



Safetica Portfolio of Products

Data Loss Prevention

Your business runs on data. When sensitive data is lost or stolen, a company's reputation, competitive advantage and profitability all suffer. There can also be legal liabilities to be faced.



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.**

Safetica DLP prevents data breaches, makes data protection regulations easy to comply with and protects your business from human error.

Safetica is an easy-to-use data loss prevention (DLP) solution affordable also for companies of all sizes.

* 2018 Cost of Data Breach Study Global Overview, Ponemon Institute, July 2018

** How Data Breaches Affect Small Businesses, withlayr.com, August 2017

How can Safetica help you?

PREVENT DATA LEAK AND INVESTIGATE INCIDENTS

Safetica protects your company data against leaks no matter where it is stored or who uses it.

- 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



ENSURE REGULATORY COMPLIANCE

Safetica helps comply with legal regulation and data protection standards.

- GDPR
- HIPAA
- SOX
- PCI-DSS
- GLBA
- ISO/IEC 27001
- CCPA

PREVENT HUMAN ERROR

Even good people can make careless mistakes that can put your business at risk. With Safetica, you can educate your employees on how to treat sensitive data without changing how they work.

What makes Safetica unique?

EASY-TO-USE AND QUICK TO DEPLOY

Safetica is designed to be fast and easy to deploy, with **no extra dedicated staff or hardware** needed.

Your most sensitive data is protected in a matter of hours, only by defining secure channels and a basic selection security policies.

CLEAR CONTEXT TO ALL YOUR DATA

When, where and how is your sensitive data used? Safetica gives you the answers and provides a clear context so that you can protect your most valuable business data.

How does Safetica protect you?

AUDIT AND DISCOVER WITH SAFETICA DISCOVERY

Identify how company data is used and where it is stored and sent, no matter where it resides or flows. Prevent deliberate data leaks with audit logs. Discover all internal processes and

organize your business environment. Safetica Discovery allows you to understand hidden risks within your organization better.

EDUCATE AND PROTECT WITH SAFETICA PROTECTION

Safetica Protection creates a secure environment throughout your company, educates your employees, identifies risks and protects your data.



Set clear policies for all data channels

Set up security policies using an individual or group approach. Select the desired workflow with configurable actions from silent auditing, through educative notifications to strict blocking.

Give your employees the confidence to work with sensitive data

Display notifications when a user potentially violates a policy. Enforce specific processes to handle the most valuable data.

Get all connected devices under control

Restrict the use of portable devices or prohibit unauthorized media connections. Control corporate mobile devices and keep track of the data that leaves the Office 365 cloud.

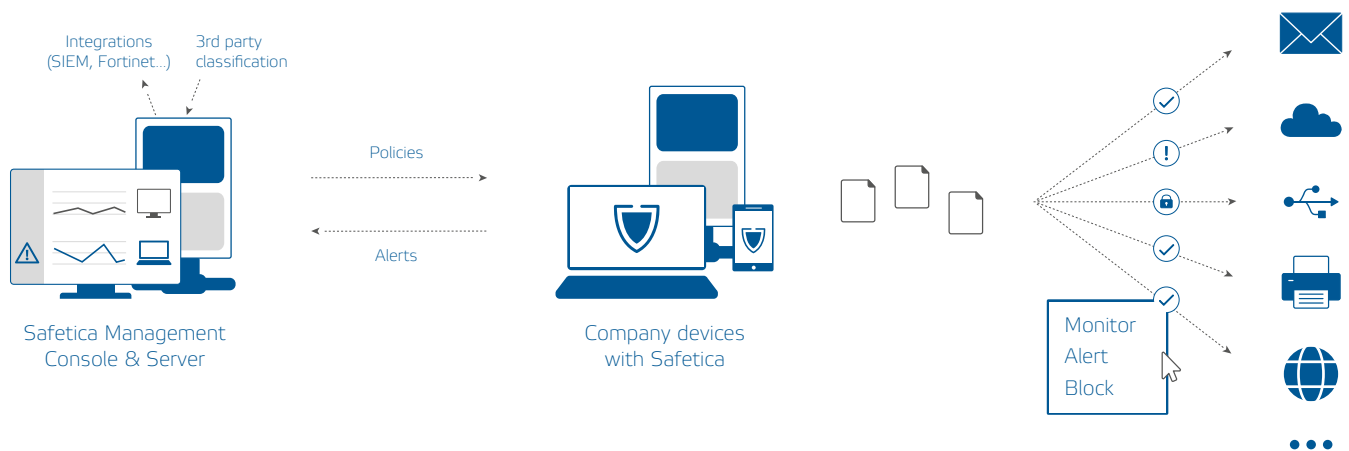
Enjoy full online and offline protection

Protect your data both on online and offline company devices. Safetica remains fully active regardless of network connection. All collected records are synchronized as soon as the connection is re-established.

