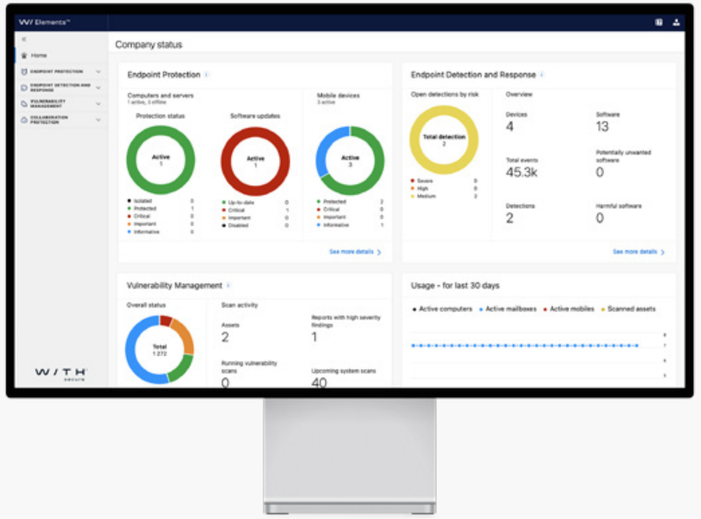
WithSecure™ Elements

WithSecure™ Elements – ogranicz ryzyko, zmniejszając stopień skomplikowania mechanizmów ochronnych oraz zwiększając ich wydajność.

Dzisiejsze środowisko biznesowe stale się zmienia w szybkim tempie. Tak samo jest w przypadku cyberzagrożeń. Podczas gdy organizacje ze wszystkich sektorów gospodarki przenoszą dane do chmury i wdrażają nowe metody pracy oparte na rozwiązaniach cyfrowych, hakerzy wykorzystują rozszerzające się obszary podatne na ataki przy użyciu bardziej zaawansowanych i wydajniejszych metod.

Powszechnym sposobem reagowania na nowe zagrożenia jest posiadanie kompleksowego zestawu specjalistycznych technologii i rozwiązań od wielu dostawców. Ten skomplikowany zestaw narzędzi jest nie tylko nieporozumieniem z punktu widzenia obsługi, ale również pozostawia luki w zabezpieczeniach.

- Wiele z tych rozwiązań wymaga szczególnych (i rzadko spotykanych) umiejętności do ich skutecznej obsługi.
- Rozproszone rozwiązania nie współpracują ze sobą ani nie wymieniają między sobą danych. Prowadzi to do ograniczenia możliwości wykrywania.



Dlaczego warto wybrać WithSecure™ Elements?

Elastyczne, modułowe i skalowalne rozwiązanie.
Wybierz pojedyncze funkcje lub pełny pakiet za jednym kliknięciem. Platforma umożliwia szybką adaptację dzięki elastycznym opcjom licencjonowania.

Wiele funkcji w jednym miejscu.
Redukcja ryzyka dzięki jednolitej i zaawansowanej technologicznie ochronie całego łańcucha bezpieczeństwa.

Świadomość sytuacyjna.
Zobacz wszystko, co istotne. Uzyskaj pełen obraz w zakresie złożonych cyberataków.

Wzmocniona reakcja.
Narzędzie zapewnia reagowanie na wiele zagrożeń czyhających na urządzenia końcowe czy rozwiązania chmurowe.

