Bottomline

CFRM Product Overview Guide

Cyber Fraud and Risk Management

Version 6.8.0

July, 2022

Legal Statement

Bottomline Technologies Cyber Fraud and Risk Management

Version 6.8.0

Bottomline Technologies

Corporate Headquarters

325 Corporate Drive

Portsmouth, NH 03801 USA

Europe, Middle East, Africa

1600 Arlington Business Park

Theale, Reading, Berkshire RG7 4SA UK

APAC Headquarters

Level 3, 69-71 Edward Street

Pyrmont, Sydney NSW 2009, AU

60 Robinson Road

#15-01 BEA Building

Singapore 068892

Table of Contents

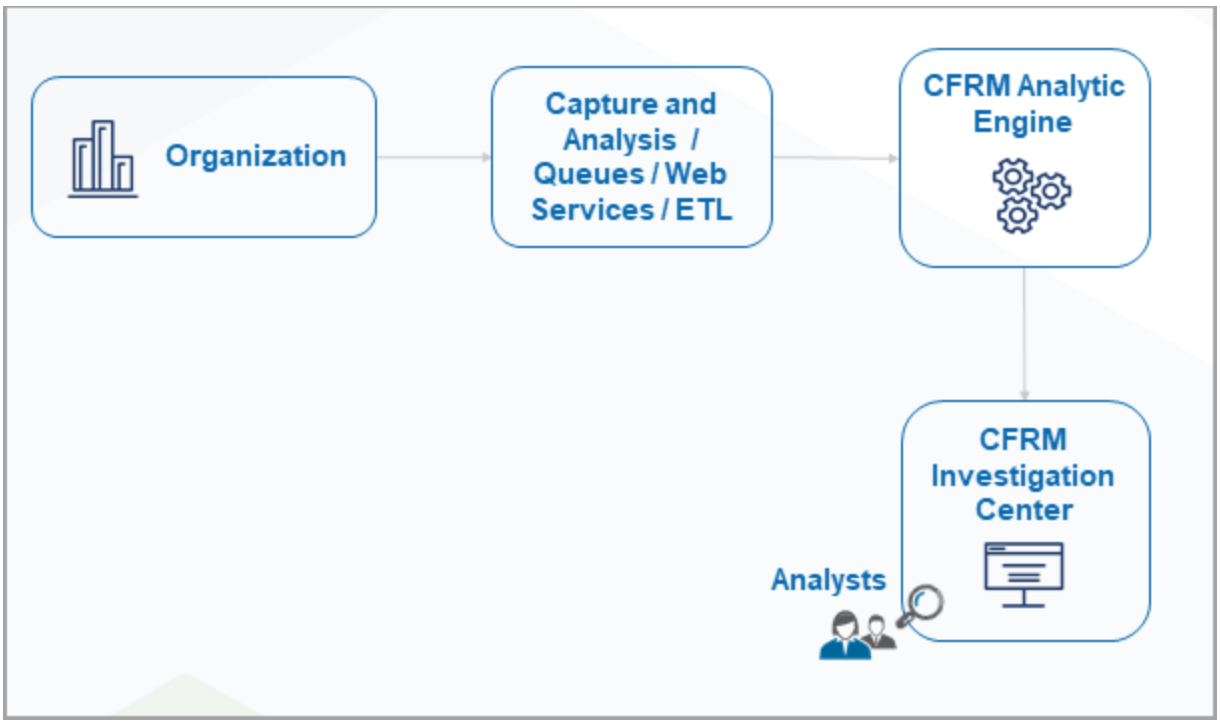
About This Guide

The *CFRM Product Overview Guide* outlines the **Cyber Fraud and Risk Management** platform, including the system's architecture, documentation, and supported infrastructure software. It also details the various solutions available, including an overview of the solution architecture and features.

1 Product Overview

Cyber Fraud and Risk Management (**CFRM**) provides a platform for end-to-end management of receiving and analyzing data, such as transactions, and then displaying the results of the analysis for investigation. The **CFRM** platform includes a component to capture and analyze network traffic (when working with sniffing), and an **Analytics Engine** server to analyze the data which is comprised of two main components, the **Rule Engine** and the **Investigation Center**.

The **Analytics Engine** can receive events from a variety of sources, such as the **Capture and Analysis Server**, web services and ETLs. After the data is received, the **Analytics Engine** is responsible for analyzing the data, identifying suspicious activity and generating alerts for investigation in the **Investigation Center**. The following diagram displays the flow of how data is processed through **CFRM**.



