

# Чому компаніям необхідне DLP-рішення та чому варто обрати Safetica?

Захист даних має бути пріоритетним завданням

10 причин, чому варто інвестувати в DLP-системи та використовувати рішення Safetica

Навіщо компаніям потрібні рішення для запобігання втраті даних (DLP)	Чому варто обрати Safetica
1 Контролювати використання конфіденційних даних компанії, зокрема де вони зберігаються, як переміщуються та хто має доступ до них.	Safetica дозволяє легко переглядати, які дані компанії поширюються різними каналами та платформами (з підтримкою macOS та Windows), забезпечуючи повний огляд незалежно від зберігання чи надходження даних.
2 Запобігати викраденню або випадковому розголошенню конфіденційної інформації співробітниками або партнерами.	Safetica аналізує внутрішні ризики, виявляє загрози та зменшує їх негативний вплив. Рішення контролює гібридний робочий простір, виявляє небажане програмне та апаратне забезпечення, аналізує поведінку співробітників.
3 Зменшити негативний вплив, ймовірність отримання штрафів та втрачений дохід, пов'язані з витоком даних.	Safetica швидко розгортається та легко інтегрується в існуючу IT-інфраструктуру, що мінімізує проблеми сумісності. Рішення забезпечує покращений захист даних та продуктивність без затримок та збоїв у роботі.
4 Дотримуватись складних нормативних вимог під час аудиту безпеки.	Safetica допомагає виявляти, запобігати порушенню нормативних актів. Можливості аудиту підтримують розслідування інцидентів, тому рішення забезпечує відповідність нормам, зокрема GDPR, HIPAA тощо.
5 Забезпечити захист даних від ризиків безпеки, спричинених використанням BYOD та IoT.	Класифікація даних Safetica захищає від спроб обійти DLP-рішення, навіть якщо файли заархівовані, зашифровані або мають інше розширення. Цей захист поширюється на нові документи та файли, які залишають захищену робочу станцію.
6 Відстежувати будь-яку неналежну чи незвичайну поведінку співробітників в організації.	Safetica аналізує, виявляє та зменшує внутрішні ризики у гібридному робочому просторі. Рішення виявляє небажане апаратне та програмне забезпечення, а також перевіряє поведінку користувачів.
7 Завчасно запобігати несанкціонованому використанню даних на робочих станціях як у корпоративній мережі, так і поза нею.	Рішення допомагає обмежити використання портативних пристроїв або неавторизованих носіїв інформації. Safetica залишається повністю активним незалежно від підключення до мережі. Після відновлення з'єднання всі зібрані записи синхронізуються.
8 Розуміти індивідуальну і командну продуктивність та знати, що робить деяких співробітників або команди більш продуктивними, ніж інші.	Safetica допомагає об'єктивно аналізувати дії користувачів у корпоративному середовищі та визначати належність використання обладнання та мережі компанії.
9 Автоматизувати корпоративне управління для покращення відповідності, економії часу та ресурсів.	Safetica дозволяє налаштувати політики безпеки для певних груп або окремих осіб. Для цього варто обрати потрібну дію для робочого процесу — від аудиту чи сповіщення до блокування.
10 Зміцнити конкурентні переваги, а також репутацію компанії на ринку.	Safetica захищає важливі дані та допомагає запобігти втраті репутації та доходу, які виникають після витоку даних.