safetica

OCHRONA PRZED WYCIEKIEM DANYCH

Chcesz gwarancji, że konkurencja nie wykradnie Twoich danych?

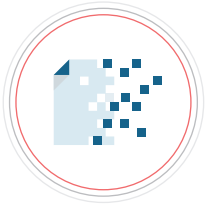
Pewności, że w firmowej sieci nie ma luk, którymi wyciekną dokumenty?

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 prześwietlając 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.

Ochrona przed wyciekiem danych

Safetica skutecznie blokuje wszystkie potencjalne kanały wycieku danych.



Szyfrowanie danych na komputerach i nośnikach wymiennych

Safetica umożliwia centralne zarządzanie programem szyfrującym BitLocker, wbudowanym w system operacyjny Windows. Zarządzanie odbywa się za pomocą konsoli. Dzięki temu oferuje pełne szyfrowanie dysków twardych, zarządzanie kluczami dostępu i ochronę danych przed wyciekiem z zabezpieczonych lokalizacji. Użytkownicy mogą również - dla zwiększenia poziomu bezpieczeństwa - szyfrować nośniki zewnętrzne typu pendrive.

Zarządzanie kanałami komunikacji

Safetica pozwala klasyfikować pliki jako dane wrażliwe zarówno w oparciu o zawartość jak i kontekst. Zabezpiecza przed wypływem informacji wskazanych jako dane wrażliwe, dzięki możliwości **ustawienia blokad:**

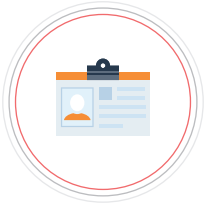
- przechowywania danych wrażliwych na dyskach lokalnych
- kopiowania danych wrażliwych na pendrive i CD
- dostępu do pendrive i urządzeń przenośnych
- wydruku danych wrażliwych na drukarkach lokalnych, sieciowych i wirtualnych
- kopiowania zawartości pliku z danymi wrażliwymi do innego pliku
- przesyłania danych wrażliwych na strony www oraz do chmury
- wysyłania danych wrażliwych poprzez email, pocztę webową, komunikatory

Raportowanie i kontrola efektywności

Safetica gromadzi najważniejsze dane nt. aktywności pracowników na stronach i w aplikacjach. Udostępnia wskazanym odbiorcom raporty, zawierające tego typu informacje.

Ochrona kluczowych informacji

Po zdefiniowaniu stref bezpieczeństwa danych i zdefiniowaniu plików wrażliwych, Safetica dyskretnie sprawdza każdą interakcję pracowników z tymi plikami.
W przypadku operacji zabronionej, blokuje i loguje zdarzenie. We wskazanych sytuacjach wysyła również e-mailem powiadomienie np. do inspektora ochrony danych (IOD).



Kontrola wydajności pracy pracowników

Dzięki funkcji generowania regularnych raportów aktywności poszczególnych pracowników lub grup roboczych, managerowie mogą mierzyć produktywność pracowników, rozumianą jako czas spędzony w konkretnych aplikacjach lub stronach www. Raporty mogą być dostarczane na skrzynkę e-mail lub przeglądane w konsoli Safetica.

Trendy i profilowanie produktywności

Rozwiązanie alarmuje kierownictwo o zmianach w aktywności pracowników i produktywności całych działów firmy, w wybranym okresie czasu. Raporty zawierają informacje o krótkoterminowych zmianach aktywności oraz trendach długoterminowych. Zmiany te często są wskaźnikami potencjalnych luk w bezpieczeństwie firmowych danych.

Blokowanie stron i aplikacji oraz kontrola druku

Safetica umożliwia blokadę wybranych aplikacji oraz stron zwiększając bezpieczeństwo firmowej sieci. Wybrane aplikacje można udostępniać w określonym wymiarze czasu. Można również spersonalizować uprawnienia dostępu do wybranych stron internetowych dla każdego pracownika. Safetica oferuje przydzielanie uprawnień do druku, określonych dokumentów, poszczególnym działom i pracownikom. Umożliwia również kontrolę użycia konkretnej drukarki przez pracownika.

Funkcjonalność

Celem Safetica jest eliminacja intencjonalnych oraz przypadkowych zagrożeń, związanych z wyciekiem danych.