1.1 Built-In Solutions

CFRM includes a number of Solutions which are based on the capabilities provided by the platform. Each solution then expands on those features to provide an end-to-end solution for analyzing and investigating events that have occurred.

The **Banking Solutions** are designed to identify different types of attacks, usually with the intention to divert funds from customers' accounts into fraudsters' accounts, to identify money laundering activities, or to identify transactions that are not compliant with guidelines from regulatory bodies. This solution can be integrated with various payment systems, so that payments from a variety of applications, such as online banking and SWIFT systems, as well as payments carried out by banking personnel, are sent to the solution for real-time evaluation with the possibility of blocking high-risk transactions. In addition,

transactions are evaluated offline to identify suspicious behavior which could indicate money laundering or other types of fraud.

1.2 Solutions List

This section lists the different solutions available:

The **Banking Solutions** includes the **Secure Payments Solution** modules and the modules which evaluate transactions offline. The **Secure Payments Solution** is comprised of several modules each designed to interact with a specific banking system. The modules include:

- **Insider and Employee Fraud (IEF) Module**: Evaluates transactions performed by employees for potential fraud.
- **Record and Replay Module**: Records activity of internal and external users in the customer applications. The system reconstructs user sessions allowing fraud investigators, security officers and internal auditors to visually replay user sessions screen by screen.
- **Enterprise Case Management**: Includes a comprehensive solution for creating and managing cases of suspicious activity, and for filing SARs to the relevant authorities, including filing with the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). The **Enterprise Case Management** solution is preconfigured with US requirements for SAR reporting to FinCEN, and is compliant with the latest FinCEN requirements.
- **Watchlist Screening Module**: Screens transactions against global watchlists to ensure they are compliant with regulations. The solution matches customers and transactions against internal and imported watch lists (OFAC, HMT, PEP, etc.)
- **SWIFT Module**: This module is integrated with network gateway applications, such as SWIFT Alliance Access, where each payment instruction is sent to the solution for real-time evaluation with the possibility of blocking high-risk transactions.
- **Online Banking Module**: This module is integrated with e-banking systems, so each transaction a user makes is sent to the solution for real-time evaluation with the possibility of blocking high-risk transactions.
- **ACH Module**: Monitors batch payments in the ACH format from different banking applications. Each transaction is sent to the solution for real-time evaluation with the possibility of blocking high-risk transactions.
- **Bulk-ISO20022 Module**: Monitors batch payments in the ISO 20022 format. This module is integrated with network gateway applications, such as SWIFT Alliance Access, where each payment transaction is sent to the solution for real-time evaluation with the possibility of blocking high-risk transactions.
- **Bulk-FIN Module**: Monitors batch payments in FIN format. This module is integrated with network gateway applications, such as SWIFT Alliance Access, where each payment transaction is sent to the solution for real-time evaluation with the possibility of blocking high-risk transactions.
- **Fedwire Module**: Monitors Fedwire payments from different banking applications that generate messages in the Fedwire format. Each transaction is sent to the solution for real-time evaluation with the possibility of blocking high-risk transactions.
- **User Behavior Monitoring Module**: This module is integrated with network gateway applications, such as SWIFT Alliance Access, where each login and operation instruction is sent to the solution for real-time evaluation with the possibility of blocking or challenging high-risk transactions.

- **Sanction Case Management Module**: Enables managing cases which are opened by sanction screening message hits.
- **SIC and other Single ISO20022 Payments Module**: This module is integrated with network gateway applications, such as GTX Operation Transactions, where each payment transaction is sent to the solution for real-time evaluation with the possibility of blocking high-risk transactions.
- **Machine Learning Supervised Modules**: The following transactions can be evaluated by the Machine Learning Supervised Modules:
  - **ACH**: Activated if the **ML-Supervised-ACH** module is active.
  - **Bulk-ISO20022**: Activated if the **ML-Supervised_BULK-ISO20022** module is active.
  - **Fedwire**: Activated if the **ML-Supervised-FEDWIRE** module is active.
  - **Online Banking**: Activated if the **ML-Supervised-Online Banking** module is active.
  - **SWIFT**: Activated if the **ML-Supervised-SWIFT** module is active.
- **Machine Learning Unsupervised Modules**: The following transactions can be evaluated by the Machine Learning Unsupervised Modules:
  - **ACH**: Activated if the **ML-Unsupervised-ACH** module is active.
  - **Fedwire**: Activated if the **ML-Unsupervised-Fedwire** module is active.
  - **Online Banking**: Activated if the **ML-Unsupervised-Online Banking** module is active.
  - **SIC**: Activated if the **ML-Unsupervised-SIC** module is active.
  - **SWIFT**: Activated if the **ML-Unsupervised-SWIFT** module is active.
  - **Bulk-FIN**: Activated if the **ML-Unsupervised_BULK-FIN** module is active.
  - **Bulk-ISO20022**: Activated if the **ML-Unsupervised_Bulk-ISO20022** module is active.
- **FATF16 Module**: Identifies transactions received from other financial institutions that are not compliant with the Financial Action Task Force's (FATF) 2012 Recommendation 16. In order to comply with these regulations, financial institutions need to provide information not just about the originator of a payment, but also the beneficiary.

