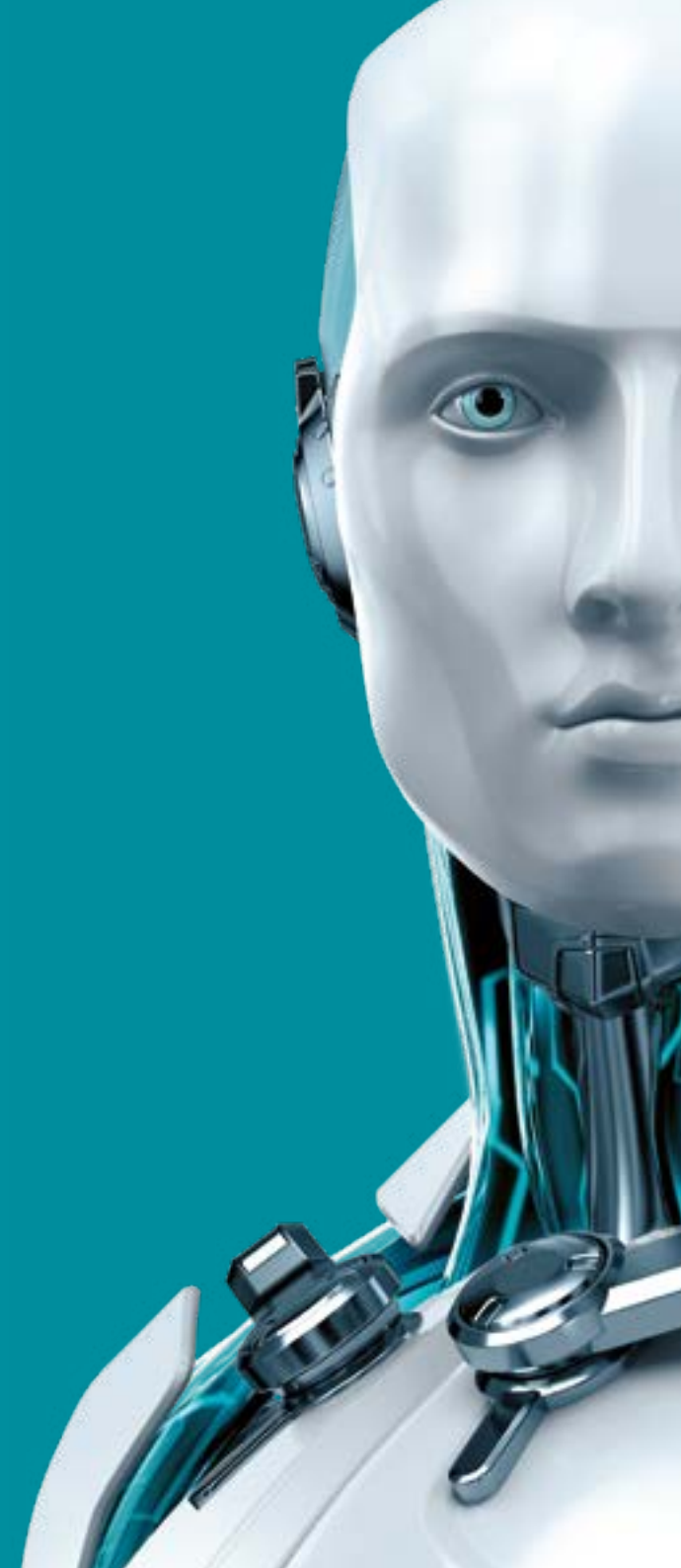
safetica

Data Leak Prevention

BUSINESS

ESET TECHNOLOGY ALLIANCE



safetica

Safetica е елегантно решение, което предотвратява изтичането на чувствителна информация от вашата компания. Проверява и защитава комуникационните канали – уебсайтове, приложения и имейл кореспонденция. Ние следим за промени в поведението на служителите и разкриваме какво се случва в организацията ви наистина. Safetica е лесна за инсталация и управление, като подсигурява всички вътрешни информационни канали.

Философията ни се гради на 3 основни стълба: завършено решение, гъвкавост и лекота на работа.

Решението ни предоставя пълни репорти за дейността на служителите ви и позволява налагането на политики за сигурност върху действията им. Safetica обединява предимствата и функционалностите на няколко типа решения за сигурност в един завършен пакет.

