



VULNERABILITY & PATCH MANAGEMENT

Śledź i rozwiązuj podatności na bieżąco
na wszystkich stacjach roboczych

Progress. Protected.

Czym jest zarządzanie podatnościami od ESET?

ESET Vulnerability & Patch Management aktywnie śledzi podatności w systemach operacyjnych i popularnych aplikacjach, a także umożliwia automatyczną aktualizację wszystkich stacji roboczych, zarządzanych z poziomu naszej zintegrowanej konsoli.

Automatyczne skanowanie oprogramowania na stacjach roboczych w połączeniu z natychmiastowym przesyłaniem raportów do konsoli pozwala na bieżąco wykrywać nowe podatności. Jeżeli zależy Ci na całkowitym bezpieczeństwie Twojej firmy, skonfiguruj automatyczne łatanie podatności, wybierając strategię aktualizacji (wszystkie, tylko dozwolone, wszystkie poza wykluczonymi) oraz definiując konkretne przedziały czasowe, w których aktualizacje mają być instalowane.



Bieżące aktualizacje systemów operacyjnych i aplikacji

Łatanie luk w zabezpieczeniach systemów operacyjnych i aplikacji to kwestia krytyczna, ale jest to jednocześnie jedno z najbardziej czasochłonnych zadań w IT. ESET Vulnerability & Patch Management to dodatkowa warstwa ochronna idealna dla organizacji, dla których aktualność aplikacji ma kluczowe znaczenie, ale zmagają się z niewystarczającymi zasobami IT. Rozwiązanie wykrywa i usuwa podatności oraz umożliwia ograniczenie ich skutków, uniemożliwiając ich wykorzystanie dzięki najnowszym aktualizacjom aplikacji i systemów operacyjnych na wszystkich stacjach roboczych.

ESET Vulnerability & Patch Management korzysta z zaawansowanych technik priorytetyzacji oraz

zautomatyzowanych narzędzi, dzięki którym świetnie spełni potrzeby Twojej infrastruktury.

Rozwiązanie jest częścią platformy ESET PROTECT, a więc nie tylko dokonuje bieżącej oceny podatności i ocenia je na podstawie stwarzanego ryzyka i łatwości ich usunięcia, ale również chroni przed zagrożeniami, które nie dotyczą jedynie samego oprogramowania. Narzędzie oferuje również najwyższej klasy ochronę przed wszelkiego rodzaju złośliwym oprogramowaniem, w tym ransomware, a także ochronę przed atakami zero-day obejmującą wszystkie stacje robocze, serwery i skrzynki e-mail – a to wszystko w ramach jednego, zintegrowanego rozwiązania.

