

**safetica**

# DATA LOSS PREVENTION

**Safetica ONE** Product Overview

**eset** TECHNOLOGY ALLIANCE

# safetica ONE

The effortless **data loss prevention**  
and **insider threat protection**

- ✓ **Easy** on users and infrastructure
- ✓ **Tough** on insider threats and data loss
- ✓ **Actively** supporting regulatory compliance



# Securing your data while increasing **operational efficiency**

Safetica ONE is the only mature data security solution designed for scalability and needs of SMB and enterprises. Get your valuable data under control with great time to value. Go beyond data loss prevention with holistic behavior analysis to detect insider threats even earlier and respond even before they turn into incidents. Leverage insights into company workspace, digital assets, and operations to optimize costs.

People and data are the fuel for modern companies. When sensitive data is lost or stolen, a company's reputation, competitive advantage, and profitability all suffer.

The average cost of a data breach is **\$3.86 million**.\*

60% of small companies go **out of business within 6 months** of a major data breach.\*\*

\*2020 Cost of Data Breach Report, Ponemon Institute; \*\* National Cyber Security Alliance, October 2012

## Every organization can secure its data

Internal security has never been easier. We help you protect your data, guide your people and support business compliance. Safetica ONE prevents data breaches and makes data protection regulations easy to comply with by securing your business from human error or malicious behavior.

### EXPERT DATA SECURITY

We cover all areas of internal data risk and protect valuable data against human error and malicious intent.

### SHORT TIME-TO-VALUE

Security should never come at the expense of productivity. Safetica ONE doesn't create extra hassle for employees or the IT department. Its time-to-value is unbeatable.

### SEAMLESS INTEGRATION

Only a seamlessly integrated security solution can work efficiently. Together with our technology partners, we protect data on all devices, all major operating systems, and in the cloud.

# Key **Data Security** scenarios

## DATA FLOW DISCOVERY AND RISK DETECTION

Safetica audits and records any attempt to intentionally or unintentionally leak the data, no matter where the sensitive information is stored, or who has accessed it. Safetica's risk analysis helps you detect and investigate how your data could be leaked or stolen.

## DATA PROTECTION & EMPLOYEE GUIDANCE

Anyone can make a mistake which could put your business at risk. With Safetica ONE, 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 employees.

## REGULATORY COMPLIANCE

Safetica ONE helps you detect and prevent regulatory violations and investigate incidents to comply with regulations and data protection standards like GDPR, HIPAA, SOX, PCI-DSS, GLBA, ISO/IEC 27001, or CCPA.

## WORKSPACE & BEHAVIOR ANALYSIS

Workspace and user behavior analysis provides an extra level of detail to detect internal risks. Also, by understanding how your employees work, print, and use expensive hardware and software licenses, you can optimize your costs and increase operational efficiency.

### SAFETICA ONE PROTECTS YOUR

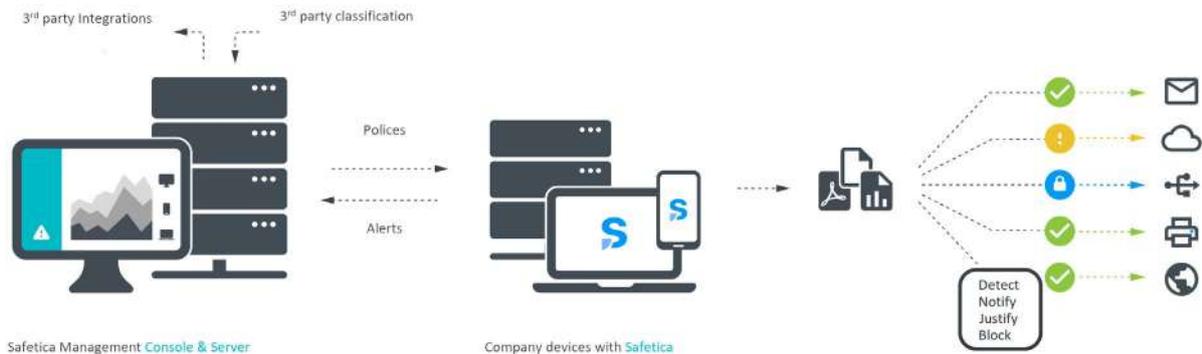
- personal data
- strategic company documents
- customer databases
- payment-related data, such as credit card numbers
- intellectual-property – industrial designs, trade secrets, and know-how
- contracts



