safetica

Intelligent Data Security

Safetica detects and secures sensitive data and helps teams work safely with information.

Safetica provides Intelligent Data Security, a smarter way to protect data that goes beyond content to understand the context of how data is being used.

Safetica covers today's most critical data security scenarios

GAIN DATA VISIBILITY AND DISCOVER SENSITIVE DATA

Safetica helps you to discover and classify valuable data using its unique Safetica Unified Classification which combines analysis of file content, file origin and file properties. It offers complete visibility and continuous monitoring, never missing a beat to instantly identify, classify, and track sensitive data.

PROTECT SENSITIVE AND BUSINESS-CRITICAL DATA

With Safetica, you can protect sensitive business- or customer-related data, source codes, or blueprints from accidental or intentional leakage. It audits all sensitive data activities no matter where the data moves, so you can report and investigate where there's a risk of leakage or theft. These findings are key for data protection.

PREVENT INSIDER RISKS AND PROMOTE SECURITY AWARENESS

Anyone can make a mistake which could put your business at risk. With Safetica, you can analyze insider risks, detect threats, and mitigate them swiftly. Notifications about how to treat sensitive data can help raise awareness around data security and educate your users.

MAINTAIN DATA SECURITY FOR REMOTE WORK

Safetica provides the full range of capabilities, including data protection, complete contextual visibility, and incident-driven training, regardless of location or network status. Get your hybrid digital work environment under control, discover unwanted software and services, analyze behavior to detect and audit high-risk users.

DETECT AND MITIGATE REGULATORY COMPLIANCE VIOLATIONS

Safetica helps you to detect, prevent, and mitigate regulatory violations. Its audit capabilities support incident investigation to comply with regulations and data protection standards like GDPR, HIPAA, SOX, PCI-DSS, GLBA, ISO/IEC 27001, or CCPA.

What makes us different

Contextual defense

Traditional DLP relies heavily on predefined rules and signature-based detection, often resulting in high false positive rates and missed threats. Contextual Defense leverages real-time behavioral analysis to understand the full context of data usage. This includes who is accessing the data, what is being done with it, and where it is being shared.


Smart Classification

Smart classification automatically catalogues all structured and unstructured data in real-time. Sensitive data is precisely detected by inspecting context signals - such as file properties, metadata, and third-party classifications – together with the content of the data.

Contextual factors such as where a file originated, if it has ever been in a specific location, has ever been modified by certain apps, or previously classified by a third-party, are combined to deliver remarkable data classification accuracy.

**Say goodbye to false positives.**
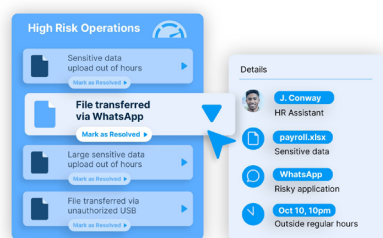
Contextual Risk Analysis

Every data operation your team carries out – such as copying a file or uploading content to a website - is analyzed and scored.

Scoring examines rich context such as time of day, destination, transfer method, and data classification, enabling high risk actions to be immediately spotted, without hindering your team's normal work.
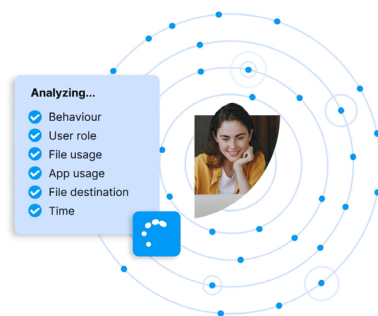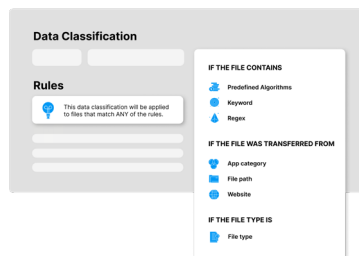
Banish alert fatigue.
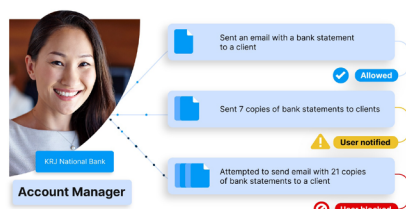
Adaptive Security

With contextual defense your security automatically adapts, applying rigorous protection to block dangerous activity without getting in the way of your teams' normal work.

