

SAFETICA 7

OCHRONA PRZED WYCIEKIEM DANYCH (DLP)

**Chcesz gwarancji, że konkurencja nie wykradnie Twoich danych?
Pewności, że w firmowej sieci nie ma już luk, którymi wyciekną dokumenty?
Przekonania, że wydatkujesz budżet IT w optymalny sposób?**

Nieograniczony dostęp pracowników do wrażliwych firmowych danych często powoduje kłopoty. Zarząd nie wie, w jaki sposób są one przetwarzane, ani gdzie i przez kogo przesyłane dalej. **Safetica rozwiązuje ten problem prześwietając i raportując wszystkie działania użytkowników pracujących z wrażliwymi danymi.** Safetica ocenia też ryzyko wystąpienia incydentów bezpieczeństwa, ostrzegając zarząd przed nieproduktywnymi i potencjalnie szkodliwymi działaniami pracowników.

KLUCZOWE ZALETY

- **Kompleksowe rozwiązanie problemu DLP (Data Leak Prevention).** Safetica skutecznie blokuje wszystkie kanały potencjalnego wycieku danych.
- **Błyskawiczne wdrożenie.** Dzięki elastycznemu podejściu do blokowania potencjalnych wycieków danych, Safetica oferuje najszybsze wdrożenie spośród produktów w swojej klasie.
- **Wysoka odporność na szkodliwe działania od wewnątrz** zapewnia spójną ochronę wszystkich kanałów potencjalnego wycieku danych nawet przed użytkownikami z uprawnieniami administratora.
- **Podejście globalne.** Ochrona danych rozwiązaniem Safetica nie jest ograniczona indywidualnymi protokołami ani aplikacjami.
- **Śledzenie dokładnego czasu aktywności.** "Otwarty" nie znaczy "aktywnie używany". Raporty aktywności rozwiązania Safetica wykazują realny czas aktywności użytkowników na stronach i w aplikacjach.
- **Automatyczna ocena aktywności i alerty.** Safetica gromadzi i sumuje najważniejsze dane w raportach wysyłanych wskazanym odbiorcom. Pełne raporty dostępne są na żądanie.
- **Zarządzanie bezpieczeństwem danych z jednego miejsca** ułatwia przydzielanie dostępu do określonych danych i konfigurowanie raportów aktywności użytkowników.
- **Analityka dla menedżerów w narzędziu WebSafetica dostarcza informacji o bezpieczeństwie firmy z poziomu przeglądarki.** WebSafetica wspiera wszystkie przeglądarki i urządzenia mobilne, pozwalając monitorować poziom ochrony w dowolnym miejscu i czasie.
- **Minimalne koszty wdrożenia i zarządzania.**
- **Aplikacja Safetica Mobile** chroni wrażliwe dane na urządzeniach mobilnych i oferuje zarządzanie wszystkimi firmowymi telefonami i tabletami z jednego miejsca.

NAJWAŻNIEJSZE FUNKCJE

Pełny audyt przesyłanych danych i aktywności użytkowników	Zyskaj pełen ogląd wszystkich potencjalnie ryzykownych akcji w twojej firmie.
Kompletna ochrona przed wyciekami danych (DLP)	Safetica blokuje wszystkie kanały potencjalnego wycieku danych będąc przy tym rozwiązaniem łatwym w instalacji i obsłudze.
Tryb Audytora i Informacyjny	Safetica pozwala etapowo wdrożyć ochronę danych. W pierwszym kroku zbieramy informacje na temat procesów, następnie edukujemy użytkowników, a dopiero na końcu wdrażamy docelowy zestaw reguł.
Trendy i profilowanie produktywności	Rozwiązanie alarmuje kierownictwo o zmianach w aktywności pracowników i produktywności całych działów firmy w wybranym okresie czasu. Zmiany te często są wskaźnikami potencjalnych luk w bezpieczeństwie firmowych danych.
Blokowanie stron i aplikacji	Safetica umożliwia korzystanie z wybranego zestawu powiązanych z pracą aplikacji i blokuje pozostałe zwiększając bezpieczeństwo firmowej sieci. Wybrane aplikacje można udostępniać w określonym wymiarze czasu. Możemy również spersonalizować uprawnienia dostępu do wybranych stron internetowych dla każdego pracownika.
Kontrola druku (redukcja kosztów)	Safetica oferuje przydzielanie uprawnień do druku określonych dokumentów poszczególnym działom i użytkownikom.
Zarządzanie nośnikami wymiennymi	Rozwiązanie uniemożliwia podłączanie do firmowej sieci urządzeń i nośników nieautoryzowanych.
Szyfrowanie komputerów i nośników wymiennych	Safetica pozwala szyfrować pamięci flash i zawartość całych komputerów, odcinając dostęp do wrażliwych informacji niepowołanym osobom.
Aplikacja Safetica Mobile	Zabezpiecz firmowe urządzenia mobilne na wypadek utraty lub kradzieży i zarządzaj ich bezpieczeństwem z jednego miejsca.
Inspekcja SSL/HTTPS	Rozwiązanie sprawdza na wypadek wycieku danych wszystkie firmowe kanały komunikacji - włącznie z protokołem HTTPS i komunikatorami (IMA - instant messaging apps).