Product tiers

Modules

# Reference Architecture



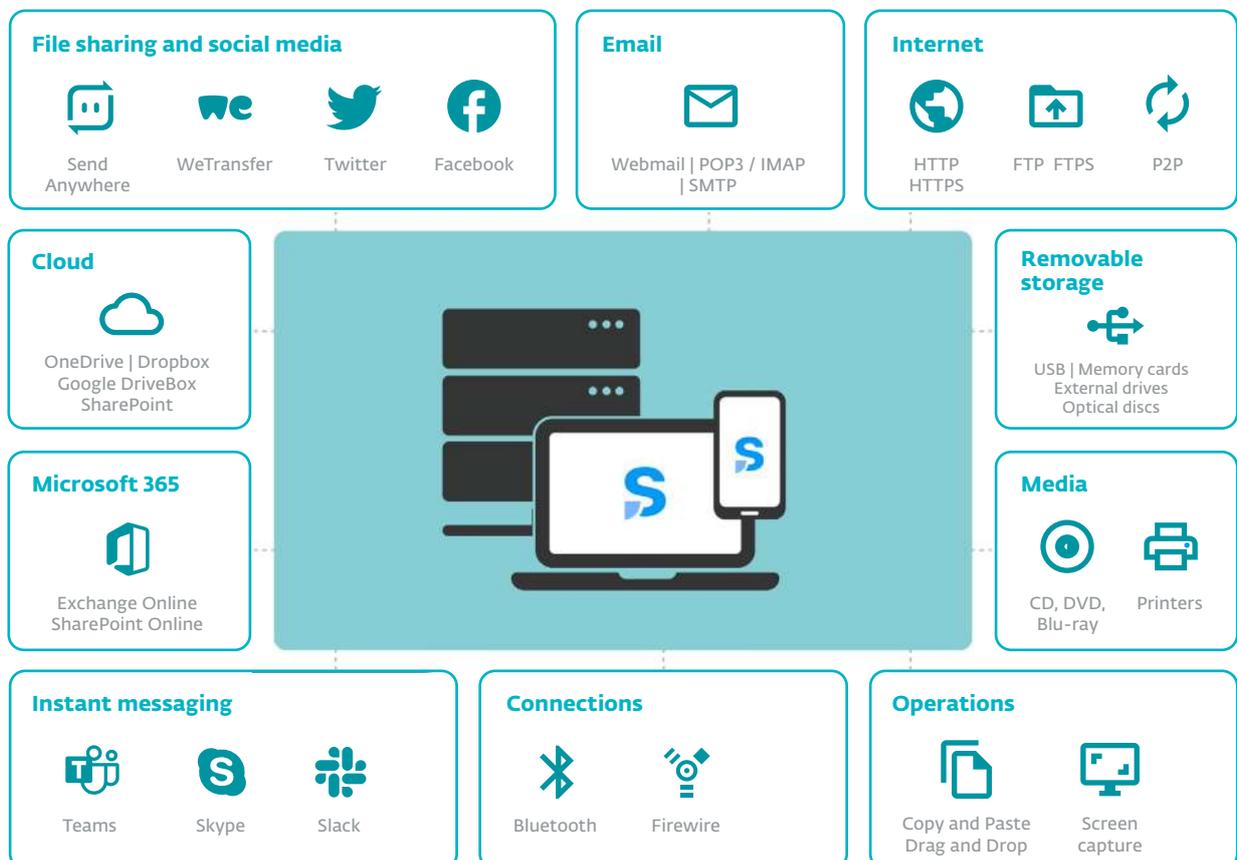
The physical or virtual server runs a database with endpoint activity and security records. The Safetica Management Console enables admins to manage security policies and display the collected information.