PROTECT ENDPOINTS INDEPENDENT ON PLATFORM

Safetica monitors the use of data both on Windows and on macOS. Integrate with Office 365 or Fortinet network appliances to gain extended control over unknown devices. Use Safetica Mobile to manage your company mobile devices from a single place.

How does Safetica work?



The server runs a database with workstation activity and security logs. The Safetica Management Console enables users to manage security policies and display overviews of all collected information.

All actions are recorded and security policies are applied on PCs, laptops, tablets and smartphones with Safetica client.

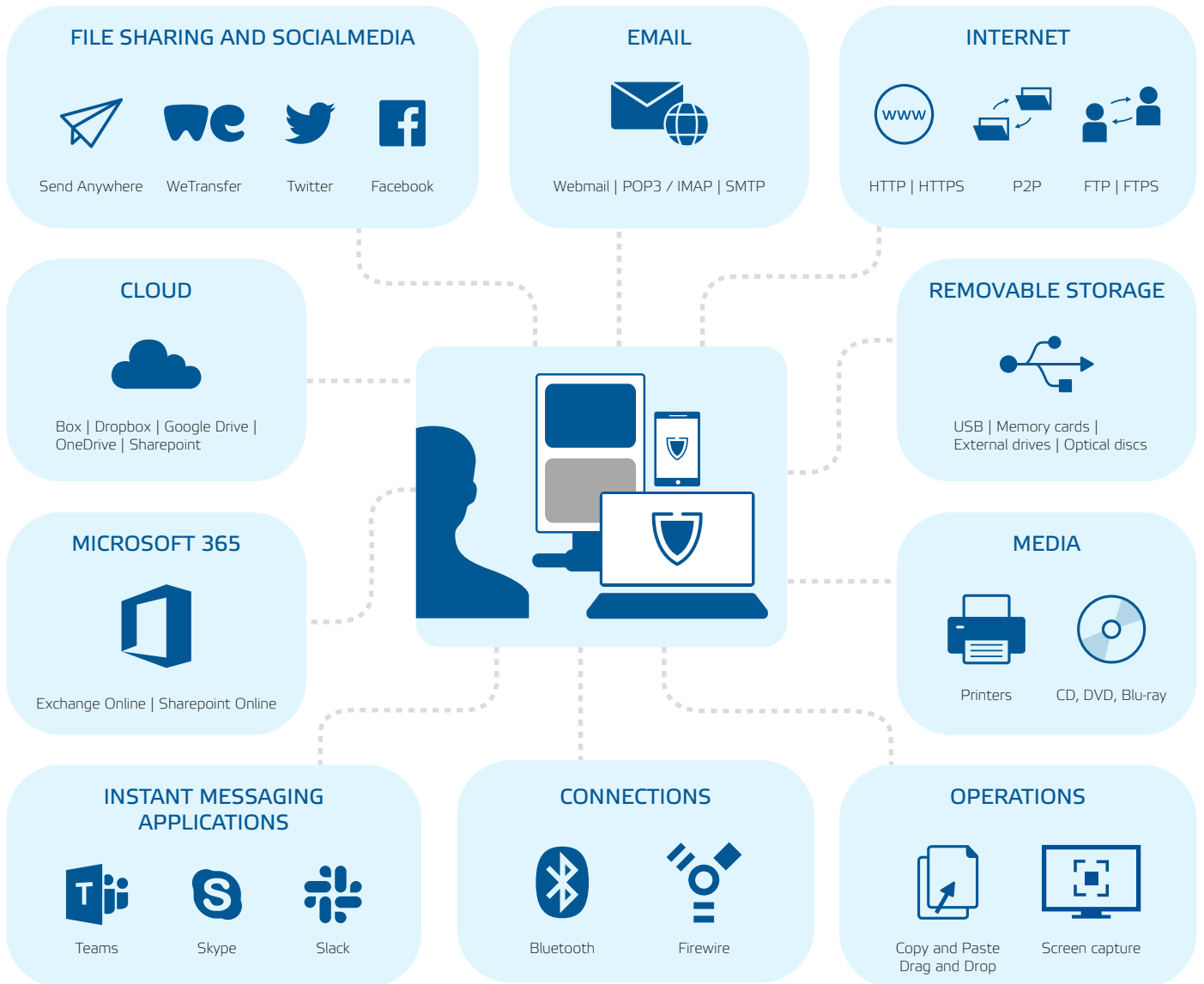
Sensitive data is protected throughout all channels.