Kluczowe funkcje

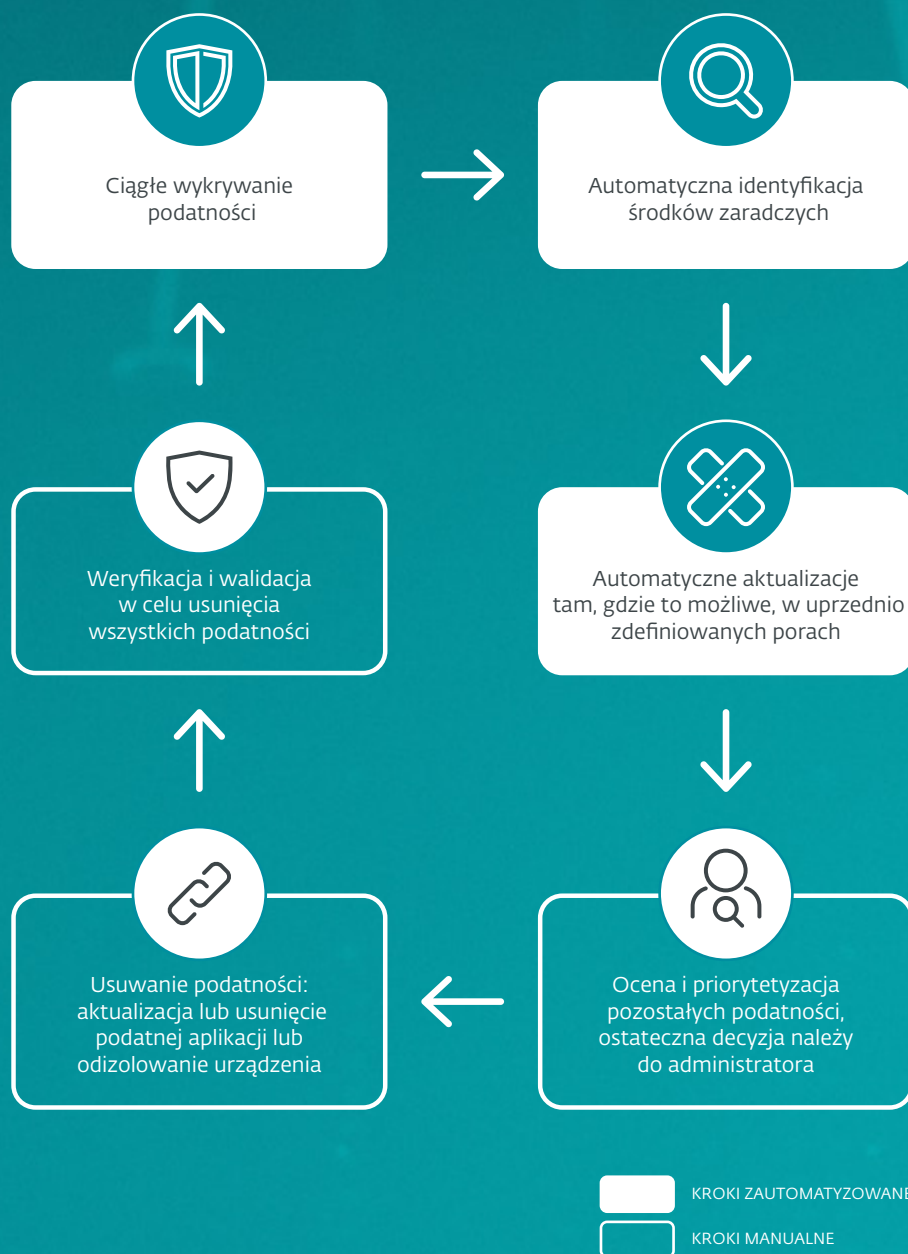
Ocena podatności

- Skanowanie tysięcy aplikacji takich jak Adobe Acrobat, Mozilla Firefox i Zoom Client oraz wsparcie dla różnych wersji systemu Windows (a wkrótce również i macOS)
- Wykrywanie ponad 35 tysięcy najczęściej spotykanych CVE – a ich lista jest stale aktualizowana
- Automatyczne skanowanie z możliwością tworzenia harmonogramów
- Priorytetyzacja i filtrowanie podatności na podstawie oceny ryzyka i zagrożenia
- Raporty na temat podatności dotyczących najbardziej narażonych programów i urządzeń
- Wsparcie funkcji wielu dzierżaw w złożonych środowiskach sieciowych; umożliwia wykrywanie podatności w konkretnych obszarach organizacji
- Baza podatności, CVSS 2.0 i CVSS 3.1
- Zintegrowany widok dzięki konsoli w chmurze ESET PROTECT, wsparcie dla różnych wersji językowych przy niskim obciążeniu infrastruktury IT

Zarządzanie aktualizacjami

- Wdrażaj natychmiastowe aktualizacje i łatki za pomocą konfigurowanych harmonogramów lub ręcznie
- Prostsze łatanie luk w zabezpieczeniach: skup się na krytycznych zasobach, a pozostałe aktualizuj w porach zmniejszonego ruchu, aby zapobiegać utrudnieniom
- Dodawaj i śledź wyjątki dotyczące aktualizowania wybranych aplikacji
- Korzystaj z aktualizowanej listy łatek zawierającej ich nazwy, nową wersję aplikacji, CVE, poziom krytyczności oraz aplikacje, jakich łatek dotyczy
- Wszystkie łatki dostępne dzięki konsoli ESET PROTECT Cloud

Jak to działa?



Przykłady zastosowania

O ile rosnąca popularność pracy zdalnej i usług chmurowych sprawia, że współczesne zagrożenia to już nie tylko podatności dotyczące oprogramowania, to regularne łatanie podatności aplikacji i systemów operacyjnych nadal ma kluczowe znaczenie, jeżeli chcemy zapobiegać naruszeniom.

Każdy administrator wie, że instalowanie aktualizacji to jedno z najbardziej czasochłonnych zadań w IT. A kiedy brakuje zasobów, aktualizacje schodzą na drugi plan, przez co podatności mogą wkradać się niemalże niezauważone. Rosnąca złożoność systemów IT może również skutkować brakiem koordynacji pomiędzy zespołami interdyscyplinarnymi, nieaktualnym inwentarzem lub ograniczoną widocznością zagrożeń.

Nie nadążamy z aktualizacjami

PROBLEM

Nasz zespół IT ma dużo pracy i zalega z aktualizacjami

ROZWIĄZANIE

Korzystaj z zaawansowanych technik priorytetyzujących i automatyzujących

- ✓ Ustalaj optymalną częstotliwość skanowania i synchronizuj skany z wdrożeniami aktualizacji, by usuwać potencjalnie niebezpieczne podatności bez dodatkowego obciążania Twoich zespołów IT
- ✓ Filtruj podatności pod względem poziomu zagrożenia; priorytetyzuj podatności, które stwarzają poważne zagrożenie dla Twojej działalności
- ✓ Dostosowuj swoją politykę aktualizacji. Priorytetyzuj krytyczne zasoby, samodzielnie usuwając najbardziej niebezpieczne podatności, a następnie automatyzuj instalowanie łatek pozostałych zasobów tak, by odbywało się ono poza godzinami wzmożonego ruchu, dzięki czemu zapobiegiesz utrudnieniom
- ✓ Dodawaj i śledź wyjątki dotyczące aktualizacji; nie musisz już śledzić każdego patcha