All actions are recorded and security policies are applied on desktops, laptops and other remote or even offline mobile devices (smartphones MDM only) with a Safetica Client.

Sensitive data is protected throughout all channels.

## Data channels covered

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



# Discovery Key Benefits

Safetica ONE Discovery audits and classifies all data flows in your organization. It identifies sensitive information and security risks using content inspection with optical character recognition (OCR). Get a quick overview of what is happening in your workspace 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



**Audit 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 notifications** and actionable **management reports** with easy-to-read risk level evaluation and incident overview



**Discover and remove** unwanted or unnecessary software, cloud services, or hardware/peripherals



**Easy-to-deploy** solution with one-click integration with **Microsoft 365** respects established processes and provides first reports within days



Objectively **analyze user activities** in your environment and determine if company **equipment and network are used properly**

## Key highlights

Identify how company data is used and where it is stored and sent, no matter where it resides or flows.

- ✓ Windows and macOS support
- ✓ One-click integration with Microsoft 365
- ✓ File content inspection and classification
- ✓ Easy to upgrade to the full-featured data security platform
- ✓ Runs on bare metal or virtualized on-prem, hosted, VM hosted in cloud



Safetica Management Console for Safetica ONE Discovery provides deep insights into all recorded file operations with different views for easy interpretation.

# Protection Key Benefits

Safetica ONE Protection identifies risks, educates your employees, and prevents people's mistakes and malicious acts to protect your data. Combination of data analytics, data classification, and data loss prevention (DLP) with insider threat protection creates a secure environment while maintaining efficient business operations.



Have full control over sensitive data flows and internal risks based on behavior analysis & content inspection



Get regular security reports and real-time incident notifications



Use Safetica Zones for simplified high-level data security



Create Shadow Copy of leaking data to keep forensic evidence for further investigation

## SET CLEAR POLICIES FOR ALL USERS AND DATA CHANNELS

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

## 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. Safetica ONE uses advanced content classification and OCR for sensitive data detection in image files and scanned PDF documents.

## EMPOWER EMPLOYEES TO WORK WITH SENSITIVE DATA

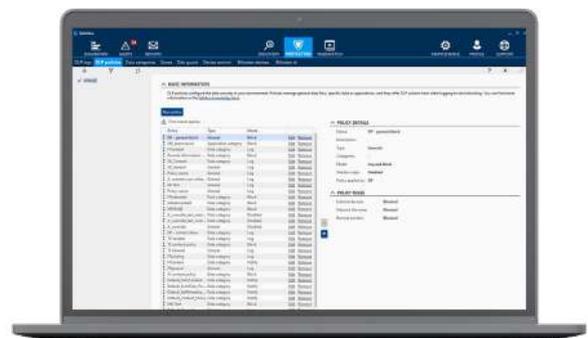
Display educational notifications to employees when there's a risk of policy violation to let them know or decide. Enforce specific processes to protect the most valuable data.

## GET ALL DEVICES UNDER CONTROL, ONLINE AND OFFLINE

Restrict the use of portable peripherals or unauthorized media. Control corporate mobile devices and keep track of data that leaves Microsoft 365. Safetica remains fully active regardless of network connection. All collected records are synchronized when connection is restored.

## Key highlights

Based on content inspection, internal risk analysis, and clear policies set up for all data channels, Safetica ONE Protection can recognize when somebody makes a mistake or takes chances with your sensitive data. Depending on which mode Safetica ONE is operating in, it can either block the risky activity, notify the admin, or remind the employee about the organization's security guidelines.



Safetica Management Console enables detailed but easy configuration of DLP policies, data categories, or reports.

# Enterprise Key Benefits

Safetica ONE Enterprise extends data loss prevention and insider threat protection by additional workflow control, automation, and seamless integration with 3rd party network security solutions, SIEMs, and data analytics tools. Built your enterprise IT security stack with ease.



Automated **third-party integration** and features for advanced use cases.



Policies for **workflow control** on company endpoints



Support for Active Directory in **multi-domain environments**



**Custom branding** of user security notifications on endpoints

## SEAMLESS INTEGRATIONS

Automation of security policies and integration with your IT stack help you protect your assets even in complex environments.