Key features set

Safetica can recognize when somebody takes chances with your confidential information. Depending on which mode Safetica is operating in, it can either block the risky activity, inform the administrator, or remind your employees about your security guidelines.

Data channels protected by Safetica

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



Powerful reports

Safetica gives you a quick and easy-to-understand overview of all possible threats in a single management interface. You receive useful information at any time on any device, even on your smartphone.

You can receive alerts about suspicious behavior via email or SIEM, add any data to the dashboard or export it to XLS or PDF for further analysis.

Technical requirements

SAFETICA SERVER

- 2.4 GHz quad-core processor
- 4 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

SAFETICA CLIENT (on protected computers)

- 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 4.5.2 and higher

MS SQL (server database)

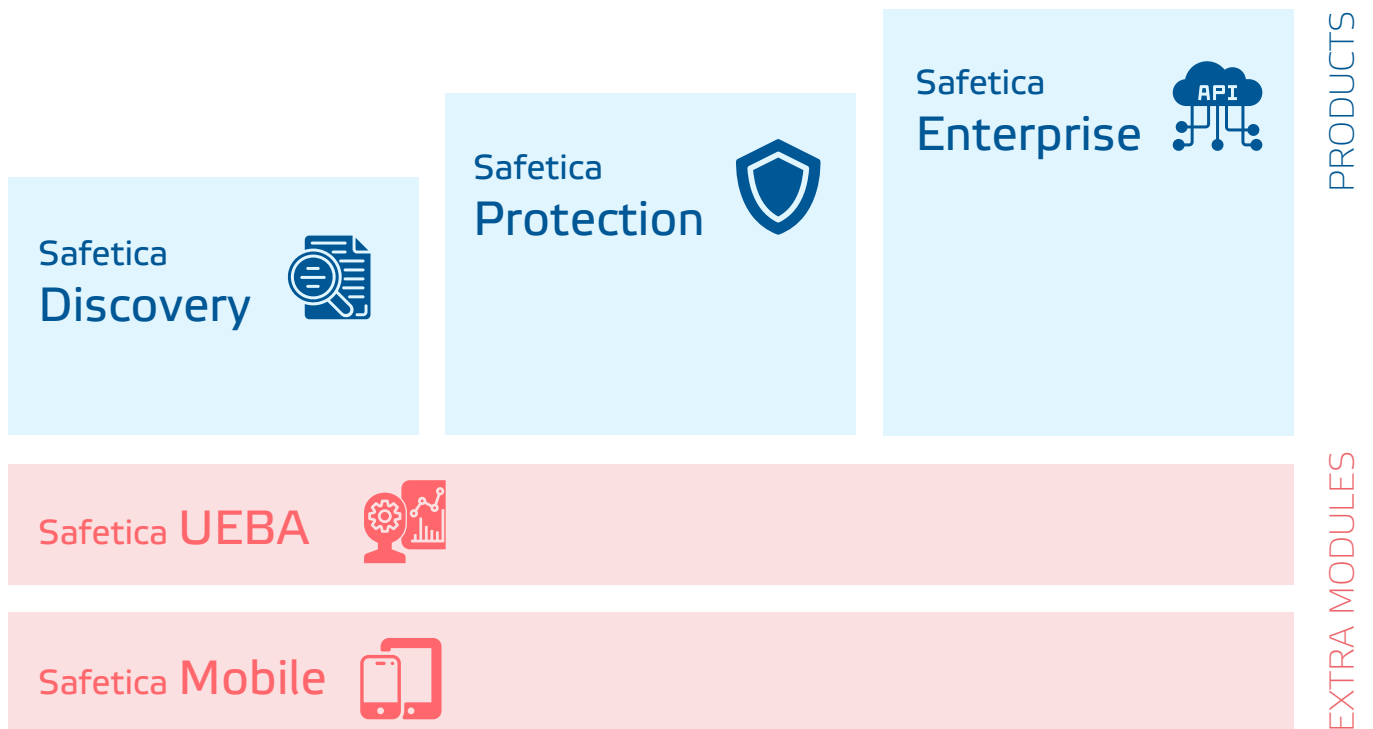
- MS SQL Server 2012 and higher, or MS SQL Express 2016 and higher, or Azure SQL. MS SQL Express is part of a universal installer and recommended for up to 200 protected endpoints.
- 200 GB of available disk space (optimally 500 GB or more, depending on the range of collected data).
- A shared or dedicated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

MAC 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.



Safetica Portfolio of Products



Extra Modules

Enhance your data protection solutions with extra modules.