Machine learning tracks how people and your business usually work with data. If contextual risk thresholds are exceeded, dynamic policies allow the user to receive a notification, with override. Continued unusual activity or more serious deviations from normal patterns are automatically blocked.

Eliminate unnecessary interruptions.

How it works

Data Classification

Rules

This data classification will be applied
to files that match ANY of the rules.

IF THE FILE CONTAINS
- Predefined Algorithms
- Keyword
- Regex

IF THE FILE WAS TRANSFERRED FROM
- App category
- File path
- Website

IF THE FILE TYPE IS
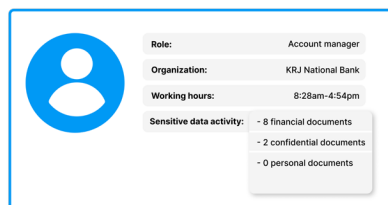- File type

1. Map and Classify Your Data

Identify, map, and categorize all sensitive information across your data landscape, whether it's in structured databases or unstructured formats like emails or documents. This process spans environments—on-premises, in the cloud, or in hybrid settings—ensuring that data is organized for better management and security.

Analyzing...
- Behaviour
- User role
- File usage
- App usage
- File destination
- Time

2. Track user and data activity

Continuously track how data is accessed and used. The Contextual Defense engine observes user actions, application usage, and data movements, building a comprehensive picture of normal behavior.
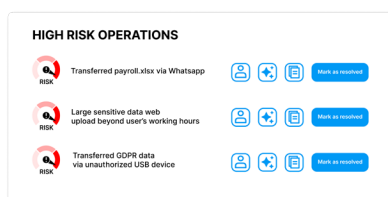
SAFETICA TRACKS EVERY DATA OPERATION.
- Attach file to email
- Send via WhatsApp
- USB upload
- Copies text to GenAI app
- Screen captures technical diagrams and more...

|	
Role:	Account manager
Organization:	KRJ National Bank
Working hours:	8:28am-4:54pm
Sensitive data activity:	- 8 financial documents
	- 2 confidential documents
	- 0 personal documents

3. Establish baselines

Define what constitutes typical activity for your organization. The engine establishes these baselines to distinguish between usual behavior and anomalies that may signal insider threats or unauthorized data activities.

HIGH RISK OPERATIONS

RISK — Transferred payroll.xlsx via Whatsapp — Mark as resolved

RISK — Large sensitive data web upload beyond user's working hours — Mark as resolved

RISK — Transferred GDPR data via unauthorized USB device — Mark as resolved

4. Evaluate Risk in Real-Time

Assess the risk of data actions continuously. For example, if someone attempts to transfer sensitive data externally, the system analyzes the action against historical behavior, the user's role, and the business context to determine if it's a legitimate or suspicious event.
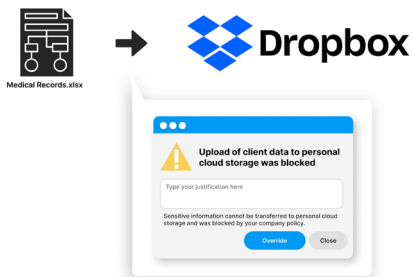
5. Trigger Adaptive Responses

Respond instantly when a threat is detected. Safetica can enforce tiered responses depending on the risk level of an action, the data involved, and the company's security culture.

Medical Records.xlsx → **Dropbox**

Upload of client data to personal cloud storage was blocked

Type your justification here

Sensitive information cannot be transferred to personal cloud storage and was blocked by your company policy.

Override   Close

ALLOW OVERRIDE WITH A BUSINESS JUSTIFICATION
Safetica can enforce policies such as blocking data transfers to unapproved destinations while allowing employees to override these restrictions for legitimate business reasons. This way, security stays strong without getting in the way of their work.

Data channels covered

Safetica keeps data protected across a multitude of channels and platforms, ensuring your data is secure wherever it flows.

