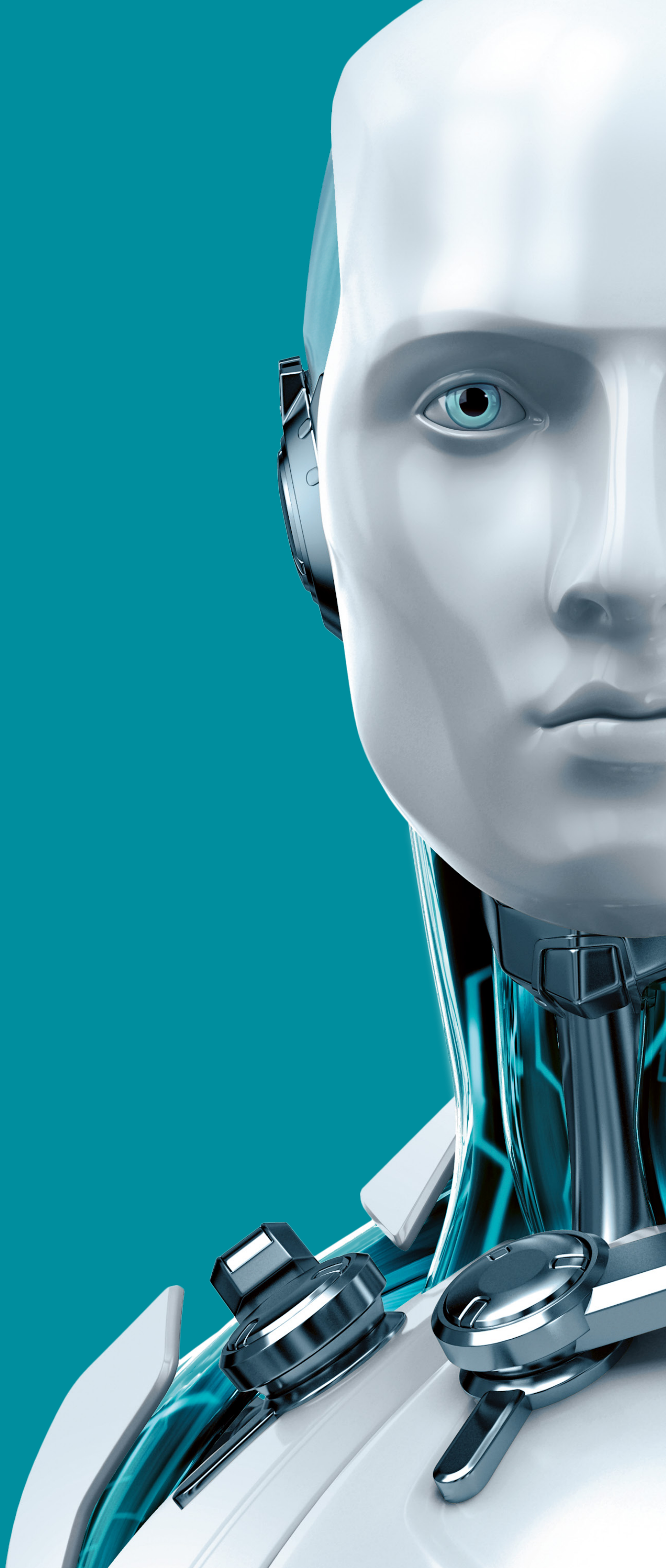
safetica

Data Leak Prevention



BUSINESS

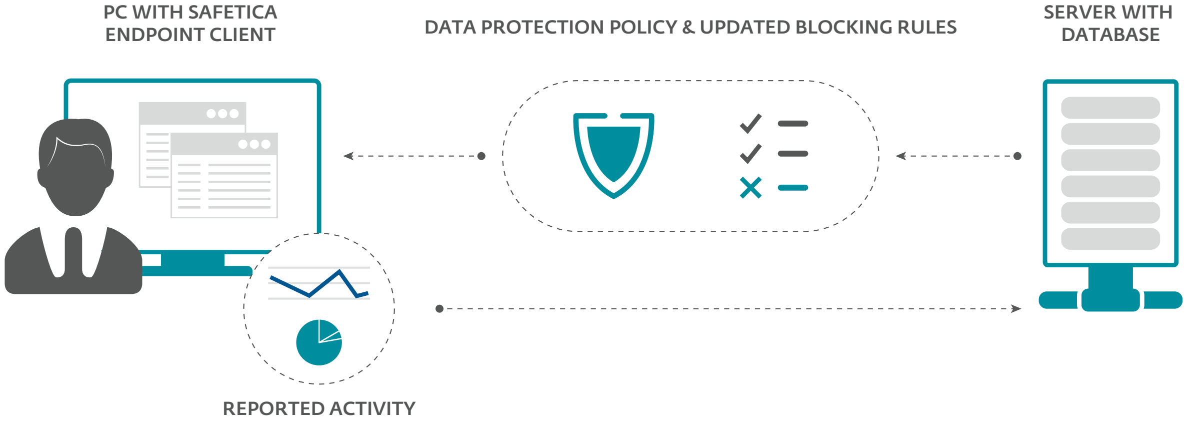
ESET TECHNOLOGY ALLIANCE

Key advantages

Full suite DLP solution	Covering all major data leak channels, Safetica provides endpoint DLP with network DLP capabilities.
Short time-to-benefit	Flexible approach to blocking data leak channels gives Safetica the fastest deployment time in its product class.
High level of tamper-resistance	Insures consistent protection, even while covering users with administrative rights.
All speciality functions covered against leakage	Safetica protects data from printscreening, clipboard stealing, virtual printing, file transformations, archiving and encrypting functions.
Agnostic approach	Safetica data protection is not limited by individual protocols or applications.
Clearly defined data policies	Managers simply select locations from which confidential data should not leave. Safetica takes care of the security.
Exact time tracking	"Opened" does not mean actively used. Safetica activity reports show the actual time users were active at visited websites or in applications.