Основни предимства

Завършено DLP решение	Спира изтичането на информация от всички основни канали.
Бърза възвращаемост на инвестицията	Гъвкаво решение срещу източване на информация с минимално време за инсталация и конфигурация.
Спира неподходящи действия	Гарантира консистентна защита – дори и при работа на служители с администраторски права.
Максимално ниво на защита от източване на информация	Safetica спира кражбата на информация чрез скрийншоти, клипборд инструменти, виртуално принтиране, копиране и изпращане на файлове, архивиране и криптиране.
Независимо решение	Safetica работи независимо и не е ограничена от индивидуални протоколи и приложения.
Ясно дефинирани политики за сигурност	Благодарение на функционалността Safe Areas, IT мениджърите могат просто да изберат границите, които информацията не може да напуска – а Safetica ще се погрижи за останалото.
Точно следене на време	Отворено приложение не означава използвано приложение. Репортите за дейността на служителите ви показват реалното време, в което те са били активни в работата си с уебсайт или приложение.
Автоматична оценка и нотификации	Safetica избира най-важната записана информация и изпраща дневен репорт на определени получатели. Завършените репорти са достъпни по всяко време.

Как работи

Решението ни работи на ниво работна станция - там, където потребителите достъпват критична информация, влизат в интернет, четат имейли, принтират и използват личните си памети и преносими харддискове. Просто инсталирайте клиента (Safetica Endpoint Client) на желаните работни станции и поддържайте редовна връзка с тях посредством общ сървър (Safetica Management Service). В този сървър се съхранява базата данни с дейността на служителите ви и се конфигурират и разпращат политиките за сигурност.

Функционалности

Защита от източване на информация (Data Leak Prevention)	Safetica защитава всички водещи канали за източване на информация, като същевременно е лесна за инсталиране и работа. Пълна информация за възможностите на решението ни може да намерите в Endpoint Events Coverage.
Профилиране на служители	Предупреждава мениджмънта на организацията в случай на резки промени в продуктивността на служителите и я показва по отдели във времето. И двете промени са потенциални сигнали за рискове, свързани със сигурността.
Репорти за продуктивност	Разкрива злоупотреби и пробиви в защитата на информацията като следи потребителските дейности за потенциални опасности – още преди да се стигне до източването на информация.
Защита от източване на информация през имейл	Гарантира, че защитената информация няма да попадне в неподходяща пощенска кутия. Записва къде са изпращани чувствителни файлове и съхранява информация за бъдещи репорти.
Контрол и графици за използване на приложения	Позволява работа само с избрани приложения, свързани с работата на служителите ви и блокира останалите, с което увеличава нивото на сигурност. Можете да задавате и часови зони, в които да бъде разрешено използването на определени приложения.
Филтриране на неподходящо уеб съдържание	Лесно прилагане на AUP (Acceptable Use Policy) – политика за използване на интернет в компанията ви – с филтриране по категории или ключови думи.
Контрол върху принтиране	Ограничава кой и какво принтира със задаване на квоти за отделни потребители или цели отдели.
Контрол върху USB памети и преносими харддискове	Спира използването на неоторизирани устройства от служителите в инфраструктурата на организацията ви. Позволява да се използват само определени устройства – или тотална забрана.
Управление на криптиране	Safetica позволява криптиране на целия диск или партишъни и позволява създаването на виртуални дискове за по-сигурно съхранение на информация. Криптираните данни могат да бъдат достъпвани чрез парола или частен ключ. Може да използвате и нашите Travel Disks, с които информацията се криптира автоматично след излизане от защитена зона.
Лесно имплементиране и задаване на тестови сценарии	Помага на организации от всякакъв мащаб да интегрират политика за защита на информация като разрешава тестването на различни сценарии, преди да бъдат въведени окончателно и да спрат бизнес процесите.
Бързо класифициране на информация и задаване на политики	Защитава информацията веднага, щом тя попадне в мрежата или на работните ви станции – или бъде класифицирана.
Централизирано управление	Safetica Management Console позволява цялостно управление на сигурността и репортинг, интегрира системите за защита на компанията и политиките за блокиране на информация.
Проверка за SSL/HTTPS	Проверява и защитава обмена на данни със сайтове, включително и такива, използващи SSL сертификати (през HTTPS), чат приложения и имейли.
Минимална обща цена на собственост (TCO)	Максимално ниво на защита без необходимост от инвестиция в допълнителни устройства за защита. Агентите на работните станции защитават цялата мрежа от източване на информация.
Гъвкави възможности за употреба	Универсалният ни подход позволява да защитавате на практика всяко приложение, чат протокол или услуга за уебмейл.

Какво следим и блокираме

Блокиране и репортинг

- Всички операции с файлове
- Дългосрочни тенденции и краткосрочни промени в тях
- Уебсайтове (поддържаме всички водещи браузъри и следим и HTTPS трафик) – активност и липса на такава
- Имейл клиент и уебмейли (всички възможни услуги)
- Търсени ключови думи (в онлайн търсачки и Windows Search)
- Чат приложения (независимо от техния тип – следим протоколите)
- Използване на приложения – с време на (не)активност
- Виртуални, локални и мрежови принтери
- Активност на екрана (интелигентно следене и скрийншоти)
- Запис на бутоните на клавиатурата

