



Safetica

Портфоліо рішень

**Запобігання витокам
даних**

Ваш бізнес працює на основі даних. Від втрати чи викрадення конфіденційних даних страждає репутація, конкурентні переваги та прибутковість компанії з можливістю виникнення юридичних зобов'язань в майбутньому.

Середній збиток
від витоку даних
становить
\$3,86 млн.*

**60% малих компаній
закриваються протягом
6 місяців після витоку
важливих даних.****

Рішення Safetica запобігає витокам даних, забезпечує дотримання положень про захист конфіденційних даних та захищає ваш бізнес від наслідків людських помилок.

Safetica – просте у використанні рішення для запобігання втраті даних (DLP), яке доступне для компаній будь-яких розмірів.

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

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

Що забезпечує Safetica?

ЗАПОБІГАННЯ ВИТОКАМ ДАНИХ ТА РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ

Захищає усі конфіденційні дані від витоку незалежно від того, де вони зберігаються та ким використовуються.

- персональні дані
- стратегічні документи
- бази даних клієнтів
- дані щодо оплати, наприклад, номери кредитних карток
- інтелектуальна власність
- промислові зразки, комерційні таємниці та ноу-хау
- контракти тощо.



ВІДПОВІДНІСТЬ НОРМАТИВНИМ АКТАМ

Safetica дозволяє легко дотримуватися будь-яких нормативних актів щодо захисту даних у вашій галузі.

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

ЗАХИСТ ВІД НАСЛІДКІВ ЛЮДСЬКИХ ПОМИЛОК

Навіть сумлінні працівники допускають ненавмисні помилки, які можуть зашкодити вашому бізнесу. Завдяки Safetica ви можете навчити співробітників, як потрібно працювати з конфіденційними даними без змін у робочому процесі.

Що робить рішення Safetica унікальним?

ЛЕГКІСТЬ ВИКОРИСТАННЯ ТА ШВИДКІСТЬ РОЗГОРТАННЯ

Safetica розроблена таким чином, щоб її можна було швидко та легко розгорнути **без потреби у висококваліфікованому персоналі чи додатковому апаратному забезпеченні**.

Важливі **конфіденційні дані будуть захищені протягом кількох годин**, необхідно лише визначити безпечні канали та обрати базові політики безпеки.

ПОВНА ІНФОРМАЦІЯ ПРО РОБОТУ З ДАНИМИ

Хто працював з конфіденційними даними, коли, де і як вони використовувались? Safetica надає відповіді та забезпечує повною інформацією, таким чином ви можете захистити найцінніші корпоративні дані.

Як Safetica захищає вас?

АУДИТ ТА ВИЯВЛЕННЯ З SAFETICA DISCOVERY

Визначає способи використання корпоративних даних, незалежно від того, де вони перебувають та як переміщуються. Завдяки журналам аудиту дозволяє запобігти навмисному витоку інформації.

Забезпечує огляд усіх внутрішніх процесів та допомагає організувати корпоративне середовище. Крім цього, Safetica Discovery дозволяє краще зрозуміти приховані ризики всередині вашої організації.

НАВЧАННЯ ТА ЗАХИСТ ІЗ SAFETICA PROTECTION

Safetica Protection створює безпечне середовище у компанії, навчає співробітників, визначає ризики та захищає корпоративні дані.



Встановіть політики для всіх каналів передачі даних

Налаштуйте політики безпеки, використовуючи індивідуальний або груповий підхід. Виберіть потрібну дію для робочого процесу – від аудиту чи сповіщення до відхилення.

Надайте співробітникам впевненість під час роботи з конфіденційними даними

Safetica відображає сповіщення, коли користувач потенційно може порушити політику. Також можна застосувати точно визначений спосіб обробки цінних даних.

Контролюйте всі підключені пристрої

Обмежуйте використання портативних пристроїв або несанкціоноване підключення медіаносіїв. Контролюйте корпоративні мобільні пристрої та відстежуйте дані, переміщені з хмарного середовища Office 365.