The **Banking Solutions** also includes the following modules which evaluate transactions offline:

- **Anti-Money Laundering**: Identifies potential money-laundering scenarios.
- **Check Fraud**: Identifies fraudulent checks.
- **Insider and Employee Fraud (IEF)**: Evaluates transactions and operations performed by employees for potential fraud.

In addition to the **Banking Solutions**, the **Healthcare Privacy and Data Security** solution identifies and tracks employee snooping and patient privacy violations.

1.3 Features which Require Additional Licenses

Some features in the product require additional licenses in order to use them. This section lists some of the key features which require additional licenses:

- **Fraud Analytics Simulation Tool (FAST)**: Enables you to modify rules, and run them on real data to determine whether different thresholds and parameters affect the number of alerts and incidents generated.
- **Public Cloud Services**: Enables recording and replaying user actions performed on applications running in AWS, Google Cloud and Azure.
- **Machine Learning**: Enables sending transactions to the Machine Learning Studio for evaluation.
- **Adaptive Scoring**: Enables adjusting the score of an incident based on the resolution of previous incidents for the same entity and rule.

2 Platform Architecture

The following section explains the architecture of the **Cyber Fraud and Risk Management** platform, which is comprised of three main components with its own distinct function: **Capture and Analysis Server** used for Network Traffic Capturing and Analysis, **Analytics Engine Server** used for Analyzing Data with the Analytics Engine, and the **Investigation Center** used for Investigation Center (Alert and Case Management).

2.1 Network Traffic Capturing and Analysis

The **Capture and Analysis Server** contains several services that when configured together support a fully monitored system ready to capture and analyze your system's network.

2.1.1 Capturer

The Capturer service is responsible for collecting network activities from a variety of network monitoring devices, such as Switch, TAP, or Aggregator.

When the Capturer is used for collecting traffic from a physical network monitoring device (TAP or network switch), it should be installed on a physical server.

2.1.2 Sensor

The Sensor service is responsible for collecting application network activities from a variety of sources such as Capturer queues, external queuing systems, data files, databases and so on and turns them into sessions and session activities.

The sensor service writes its output session activities into one or more output queues that are later read by the Data Channel (Analyzer)'s services.

A sensor can be installed on a virtual machine.

2.1.3 Data Channel (Analyzer)

The Data Channel service is responsible for receiving session activities from an Input Queue (provided by the Sensor), creating temporary recording files for each session, and performing audit and user event identification. The Data Channel service performs the following tasks:

- Recognize Audit Events - Screens/ Web pages/ Messages:

  Recognition of a specific event by identifying a certain text or several text strings (such as transaction name or screen header), which appear in specific locations in the message or screen. The Analyzer performs predefined logic of processing data gathered from the event. The logic may also include sending the event information to the Analytics Engine Rule Engine.

- Identify Business Processes (User Activity Events):

  A User Activity Event is a business transaction performed by a user by navigating between one or more application screens/web pages/messages. It is defined by specifying a scenario by which a user navigates between audit events in order to perform a certain business function (such as opening a new customer account may require navigation between five screens).

The outcome of the Data Channel service is sent for storage by the Backlog Writer and for events evaluation by the Analytics Engine Rule Engine using a queuing mechanism.

The data channel you define depends on the applications and protocols in your system. The data channels available are:

- Screen Data Channel: Define this data channel when monitoring and processing screen character based protocols such as, MF 3270, AS400 5250, Unix/Linux VT and SSH.
- Web Data Channel: Define this data channel when monitoring and processing WEB protocols such as, HTTP/S, SOAP and REST.
- Structured Data Channel: Define this data channel when monitoring a client/server environment based on proprietary application protocols. A large number of application protocols and formats can be analyzed including, ISO8583, SWIFT, XML, JSON.
- Custom Data Channel: Define this data channel when creating a custom analytic functionality for monitoring proprietary network and application protocols.

The Data Channel can be installed on a virtual machine.

2.1.4 Backlog Writer

The Backlog Writer is a service responsible for storing session information, screen information, and user event information in the system back-end database. In addition, the Backlog Writer creates a recording for each session.