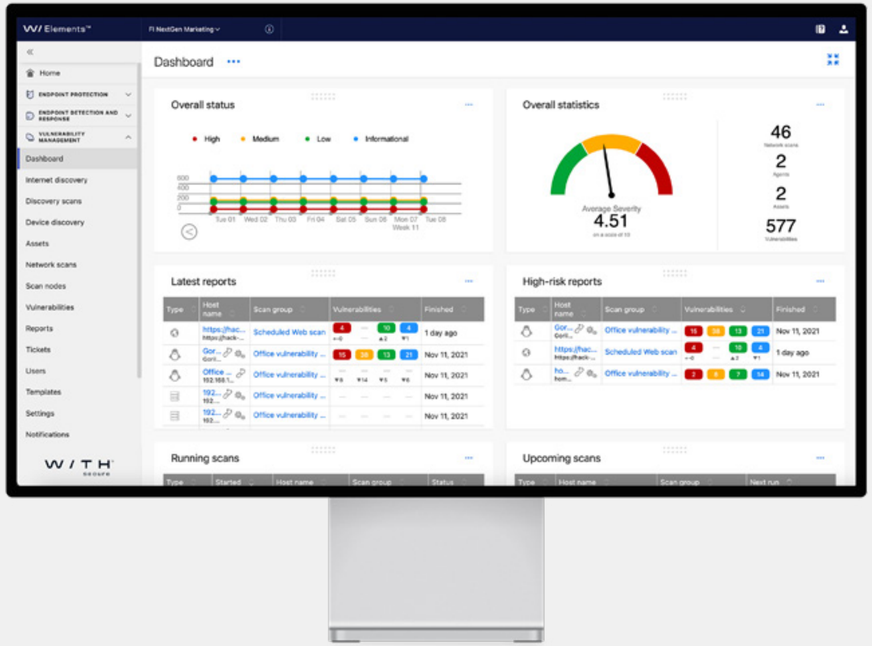
Uproszczone zarządzanie.
Zwiększ wydajność dzięki usprawnionemu i centralnemu zarządzaniu.

Lekka jak chmura.
Platforma umożliwia skrócenie czasu wdrożenia i redukcję kosztów operacyjnych dzięki oparciu na technologii chmury bez zbędnych elementów.

WithSecure™ Elements zwiększa bezpieczeństwo i ułatwia jego zapewnienie.

Uzyskaj kompleksową ochronę dzięki jednolitej platformie opartej na chmurze, będącej wzorcem wśród rozwiązań dbających o cyberbezpieczeństwo. Scentralizowana platforma łączy w sobie zaawansowane funkcje predykcyjne, prewencyjne i reagowania w zakresie bezpieczeństwa, tworząc inteligentną ochronę przed zagrożeniami od ransomware po ataki ukierunkowane. Modułowa struktura rozwiązania pozwala na wybór funkcji, a elastyczne modele cenowe dają swobodę rozwoju. Niezrównana prostota pozwala skupić się na tym, co robisz najlepiej.

- **Pojedynczy panel:** zyskaj niezrównaną widzialność i pełną świadomość sytuacyjną.
- **Bezproblemowa integracja:** rozwiązania korzystają z scentralizowanego repozytorium i współpracują ze sobą w zakresie zagrożeń, zapewniając wyjątkowe możliwości wykrywania.
- **WithSecure™ Elements Security Center:** pozwala na usprawnienie działań dzięki scentralizowanemu zarządzaniu cyberbezpieczeństwem.
- **Platforma SaaS oparta na chmurze:** brak potrzeby zakupu dodatkowego sprzętu lub oprogramowania pośredniczącego. Dostosujesz i wdrożysz ją za jednym kliknięciem.
- **W ramach usługi zarządzania:** możesz współpracować z naszymi certyfikowanymi partnerami lub zarządzać oprogramowaniem samodzielnie. Niezależnie od tego, co wybierzesz, zapewnimy Ci wsparcie.



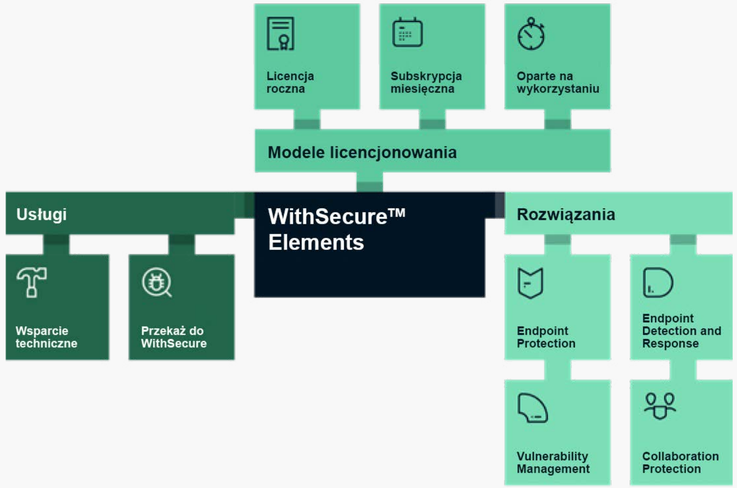
WithSecure™ Elements Endpoint Protection

Pionierska ochrona przed współczesnym złośliwym oprogramowaniem i ransomware.