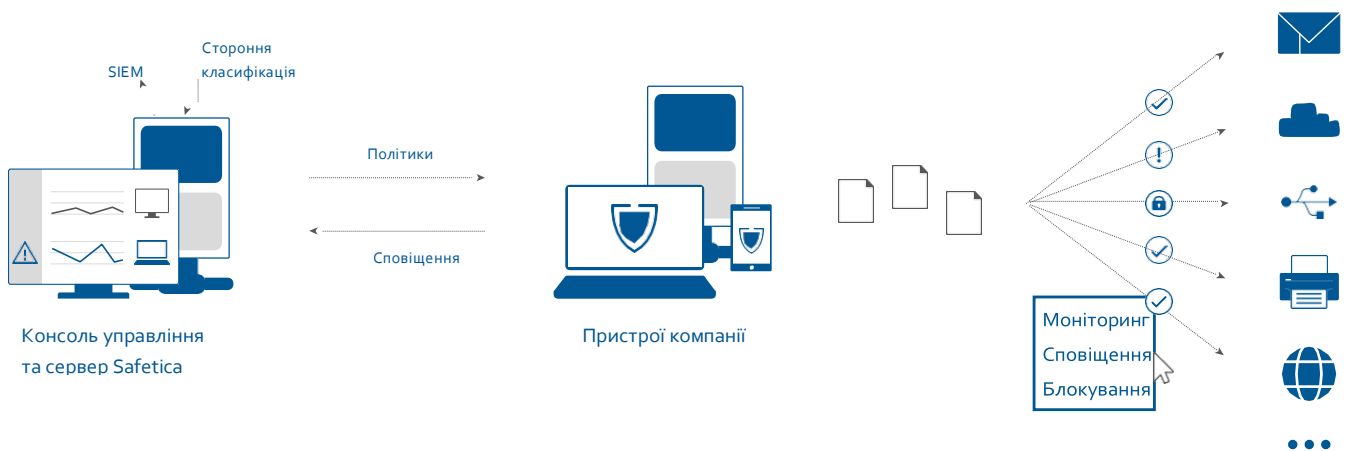
Насолоджуйтеся повним захистом в режимі офлайн

У режимі офлайн забезпечується такий самий рівень захисту, як і в режимі онлайн. Усі зібрані записи синхронізуються одразу після відновлення з'єднання.

ЗАХИСТ РОБОЧИХ СТАНЦІЙ НЕЗАЛЕЖНО ВІД ПЛАТФОРМИ

Safetica контролює використання даних на пристроях Windows та macOS. Також доступна інтеграція з мережевими пристроями, Office 365 для отримання розширеного контролю над невідомими пристроями. Модуль Safetica Mobile дозволяє відстежувати та управляти смартфонами та планшетами компанії з однієї консолі.

Як працює Safetica?



Сервер запускає базу даних із робочими станціями та журналами безпеки. Консоль управління Safetica дозволяє користувачам управляти політиками безпеки та переглядати всю зібрану інформацію.

Усі дії реєструються, а політики безпеки застосовуються на ПК, ноутбуках, планшетах та смартфонах із клієнтом Safetica.