The Backlog Writer can be installed on a virtual machine.

2.1.5 Backlog Viewer

The Backlog Viewer is a service responsible for retrieving and viewing information stored in the backlog database. The displayed information includes a visual session replay (screens/messages/web pages), audit event information, and user events information. The data is displayed according to search criteria entered by the user in the Event Viewer Reports in the Investigation perspective.

The Backlog can be installed on a virtual machine.

2.2 Analyzing Data with the Analytics Engine

The Analytics Engine Server is a J2EE WEB application, which can run on any of the standard application servers (such as Apache/Tomcat and JBoss) and is comprised to two main components: the **Rule Engine** and the **Investigation Center**.

The **Analytics Engine Server** receives events from a variety of sources, including the **Capture and Analysis Server**, input queues, web services, MQ and APIs. Data can also be loaded using ETL functionality from external data sources. A large number of external data sources, application protocols and formats can be analyzed including, ISO8583, SWIFT, XML, JSON.

The **Analytics Engine Server** is responsible for the following tasks:

- **Collecting events**: Events can be either collected in real-time from the Capture and Analysis Data Channels and external APIs or loaded using ETL functionality from external data sources.
- **Applying business rules to events**: Rules are developed to define the criteria for identifying suspicious behavior. Rules can be developed in Flow (proprietary), or Java.
- **Generating alerts which notify the investigator when suspicious activity has occurred**: When the rule conditions are met, an incident is generated. Incidents are evaluated according to a predefined scoring model which determines the severity of the incident. Only incidents which pass the threshold defined in the scoring model trigger an alert. In addition, you can define profiles which evaluate user behavior and determine whether a specific action is suspicious based on the user's normal behavior.
- **Provide Full-Text Search Engine Using OpenSearch**: OpenSearch is a powerful full-text search engine, with sophisticated indexing and real-time search and analytics capabilities as well as support for multitenant environments. Setting up your project to enable indexing and searching recorded user sessions using OpenSearch provides the investigator a strong search engine capable of analyzing and searching within data in real time.

2.3 Investigation Center (Alert and Case Management)

The **Investigation Center** enables fraud investigators and other business users to utilize the capabilities of the Fraud Management Solution through a friendly web-based user interface. The application provides a unique combination of comprehensive data capture directly from the corporate network with cross channel analytics, and real-time alerting. This enables organizations to detect and prevent internal and external fraud, information leakage and IT sabotage and comply with government regulations.

The **Investigation Center** is comprised of a set of integrated functions, each dealing with a different aspect of the fraud investigation process. The **Investigation Center** enables investigators with no technical background to fully control the investigation environment and processes. Investigators can manage alerts and cases, configure workflows, control business rules parameters and thresholds, set scoring calculation functions, maintain safe and deny lists, configure visual link analysis, and define reports and chart. The **Investigation Center**, also, enables the investigator to view all information relevant to an alert, case or profile in one consolidated view with flexible drilldown options on each related entity.