SAFETICA UEBA (USER AND ENTITY BEHAVIOR ANALYTICS)

- Understand real user activity and behaviour in detail.
- Get a comprehensive overview of work time usage.
- Use the insight to secure your data and workspace.

SAFETICA MOBILE

- Protect data on mobile devices, e.g. smartphones and tablets.
- Get an overview of mobile device status to identify risks.
- Audit activity both within apps and on websites.

SAFETICA DISCOVERY

- Understand your company's sensitive data flow.
- Detailed reports of all critical company data.
- Basic overview of company user behavior included.
- Security audit and regulatory compliance audit.
- First data security reports within days.



SAFETICA PROTECTION

- All-in-one security solution combining data analytics, data classification and data loss prevention (DLP).
- Full control over sensitive data flow.
- Regular security reports and real-time incident notifications.
- Safetica Zones for simplified high-level data security.
- Easy-to-deploy solution with respect for business-as-usual.



SAFETICA ENTERPRISE

- Data protection solution to complete your enterprise IT security stack.
- Automated third-party integration and features for advanced use cases.
- Workflow and process control and support for multi-domain environments.
- Customize Safetica to include your company's branding.



Safetica Complete Documentation
go.safetica.com/complete_documentation

Features overview

Compatibility on



Safetica
Discovery



Safetica
Protection



Safetica
Enterprise

Security Audit



Data-flow security audit



Security audit of data-flow in all channels, including external devices, web upload, email, instant messaging, print, and cloud drives.

Office 365 file and email audit



Audit of file operations and outgoing email communication in Office 365.

Regulatory compliance audit



Discover violations of most common regulations, such as PCI-DSS, GDPR, or HIPAA in all regional variations.

Workspace security audit



Audit usage of company devices, applications, networks, and print. Discover unused or misused resources to maintain workspace, ensure retention, and reduce costs.

Content inspection classification



Classify sensitive files and emails by powerful content inspection with predefined templates or custom rules and dictionaries.

Detection of suspicious activities



React fast thanks to real-time detection of suspicious activities and immediate email alerts.

Endpoint Data Protection



Email and network protection



Data protection for email, web upload, instant messaging, and network shares.

Devices and print protection



Manage data-flow to external devices and protect sensitive data against forbidden printing on local, network, or virtual printers.

Remote work protection



Avoid data leaks on remote endpoints or remote desktop connections. Support a wide range of remote access solutions.

Advanced data classification



Use advanced technologies to detect and mark 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.

Different remediation policies



React flexibly to detected incidents to empower and educate your employees. Incidents can be logged, blocked, or justified/blocked with override.

Incident Shadow Copy 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.	×	✓	✓
Workspace control 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.	×	✓	✓
Safetica Zones Easy management of safe data perimeter with unique Safetica Zones, which significantly reduce the number of data protection policies.	×	✓	✓
BitLocker encryption management Centralized management of local drives and external devices with BitLocker encryption.	×	✓	✓
Cloud Data Protection	×	✓	✓
Endpoint cloud sync protection Data protection for cloud drives on endpoints, e.g. OneDrive, Google Drive, Dropbox, Box, etc.	×	✓	✓
Endpoint Office 365 protection Data protection for Office 365 and SharePoint from endpoints. Prevent sharing or uploading data you want to keep away from the cloud.	×	✓	✓
Azure Information Protection Detection of data classifications from Microsoft Azure Information Protection, even in encrypted form.	×	✓	✓
Exchange Online Protection Unify email policies across endpoints and cloud email. Manage and filter outgoing data from endpoints and Exchange Online.	×	✓	✓
Enterprise Features	×	×	✓
End-user rebranding End-user notification rebranding, e.g. changing the logo.	×	×	✓
Workflow control Application policies and expert policy settings for aligning endpoint workflow with company processes.	×	×	✓
Multi-domain support Multiple domain enterprise support for Active Directory.	×	×	✓
Security Automation	×	×	✓
SIEM integration Automated reporting of incidents to SIEM solutions (Splunk, QRadar, LogRhythm, ArcSight, etc.).	×	×	✓
FortiGate integration Automated security integration with FortiGate network appliances to create a robust endpoint-to-network security solution.	×	×	✓

ABOUT SAFETICA

Safetica is a Czech software company that provides its data loss prevention solution to companies of all shapes and sizes. Because in Safetica we believe that every company deserves to know that their data is secure.

300,000+

protected devices



1,600+

satisfied customers



120+

countries



80+

security experts



TECHNOLOGY ALLIANCES



AWARDS & ACHIEVEMENTS



THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

FORRESTER

Gartner



 @Safetica

 Safetica

 @Safetica

And what about your data?

Try Safetica demo now!
www.safetica.com/try-safetica