Hakerzy stale skanują podłączone urządzenia pod kątem luk w zabezpieczeniach, a w momencie pojawienia się szansy, nie zastanawiają się. Większości zagrożeń cybernetycznych można zapobiec dzięki skutecznemu rozwiązaniu w zakresie ochrony urządzeń końcowych i nieustannemu wdrażaniu poprawek.

WithSecure™ Elements Endpoint Protection zapewnia autonomiczną i wielokrotnie nagradzaną ochronę, która zapobiega współczesnym zagrożeniom, począwszy od ransomware, poprzez nigdy wcześniej niespotkane złośliwe oprogramowanie, a kończąc na atakach zero-day. Uzyskaj kompleksową ochronę telefonów komórkowych, komputerów stacjonarnych, laptopów i serwerów. Najwyższa dokładność oznacza mniejsze ryzyko dla biznesów i mniejszy nakład pracy działu IT w celu przywrócenia prawidłowego funkcjonowania. Filtrowane alarmy i wysoki poziom automatyzacji zapewniają maksymalną wydajność. Zachowaj zasoby, aby wykonać pracę, która ma znaczenie.

- **Autonomiczna ochrona** przez całą dobę oznacza małą ilość ręcznych operacji i brak konieczności posiadania specjalistycznej wiedzy.
- **Ochrona przed niewidocznymi zagrożeniami i atakami** dzięki analizie heurystycznej i behawioralnej, zaawansowanemu uczeniu maszynowemu i dynamicznemu gromadzeniu danych o zagrożeniach w czasie rzeczywistym.
- **Wdrażanie poprawek w momencie ich pojawienia się** dzięki w pełni zautomatyzowanemu zarządzaniu poprawkami.
- **Blokowanie uruchamiania aplikacji i skryptów** zgodnie z regułami utworzonymi przez pentesterów lub określonymi przez Twojego administratora.
- **Ochrona użytkowników przed cyberzagrożeniami** w tym wchodzeniem na strony ze złośliwym oprogramowaniem.
- **Wykrywanie złośliwego oprogramowania** oraz zapobieganie niszczeniu i manipulowaniu danymi za pomocą technologii DeepGuard i DataGuard.
- **Zapobieganie przedostawaniu się zagrożeń** lub wyciekowi danych z systemu za pośrednictwem urządzeń zewnętrznych.
- **Zapobieganie nieuprawnionemu dostępowi aplikacji** do plików i zasobów systemowych.



52%
firm doświadczyło naruszenia ochrony danych

42%
przypadków naruszenia ochrony danych w 2020 r. nastąpiło z powodu niewdrożenia dostępnej poprawki.

57%
organizacji nie wie, które podatności w zabezpieczeniach stanowią największe zagrożenie.

Istotne cechy platformy:

Ochrona urządzeń końcowych i usług w chmurze

Ochrona przed złośliwym oprogramowaniem i ransomware

Wykrywanie luk i wdrażanie poprawek

Wykrywanie i wyszukiwanie zagrożeń

Ochrona przed phishingiem i zaawansowanymi zagrożeniami na platformie Microsoft Office 365

Wykrywanie zaatakowanych kont firmowych

Szybka reakcja na ataki dzięki automatyzacji, wskazówkom i obsłudze 24/7

WithSecure™ Elements Endpoint Detection Response

Wyprzedź hakerów i zapewnij ochronę przed zaawansowanymi atakami.