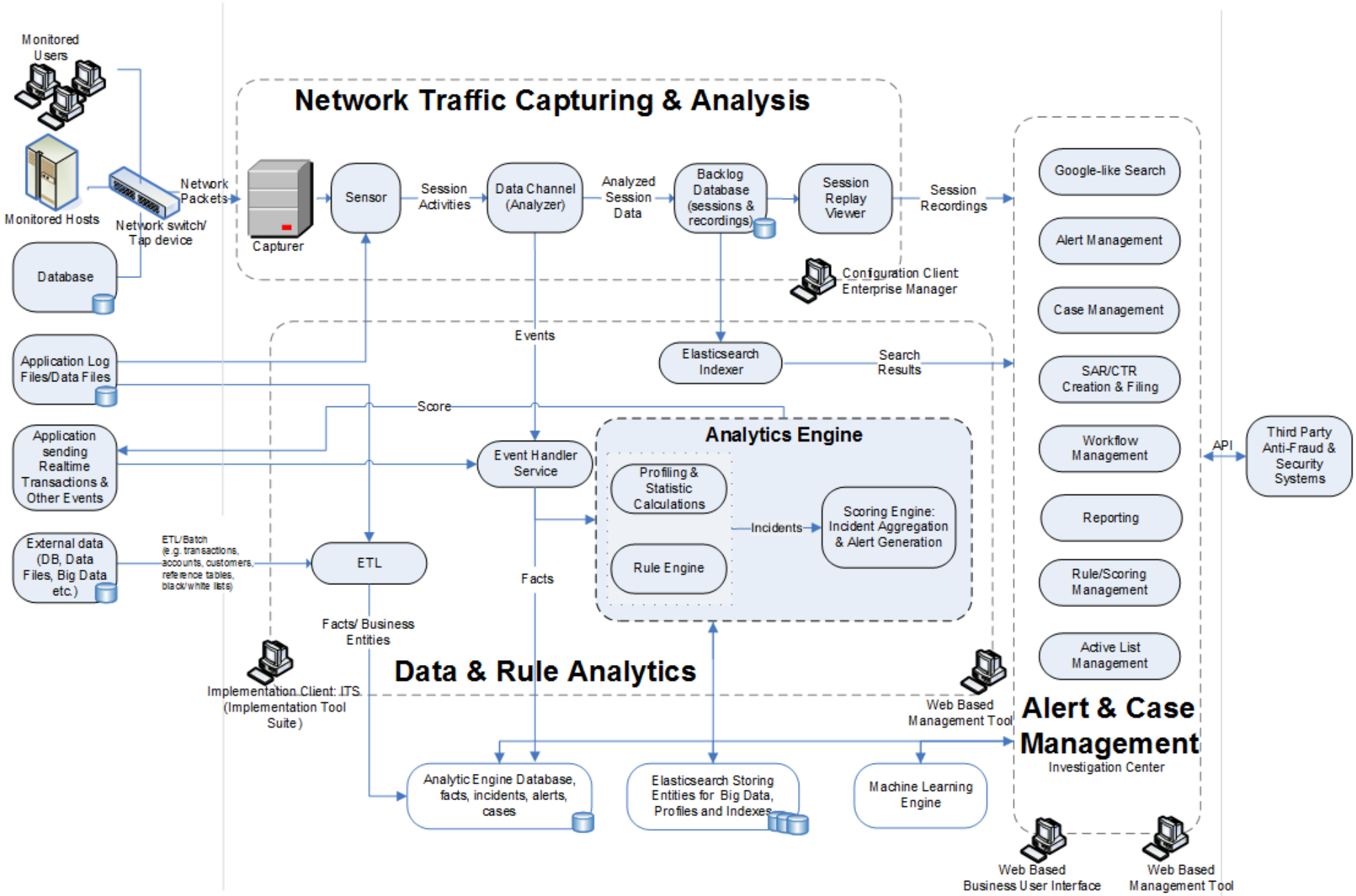
The **Investigation Center** can be easily integrated with other systems in multiple directions. Alerts, incidents or cases can be sent from the **Investigation Center** to external case management systems. These objects can also be received as inputs from other systems.

The **Investigation Center** is comprised of the following elements:

- **Case Management**: Cases are a way to group various data related to a single investigation. You can associate various items related to an investigation to a case or alert such as activities and notes. Each case is associated with a workspace and can be assigned to either a user or workgroup for investigation.
- **Alert Management**: An alert represents a collection of issues with a common topic that requires attention or intervention. Investigators are notified, for example, if there are an extensive number of suspicious transactions involving the same employee, which could then generate an Employee Alert. Alerts can be viewed and sorted according to a defined criteria.

- **Rule Scoring Management**: The scoring for an alert is determined in the Rules Management area. Rule parameters can be defined as well as made active and/or inactive by the business user. All rule editing actions are logged in the **Audit Trail**.
- **Workflow Management**: The Workflow Management system ensures that the proper procedure is followed when investigating a case or alert, and that the investigation follows complies with the necessary organizational requirements. The system comes with out-of-the-box default case and alert workflows, which can be tailored to fit your organization's needs.
- **Reports**: Reports can be created to view data in a variety of methods. Reports can be created based on a business entity or by using one of the templates. Reports can be scheduled to run automatically and exported to a number of different formats.
- **Google-like Search**: The Search feature enables users to find recordings, cases, and alerts by using a free text search utility. Searches are performed according to specific user-defined criteria. A search can be performed using a user ID, keywords, a time frame or fields within a record.
- **Active List Management**: The Active List feature enables the user to create special lists that are used to calculate the basic score for incidents and alerts based on specific entities (accounts, employees, etc.). Each active list identifies which entity or combination of entities should be considered for a scoring adjustment. An active list can contain multiple entities.

The diagram below is a pictorial representation of the entire product architecture and how the components interact together to support a fully monitored application with a built-in Rule Management System.