Native integration with **Microsoft 365** or **Fortinet** network appliances provides extended control over unknown devices and creates a robust endpoint-to-network security solution.

All audited incidents and logs can be automatically sent to SIEM solutions e.g., **Splunk**, **IBM QRadar**, **LogRhythm**, or **ArcSight** for further investigation. REST API provides collected data to tools like **Power BI** or **Tableau** for advanced analysis.

## POWERFUL WORKFLOW CONTROL

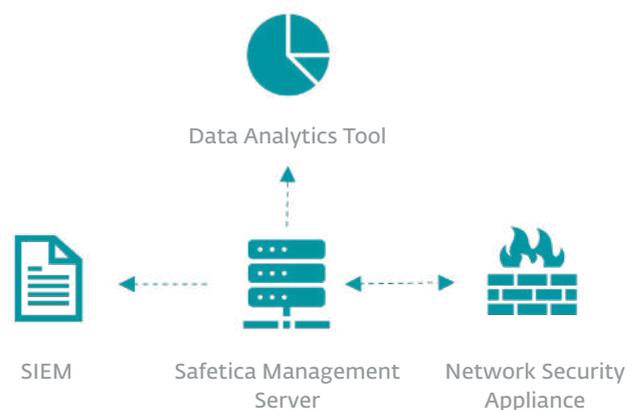
Set of control features enables you to define how users are allowed to work, regardless of the data involved.

With workflow control, you can enforce a specific secure process and block all other ways of performing an action.

Workflow control includes **application DLP policies** to manage behavior of various types of applications like CRM or IM and **DLP policy rules** with custom configurations applied to different networks, local paths, or exclusive access for privileged users.

## Key highlights

- ✓ Windows and macOS support
- ✓ One-click integration with Microsoft 365
- ✓ Fortinet network appliances integration
- ✓ API integration with Power BI or Tableau
- ✓ Immediate notifications delivered to your inbox
- ✓ File content inspection with pre-defined templates
- ✓ Content classification based on various approaches



# UEBA Module Key Benefits

Knowledge is the first and most important step in understanding your company's workflow, employees' work habits and productivity. Enrich any Safetica ONE product with User and Entity Behavior Analytics module 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 labelling and categorization of apps used and websites visited by specific users



## Get deeper insights in email communication

with records of all incoming and outgoing emails with respect to employee's privacy



## Track changes in user behavior

with overview and visualization of trends and changes in user behavior in your network over time



## Audit resource usage

to get precise overview whether purchased hardware and software licenses are distributed and used efficiently



## Get comprehensive reports and real-time alerts

about individual user activities, even when working remote, such as via remote desktop etc.



## Audit job searches

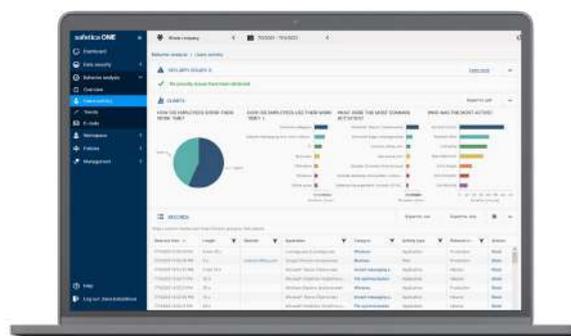
to identify job portals visited by specific users, who might pose a future data security risk

## IDENTIFICATION OF ANOMALIES ROOT CAUSES

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

## WORK TRANSPARENCY EVEN ON REMOTE

Let top management and department leaders see how their individual reports work. Stay on top of things even when your employees work from home or on the go. Prevent security risks and manage employee's efficiency by identifying idle workers, job search, and suspicious behavior patterns.



WebSafetica provides easy-to-understand overview of all possible threats. Get important statistics on the dashboard, set up custom record views and reports.

# Mobile Module Key Benefits

Safetica ONE Mobile is a light-weight Mobile Device Management (MDM) tool that increases data security on smartphones and tablets to make them a trusted part of your IT environment. Get an overview of mobile device status to identify security risks and be able to respond quickly. All from single pane of glass.