ZASTOSOWANIA

Ochrona kluczowych informacji

Po zdefiniowaniu stref bezpieczeństwa danych i umieszczeniu w nich plików Safetica dyskretnie sprawdza każdą interakcję użytkowników z tymi plikami, a w przypadku operacji zabronionej blokuje i loguje zdarzenie. W zdefiniowanych sytuacjach wysyła również e-mailem powiadomienie np. do administratora bezpieczeństwa informacji (ABI).

Zarządzanie kanałami komunikacji

Zarządzaj nośnikami wymiennymi, blokuj ryzykowne strony www i zastrzeż wysyłanie e-maili z wrażliwymi danymi, dzięki czemu Twój dział IT zyska kontrolę nad przepływem krytycznych informacji.

Szyfrowanie danych

Safetica oferuje pełne szyfrowanie dysku, zarządza kluczami dostępu i chroni dane przed wyciekiem z zabezpieczonych lokalizacji. Użytkownicy mogą też szyfrować nośniki zewnętrzne dla zwiększenia poziomu bezpieczeństwa.

Spełnienie wymogów prawnych

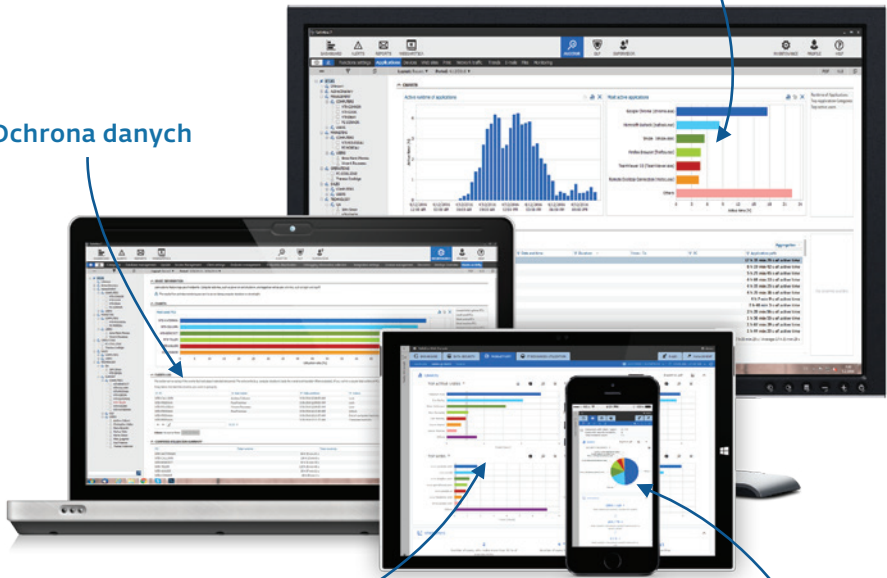
Poprzez aktywne polityki bezpieczeństwa w konsoli Safetica Management Console oraz rozwiązywanie Safetica Endpoint Client na stacjach roboczych, spełniasz prawne wymogi przetwarzania i wykorzystania danych wrażliwych. Ustaw reguły w konsoli na stacji roboczej, a potem monitoruj je online narzędziem WebSafetica.

Kontrola wydajności pracy pracowników

Menedżerowie mogą otrzymywać regularne raporty aktywności poszczególnych użytkowników oraz ich grup. Raporty mogą być dostarczane na skrzynkę e-mail, przeglądane w konsoli Safetica lub usłudze WebSafetica.

Najaktywniejsze aplikacje

Ochrona danych



Produktywność

Incydenty bezpieczeństwa

WYBRANE REFERENCJE

Coca-Cola Sabco

JTEKT



PRAGUE 4
CITY DISTRICT

ARCHITEKTURA



Stacje robocze, laptopy i urządzenia mobilne z zainstalowanym klientem Safetica

Aplikacja (możliwa do ukrycia przed użytkownikiem) rejestruje wszystkie działania na chronionym urządzeniu, narzucając polityki bezpieczeństwa wyznaczone przez Administratora.

Serwer i baza danych

Dane klientów są automatycznie przesyłane do serwera zdalnej administracji. W przypadku laptopów i urządzeń mobilnych synchronizacja następuje przy pierwszym połączeniu do firmowej sieci.