Nikt nie jest odporny na cyberzagrożenia i nie ma czegoś takiego jak doskonałe zapobieganie. Dzisiejsze najbardziej zaawansowane ataki są w stanie ominąć nawet najlepsze środki zapobiegawcze. Dodatkowo można je łatwo przeoczyć, co pozwoli atakującym na spowodowanie szkód i naruszenie danych.

WithSecure™ Elements Endpoint Detection and Response chroni przed zaawansowanymi i ukierunkowanymi atakami cybernetycznymi z wiodącymi w branży możliwościami wykrywania. Rozwiązanie to pozwala na utrzymanie ochrony i szybkie odzyskanie kontroli dzięki praktycznym poradom i jasnym wskazówkom.

- Podgląd sytuacji na urządzeniach końcowych w czasie rzeczywistym. Platforma wspiera systemy Windows, macOS i Linux.
- Szybkie i dokładne wykrywanie zagrożeń dzięki funkcji Broad Context Detection. Obserwacja podejrzanych zachowań, nawet jeśli wydają się być niegroźne. Brak męczących alertów.
- Skuteczne szukanie zagrożeń dzięki wyszukiwaniu i filtrowaniu zdarzeń.
- Uproszczone wizualizacje pozwalające na zrozumienie skorelowania łańcuchów zdarzeń.
- Natychmiastowe reagowanie na zagrożenia za pomocą zautomatyzowanych akcji reagowania, w tym izolacji hosta od sieci.
- Powstrzymuj ataki dzięki jasnym i łatwym w realizacji wskazówkom i opcji przekazania wymagających przypadków kadrze naszych łowców zagrożeń dostępnych 24/7.
- Platforma umożliwia spełnienie wymogów PCI, HIPAA i GDPR, które wymagają zgłaszania przypadków naruszenia ochrony danych w ciągu 72 godzin.

WithSecure™ Elements Collaboration Protection

Warstwowa ochrona zapewniająca wykrywanie i zapobieganie zaawansowanym zagrożeniom i atakom phishingowym.

Nastał złoty wiek danych. Biznesowe wiadomości e-mail zawierają dużą ilość wrażliwych i poufnych informacji. Magazyny w chmurze, takie jak Microsoft SharePoint, są skarbami w zakresie własności intelektualnej firmy. Firmowe konta e-mail są często połączone z wieloma krytycznymi aplikacjami biznesowymi. Dane użytkowników w rękach atakujących pozwalają im na podszywanie się i dostęp do systemów firmowych.

Usługa Microsoft Office 365 jest najpopularniejszą na świecie usługą poczty e-mail. Jej popularność zmusza hakerów do projektowania metod omijania standardowych mechanizmów kontroli bezpieczeństwa firmy Microsoft. Podstawowe zabezpieczenia poczty e-mail Microsoft nie zapewniają odpowiedniej ochrony przed zaawansowanymi atakami lub próbami wyłudzenia informacji.

WithSecure™ Elements Collaboration Protection wzmacnia wbudowane funkcje Microsoft w zakresie zabezpieczeń, zapewniając ochronę przed coraz bardziej zaawansowanymi atakami phishingowymi i złośliwą zawartością w wiadomościach e-mail, kalendarzach, zadaniach i na platformie SharePoint. Rozbudowane możliwości detekcji obejmują wykrywanie zagrożeń w skrzynkach odbiorczych i włamań na konta e-mail. Rozwiązanie chmurowe zostało zaprojektowane dla usługi Microsoft Office 365 i stanowi niemal niewidoczne rozszerzenie zabezpieczeń Elements dla urządzenia końcowego.

