safetica

System DLP do ochrony danych

Chroń swoją firmę przed utratą danych
i zagrożeniami wewnętrznymi

www.safetica.pl

safetica ONE

Zabezpieczaj dane i jednocześnie zwiększaj wydajność

Safetica ONE to jedyne profesjonalne rozwiązanie do zabezpieczania danych zaprojektowane z myślą o skalowalności i potrzebach MŚP.

Uzyskaj kontrolę nad wartościowymi danymi z wysoką efektywnością. Wykraczaj poza zapobieganie utracie danych, stosując holistyczną analizę zachowań do jeszcze wcześniejszego wykrywania zagrożeń dla informacji poufnych i reagowania, zanim przerodzą się w incydenty. Wykorzystaj wgląd w przestrzeń roboczą firmy, zasoby cyfrowe i operacje, aby zoptymalizować koszty.

W przypadku utraty lub kradzieży danych wrażliwych firma traci reputację, przewagę konkurencyjną i rentowność.

- Średni koszt naruszenia bezpieczeństwa danych wynosi **15,75 mln zł**.*
- 60% małych przedsiębiorstw **bankrutuje w ciągu 6 miesięcy** od istotnego naruszenia bezpieczeństwa danych.**

* Raport „Cost of Data Breach" (Koszty naruszenia bezpieczeństwa danych) z 2020 r., Ponemon Institute;
** National Cyber Security Alliance, październik 2012 r.

Każde przedsiębiorstwo może zabezpieczyć swoje dane

Bezpieczeństwo wewnętrzne nigdy nie było tak proste. Pomagamy chronić Twoje dane, wspieramy Twoich pracowników i zapewniamy zgodność Twojej firmy z przepisami. Safetica ONE zapobiega naruszeniom bezpieczeństwa danych i ułatwia przestrzeganie przepisów dotyczących ochrony danych poprzez zabezpieczanie przed występowaniem błędów ludzkich lub złośliwego zachowania.

- **Łatwe do wdrożenia i integracji**

  Zgodnie z raportem SoftwareReviews 2021 DLP Data Quadrant Report, Safetica ONE przoduje w łatwości wdrożenia i bezproblemowej integracji z architekturą IT.

- **Zaawansowana kontrola przestrzeni roboczej i analiza zachowań**

  Uzyskaj kontrolę nad sprzętem i oprogramowaniem, aby zoptymalizować koszty. Dzięki dodatkowemu modułowi możesz również uzyskać szczegółowe informacje o ryzykownych zachowaniach użytkowników oraz zmianach w obszarze roboczym.

- **Bardzo niskie wymagania sprzętowe**

  Backend Safetica ONE można wdrożyć na dostępnych serwerach bez kupowania dodatkowego sprzętu. Klient Safetica nie obniża wydajności urządzeń, ponieważ wykorzystuje poniżej 3% zasobów sprzętowych.

safetica ONE

Najważniejsze scenariusze związane z bezpieczeństwem danych

Klasyfikacja danych i audyt przepływu danych

Safetica ONE pomaga odkrywać i klasyfikować cenne dane firmy na podstawie inspekcji treści, kontekstu i właściwości plików. Narzędzie kontroluje wszystkie działania związane z danymi wrażliwymi bez względu na to, gdzie są przechowywane lub przenoszone, dzięki czemu możesz identyfikować i badać, gdzie istnieje ryzyko wycieku lub kradzieży danych. Te informacje mają kluczowe znaczenie dla ochrony danych.

Wykrywanie i łagodzenie skutków naruszeń przepisów

Safetica ONE pomaga wykrywać, zapobiegać i łagodzić naruszenia przepisów. Jego funkcje audytu wspierają badanie incydentów w celu zapewnienia zgodności z przepisami i standardami ochrony danych, takimi jak RODO, HIPAA, SOX, PCI-DSS, GLBA, ISO/IEC 27001 lub CCPA.