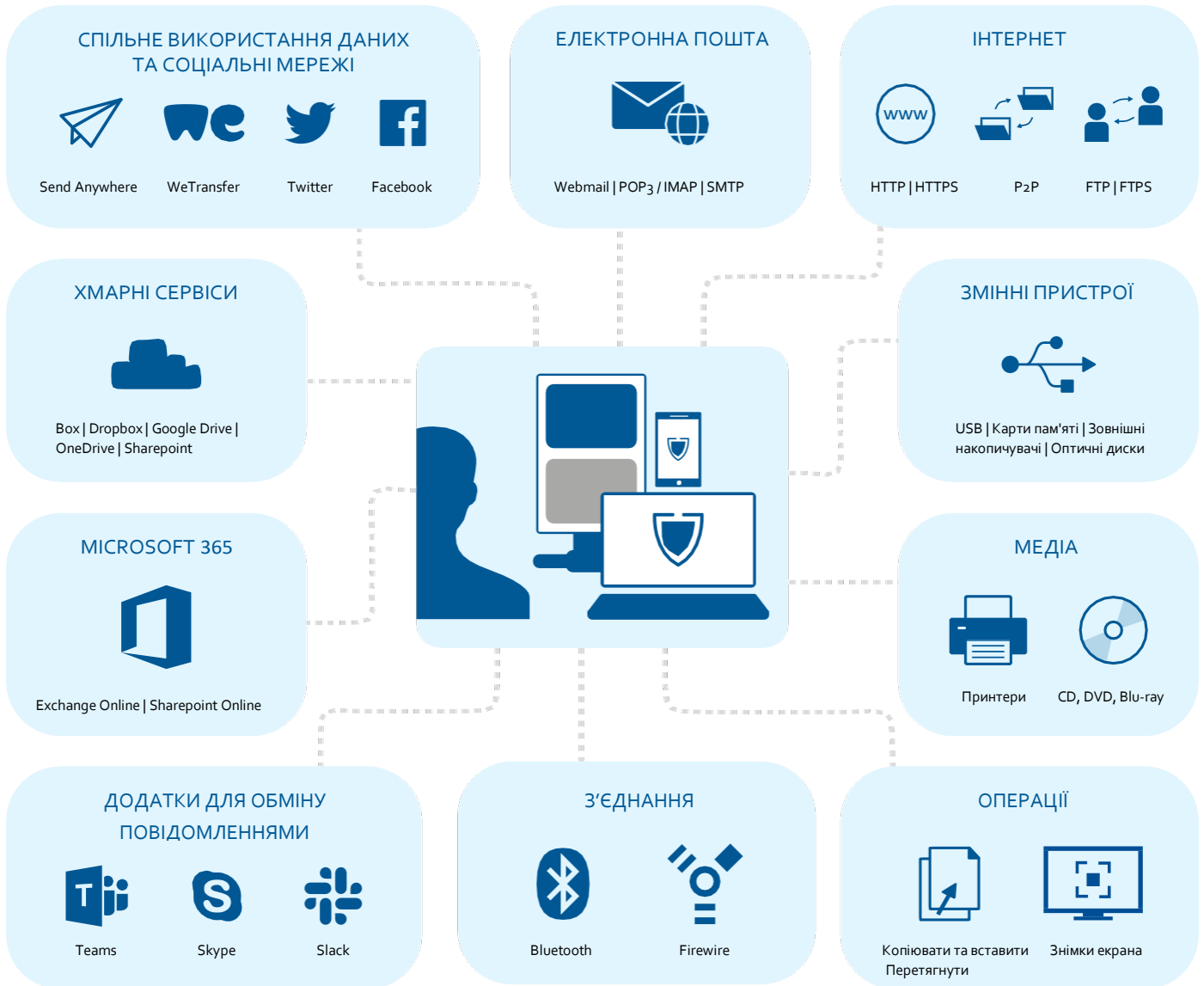
Конфіденційні дані захищені у всіх каналах.

Основні функції

Safetica розпізнає потенційні ризики для конфіденційної інформації. Залежно від того, в якому режимі працює Safetica, рішення може заблокувати підозрілу діяльність, повідомити адміністратора або нагадати працівникам правила безпеки.

Канали даних, які захищає Safetica

Safetica захищає усі конфіденційні дані, перш ніж вони опиняться за межами компанії, незалежно від того, де вони зберігаються та як переміщуються.



Детальні звіти

Safetica забезпечує швидкий та легкий для розуміння огляд усіх можливих загроз з єдиної консолі. Ви маєте можливість отримувати повну інформацію у будь-який час та з будь-якого пристрою, навіть з вашого смартфона.

Ви можете отримувати сповіщення про підозрілу поведінку за допомогою електронної пошти або SIEM, додавати будь-які дані на інформаційну панель та експортувати в формати XLS або PDF для подальшого аналізу.