## Data protection on mobile devices

Separate work-related apps and data into a protected workspace, identify harmful apps on particular devices, and remotely block or wipe lost or stolen devices.



## Overview of user and device status

Monitor device security and connectivity, track and find lost devices with remote localization.



## Centralized remote management

Use enhanced app management to control app settings and behavior, set security policies for device groups and automatically configure and manage them from a single place.

## SECURE AND MANAGE ALL MOBILE DEVICES

Check all company devices and discover security risks in a single glance. Set up device policies and even Wi-Fi accounts remotely. Utilize Android EMM and iOS Managed Apps to create a separate workspace on company devices and use them for remote work and private purposes.

## AUDIT INCOMING FILES ON ANDROID

Get an overview of where your data is stored also on corporate mobile devices (available for Android 6-10). Using Safetica ONE Mobile with WebSafetica, you can spot security incidents in single pane of glass, whether they happen on your phone, computer, or in the Microsoft 365 cloud.

## ANTI-THEFT PROTECTION

Loss of company mobile devices and employee fluctuation are common issues that may your sensitive data at risk. Safetica ONE Mobile can find corporate mobile devices and remotely wipe them if unreachable. This helps you to secure your infrastructure and keep critical data as your property.

## Key highlights

- ✓ MDM and security: secured workspace, device policies, app management with remote config, security status
- ✓ Anti-theft protection: localization, password strength, remote lock, remote data wiping

## SYSTEM REQUIREMENTS

- Android: min. Android 6+ and Google Play Services
- iOS: min. iOS 10+

# Detailed **Features** List I

Compatible with Windows, macOS, Microsoft 365, Android, iOS	Safetica ONE Discovery	Safetica ONE Protection	Safetica ONE Enterprise
<b>Security Audit</b>	✓	✓	✓
<b>Data-flow security audit</b> Security audit of data-flow in all channels, including external devices, web upload, email, instant messaging, print, and cloud drives.	✓	✓	✓
<b>Office 365 file and email audit</b> Audit of file operations and outgoing email communication in Office 365.	✓	✓	✓
<b>Regulatory compliance audit</b> Discover violations of most common regulations, such as PCI-DSS, GDPR, or HIPAA in all regional variations.	✓	✓	✓
<b>Workspace security audit</b> Audit usage of company devices, applications, networks, and print. Discover unused or misused resources to maintain workspace, ensure retention, and reduce costs.	✓	✓	✓
<b>Content inspection</b> Classify sensitive files and emails by powerful content inspection with predefined templates or custom rules and dictionaries.	✓	✓	✓
<b>Detection of suspicious activities</b> React fast thanks to real-time detection of suspicious activities and immediate email alerts.	✓	✓	✓
<b>Endpoint Data Protection</b>	✗	✓	✓
<b>Email and network protection</b> Data protection for email, web upload, instant messaging, and network shares.	✗	✓	✓
<b>Devices and print protection</b> Manage data-flow to external devices and protect sensitive data against forbidden printing on local, network, or virtual printers.	✗	✓	✓
<b>Remote work protection</b> Avoid data leaks on remote endpoints or remote desktop connections. Support a wide range of remote access solutions.	✗	✓	✓
<b>Advanced data classification</b> Use advanced technologies to detect and label sensitive data based on origin, workflow context, or file type. Take advantage of metadata detection to use 3rd party classifications. Allow users to classify files themselves.	✗	✓	✓
<b>Different remediation policies</b> React flexibly to detected incidents to empower and educate your employees. Incidents can be logged, blocked, or justified/blocked with override.	✗	✓	✓
<b>Incident Shadow Copy</b> Keep forensic evidence for incidents by creating shadow copies of leaking data. Shadow copies are fully encrypted and can be kept on local computers with a retention policy.	✗	✓	✓