Automatic evaluation and alerts	Safetica picks the most important logged details and sends a summary report to designated recipients. Complete details are available as needed.

How it works

The endpoint workstation is where the action happens. Users work with business critical data, access the internet, read emails, send documents to the printer and plug in their portable media. Safetica deploys an agent (**Safetica Endpoint Client**) to desired endpoints and maintains regular connection with them through the server (**Safetica Management Service**). This server builds a database of workstation activity and distributes new data protection policies and regulations to each workstation.


PC WITH SAFETICA ENDPOINT CLIENT
DATA PROTECTION POLICY & UPDATED BLOCKING RULES
SERVER WITH DATABASE
REPORTED ACTIVITY

safetica

Safetica security software offers a full DLP (Data Leak Prevention) solution which covers a wide range of security threats that originate from a common source – the human factor. Safetica defends against planned or accidental data leaks, malicious insider actions, productivity issues, BYOD dangers and more.

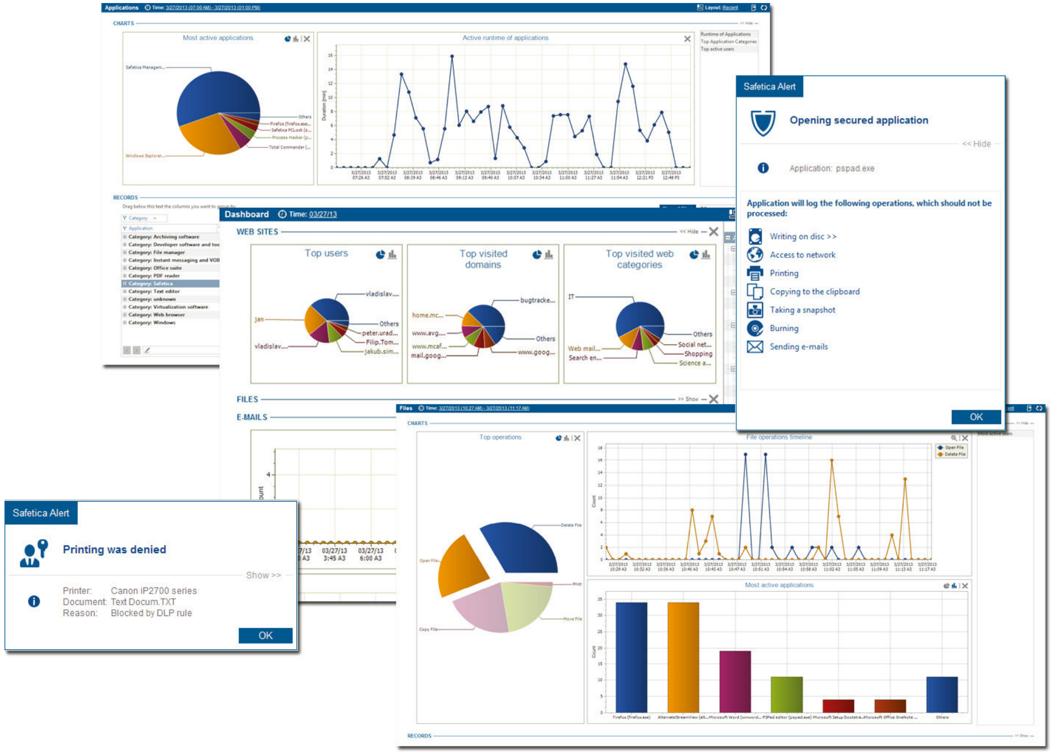
Safetica's security philosophy is based on three pillars: completeness, flexibility and ease of use.