File sharing and social media

Send Anywhere   WeTransfer   X   Facebook

Email

Webmail | POP3 / IMAP | SMTP

Internet

HTTP HTTPS   P2P

Cloud

OneDrive | Dropbox Google Drive | Box | SharePoint

Connections

Bluetooth

Microsoft 365

Exchange Online SharePoint Online

Media

Printers

Instant messaging

Teams   Skype   Slack   Zoom   Google Meet

Removable storage

USB | Memory cards External drives | Optical discs

Operations

Copy and Paste Drag and Drop   Screen capture

Safetica Essentials key benefits

Safetica Essentials audits and classifies all data flows in your organization. It identifies sensitive information and data security risks using content inspection and context awareness. Get a quick overview of what is happening in your work environment in real-time. Better understand all internal activities, processes and data risks to enhance your data security and internal efficiency.

Get insight into data security incidents and regulatory compliance violations to be able to respond and mitigate their impacts

Discover and classify your sensitive data flows in any channel or activity to find out where your data is at risk of loss or theft

Get instant actionable notifications with easy-to-read risk evaluation and incident overview

Get general information about user activities to discover shadow IT – unwanted or unnecessary software, cloud services, devices and peripherals
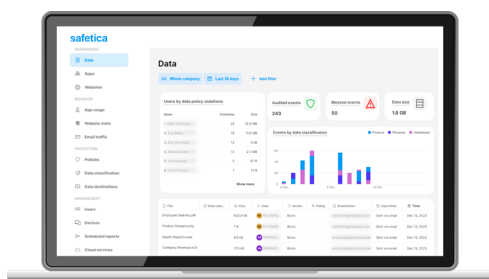
Safetica Console

Web-based central management console that offers optimized features and seamless user experience:

- Data flow visibility, user activity visibility across email, applications, websites and external devices
- Protected device maintenance, interactive reporting, and data analysis
- Real-time alerts and incident investigation

Data protection starts with data visibility

Identify how company data is used and where the data flow.

- Full Windows and macOS support
- Content inspection and context-aware classification with out-of-box templates
- Data security incident detection
- Easy to upgrade to the full-featured data security platform

Safetica Pro key benefits

Safetica Pro identifies risks, prevents human errors and malicious acts, and educates users to protect your data. Adding an intelligent layer to data classification, data loss prevention (DLP) and insider risk management creates a secure environment and supports efficient business operations.

Have full control over sensitive data flows and internal risks based on user behavior and complete content and context analysis

Protect data seamlessly across diverse data storage platforms including clouds, network shares, and Windows & macOS endpoints

Reduce risk and ensure compliance with real-time incident-based user training

GET YOUR DATA UNDER CONTROL, ONLINE AND OFFLINE

Unmatched data visibility across all endpoints, networks, and cloud environments for complete data protection and threat prevention. Safetica uses advanced content classification and OCR for sensitive data detection in image files and scanned documents.

DETECT POTENTIAL THREATS AND ANALYZE INTERNAL RISKS

Respond to threats even before a major incident happens thanks to early discovery of behavior anomalies and data flow risks in your organization

SET CLEAR POLICIES FOR ALL USERS AND DATA CHANNELS

Set up policies for specific groups or individuals. Select the desired workflow with configurable actions from silent auditing, through user notifications to strict blocking.

EMPOWER USERS TO WORK WITH SENSITIVE DATA

Display educational notifications to users when there's a risk of policy violation to let them know or decide. Enforce specific processes to protect the most valuable data.

Built to address the risks of today's work environment

- Safetica smart classification enables content- and context-based approaches
- Pre-defined templates and custom policies
- Flexible DLP actions: record only, notify, justify, or block
- Real-time email notifications
- Multiple hosting options
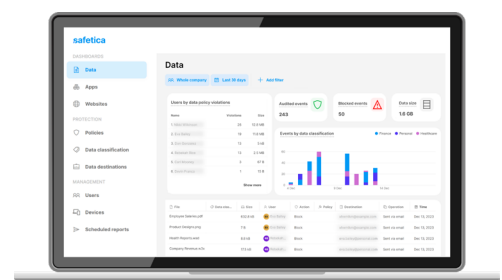
The Safetica Console enables detailed but easy configuration of data classifications, policies, or reports.