# Detailed **Features** List II

Compatible with Windows, macOS, Microsoft 365, Android, iOS	Safetica ONE Discovery	Safetica ONE Protection	Safetica ONE Enterprise
<b>Endpoint Data Protection</b>	✗	✓	✓
<b>Workspace control</b> Define your secured workspace and reduce perimeter by application and website control. Avoid undesirable behavior in your company and reduce the cost of security management.	✗	✓	✓
<b>Safetica Zones</b> Easy management of safe data perimeter with unique Safetica Zones, which significantly reduce the number of data protection policies.	✗	✓	✓
<b>BitLocker encryption management</b> Centralized management of local drives and external devices with BitLocker encryption.	✗	✓	✓
<b>Cloud Data Protection</b>	✗	✓	✓
<b>Endpoint cloud sync protection</b> Data protection for cloud drives on endpoints, e.g., OneDrive, Google Drive, Dropbox, Box, etc.	✗	✓	✓
<b>Endpoint Microsoft 365 protection</b> Data protection for Microsoft 365 and SharePoint from endpoints. Prevent sharing or uploading data you want to keep away from the cloud.	✗	✓	✓
<b>Azure Information Protection</b> Detection of data classifications from Microsoft Azure Information Protection, even in encrypted form.	✗	✓	✓
<b>Exchange Online Protection</b> Unify email policies across endpoints and cloud email. Manage and filter outgoing data from endpoints and Exchange Online.	✗	✓	✓
<b>Enterprise Features</b>	✗	✗	✓
<b>Notifications branding</b> End-user notification custom branding (logo).	✗	✗	✓
<b>Workflow control</b> Application policies and expert policy settings for aligning endpoint workflow with company processes.	✗	✗	✓
<b>Multi-domain support</b> Multiple domain enterprise support for Active Directory.	✗	✗	✓
<b>Security Automation</b>	✗	✗	✓
<b>SIEM integration</b> Automated reporting of incidents to SIEM solutions (Splunk, QRadar, LogRhythm, ArcSight, etc.).	✗	✗	✓
<b>FortiGate integration</b> Automated security integration with FortiGate network appliances to create a robust endpoint-to-network security solution.	✗	✗	✓
<b>Reporting API</b> API for reporting Safetica data to analytics and visualization services.	✗	✗	✓

# Tech Specs and Requirements

## SERVER

- 2.4 GHz quad-core processor
- 8 GB RAM and more
- 100 GB of available disk space
- A shared or dedicated server, support of virtual machines and cloud hosting
- Requires connection to server with MS SQL 2012 and higher or Azure SQL
- MS Windows Server 2012 and higher

## DATABASE

- MS SQL Server 2012 and higher, or MS SQL Express 2016 and higher, or Azure SQL.
- MS SQL Express is part of a universal installer and recommended for up to 200 protected endpoints.
- 200 GB of available disk space (optimally 500 GB or more, depending on the range of collected data).
- A shared or dedicated server, support of virtual machines and cloud hosting. It can be hosted with Safetica server together.

## WINDOWS CLIENT

- 2.4 GHz dual-core processor, 2 GB RAM and more
- 10 GB of available disk space
- MS Windows 7, 8.1, 10 (32-bit [x86] or 64-bit [x64])
- MSI installation package
- .NET 4.7.2 and higher

## MACOS CLIENT

- 2.4 GHz quad-core processor, 2 GB RAM and more
- 10 GB of available disk space
- macOS 10.10 and higher (for full DLP feature set recommend 10.15 and higher)

## MOBILE CLIENT

- Android: min. Android 6+ and Google Play Services
- iOS: min. iOS 10+

## SUPPORTED CLOUD PROVIDERS

- Microsoft Azure, Microsoft 365

## SELECTED CERTIFICATIONS

- ISO 9001 & ISO/IEC 27001
- Member of Cybersecurity Tech Accord
- Microsoft Gold Partner
- Member of ESET Technology Alliance
- Member of the Fortinet Technology Alliance



Safetica is a Czech software company that provides Data Loss Prevention and Insider Threat Protection solutions to organizations of all shapes and sizes. Here at Safetica, we believe everyone deserves to know that their data is safe.



ESET Technology Alliance aims to better protect businesses with a range of complementary IT security solutions. We provide customers with a better option when staying protected in the ever-changing security environment by combining our proven and trusted technology with other best-of-breed products.