

Information Security White Paper

Table of Contents

Introduction.....2

The Intelligence Cloud Platform.....2

Customer Data Collection and Handling.....3

 Network and Data Access Security.....4

 User Access Control.....4

 Network and System Security.....4

 Data Storage and Encryption.....5

 Logging and Monitoring.....5

Operational Security.....5

 Information Classification.....5

 Software Development Life Cycle and Change Management.....5

 Incident Management.....6

Compliances.....6

Introduction

Recorded Future is the most comprehensive and independent threat intelligence cloud platform in the world. It enables organizations to identify and mitigate threats across cyber, supply chain, physical, and fraud domains. It is trusted by clients of all sizes and sectors worldwide to provide real-time, unbiased, and actionable intelligence.

In such a system, it is vital to distinguish between information that must be protected and information that should be made available. This paper provides an overview of Recorded Future's system for managing information security, including principles, policies, and methods.

"Always act ethically" is a core value at Recorded Future. The company's approach to data security is guided by these principles:

- **Confidentiality:** Ensure that only authorized persons have access to information.
- **Integrity:** Safeguard the accuracy and completeness of information itself and the processes that handle it.
- **Availability:** Ensure that authorized users have access to the information they require, when they require it.
- **Privacy:** Ensure that data is handled in compliance with applicable laws, contracts, and internal policies.

Additionally, Recorded Future is a key customer of its own services, employing them in concert with conventional security technologies and practices to create a comprehensive security program that safeguards the business.

The Intelligence Cloud Platform

All Recorded Future offerings are built on the Intelligence Cloud Platform. The Platform indexes unstructured information from the open web as well as the dark web, technical web, social media, underground forums, and customer provided sources, among others.

At the heart of the platform, the Intelligence Engine analyzes this raw information using multiple methods, including machine learning and natural language processing, as well as expert human analysis. References to significant entities in the data, such as evidence of a planned cyberattack, are evaluated for frequency of occurrence, credibility, correlation with other entities, and other factors.

Applications powered by the Intelligence Cloud Platform provide insight into existing security vulnerabilities, awareness of past and current trends and events, and statistical predictions of probable future threats.

Customers access the Intelligence Cloud Platform in the following ways:

- Recorded Future Web-Based Portal
- Recorded Future's Browser Extension
- Recorded Future's Mobile Application
- Recorded Future's Connect Application Programming Interface (API) that can power multiple third-party software integrations