Wykrywanie i reagowanie na zagrożenia wewnętrzne

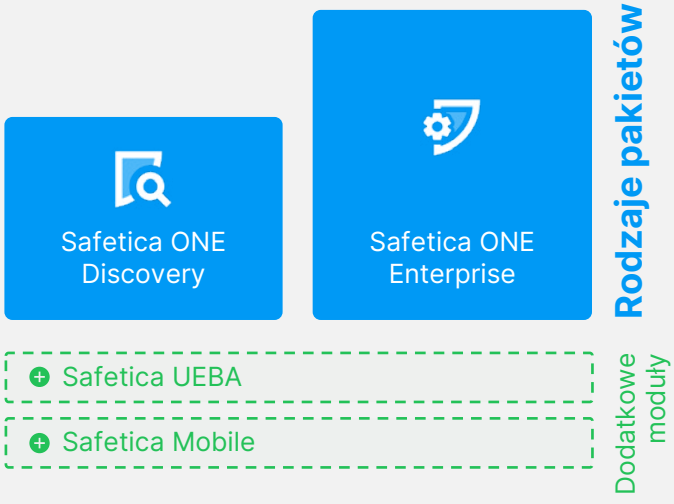
Każdy może popełnić błąd, który może narazić Twoją firmę na ryzyko. Dzięki Safetica ONE możesz analizować zagrożenia wewnętrzne, wykrywać je i szybko reagować. Kontroluj swoją cyfrową przestrzeń roboczą, wykrywaj niechciane oprogramowanie i sprzęt, analizuj zachowanie w celu wykrywania i audytowania pracowników wysokiego ryzyka.

Własność intelektualna i ochrona danych wrażliwych

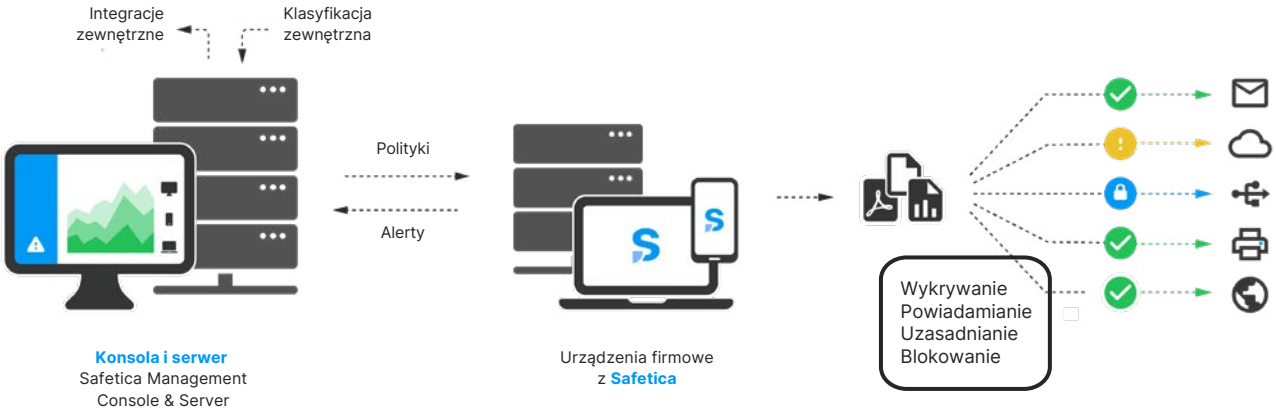
Dzięki Safetica ONE możesz chronić wrażliwe dane biznesowe lub te związane z klientami, kody źródłowe czy projekty przed przypadkowym lub celowym wyciekiem. Powiadomienia o tym, jak postępować z danymi wrażliwymi, mogą pomóc w podnoszeniu świadomości na temat bezpieczeństwa danych i edukować pracowników.