Konsola zarządzająca Safetica

Podgląd i wizualizacje wszystkich danych gromadzonych przez aplikacje klienckie. Z tego poziomu Administrator ma też możliwość zmiany ustawień.

WebSafetica

Narzędzie analityczne WebSafetica oferuje podgląd danych z aplikacji klientów w dowolnej przeglądarce (również na urządzeniach mobilnych).

KOMPLEKSOWA OCHRONA STACJI ROBOCZYCH

Raportowanie i blokowanie aktywności

- wszystkie operacje na plikach, wsparcie dla zdalnego dostępu (RDP) i dysków chmurowych
- krótkoterminowe zmiany aktywności, trendy długoterminowe
- czas aktywności i nieaktywności użytkowników na stronach www (wszystkie przeglądarki włącznie z ruchem HTTPS) i w aplikacjach
- poczta e-mail i webmail (przez przeglądarkę) na protokołach SMTP, POP, IMAP, Microsoft Outlook / MAPI
- drukarki wirtualne, lokalne i sieciowe
- wykorzystanie komputera i sieci lokalnej
- wsparcie dla serwerów terminalowych

Ochrona przed wyciekami danych

- wszystkie dyski twarde, nośniki USB, CD/DVD, FireWire, karty pamięci SD/MMC/CF, Bluetooth i inne
- transfer plików wewnątrz firmowej sieci (chronionej i niechronionej) - HTTPS/SSL
- poczta e-mail (protokoły SMTP, POP, IMAP, Microsoft Outlook / MAPI)
- wykrywanie i blokada dysków chmurowych
- wysyłka i pobieranie plików przez przeglądarki
- szyfrowanie dysków twardych oraz dysków przenośnych
- kopiowanie na zasadach „kopiuj/wklej”, „przeciągnij/upuść”, możliwość blokady schowka systemu
- drukarki wirtualne, lokalne i sieciowe
- kontrola dostępu do plików przez aplikacje

WSPARCIE TECHNICZNE

Strona produktu:

www.eset.pl/Safetica

Wsparcie techniczne:

32 259 11 88 / pomoc@dagma.pl

Baza wiedzy:

www.safetica.com/support

O FIRMIE SAFETICA TECHNOLOGIES

Safetica Technologies to wiodący dostawca rozwiązań bezpieczeństwa IT w zakresie wewnętrznej ochrony firmowej sieci. Misją firmy jest eliminacja zagrożeń powodowanych wspólną przyczyną - czynnikiem ludzkim. Celem Safetica jest eliminacja zagrożeń wywołanych przez użytkowników tak, by chronione przed nimi firmy i organizacje mogły się skupić na prowadzeniu biznesu. Rozwiązania Safetica dostępne są w ponad 50 krajach na 5 kontynentach.

MINIMALNE WYMAGANIA SPRZĘTOWE

Safetica Endpoint Client

(oprogramowanie na stacje robocze)

- 2,4 GHz dual-core procesor 32-bit (x86) lub 64-bit (x64)
- 2 GB pamięci RAM
- 10 GB miejsca na dysku twardym
- MS Windows 10, 8.1., 8, 7 (32-bit i 64-bit)

Safetica Management Service

(komponent serwera)

- 2 GHz dual-core procesor 32-bit (x86) lub 64-bit (x64)
- 4 GB pamięci RAM
- 20 GB miejsca na dysku twardym
- instalacja na serwerze aplikacyjnym lub dedykowanym (z możliwością wirtualizacji)
- wsparcie dla Active Directory
- MS Windows Server 2003 SP2, 2008, 2008 R2, 32-bit i 64-bit
- wymaga łączenia z serwerem za pomocą MS SQL2008 lub wyższej wersji
- przy współdzieleniu z MS SQL rekomendowana konfiguracja to 8 GB pamięci RAM i minimum 100 GB miejsca na dysku

MS SQL

(baza danych dla serwera)

- wewnętrzne wymagania SQL
- przy korzystaniu ze współdzielonego lub dedykowanego serwera rekomendowana konfiguracja to minimum 100 GB miejsca na dysku
- wsparcie dla MS SQL 2008 R2 i wyższych wersji oraz MS SQL 2012 Express (bezpłatne narzędzie) i wyższych wersji
- instalacja MS SQL 2012 Express jest opcjonalna
- WebSafetica jest dostępna wyłącznie dla MS SQL 2012 i wyższych wersji

Biuro Bezpieczeństwa IT DAGMA sp. z o.o.

ul. Bazantów 4/2, 40-668 Katowice
tel. 32 793 11 00 | handel@dagma.pl