Технічні вимоги

СЕРВЕР SAFETICA

- Чотириядерний процесор 2,4 ГГц.
- 4 ГБ оперативної пам'яті та більше.
- 100 ГБ вільного місця на диску.
- Спільний або виділений сервер, підтримка віртуальних машин та хмарного хостингу.
- Підключення до сервера з MS SQL 2012 та вище або Azure SQL.
- MS Windows Server 2012 та вище.

КЛІЄНТ SAFETICA

(на захищених комп'ютерах)

- Двоядерний процесор 2,4 ГГц, 2 ГБ оперативної пам'яті та більше.
- 10 ГБ вільного місця на диску MS.
- Windows 7, 8.1, 10.
(32-бітна [x86] або 64-бітна [x64]).
- Пакет інсталяції MSI.
- .NET 4.5.2 та вище.

MS SQL (база даних сервера)

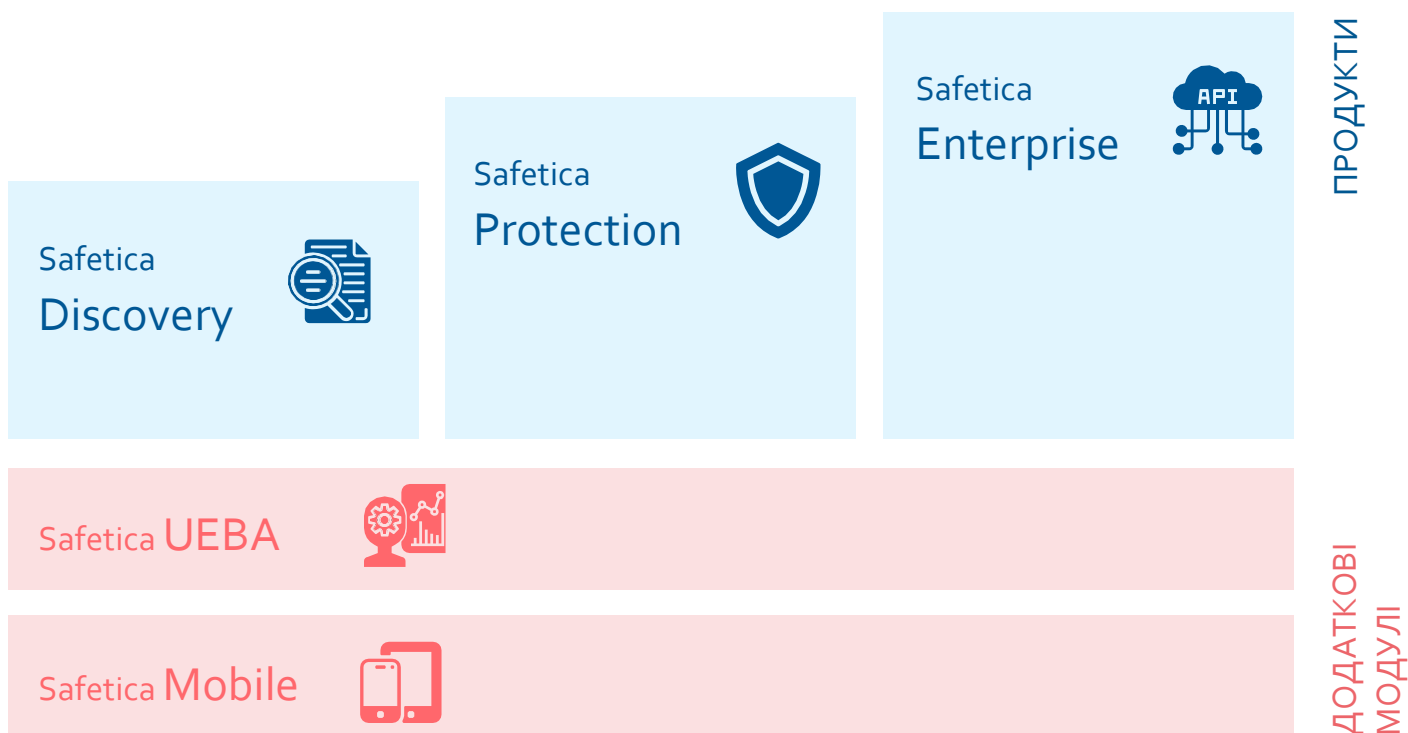
- MS SQL Server 2012 та вище, MS SQL Express 2016 та вище або Azure SQL.
- MS SQL Express є частиною універсального інсталятора та рекомендується для використання до 200 робочих станцій.
- 200 ГБ вільного місця на диску (оптимально 500 ГБ або більше залежно від діапазону зібраних даних).
- Спільний або виділений сервер, підтримка віртуальних машин та хмарний хостинг. Може розміщуватися разом із сервером Safetica.