Safetica ONE chroni Twoje:

- dane osobowe
- strategiczne dokumenty firmowe
- bazy danych klientów
- dane dotyczące płatności, takie jak numery kart kredytowych
- elementy własności intelektualnej – projekty przemysłowe, tajemnice handlowe i know-how
- umowy



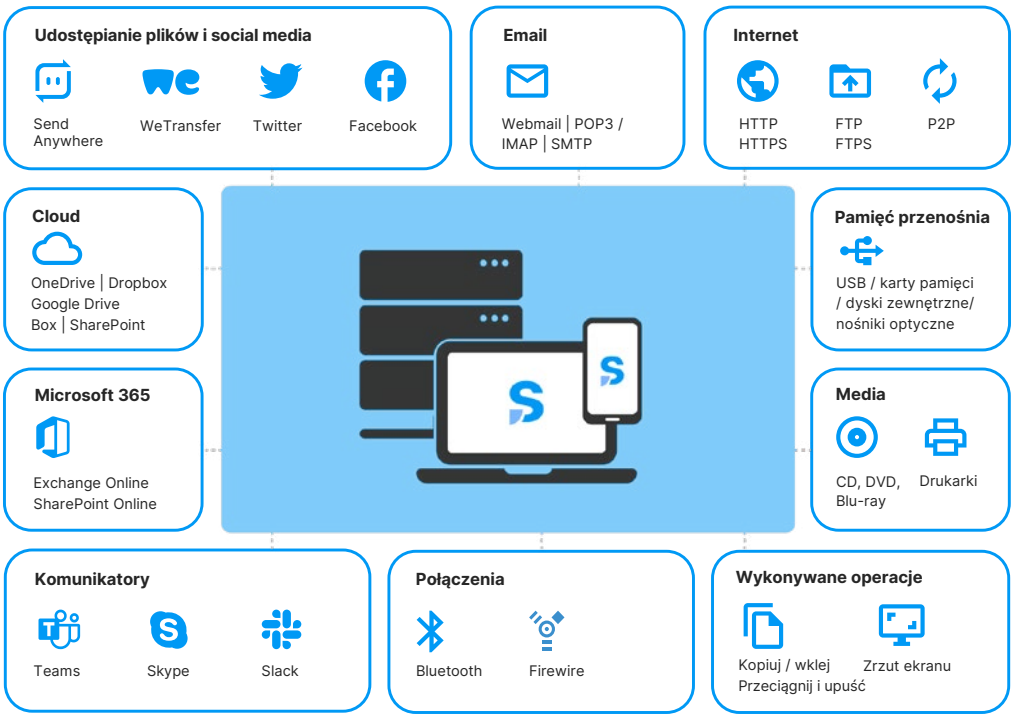
Podstawowe założenia architektury



- Na serwerze fizycznym lub wirtualnym działa baza danych zawierająca rekordy dotyczące działań i bezpieczeństwa na stacjach roboczych. Safetica Management Console pozwala administratorom na zarządzanie politykami dotyczącymi bezpieczeństwa i wyświetlanie zebranych informacji.
- Wszystkie działania są rejestrowane, a polityki dotyczące bezpieczeństwa są stosowane na komputerach stacjonarnych, laptopach i innych urządzeniach zdalnych lub nawet urządzeniach mobilnych działających w trybie off-line (tylko smartfony z MDM) z klientem Safetica Client.
- Dane wrażliwe są chronione we wszystkich kanałach.

Obsługiwane kanały danych

Safetica chroni dane na wielu kanałach i platformach - zapewnia, że są one bezpieczne zarówno podczas przechowywania, jak i przesyłu.



safetica ONE

Moduł Discovery
Najważniejsze korzyści

Moduł Safetica ONE Discovery kontroluje i klasyfikuje wszystkie dane przesyłane w obrębie Twojej organizacji. Identyfikuje informacje wrażliwe i zagrożenia dla bezpieczeństwa, dokonując kontroli treści z wykorzystaniem technologii optycznego rozpoznawania znaków (OCR). Daje szybki podgląd działań podejmowanych w przestrzeni roboczej w czasie rzeczywistym. Umożliwia lepsze zrozumienie wszystkich wewnętrznych działań, procesów i zagrożeń dla bezpieczeństwa danych, zwiększając bezpieczeństwo danych i wydajność wewnętrzną.

Uzyskaj wgląd w incydenty dotyczące bezpieczeństwa danych i naruszenia **zgodności z przepisami** w celu odpowiedniego reagowania i minimalizowania ich skutków.