Monitored Users
Monitored Hosts
Network switch/ Tap device
Network Packets
Database
Network Traffic Capturing & Analysis
Capturer
Sensor
Session Activities
Data Channel (Analyzer)
Analyzed Session Data
Backlog Database (sessions & recordings)
Session Replay Viewer
Session Recordings
Configuration Client Enterprise Manager
Google-like Search
Alert Management
Case Management
SAR/CTR Creation & Filing
Workflow Management
Reporting
Rule/Scoring Management
Active List Management
API
Third Party Anti-Fraud & Security Systems
Application Log Files/Data Files
Events
Elasticsearch Indexer
Search Results
Score
Application sending Realtime Transactions & Other Events
Event Handler Service
Analytics Engine
Profiling & Statistic Calculations
Incidents
Scoring Engine: Incident Aggregation & Alert Generation
Rule Engine
External data (DB, Data Files, Big Data etc.)
ETL/Batch (e.g. transactions, accounts, customers, reference tables, black/white lists)
ETL
Facts
Facts/ Business Entities
Implementation Client: ITS (Implementation Tool Suite)
Data & Rule Analytics
Web Based Management Tool
Alert & Case Management
Investigation Center
Analytic Engine Database, facts, incidents, alerts, cases
Elasticsearch Storing Entities for Big Data, Profiles and Indexes
Machine Learning Engine
Web Based Business User Interface
Web Based Management Tool

3 Documentation

This section provides an overview of the documentation provided with this release for the platform and prepackaged solutions.

3.1 Platform Documentation

Title	Description
Record and Replay Configuration Guide - using the Enterprise Manager	Provides the details of the major components of the Enterprise Manager. Explains installing on Windows and Linux. Describes performing administrative operations such as working with Data Channels and Sensors.
Analytics Engine Implementation Guide - using the Implementation Tool Suite	Details for Implementers how to define the Data Model used as the basis for Fraud Management on the Investigation Center web based application. This Data Model includes defining Business Entities, Facts, Alerts, etc. Projects are created and tested in different environments in the Implementation Tool Suite. They are exported to the Investigation Center where they are implemented by the Users. Within the Projects, you are able to define Models, Rules, Reports and ETL jobs.
Investigation Center Installation and Configuration Guide	Contains installation instructions for Investigation Center on Windows and Linux. Explains installing the Investigation Center on Tomcat. Includes first time configurations for items such as text search, and users and groups.
Investigation Center User Guide	Describes how to optimize the investigation process using various components such as Cases, Alerts, and Reports.
Investigation Center Administration Guide	Explains configuring the System, Model, and Security aspects of the Investigation Center. Describes how to create custom tabs and configure Incident and Alert Scoring.
Flow API	Explains the Flow API's used in the Enterprise Manager and Implementation Tool Suite. Includes information on variables, functions and elements available in flow scripting.
Open Source and Dependencies Guide	Describes which open-source software is used by the products and the license for each of them. Also included is the version of the software included in the product.

Title	Description
Product Security Hardening Guide	Provides the various steps needed to configure the **Capture and Analysis Server**, Analytics Server, and **Investigation Center** in a secured manner, so the system complies to the known software security standards and web application best practices (such as OWASP Top 10 Guidelines).
Upgrade Guide	Details the different upgrade procedures for upgrading to the current version as the instructions differ depending on the version from which you are upgrading. This guide also describes the modifications between the versions.
Release Notes	Contains an overview of the new features, enhancements, and fixes in this release.

3.2 Prepackaged Solutions Documentation

The prepackaged solutions are divided into banking solutions and healthcare solutions.

3.2.1 Banking Documentation

The Banking solution includes the **Secure Payments Solution**, the **Insider and Employee Fraud Solution**, the **Check Fraud Solution**, **Enterprise Case Management** and the **Anti-Money Laundering Solution**.

Title	Description
CFRM Banking Solutions Release Notes	Contains an overview of the new features, enhancements, and fixes in this release for the Solutions Model and Rules Common to all Solutions including the Rules Common to all Solutions includes the following solutions: **Secure Payments Solution**, **Insider and Employee Fraud Solution**, **Anti-Money Laundering Solution**, and **Check Fraud Solution**.
CFRM Banking Solutions Upgrade Guide	Details the different upgrade procedures for upgrading to the current version of the Secure Payments Solution as the instructions differ depending on the version from which you are upgrading. This guide also describes the modifications between the versions.
CFRM Banking Solutions User Guide	Provides information about case management and instructs how to use the **Secure Payments Solution** to detect and report suspicious behavior and privacy violations.