Pełen audyt przesłanych danych i aktywności użytkowników

Zyskaj pełen ogląd wszystkich potencjalnie ryzykownych aktywności w twojej firmie.

Tryb discovery 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.

Inspekcja SSL/HTTPS

Rozwiązanie sprawdza wszystkie firmowe kanały komunikacji – włącznie z protokołem HTTPS i komunikatorami (IMA – instant messaging apps).

Błyskawiczne wdrożenie

Dzięki elastycznemu podejściu do blokowania potencjalnych wycieków danych, Safetica oferuje najszybsze wdrożenie spośród produktów DLP.

Zarządzanie bezpieczeństwem danych z jednego miejsca

Safetica pozwala na centralne zarządzanie: dystrybucję uprawnień oraz dostępu do danych, a także konfigurowanie raportów z jednego miejsca.

WebSafetica

To narzędzie webowe (dostępne przez przeglądarki internetowe) dostarczające informacji nt. bezpieczeństwa firmy.

Spełnienie wymogów prawnych RODO

Safetica gromadzi najważniejsze dane nt. aktywności pracowników na stronach i w aplikacjach. Udostępnia wskazanym odbiorcom raporty, zawierające tego typu informacje.

§

art. 5.2 RODO

Wsparcie dla wymogów rozliczalności

Administrator Safetica ma wiedzę na temat tego, co dzieje się z danymi, które zostały otagowane jako wrażliwe / poufne (sklasyfikowane jako dane osobowe z punktu widzenia RODO lub informacje stanowiące tajemnicę przedsiębiorstwa).

§

art. 5.1c RODO

Wsparcie dla wymogów minimalizacji danych (adekwatności)

Zapobiega wykorzystaniu danych do celów niezgodnych z pierwotnymi celami. Safetica pozwala otagować pliki wrażliwe i nie zezwoli na wykonanie zdefiniowanych operacji na tych plikach.

§

art. 25 RODO

Wsparcie dla ochrony w fazie projektowania (security by design)

Safetica posiada wbudowane mechanizmy pozwalające chronić przed utratą danych bądź ich nieautoryzowanym użyciem, przy wykorzystaniu bądź wsparciu dla technologii Data at Rest / Data in Motion.

§

art. 5.2, 32.1a
32.1b, 33.1 RODO

Wsparcie dla dokumentowania stosowanych zabezpieczeń w przypadku naruszenia ochrony danych

Dzięki modułowi zarządzania systemem BitLocker, administrator jest w stanie wykazać, że skradziony sprzęt był zaszyfrowany. Zatem jest w stanie wykazać, że podstawowe atrybuty bezpieczeństwa – poufność, integralność i dostępność nie zostały naruszone.

§

art. 33.5 RODO

Zapobiega bądź utrudnia wystąpienie naruszenia ochrony danych osobowych

Dzięki zastosowaniu metod DLP zmniejszamy ryzyko wystąpienia naruszeń ochrony danych osobowych. Pozwala to uniknąć sytuacji, w których konieczne byłoby zgłaszanie incydentów organowi nadzorczemu i informowanie osób, których dane dotyczą, na mocy art. 33.5.

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 laptoptów i urządzeń mobilnych synchronizacja następuje przy pierwszym podłączeniu 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).

Minimalne wymagania sprzętowe

Safetica Endpoint Client

(oprogramowanie na stacje robocze)

- dwurdzeniowy procesor 2,4 GHz 32-bit / 64-bit
- 2 GB pamięci RAM
- 10 GB miejsca na dysku twardym
- MS Windows 10, 8.1 (32-bit i 64-bit)

Safetica Management Service

(komponent serwera)

- dwurdzeniowy procesor 2.4 GHz 32-bit / 64-bit
- 4 GB pamięci RAM
- 30 GB miejsca na dysku twardym

MS SQL

(baza danych dla serwera)

- MS Windows Server 2008 R2*, 2012, 2012 R2, 2016
  (*SQL Express 2016 nie jest kompatybilny z systemami Windows Server 2008 R2)
- przy współdzieleniu z MS SQL rekomendowana konfiguracja to 8 GB pamięci RAM i minimum 100 GB miejsca na dysku
- WebSafetica jest dostępna wyłącznie dla MS SQL 2012 i wyższych wersji