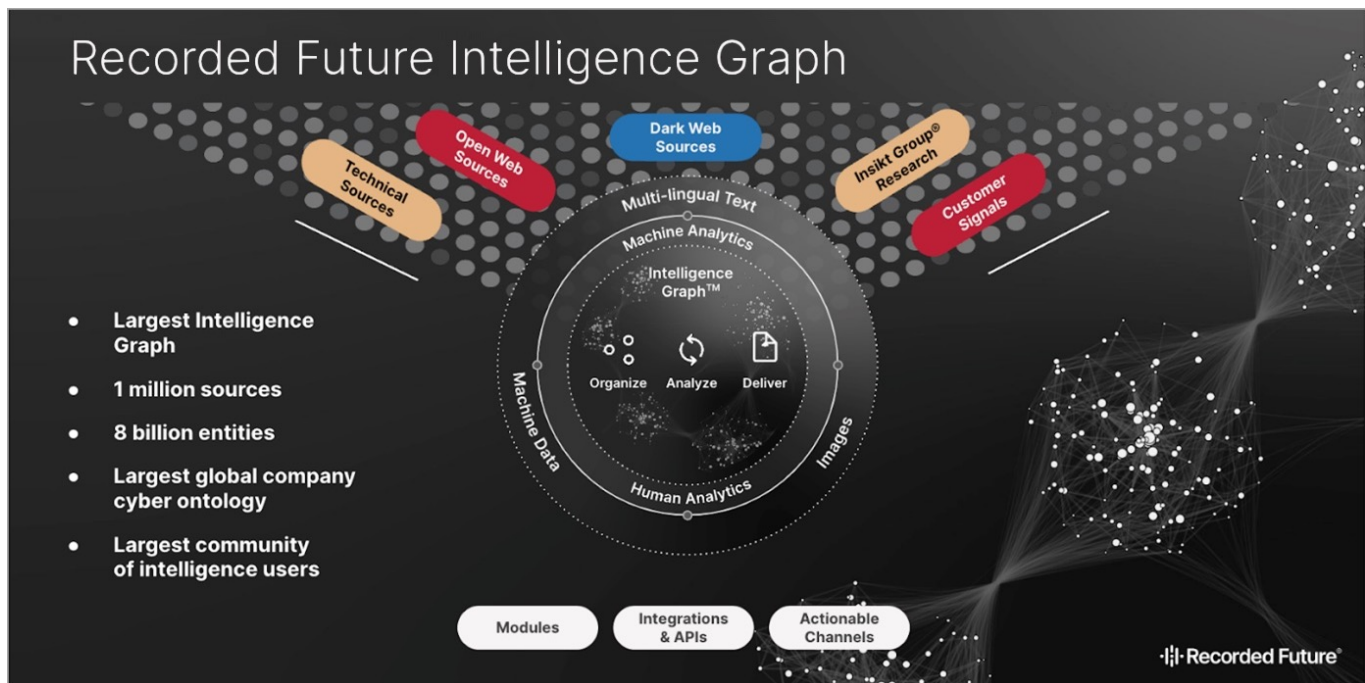


Figure 1: Intelligence Engine Data Collection and Analyzation Process

The Intelligence Cloud Platform is primarily hosted in a virtual private cloud (VPC) on Amazon Web Services (AWS). AWS data centers offer industry-leading physical and information security. The data centers are distributed globally and are not physically accessible by Recorded Future personnel.

The Recorded Future network comprises multiple subnets, with a public subnet as a single point of access from the Internet. The servers that host Customer Data can only be accessed through a VPN with hardware-based multi-factor authentication (MFA).

Customer Data Collection and Handling

The Intelligence Cloud Platform collects, processes, and surfaces available information to identify the clients' potential threats and vulnerabilities.

To the extent applicable, Recorded Future securely keeps billing information and credentials confidential and protected.

Recorded Future also stores and protects certain Customer Data related to the use of its products, including:

- Sandbox submissions
- Saved Queries and Alerts
- User-generated Analyst Notes
- Observed Correlations and Notes
- Reports
- Watch Lists and other Lists

This data is used to provide services and product features such as the search history and user-configured alerts.

Recorded Future also uses unattributed Customer Data to improve its products, providing development teams with insight into the most-referenced types of data, where to concentrate research efforts, and ideas for potential feature improvements.

When a customer terminates their subscription to Recorded Future products, all stored Customer Data is either deleted or rendered unattributable.

Recorded Future does not share Customer Data with any unaffiliated organization or individual except as required to:

- Provide the Services;
- Satisfy a valid law enforcement request or as required by law
- Enforce applicable Terms of Service, Terms of Use, or other contractual obligations
- Investigate a security or safety incident
- In case of emergency, to protect the property, safety, security, and rights of Recorded Future, its users, or the general public

To protect customer privacy, Recorded Future shares information as narrowly as possible when required to do so by law.

Network and Data Access Security

This section provides an overview of the practices and methods that Recorded Future uses to secure stored data and communications.

User Access Control

Clients generally access Recorded Future products using their own Identity-Provider Initiated single sign-on (SSO). Supported SSO technologies include:

- OpenID Connect (OIDC)
- SAML v2.0
- Auth (via Google)

To the extent technically feasible, Recorded Future also requires multi-factor authentication for all users (unless a client requests a specific exemption).

User passwords, if handled by the Recorded Future Platform instead of SSO, are stored as salted hashes, with robust length and complexity requirements.

The Platform automatically locks accounts temporarily after multiple unsuccessful login attempts.

