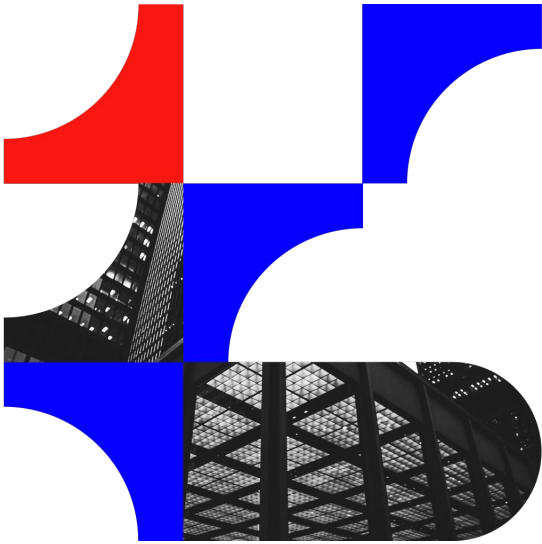
- Get a 360° view of the threats that matter most
- Connect the dots between internal and external events
- Establish a proactive security posture



Customer Outcomes

- Reduction in time spent analyzing malware samples
- Faster deployment of protective controls
- Improvement in malware variant detection
- Decrease in successful malware infections

The average team saves 11 hours saved weekly on threat analysis, hunting, and reporting efforts with Malware Intelligence (Source)

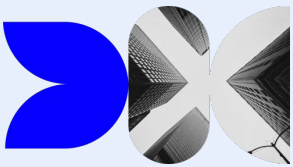


Get Started Today

Available now as part of the Threat Intelligence Module

- See it in action at RSA Conference 2025
- Request a personalized demo
- Contact your Recorded Future representative for more information

For customers that have requirements exceeding daily usage limits, additional fees may apply.



Recorded Future: The World's Largest Intelligence Company

Secure your organization with Threat Intelligence that focuses on what matters most to your business.

"Recorded Future's Malware Intelligence has transformed the way we hunt threats. With natural language processing, we can search in plain English, easily map TTPs, with the option for analysts to build both broad and targeted queries, and identify adversaries using similar tactics. It helps us move beyond IOCs to gain a deeper understanding of threats—strengthening our defenses and streamlining threat hunting."

Mark Paranto, Cyber Defense Senior Threat Hunter, **SAP**