UEBA key benefits

Knowledge is the first and most important step in understanding your company's workflow, users work habits and productivity. Enrich Safetica product with User and Entity Behavior Analytics add-on to see user activities in detail and uncover their behavior anomalies. Ensure smooth business operations, even when working remotely.

Recognize undesirable user activities with work activity audit and automated categories for apps used and websites visited by specific users

Get deeper insights into email communication with records of all incoming and outgoing emails with respect to user privacy

Track changes in user behavior with detailed overview of user behavior in your organization over time

Get comprehensive overview and real-time alerts about individual user activities, even when working remote, such as via remote desktop etc.

Detect underlying reasons for anomalies

Dig deeper and pinpoint troublesome elements in your environment to address security or business efficiency concerns. Analyze work-related activities of individual users with detailed information. Find out if anyone visits dangerous websites or uses undesirable applications and services.

Maintain transparency in work, even when working remotely

Let top management and department leaders see how their individual reports work. Stay on top of things even when your users work from home or on the go. Prevent security risks and manage users' efficiency by identifying idle workers, and suspicious behavior patterns.
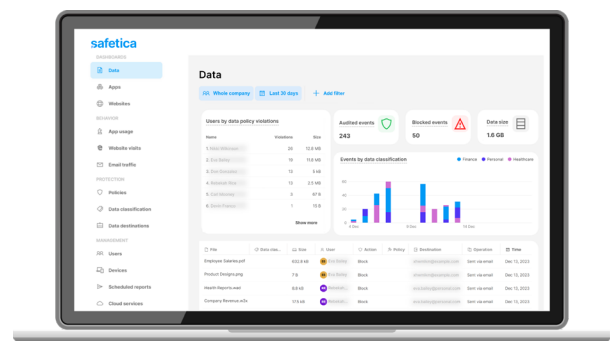
The Safetica Console provides easy-to-understand overview of all possible insider risks. Set up your own overview with customizable views.

Cloud data protection key benefits

Protect your data in the cloud and prevent any unauthorized access or leaks to cloud storage. Secure emailing and file-sharing, safeguard data, and maximize the value of your cloud investment with a dedicated security solution for Microsoft 365.

Safetica extends data security to the cloud

MONITOR AND CONDUCT AUDITS OF FILE UPLOADS AND DOWNLOADS TO CLOUD STORAGE PLATFORMS

Safetica can monitor and classify files directly during user operations, such as exports, uploads and downloads, opening files, copying files to a different path, uploading files via web browsers, sending files via email or IM apps, and others.
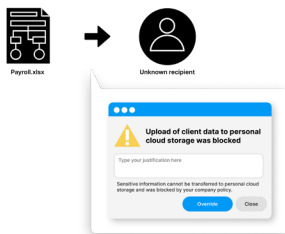
TAKE REAL-TIME ACTION TO PROTECT DATA AND EDUCATE USERS

Safetica's flexible protection policies:

- Prevent sensitive data from being stolen or lost
- Inform and instruct users to improve security awareness
- Enable override with a valid justification

Safeguard remote and mobile work with Microsoft 365 anywhere, anytime

- Protect, audit, and control access to any data file as you collaborate in Microsoft 365, no matter where the document is stored or who it's shared with.
- Fully leverage the potential of Microsoft 365 cloud applications (OneDrive, Outlook, SharePoint and Teams) on mobile devices
- Automatically apply controls, even when user devices are not within the organization's network.

Who we are

Safetica is a global Intelligent Data Security platform that helps organizations protect sensitive data, uncover risk, and ensure compliance—without slowing down their teams.

Powered by AI, Safetica combines data protection, discovery, insider risk management, and compliance enforcement into a single solution for on-prem, cloud, and hybrid environments.

1M+	**120+**	**110+**	**4**
Protected Devices	Countries	Security Evangelists	Offices

TECHNOLOGY ALLIANCES

FORTINET FABRIC-READY

Microsoft

AWARDS & ACHIEVEMENTS

G2 Top 50 Security Products BEST SOFTWARE AWARDS 2024

THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

GetApp CATEGORY LEADERS 2024

THE CHANNEL CO. MES MIDMARKET 100 2024

SOURCEFORGE Customers Love Us

FORRESTER

Gartner

Software Reviews CHAMPION 2023 DATA LOSS PREVENTION