Odkrywaj i usuwaj niechciane lub niepotrzebne oprogramowanie, usługi w chmurze lub sprzęt / urządzenia peryferyjne.

Kontroluj i klasyfikuj dane wrażliwe przesyłane w ramach dowolnego kanału lub działania, aby wiedzieć w którym miejscu są narażone na ryzyko utraty lub kradzieży.

Łatwe we wdrożeniu rozwiązanie z możliwością integracji z pakietem **Microsoft 365** za pomocą jednego kliknięcia działa zgodnie z ustalonymi procesami i generuje pierwsze raporty już po upływie kilku dni.

Otrzymuj **natychmiastowe powiadomienia** oraz **raporty** z możliwością podejmowania dalszych działań, zawierające łatwe do odczytu oceny poziomu ryzyka i podsumowania incydentów.

Obiektywnie **analizuj działania użytkowników** w swoim środowisku i ustalaj, czy firmowe **urządzenia i sieć są wykorzystywane prawidłowo**.

Najważniejsze funkcje

Określaj sposób, w jaki dane firmowe są wykorzystywane oraz gdzie są przechowywane i wysyłane, niezależnie od tego, gdzie się znajdują lub są przesyłane.

- Obsługa systemów Windows i MacOS
- Integracja z Microsoft 365 za pomocą jednego kliknięcia
- Kontrola i klasyfikacja zawartości plików
- Łatwa modernizacja do zaawansowanej platformy ochrony danych ze wszystkimi funkcjami
- Działanie na fizycznych lub wirtualnych sprzętach lokalnych lub hostowanych na maszynach wirtualnych w chmurze

Konsola Safetica Management Console do modułu Safetica ONE Discovery daje zaawansowany wgląd we wszystkie operacje na zapisanych plikach, z zastosowaniem różnych widoków na potrzeby łatwej interpretacji.

safetica ONE

Moduł Enterprise
Najważniejsze korzyści I

Moduł Safetica ONE Enterprise służy do identyfikacji zagrożeń, szkolenia pracowników oraz zapobiegania błędom ludzkim i działaniom złośliwym w celu ochrony danych. Stanowi połączenie analityki, klasyfikacji i zapobiegania utracie danych (DLP) oraz ochrony przed zagrożeniami dla informacji poufnych, tworząc bezpieczne środowisko z zachowaniem odpowiedniej wydajności operacji biznesowych.

Zachowaj **pełną kontrolę nad przesyłaniem danych wrażliwych** oraz **zagrożeniami wewnętrznymi** w oparciu o analizę zachowań i kontrolę treści.

Uzyskuj regularne **raporty dotyczące bezpieczeństwa** oraz **powiadomienia** o incydentach w czasie rzeczywistym.

Korzystaj z bezpiecznych stref dla uproszczonego bezpieczeństwa danych na poziomie ogólnym.

Twórz **kopie danych w tle** które wyciekły, aby dysponować materiałem dowodowym w przypadku ewentualnego śledztwa.

Ustalaj jasne zasady dla wszystkich użytkowników i kanałów danych

Ustalaj zasady bezpieczeństwa dla poszczególnych grup lub osób. Wybieraj pożądane przepływy pracy z uwzględnieniem konfigurowalnych działań: od kontroli w tle, przez powiadomienia dla użytkowników do restrykcyjnego blokowania.

Wykrywaj potencjalne zagrożenia i analizuj ryzyko wewnętrzne

Reaguj na zagrożenia jeszcze przed wystąpieniem poważnego incydentu dzięki wczesnej detekcji nieprawidłowości zachowań i zagrożeń dla przepływu danych w Twojej organizacji. W platformie Safetica ONE zastosowano zaawansowaną klasyfikację treści i technologię OCR do wykrywania danych wrażliwych w plikach obrazów i zeskanowanych dokumentach PDF.

Upoważniaj pracowników do obsługi danych wrażliwych

Wyświetlaj pracownikom powiadomienia szkoleniowe, gdy występuje ryzyko naruszenia zasad, aby dać im możliwość uzyskania informacji lub podjęcia decyzji. Egzekwuj konkretne procesy, aby chronić najbardziej wartościowe dane.