Network and System Security

Recorded Future uses multiple complementary technologies and employs best practices to secure the network and connected systems, including:

- **The Recorded Future Intelligence Platform:** Used to track potential vulnerabilities, identify threat actors, and monitor both its own attack surface and the security of third-party partners.
- **Distributed Denial of Service (DDoS) mitigation:** Recorded Future employs best-in-class services to provide network and website protection against DDoS attacks, with rapid response to threats and robust network capacity.
- **Web application firewall (WAF) service:** Recorded Future employs an industry leading WAF to detect and block a variety of threats, including site scraping and brute force attempts.
- **Software and firmware patches:** Applied promptly and comprehensively to address vulnerabilities and maintain system security.

- **Secure system configuration:** Before a system is deployed into service, unnecessary functionality and default accounts are removed and audit logging and monitoring controls are set up. Each server performs a single primary function and has only the necessary services and protocols enabled.
- **Segmentation:** All network traffic is subject to firewall rules with a default deny posture. Only a minimum set of connections are approved.
- **Penetration Testing:** Recorded Future leverages the expertise of the security community by regularly conducting external penetration tests.
- **Bug Bounty Program:** Managed by HackerOne, the program incentivizes independent testing for reproducible security vulnerabilities, with an award structure based on severity.

Data Storage and Encryption

As a cloud-first business, Recorded Future relies on industry-leading hosting providers such as AWS to ensure the availability of stored data. Data is stored at geographically distributed facilities, with incremental and full backups created on a daily schedule.

All databases controlled by Recorded Future are encrypted, as are computers and other devices that store protected data.

All Customer Data is encrypted, both at rest and in transit:

- **Data at rest:** Encrypted using Advanced Encryption Standard (AES) 256-bit encryption
- **Data in transit:** Encrypted using Transport Layer Security (TLS) 1.2 or higher

Encryption keys are safeguarded by strict policies regarding their generation, storage, transmission, availability, and replacement.

Logging and Monitoring

Recorded Future monitors both the physical security of its facilities and its information systems, including Internet traffic and email.

Automatic logging and the routine review of a broad spectrum of system and network events enables the security team to maintain awareness of potential issues and address them quickly.

Operational Security

The topics in this section describe the internal policies and controls that Recorded Future implements to minimize the risk involved with data access, IT changes, and software development.

Information Classification

The Sensitive Data Policy categorizes data according to its level of sensitivity and defines the controls that apply to each category: Public, Internal Use Only, Confidential, or Restricted. This ensures that Recorded Future and its third parties abide by all legal, ethical, and operational obligations.

By default, all information (including Customer Data) is treated as Confidential until it is otherwise classified. Recorded Future trains its employees on how to properly manage sensitive data.

Software Development Life Cycle and Change Management

Changes to the company's technical environment follow a well-defined change management process that determines the necessary requirements for each individual change, including the necessary level of authority and other associated security measures required before implementation.

Recorded Future's software development life cycle (SDLC) policies are aligned with NIST 800-218 and ensure that new products and features are planned, designed, implemented, tested, and maintained according to security and industry best practices.

In addition, static and dynamic application security testing (SAST/DAST) tools are used to scan product code to identify potential issues and vulnerabilities.

Incident Management

The Incident Response Plan defines the roles and responsibilities for identifying potential security incidents, assessing their scope, and taking action to contain the incident and mitigate the harm. The plan is continually developed, with periodic testing, improvement, and personnel training.

The Computer Security Incident Response Team (CSIRT) comprises the CISO and other officers, security engineers, and cybersecurity experts from across the business.

Compliance

Recorded Future's compliance program monitors and enforces adherence to laws, regulations, and standards.

Recorded Future abides by all applicable laws when collecting data, including laws related to intellectual property and unauthorized access. Security policies are routinely subjected to legal review and updated as needed.

The Recorded Future SDLC program is ISO 27001/27701, 27017, 9001, and NIST 800-218 certified.

Additional Reading

Recorded Future Security FAQ

www.recordedfuture.com/faq/security