КЛІЄНТ MAC

- Чотириядерний процесор 2,4 ГГц, 2 ГБ оперативної пам'яті та більше.
- 10 ГБ вільного місця на диску.
- macOS 10.10 ТА вище.
Для повноцінної роботи функцій DLP рекомендовано використовувати macOS.



Портфоліо рішень Safetica



Додаткові модулі

Розширені можливості захисту даних завдяки додатковим модулям.

SAFETICA UEBA (USER AND ENTITY BEHAVIOR ANALYTICS)

- Детальна інформація про реальну активність та поведінку користувачів.
- Вичерпний огляд про використання робочого часу.
- Дії на основі інформації про захист даних та відповідність політикам безпеки.

SAFETICA MOBILE

- Захист даних на мобільних пристроях – смартфонах та планшетах.
- Огляд стану мобільних пристроїв для виявлення ризиків.
- Аудит діяльності як у додатках, так і на веб-сайтах.

SAFETICA DISCOVERY

- Інформація про переміщення конфіденційних даних.
- Детальні звіти про всі важливі дані компанії.
- Базовий огляд поведінки користувачів.
- Аудит безпеки та дотримання нормативних вимог.
- Перші звіти про безпеку даних доступні вже через декілька днів.



SAFETICA PROTECTION

- Універсальне рішення з безпеки, яке поєднує аналітику та класифікацію даних, а також запобігання втраті даних (DLP).
- Повний контроль над переміщенням конфіденційних даних.
- Регулярні звіти про безпеку та повідомлення про інциденти в режимі реального часу.
- Зони Safetica для спрощення захисту даних на високому рівні.
- Просте у розгортанні рішення.



SAFETICA ENTERPRISE

- Рішення для захисту даних, яке дозволяє доповнити систему кібербезпеки підприємства.
- Автоматизована інтеграція рішень сторонніх розробників та функціоналу для розширення можливостей захисту.
- Управління робочими процесами та підтримка багатодомених середовищ.
- Можливість додати до Safetica елементи бренду вашої компанії.



Документація рішення Safetica
go.safetica.com/complete_documentation

Огляд функцій

Сумісність з



Safetica
Discovery



Safetica
Protection



Safetica
Enterprise

Аудит безпеки



Аудит безпеки потоків даних

Здійсніть аудит безпеки потоків даних у всіх каналах, зокрема зовнішніх пристроях, завантаженнях через Інтернет, електронній пошті, додатках для обміну миттєвими повідомленнями, друзі та хмарних сервісах.



Аудит файлів та електронної пошти Office 365

Здійсніть аудит файлових операцій та вихідних повідомлень електронної пошти в Office 365.



Аудит дотримання нормативних вимог

Виявляйте порушення нормативних актів, таких як PCI-DSS, GDPR або HIPAA.



Аудит безпеки робочого простору

Здійсніть аудит використання корпоративних пристроїв, програм, мереж та друку. Для збереження та зменшення витрат знаходьте ресурси, які не використовуються або використовуються неправильно.



Класифікація перевірки вмісту

Класифікуйте конфіденційні файли та електронні листи завдяки потужному контролю вмісту за допомогою заздалегідь визначених шаблонів або спеціальних правил та словників.