Sprawuj kontrolę nad wszystkimi urządzeniami działającymi w trybie on-line i off-line

Ograniczaj użytkowanie przenośnych urządzeń peryferyjnych lub niezatwierdzonych nośników danych. Kontroluj firmowe urządzenia mobilne i śledź dane wysyłane z pakietu Microsoft 365. Platforma Safetica pozostaje w pełni aktywna niezależnie od stanu połączenia sieciowego. Wszystkie gromadzone rekordy są synchronizowane po przywróceniu połączenia.

safetica ONE

Moduł Enterprise
Najważniejsze korzyści II

Moduł Safetica ONE Enterprise rozszerza zapobieganie utracie danych i ochronę przed zagrożeniami wycieku informacji poufnych oraz zapewnia płynną integrację z zewnętrznymi rozwiązaniami z zakresu bezpieczeństwa sieci, rozwiązaniami SIEM (z zakresu zarządzania informacjami i zdarzeniami bezpieczeństwa) oraz narzędziami do analizy danych. Dzięki niemu budowanie systemu bezpieczeństwa IT w przedsiębiorstwie staje się łatwe.

Automatyczna **integracja z rozwiązaniami zewnętrznymi**.

Zasady do **kontroli przepływu pracy** na stacjach roboczych w obrębie firmy.

Obsługa Active Directory **w środowiskach wielodomenowych**.

Niestandardowe oznaczanie powiadomień o bezpieczeństwie przekazywanych użytkownikom na stajach roboczych.

Kontrola przepływu pracy

Zestaw funkcji kontrolnych umożliwia określanie metod dopuszczania użytkowników do pracy, niezależnie od obsługiwanych danych. Z kontrolą przepływu pracy możesz wykonać określony proces bezpieczeństwa i zablokować wszystkie inne sposoby wykonania danej czynności.

Kontrola przepływu pracy obejmuje **zasady DLP w zakresie aplikacji** do zarządzania zachowaniami poszczególnych typów aplikacji, takich jak CRM czy IM, oraz **zasady DLP** z zastosowaniem konfiguracji niestandardowych w odniesieniu do poszczególnych sieci i ścieżek lokalnych lub zastrzeżonego dostępu dla uprzywilejowanych użytkowników.

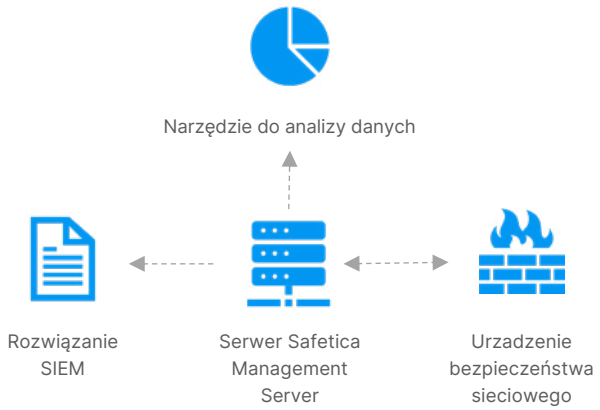
Płynna integracja

Automatyzacja zasad bezpieczeństwa i integracji z istniejącym systemem IT pomaga chronić aktywa nawet w złożonych środowiskach. Integracja natywna z pakietem **Microsoft 365** lub urządzeniami sieciowymi **Fortinet** zapewnia rozbudowaną kontrolę nad nieznanymi urządzeniami i tworzy solidne rozwiązanie z zakresu bezpieczeństwa obejmujące obszar od stacji roboczych do sieci.

Wszystkie podlegające kontroli incydenty i dzienniki mogą być automatycznie przesyłane do rozwiązań SIEM, takich jak **Splunk, IBM QRadar, LogRhythm** lub **ArcSight** do dalszego badania. API REST odpowiada za przesyłanie zgromadzonych danych do narzędzi, takich jak **Power BI** czy **Tableau** na potrzeby zaawansowanej analizy.