Title	Description
Secure Payments Quick Start Guide	Provides an introduction to the **Secure Payments Solution** with explanations of how to perform common tasks in the **Investigation Center**. There is a separate Quick Start Guide for each module in the Secure Payments Solution.
CFRM Banking Solutions Administration Guide	Explains configuring the System, Model, and Security aspects of the **Investigation Center** for the **Secure Payments Solution**.
CFRM Banking Solutions Implementer's Guide	Explains how to build a CFRM Banking project and to configure it to match your environment and business needs using the **Implementation Tool Suite**.
CFRM Banking Solutions Investigation Center Installation and Configuration Guide	Contains installation instructions for the **Secure Payments Solution Investigation Center** on Windows and Linux. Explains installing the **Secure Payments Solution Investigation Center** on Tomcat. Includes first time configurations for items such as text search, and users and groups.
Secure Payments for ACH Controls Reference Guide	Provides descriptions of the **ACH Module**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.
Secure Payments for Fedwire Controls Reference Guide	Provides descriptions of the **Fedwire Module**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.
Secure Payments for Bulk-FIN Controls Reference Guide	Provides descriptions of the **Bulk-FIN Module**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.
Secure Payments for Bulk-ISO20022 Controls Reference Guide	Provides descriptions of the **Bulk-ISO20022 Module**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.
Secure Payments for SWIFT Controls Reference Guide	Provides descriptions of the **SWIFT Module**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.
Secure Payments for User Behavior Monitoring Controls Reference Guide	Provides descriptions of the **User Behavior Monitoring Module**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.
Secure Payments for SIC and other Single ISO20022 Payments Controls Reference Guide	Provides descriptions of the **SIC and other Single ISO20022 Payments Module**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.
Secure Payments for FATF16 Controls Reference Guide	Provides descriptions of the **FATF16 Module**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.

Title	Description
Secure Payments for Online Banking Controls Reference Guide	Provides descriptions of the **Online Banking Module**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.
Secure Payments for Corporate Online Banking Controls Reference Guide	Provides descriptions of the **Corporate Online Banking module**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.
Secure Payments for Online Banking Integration Guide	Provides details of the API available for the **Online Banking Module**.
Secure Payments Integration Guide	Provides details of the APIs available for the **Secure Payments Solution**.
Secure Payments for User Behavior Monitoring Integration Guide	Provides details of the APIs available for the **User Behavior Monitoring Module**.
Secure Payments for Sanctions Screening Case Management Integration Guide	Provides details of the APIs available for the **Sanctions Screening Module**.
Secure Payments for FATF16 Recommendations Integration Guide	Provides details of the APIs available for the **FATF16 Module**.
CFRM Banking Solutions Monitoring Guide	Provides details of the main tasks that are required to monitor and maintain the system.
Insider and Employee Fraud Controls Reference Guide	Provides descriptions of the **Insider and Employee Fraud Solution**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.
Check Fraud Controls Reference Guide	Provides descriptions of the **Check Fraud Solution**'s alert targets, rules, and reports for identifying and tracking suspicious account behavior.
Anti-Money Laundering Solution Transaction Monitoring Reference Guide	Provides descriptions of the **Anti-Money Laundering Solution**'s alert targets, rules, and reports for identifying and tracking suspicious behavior.
Enterprise Case Management User Guide	Provides information about case management and instructs how to use the **Enterprise Case Management** solution to detect and report suspicious behavior and fraudulent activity.
Enterprise Case Management Implementer's Guide	Familiarizes you with the **Implementation Tool Suite** and the various features and capabilities it offers, so you can understand how to build on the **Enterprise Case Management** solution to configure it to match your environment and business needs.

Title	Description
Enterprise Case Management Alert API Guide	Provides details of the how to use the external fraud alert API to send alerts generated in external systems to the **Investigation Center**.
CFRM Banking Solutions Open Source and Dependencies Guide	Provides details of the open source components used in the CFRM Banking Solution.

3.2.2 Healthcare Documentation

Title	Description
Healthcare Privacy and Data Security User Guide	Provides information about case management and instructs how to use the **Healthcare Privacy and Data Security** solution to detect and report suspicious behavior and privacy violations.
Healthcare Privacy and Data Security Quick Start Guide	Provides an introduction to the **Healthcare Privacy and Data Security** with explanations of how to perform common tasks in the **Investigation Center**.
Healthcare Privacy and Data Security Investigation Center Administration Guide	Explains configuring the System, Model, and Security aspects of the **Investigation Center** for the **Healthcare Privacy and Data Security**. Describes how to create custom tabs and configure Incident and Alert Scoring.
Healthcare Controls Reference Guide	Provides descriptions of the **Healthcare Privacy and Data Security** solution's alert targets, rules, and reports for identifying and tracking suspicious behavior.
Healthcare Privacy and Data Security Release Notes	Contains an overview of the new features, enhancements, and fixes in this release for the **Healthcare Privacy and Data Security**.