- **Wielowarstwowa i przystępna cenowo ochrona** zapewniająca ciągłość działania.
- **Ciągła ochrona** niezależnie od urządzenia dostępowego użytkownika końcowego. Brak przerw lub przestojów bramy poczty e-mail.
- **Uproszczony workflow** dzięki jednolitemu zarządzaniu zabezpieczeniami w urządzeniach końcowych i chmurze.
- **Bezproblemowe wdrożenie dzięki integracji chmura-chmura.** Brak potrzeby stosowania oprogramowania pośredniczącego ani rozbudowanej konfiguracji.
- **Blokowanie złośliwej zawartości,** w tym złośliwego oprogramowania, ransomware i prób wyłudzenia informacji.
- **Wykrywanie nawet najbardziej zaawansowanego złośliwego oprogramowania,** uruchamiając i analizując podejrzane pliki wykryte w programach Outlook i SharePoint w izolowanym środowisku typu sandbox.
- **Możliwość sprawdzenia,** czy miały miejsce włamania na konta firmowe dzięki informacjom dotyczącym sposobu, kont, czasu i stopnia zaawansowania.
- **Zaufaj swojej skrzynce odbiorczej.** Zabezpieczenie to zapewnia wykrywanie anomalii behawioralnych, takich jak złośliwe reguły forwardowania wiadomości.
- **Przyspieszenie wydajności** dzięki automatycznym skanom.

„Wybraliśmy rozwiązania WithSecure zamiast rozwiązania SIEM, ponieważ system wykrywania zachowań aplikacji oparty na uczeniu maszynowym radykalnie ograniczył liczbę fałszywych alertów i przedstawił je w sposób znacznie ułatwiający analizę i podejmowanie decyzji”.

Jeovane Monteiro Guimarães, Kierownik działu IT, Móveis Itatiaia

WithSecure™ Elements Vulnerability Management

Zobacz i poznaj prawdziwe obszary podatne na ataki.

Dynamiczne i złożone biznesowe środowiska informatyczne mają wiele obszarów podatnych na zagrożenia. Atakujący nieustannie szukają możliwości wykorzystania niezaktualizowanych systemów do nieuprawnionego dostępu do cennych informacji. Nowe poprawki zabezpieczeń są codziennie publikowane, a ich terminowe stosowanie ma kluczowe znaczenie dla zabezpieczenia danych i ciągłości działania. Wzmocnienie pozycji bezpieczeństwa cybernetycznego zaczyna się od znajomości zasobów i konfiguracji.

WithSecure™ Elements Vulnerability Management identyfikuje zasoby Twojej organizacji, wskazuje zagrożone obszary oraz najbardziej krytyczne luki w zabezpieczeniach. Dzięki temu rozwiązaniu zredukujesz obszary podatne na zagrożenia. Funkcjonalność ta pozwala na odnalezienie słabych punktów wewnętrznych i zewnętrznych zanim zrobią to inni.

- **Pełen obraz i dokładne** odwzorowanie wszystkich zasobów, systemów i aplikacji oraz shadow IT.
- **Redukcja obszaru podatnego na zagrożenia** poprzez identyfikację podatnych zarządzanych i niezarządzanych systemów, oprogramowania i niewłaściwych konfiguracji.
- **Minimalizacja ryzyka** poprzez zastosowanie środków predykcyjnych i zapobiegawczych przed wystąpieniem jakichkolwiek incydentów.
- **Usprawnienie workflow** dzięki zautomatyzowanym i zaplanowanym skanom. Priorytetowe traktowanie działań naprawczych z wbudowaną punktacją ryzyka.
- **Rozszerzenie skanowania** w zakresie podatności na urządzenia zdalne poza siecią przy pomocy agenta punktu końcowego systemu Windows.
- **Pokaż i uzasadnij swoją wartość** w zachowaniu ciągłości działania za pomocą standardowych i niestandardowych raportów dotyczących stanu bezpieczeństwa i ryzyka.
- **Łatwiejsze spełnianie wymagań zgodności** – możliwość wygenerowania raportu opartego na kryteriach PCI ASV, na który można powołać się przy certyfikacji zgodności.

Znamy się na cyberbezpieczeństwie

Mamy 30-letnie doświadczenie w zwalczaniu cyberprzestępczości z podejściem opartym na badaniach, potwierdzonym solidnymi wynikami niezależnych ocen.

withsecure.com/elements
twitter.com/withsecure
linkedin.com/withsecure

Wypróbuj już dziś

MITRE | ATT&CK