Najważniejsze funkcje

- Obsługa systemów Windows i MacOS
- Integracja z Microsoft 365 za pomocą jednego kliknięcia
- Natychmiastowe przesyłanie powiadomień do skrzynki odbiorczej
- Integracja API z narzędziami Power BI lub Tableau
- Integracja z urządzeniami sieciowymi Fortinet
- Kontrola zawartości plików z zastosowaniem wstępnie zdefiniowanych szablonów
- Klasyfikacja treści w oparciu o różne podejścia



safetica ONE

Moduł UEBA
Najważniejsze korzyści

Wiedza to pierwszy i najważniejszy krok ku dokładnemu zrozumieniu przepływu pracy, nawyków Twoich pracowników i zdolności produkcyjnych w Twojej firmie. Wykorzystaj moduł User and Entity Behavior Analytics, który jest dostępny za darmo w ramach Safetica Enterprise aby uzyskać szczegółowy wgląd w działania użytkowników i sprawdzić, które z nich odbiegają od normy. Zadbaj o płynną działalność swojej firmy, nawet przy pracy zdalnej.

Rozpoznawaj niepożądane działania użytkowników za pomocą kontroli działań podejmowanych podczas pracy oraz automatycznego oznaczania i klasyfikowania aplikacji oraz witryn używanych i odwiedzanych przez poszczególnych pracowników.

Uzyskaj głębszy wgląd w korespondencję elektroniczną oraz ewidencję wszystkich wiadomości odebranych i wysłanych z poszanowaniem prywatności pracownika.

Śledź zmiany w zachowaniu użytkowników wykorzystując podgląd i wizualizację trendów oraz zmian w zachowaniu użytkowników w sieci lokalnej w funkcji czasu.

Kontroluj wykorzystanie zasobów aby dokładnie wiedzieć, czy zakupione sprzęty i licencje oprogramowania są rozprowadzane i używane w efektywny sposób.

Generuj kompleksowe raporty i alerty w czasie rzeczywistym dotyczące działań podejmowanych przez poszczególnych użytkowników, nawet tych, którzy pracują zdalnie, np. za pośrednictwem pulpitu zdalnego itp.

Kontroluj odwiedzane strony w celu określenia jakie portale internetowe są odwiedzane przez konkretnych użytkowników.

Identyfikacja nieprawidłowości i ich przyczyn źródłowych

Przeprowadzaj dogłębne badania i wskazuj kłopotliwe elementy w swoim środowisku, aby rozwiązywać problemy związane z bezpieczeństwem lub wydajnością przedsiębiorstwa. Obiektywnie analizuj działania związane z pracą podejmowane przez poszczególnych pracowników, wykorzystując szczegółowe informacje. Ustalaj, czy nikt nie odwiedza niebezpiecznych witryn lub nie korzysta z niepożądanych aplikacji.

Transparentność pracy nawet wykonywanej zdalnie

Daj swojemu kierownictwu najwyższego szczebla i kierownikom działów narzędzia do monitorowania raportów. Trzymaj rękę na pulsie nawet wtedy, gdy Twoi pracownicy wykonują swoje obowiązki z domu lub z dowolnego innego miejsca. Zapobiegaj zagrożeniom dla bezpieczeństwa i zarządzaj wydajnością pracowników, identyfikując osoby nieaktywne, poszukiwania pracy cz podejrzane wzorce zachowań.