Safetica's corporate level DLP gives management complete activity reports and enforces company security policies.

Safetica offers a full set of security tools in a single software package which would otherwise require several security solutions from different vendors.

Key features

Complete data leak prevention	Safetica covers all data leaks channels while being easy to install and operate. See Endpoint Events Coverage for proof of Safetica's comprehensive coverage.
Trends & productivity profiling	Warns company management in the event of sudden changes in employee activity and shows productivity changes by department over time. Both changes are indications of possible security risks.
Activity reporting	Uncovers security breaches on multiple fronts by checking all user activities for signs of potential danger, even before the actual transfer of data.
Email DLP	Ensures protected data stays out of the wrong mailbox. Records where sensitive files have been sent and stores this information for future reports.
Application control with time rules	Enables selected package of work-related applications and blocks others for a more secure environment. Applications can be made available only for a specified time frame.
Web filtering	Easily enforces company AUP (Acceptable Use Policy) with carefully preselected categories and keyword filtering.
Print control	Limits what can be printed and by whom with quotas for individual users and departments.
Device Control	Prevents employees from connecting unauthorized devices at work. Common ports can be enabled for particular devices or blocked for all of them.
Encryption management	Safetica offers Full Disc Encryption or encrypts whole partitions and creates local or network virtual drives for secure file storage. In addition to password and key access methods, Safetica offers secured Travel Disks and an “encrypt when copying out” feature for data leaving the Safe Area.
Informative & testing mode	Helps companies progressively integrate data protection by enabling tests for all “what-if” situations without halting business processes.
On the fly data classification	Protects new information immediately after a classified file is created or received.
Unified management console	Safetica Management Console enables one-stop security management and reporting, integrates all company data protection, reporting and blocking policies.
SSL/HTTPS inspection	Checks and protects secured communication lines including websites using HTTPS protocol, IM applications with secured connections and secured email transmissions.
Minimal total cost of ownership (TCO)	Frees users from the need to buy extra security appliances. The endpoint agents deployed in Safetica also provide Data Leak Prevention features for company networks.
Flexible use	Safetica covers any application, Instant Messaging protocol or webmail service thanks to its unique universal approach.



Safetica Alert

Opening secured application

<< Hide

Application: pspad.exe

Application will log the following operations, which should not be processed:

- Writing on disc >>
- Access to network
- Printing
- Copying to the clipboard
- Taking a snapshot
- Burning
- Sending e-mails

OK

Safetica Alert

Printing was denied

Show >>

Printer: Canon iP2700 series
Document: Text Docum.TXT
Reason: Blocked by DLP rule

OK

Endpoint events coverage

Reporting and activity blocking

- All file operations
- Long-term trends, short-term activity fluctuations
- Websites (all browsers supported including HTTPS traffic)—active and inactive time
- Emails & webmails (virtually all providers)
- Searched keywords (majority of engines supported, Windows
Search supported)
- Instant messaging (application independent—all protocols)
- Application usage with both active and inactive time
- Virtual, local & network printers
- Screen activity (intelligent capturing)
- Keylogging