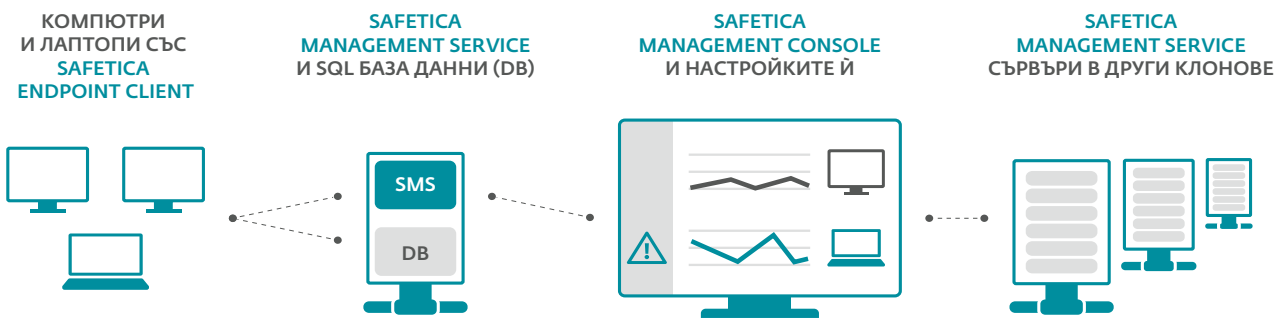
Защита от изтичане на информация (DLP)

- Всички видове харддискове, USB, FireWire, SD/MMC/CF карти, SCSI дискове
- Трансфер на данни през мрежа (защитен и незащитен)
- Имейли (SMTP, POP, IMAP, Microsoft Outlook/ MAPI протоколи)
- SSL/HTTPS (всички браузъри и приложения със стандартно управление на сертификати)
- Копиране/поставяне на информация, клипборд, drag & drop
- Виртуални, локални и мрежови принтери
- Bluetooth, IR/COM/parallel портове
- CD/DVD/BluRay четящи и записващи устройства
- Контрол на достъпа до файлове от приложения

С какво можем да сме полезни:

Защита на ключова информация за бизнеса ви	Следим (без видим ефект) всяка интеракция с определените за ключови файлове и директории с информация за неоторизирани действия, които блокираме – или коригираме с други, позволени такива и зададени от вас. Определените от вас служители (например, мениджър по сигурността) могат да получават известия за всяко събитие. Данните могат да бъдат автоматично криптирани. Може да зададете какво да случи при дадено поведение, за да защитите информацията на лаптопи, USB памети, преносими харддискове – дори и те да се намират извън пределите на организацията ви.
Управление на преносими памети и харддискове	Пълен контрол от страна на мениджмънта на това кой какви устройства за пренос на данни използва – с което елиминирате един от основните канали за изтичане на данни.
Съвместимост с регулации	Инсталацията на Safetica Endpoint Client на работните станции на служителите и активирането на политики чрез Safetica Management Console позволява да покриете по-лесно изискванията на различни регулации, свързани с работата и преноса на лични данни – включително и GDPR.
Криптиране на информация	Safetica позволява да управлявате криптирането на дискове, както и да управлявате свързаните ключове и да забраните съхраняването на информация на локации с ниско ниво на сигурност.
Контрол на производителността	Получавайте регулярни репорти за дейността на отделни или групи от служители на мейла си или ги следете през администраторския панел.

Архитектура



1. Записва се активността и се налагат политики посредством малко клиентско приложение (може да бъде и скрито за потребителя).

2. Информацията се прехвърля автоматизирано от компютрите в мрежата на сървъра, като данните от преносимите компютри се прехвърлят при свързване с мрежата. Настройките на клиентското приложение се синхронизират в обратен ред.

3. Цялата събрана информация може да бъде преглеждана през приложението за управление. Могат да се задават и коригират настройки и политики.

4. Safetica поддържа управлението на повече от един клон от едно място.

Системни изисквания

Safetica клиент

- двуядрен процесор, 2,4 GHz
- 2 GB RAM памет
- 10 GB свободно дисково пространство
- MS Windows 7 или по-нова версия, 32- или 64-битова

Safetica сървър

- двуядрен процесор 2 GHz (препоръчваме използването на четириядрена архитектура)
- 4 GB RAM памет
- 20 GB свободно дисково пространство
- Инсталация на приложение на споделен или собствен сървър (може и виртуален)
- Поддръжка на Active Directory
- MS Windows Server 2008 R2 и по-нови версии, 32- и 64-битови
- Изисква свързаност на сървъра с MS SQL 2008 R2 или по-нова версия
- При сподеяне с MS SQL препоръчваме поне четириядрен процесор, 8 GB RAM и 100 GB свободно дисково пространство

MS SQL (база данни за сървъри)

- Конфигурация спрямо версията на MS SQL
- Споделен или собствен сървър, препоръчваме поне 100 GB свободно дисково пространство
- MS SQL 2008 R2 и по-нова версия, MS SQL 2012 Express и по-нова версия (безплатна версия)
- MS SQL 2012 Express може да бъде част от инсталацията