safetica ONE

Wybierz właściwe rozwiązanie dla swojej firmy

Kompatybilne z: Windows, macOS, Microsoft 365, Android, iOS	Safetica ONE Discovery	Safetica ONE Enterprise
Audyt bezpieczeństwa	✓	✓
Audyt bezpieczeństwa przepływu danych Audyt bezpieczeństwa danych wymienianych w różnych kanałach, w tym przez podłączane urządzenia, transfer, w wiadomościach e-mail i komunikatorach, wydrukach oraz udostępnianych w chmurze.	✓	✓
Audyt plików i wiadomości e-mail w Office 365 Audyt operacji na plikach i wychodzących wiadomości e-mail w Office 365.	✓	✓
Audyt zgodności norm bezpieczeństwa Wykrywanie naruszeń najpopularniejszych regulacji prawnych i ustaw, takich jak PCI-DSS, RODO lub HIPAA, w wersjach specyficznych dla różnych regionów.	✓	✓
Audyt wykorzystania urządzeń Weryfikacja wykorzystywania firmowych urządzeń, aplikacji, sieci i urządzeń drukujących. Wyszukiwanie nieużywanych lub niewłaściwie wykorzystywanych zasobów, aby wydajnie zarządzać firmowymi zasobami i urządzeniami, i redukować koszty.	✓	✓
Klasyfikacja danych Nadawanie poufnej klasyfikacji plikom i wiadomościom e-mail dzięki zaawansowanej inspekcji treści, wykorzystując wstępnie zdefiniowane szablony oraz niestandardowe reguły i słowniki.	✓	✓
Wykrywanie podejrzanych aktywności Reaguj szybko dzięki wykrywaniu podejrzanych działań w czasie rzeczywistym i natychmiastowym alertom e-mailowym.	✓	✓
Ochrona danych na stacjach roboczych	✗	✓
Ochrona sieci i wiadomości e-mail Ochrona danych udostępnianych w wiadomościach e-mail, komunikatorach, poprzez transfer i udziały sieciowe.	✗	✓
Ochrona urządzeń wymiennych i drukowania Zarządzanie przepływem danych do urządzeń zewnętrznych i chroń poufne dane przed drukowaniem na drukarkach lokalnych, sieciowych lub wirtualnych.	✗	✓
Ochrona podczas pracy zdalnej Unikanie wycieków danych na stacjach połączonych zdalnie lub podczas korzystania z usługi zdalnego pulpitu. Kompatybilność z szeroką gamą rozwiązań dostępu zdalnego.	✗	✓
Zaawansowana klasyfikacja danych Wykorzystywanie zaawansowanych technologii, celem wykrywania i oznaczania danych wrażliwych na podstawie pochodzenia, wykorzystanego urządzenia lub typu pliku.	✗	✓
Różny poziom restrykcji polityk bezpieczeństwa Elastyczna reakcja na wykrywane incydenty, aby uświadamiać i szkolić pracowników. Incydenty mogą być rejestrowane, blokowane lub usprawiedliwiane / blokowane z funkcją zastępowania.	✗	✓
Mechanizm „Shadow Copy” Możliwość przechowywania dowodów dla incydentów bezpieczeństwa, poprzez tworzenie w tle kopii wyciekających danych. Utworzone kopie są w pełni zaszyfrowane i mogą być przechowywane na komputerach lokalnych z zachowaniem zasad dostępu do plików.	✗	✓