Виявлення підозрілої діяльності

Швидко реагуйте завдяки виявленню підозрілої діяльності в режимі реального часу та миттєвих сповіщеннях електронною поштою.



Захист даних на робочих станціях



Захист електронної пошти та мережі

Застосовуйте захист даних для електронної пошти, завантажень через Інтернет, додатків для обміну миттєвими повідомленнями та спільного використання мережі.



Захист пристроїв та друку

Управляйте потоками даних на зовнішніх пристроях та захищайте конфіденційні дані від несанкціонованого друку на локальних, мережевих або віртуальних принтерах.



Захист під час віддаленої роботи

Запобігайте витокам даних на віддалених робочих станціях або під час підключення до віддаленого робочого столу. Володіє підтримкою багатьох рішень для віддаленого доступу.



Розширена класифікація даних

Використовуйте передові технології для виявлення та позначення конфіденційних даних на основі походження, контексту робочого процесу або типу файлу. Відчуйте переваги виявлення метаданих під час використання класифікацій сторонніх виробників. Дозвольте користувачам самостійно класифікувати файли.



Різні політики відновлення

Гнучко реагуйте на виявлені інциденти для навчання власних співробітників. Інциденти можна реєструвати, блокувати або об'єднувати/блокувати за допомогою скасування.



Тіньова копія інциденту Зберігайте докази інцидентів, створюючи тіньові копії даних. Тіньові копії повністю зашифровані і можуть зберігатися на локальних комп'ютерах із дотриманням політики збереження.	×	✓	✓
Контроль робочого простору Визначте свій захищений робочий простір та зменште периметр за допомогою контролю додатків та веб-сайтів. Уникайте небажаної поведінки у вашій компанії та зменшуйте витрати на управління безпекою.	×	✓	✓
Зони Safetica Просте управління безпекою периметра даних за допомогою унікальних зон Safetica, які значно зменшують кількість політик захисту даних.	×	✓	✓
Управління шифруванням BitLocker Централізоване управління локальними дисками та зовнішніми пристроями за допомогою шифрування BitLocker.	×	✓	✓
Захист хмарних даних	×	✓	✓
Захист хмарної синхронізації робочої станції Захищайте дані для хмарних дисків на робочих станціях, наприклад OneDrive, Google Drive, Dropbox, Box тощо.	×	✓	✓
Захист робочої станції Office 365 Захищайте дані на робочих станціях Office 365 і SharePoint. Перешкоджайте обміну або завантаженню певних даних в хмару.	×	✓	✓
Azure Information Protection Виявляйте класифікації даних в Microsoft Azure Information Protection навіть в зашифрованій формі.	×	✓	✓
Exchange Online Protection Об'єднайте правила електронної пошти для робочих станцій та хмарної пошти. Управляйте та фільтруйте вихідні дані з робочих станцій та Exchange Online.	×	✓	✓
Особливості для корпорацій	×	×	✓
Використання бренду компанії Можливість зміни логотипу у сповіщеннях для користувачів.	×	×	✓
Контроль робочого процесу Налаштування прикладних та експертних політик для узгодження робочих процесів кінцевих користувачів та компанії.	×	×	✓
Багатодоменна підтримка Багатодоменна підтримка для Active Directory.	×	×	✓
Автоматизація безпеки	×	×	✓
Інтеграція з SIEM Автоматизоване звітування про інциденти для SIEM-рішень (Splunk, QRadar, LogRhythm, ArcSight тощо).	×	×	✓

ПРО SAFETICA

Safetica – чеська компанія, яка займається розробкою програмного забезпечення для запобігання втраті даних компаній усіх розмірів. Адже кожна компанія має знати, що її конфіденційні дані надійно захищені.

300 000+

захищених
пристроїв



1 600+

користувачів



120+

країн



80+

експертів
із безпеки



ТЕХНОЛОГІЧНІ АЛЬЯНСИ



НАГОРОДИ ТА ДОСЯГНЕННЯ



THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

FORRESTER

Gartner



А як щодо ваших даних?

Спробуйте пробну версію
Safetica вже зараз!