4 Supported Software

4.1 Supported Operating Systems

Each component in the product has its own supported operating system. This section lists the operating systems supported for each component as follows:

4.1.1 Capture and Analysis Server (when applicable)

The following operating systems are supported for running the **Capture and Analysis Server**:

- Linux Red Hat 7
- Linux Red Hat 8

The following are supported for existing customers using version 6.5 or lower, or until those components have reached end of life (whichever is first):

- Windows 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

4.1.2 Enterprise Manager Client

The following operating systems are supported for running the **Enterprise Manager**:

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows 10
- Windows Server 2016

4.1.3 Implementation Tool Suite

The following operating systems are supported for running the **Implementation Tool Suite**:

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows 10
- Windows Server 2016

4.1.4 Investigation Center /Analytics Engine

The **Investigation Center** server is a J2EE Web application and the following (64-bit) operating systems are supported for the Investigation Center/Analytics Engine:

- Linux Red Hat 7
- Linux Red Hat 8

The following are supported for existing customers using version 6.5 or lower, or until those components have reached end of life (whichever is first). These operating systems will no longer be supported once you have installed or upgraded to version 6.6:

- Windows 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

4.2 Supported Backlog/Analytics Engine (Rule Engine & Job Management)/Investigation Center Databases

The section below details the supported Backlog/Analytics Engine (Rule Engine & Job Management)/**Investigation Center** database types, and the built-in database schemas.

Note: You must have a database that supports partitions, such as the Oracle Enterprise edition and PostgreSQL.

Supported Database Types

- Oracle 18c
- Oracle 19c
- PostgreSQL 12.4

The following are supported for existing customers using version 6.5 or lower, or until those components have reached end of life (whichever is first). These databases will no longer be supported once you have installed or upgraded to version 6.6:

- MSSQL 2017
- DB2 11
- MariaDB 10.4

Database Schemas

This section describes the database schemas that are predefined in the project.

Note: The actual name of the schemas will differ between projects.

In projects using the platform only, the following schemas are predefined:

- **Investigation Center database** - The main schema used by the Investigation Center. Stores data such as transactions, alerts, incidents, cases and their related entities. It also stores reference data and rule configurations.
- **Jobs database** - Stores information related to the Investigation Center jobs. It contains information of all the active jobs, their instances that have been executed and the execution parameters.

Projects with CFRM Banking Solutions have the following schemas predefined, in addition to the platform schemas:

- **Cloud database** - Stores tenant configuration data. It also contains administrator-level users, groups and group members.
- **Staging database** - An intermediary database between the database of the customer and that of the product. Working with staging tables improves ETL job performance by enabling to prevent duplicate data records and facilitating uploading data to the product database by combining data from multiple sources into one table. It also enables you to check data integrity and quality.

Projects that include the Record and Replay solution, use the **Backlog database** (defined in the Enterprise Manager) in addition to the databases specified above. For more information, refer to the *Record and Replay Configuration Guide*.

4.3 Supported Application Servers (Investigation Center/Analytics Engine)

The following application servers are supported:

- Apache Tomcat 9.0.45

4.4 Supported Internet Browsers

The following Internet browsers are supported for running the **Investigation Center**:

- Firefox version 73 (running on Windows 10)
- Google Chrome version 85 (running on Windows 10)

Note: When running the **Investigation Center** using Google Chrome, certain Java-based features do not work (such as Link Analysis and exporting to PDF when replaying sessions) due to Google's decision (from September 2015) not to support Java anymore in Google Chrome. For more information, see http://blog.chromium.org/2014/11/the-final-countdown-for-npapi.html.

4.5 Supported Screen Resolutions

The following screen resolutions are supported for working with the **Investigation Center**:

- 1920 X 1080

5 Supported Cloud Infrastructure Software

CFRM for Cloud can be installed on AWS, Google Cloud or Azure Cloud environments.

Note: This requires a separate license for each provider used.

5.1 dSupported Operating Systems

Each component in the product has its own supported operating system. This section lists the operating systems supported for each component as follows:

Capture and Analysis for Cloud

- Linux Red Hat 7
- Linux Red Hat 8

Investigation Center / Analytics Engine for Cloud

- Linux Red Hat 7
- Linux Red Hat 8

5.2 Supported Capture and Analysis for Cloud / Investigation Center Databases

The following databases are supported:

Note: You must have a database that supports partitions, such as the Oracle Enterprise edition and PostgreSQL.

- Oracle 12.1g or higher
- PostgreSQL 12.4
- Amazon RDS for Oracle