safetica ONE

Wybierz właściwe rozwiązanie dla swojej firmy

Kompatybilne z: Windows, macOS, Microsoft 365, Android, iOS	Safetica ONE Discovery	Safetica ONE Enterprise
Ochrona danych na stacjach roboczych	✗	✓
Kontrola sprzętu Możliwość zdefiniowania zabezpieczonego obszaru roboczego oraz wyznaczania czasu pracy, dzięki kontroli aplikacji i stron internetowych. Redukcja niepożądanych incydentów w firmie i kosztów zarządzania bezpieczeństwem.	✗	✓
Mechanizm stref Łatwe zarządzanie bezpieczną strefą za pomocą unikalnego mechanizmu dostępnych w Safetica, co umożliwia znaczne zmniejszenie ilości polityk ochrony danych.	✗	✓
Szyfrowanie: zarządzanie bitlockerem Scentralizowane zarządzanie zaszyfrowanymi dyskami lokalnymi i urządzeniami zewnętrznymi wykorzystującymi technologię BitLocker.	✗	✓
Ochrona danych w chmurze i Office 365	✗	✓
Ochrona synchronizacji stacji roboczej z chmurą Ochrona danych na podłączonych dyskach chmurowych wykorzystując np. OneDrive, Dysk Google, Dropbox, Box itp.	✗	✓
Integracja i ochrona Office 365 Ochrona danych w Office 365 i SharePoint z poziomu stacji roboczych. Zapobieganie udostępnianiu oraz przesyłaniu danych, które nie powinny trafić do chmury.	✗	✓
Integracja i ochrona Azure Information Protection Wykrywanie klasyfikacji danych utworzonej przez Microsoft Azure Information Protection, nawet w postaci zaszyfrowanej.	✗	✓
Integracja i ochrona Exchange Online Ujednolicenie reguł dotyczących poczty elektronicznej na stacjach roboczych i w chmurze. Zarządzanie i filtrowanie danych wychodzących bezpośrednio na stacjach i w Exchange Online	✗	✓
Funkcjonalności dodatkowe	✗	✓
Kastomizacja Możliwość dostosowania powiadomień wyświetlanych użytkownikom.	✗	✓
Kontrola czasu pracy Polityki umożliwiające kontrolę czasu i godzin pracy.	✗	✓
Obsługa wielu domen Obsługa wielu domen dla usługi Active Directory.	✗	✓
Automatyzacja zabezpieczeń	✗	✓
Integracja z SIEM Automatyczne raportowanie incydentów do rozwiązań SIEM (Splunk, QRadar, LogRhythm, ArcSight itp.).	✗	✓
Integracja z FortiGate Zautomatyzowana integracja bezpieczeństwa z urządzeniami FortiGate w celu stworzenia rozwiązania zabezpieczającego połączenie stacji do sieci.	✗	✓

safetica ONE

Wymagania techniczne

Server

- Czterordzeniowy procesor 2,4 GHz
- 8 GB RAM i więcej
- Minimum 100 GB wolnego miejsca na dysku
- Instalacja na dedykowanym serwerze lub wraz z innymi rozwiązaniami, wsparcie dla instalacji w środowisku wirtualnym oraz na serwerze hostowanym w chmurze
- Wymagana baza danych MS SQL 2012 lub nowsza bądź Azure SQL
- System operacyjny MS Windows Server 2012 i wyższe

Baza danych

- System operacyjny MS Windows Server 2012 i wyższe
- MS SQL Express jest częścią instalatora kompleksowego, a jego wykorzystywanie jest zalecane do ochrony maksymalnie 200 stacji roboczych
- Minimum 200 GB wolnego miejsca na dysku (najlepiej 500 GB i więcej w zależności od stopnia szczegółowości logowanych danych)
- Instalacja na serwerze dedykowanym lub wraz z innymi rozwiązaniami, wsparcie dla instalacji w środowisku wirtualnym oraz na serwerze hostowanym w chmurze. Baza danych może znajdować się na tej samej maszynie co Safetica Server.

Windows Client

- Dwurdzeniowy procesor 2,4 GHz 32-bit, 2 GB RAM i więcej
- 10 GB wolnego miejsca na dysku
- System operacyjny MS Windows 7, 8.1, 10, 11, (32-bit [x86] lub 64-bit [x64])
- pakiet instalacyjny MSI
- Framework .NET 4.7.2 lub nowszy

macOS Client

- Czterordzeniowy procesor 2,4 GHz, 2 GB RAM i więcej
- 10 GB wolnego miejsca na dysku
- System macOS 10.10 lub nowszy. Celem pełnego wykorzystania modułu DLP rekomendowana jest instalacja na systemie w wersji 10.15 i wyższych.

Mobile Client

- System Android: minimum Android 6+ i dostęp do Google Play Services
- system iOS: minimum 10+

Wspierani dostawcy usług chmurowych

- Microsoft Azure, Microsoft 365

Wybrane certyfikacje

- ISO 9001 & ISO/IEC 27001
- Członek Cybersecurity Tech Accord
- Złoty Partner Microsoft
- Partner ESET Technology Alliance
- Partner Fortinet Technology Alliance
- Partner Netwrix Technology

safetica

www.safetica.pl

DAGMA
BEZPIECZEŃSTWO IT

główny dystrybutor
rozwiązań Safetica
w Polsce