Data leak prevention

- All harddrives, USB, FireWire, SD/MMC/CF cards, SCSI drives
- Network file transfer (unsecured, secured)
- Emails (SMTP, POP, IMAP, Microsoft Outlook/ MAPI protocols)
- SSL/HTTPS (all browsers & applications with standard certificate management)
- Copy/paste, clipboard, drag & drop
- Virtual, local & network printers
- Bluetooth, IR/COM/parallel ports
- CD/DVD/BluRay readers & recorders
- Controls application file access

ESET®

TECHNOLOGY ALLIANCE

ESET Technology Alliance aims to better protect businesses with a range of complementary IT security solutions. We provide superior options for staying protected in an ever-changing security landscape by combining our proven and trusted technology with other best-of-breed products.

Use cases

Securing key business information

Once safe areas for all protected data have been established, Safetica silently checks every interaction with these files and, in case of a forbidden operation, blocks it or performs other selected actions. These company-defined actions can include informing security manager of each event, encrypting data, and offering other safe location for data. Data is protected on laptops and flashdrives even outside of the company walls.

Management of removable devices

Safetica gives management final control over who plugs what into company computers, removing another channel for data leaks and dramatically decreasing the number of required service interventions.

Reach regulatory compliance

With Safetica Endpoint Client present on company computers and policy management activated in the Safetica Management Console, you are able to comply with regulations governing the movement and usage of sensitive data.

Data encryption

Safetica offers Full Disc Encryption, can oversee a secure encrypted file storage system, manage connected keys and prevent data from being stored in unsecure locations.

Productivity control

Even without directly using the Safetica Management Console GUI, managers can receive regular summary reports on selected endpoint users or groups.

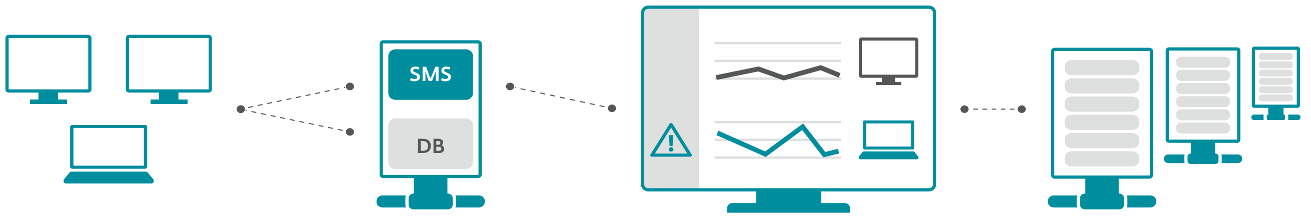
Architecture

PCS AND LAPTOPS WITH SAFETICA ENDPOINT CLIENT

SAFETICA MANAGEMENT SERVICE AND SQL DATABASE

SAFETICA MANAGEMENT CONSOLE WITH SETTINGS AND OUTPUTS

SAFETICA MANAGEMENT SERVICE SERVERS IN OTHER BRANCHES



1 Actions are recorded and policy rules enforced via a small agent application (optionally hidden from the user).

2 Data is automatically transferred from network computers to the server with laptop data synchronized upon connecting to the network. Client settings are synced in reverse order.

3 All data can be viewed or visualized from the management application. All settings can be adjusted here as well.

4 Safetica supports multiple branches from a single management console.

System requirements

Safetica client

- 2.4 GHz dual-core processor
- 2 GB of RAM memory
- 10 GB of free disk space
- Installation on client
- MS Windows 7 and higher, 32-bit and 64-bit

Safetica server

- 2 GHz dual-core processor (we recommend quad-core)
- 4 GB of RAM memory
- 20 GB of free disk space
- Installation on application server or a dedicated server (virtualization is possible)
- Active Directory Support
- MS Windows Server 2008 R2 and higher, 32-bit and 64-bit
- Requires connection to server with MS SQL 2008 R2 and higher
- When sharing with MS SQL we recommend at least a quad-core processor, 8 GB RAM and 100 GB of free disk space

MS SQL (database for server)

- Requirements as per MS SQL edition
- Shared or dedicated server, we recommend at least 100 GB or free disk space
- MS SQL 2008 R2 and higher, eventually MS SQL 2012 Express and higher (free version)
- MS SQL 2012 Express is an optional part of installation

ENJOY SAFER TECHNOLOGY®