Niewystarczające zasoby IT

PROBLEM

Zależy mi na tym, by nasze aplikacje były aktualizowane na bieżąco, ale brakuje nam zasobów IT

ROZWIĄZANIE

Korzystaj z całkowicie zaktualizowanej oceny podatności i zarządzania aktualizacjami, a także wsparcia ekspertów ESET:

- ✓ Automatyczne skanowanie oprogramowania stacji roboczych oraz aplikacji zewnętrznych, a także natychmiastowe raportowanie do konsoli, pozwalające wykrywać podatności na bieżąco
- ✓ Aby zagwarantować ciągłość ochrony w Twojej organizacji, skonfiguruj automatyczne łatanie podatności, wybierając strategię aktualizacji (wszystkie, tylko dozwolone, wszystkie poza wykluczonymi) oraz określając przedziały czasowe, w których aktualizacje mają być instalowane

Rosnący poziom skomplikowania infrastruktury, wyzwania w kwestii koordynacji

PROBLEM

Stopień złożoności infrastruktury IT stale rośnie, przez co koordynacja pomiędzy zespołami interoperacyjnymi staje się coraz trudniejsza

ROZWIĄZANIE

Wybierz platformę ESET PROTECT, dzięki której możesz zarządzać rozwiązaniem ESET Vulnerability & Patch Management oraz zabezpieczeniami wszystkich Twoich zasobów i aktywów cyfrowych

- ✓ Zintegruj i zautomatyzuj różne zadania dotyczące bezpieczeństwa i zarządzania IT dzięki konsoli ESET PROTECT, w skład której wchodzi rozwiązanie ESET Vulnerability & Patch Management.* Uprość zarządzanie swoją infrastrukturą IT
- ✓ Skorzystaj z funkcjonalności wielu dzierżaw oferowanej przez ESET Vulnerability & Patch Management: ciesz się odpowiednim przeglądem Twojej sieci z jednoczesnym wglądem w jej konkretne obszary
- ✓ Prowadź aktualną listę podatności i łataj luki w zabezpieczeniach Twojej infrastruktury
- ✓ Zyskaj dzięki strategiom zapobiegania, wykrywania i reagowania ESET PROTECT, dzięki którym zminimalizujesz ryzyko zagrożeń wykraczających poza samo oprogramowanie
- ✓ ESET Vulnerability & Patch Management ułatwia osiągnięcie zgodności z RODO oraz innymi wymogami dotyczącymi bezpieczeństwa danych nakładanymi przez instytucje branżowe, rządowe i regulacyjne

Ograniczona widoczność infrastruktury IT

PROBLEM

Brakuje mi przeglądu zabezpieczeń mojej infrastruktury IT

ROZWIĄZANIE

Skorzystaj ze zintegrowanego widoku, jaki oferuje konsola ESET PROTECT Cloud

- ✓ Ciesz się całkowitą weryfikacją stacji roboczych, licencji oraz statusów podatności i aktualizacji wszystkich zasobów Twojej organizacji, dzięki czemu zawsze będziesz na bieżąco
- ✓ Śledź stan swoich zabezpieczeń w czasie rzeczywistym dzięki konsoli ESET PROTECT Cloud
- ✓ Łącz się z dowolnego miejsca o dowolnej porze, korzystając z Twojej ulubionej przeglądarki – a tym samym natychmiast reaguj na zdarzenia
- ✓ Twórz przydatne raporty na temat postępów i skuteczności polityk zarządzania podatnościami i aktualizacjami

* Tylko ESET PROTECT Complete oraz ESET PROTECT Elite

OPCJE ZAKUPU:

Rozwiązanie ESET Vulnerability & Patch Management
dostępne jest w ramach następujących pakietów:

 PROTECT COMPLETE

 PROTECT ELITE

O ESET

TECHNOLOGIA UMOŻLIWIA POSTĘP, ESET JĄ ZABEZPIECZA.

ESET to ponad 30 lat innowacji technologicznych, dzięki którym firma dostarcza najbardziej zaawansowane zabezpieczenia na rynku cyberbezpieczeństwa. Nasze nowoczesne zabezpieczenia stacji roboczych korzystają z wyjątkowych technologii bezpieczeństwa ESET LiveSense® w połączeniu z uczeniem maszynowym i usługami chmurowymi. Dzięki mechanizmowi threat intelligence i przełomowym badaniom produkty ESET to optymalne połączenie zdolności zapobiegania, wykrywania i reagowania. Łatwość użytkowania i niezrównana szybkość gwarantuje skuteczną ochronę naszych klientów.

ESET W LICZBACH

1mln+

użytkowników
na świecie

400k+

klientów
biznesowych

195

krajów
i terytoriów

13

centrów
badawczo-
rozwojowych

NASI KLIENTCI



chronione przez ESET od 2017
ponad 9 000 stacji roboczych



chroniony przez ESET od 2016
ponad 4 000 skrzynek
mailowych



chroniony przez ESET od 2016
ponad 32 000 stacji
roboczych



partner ISP od 2008
baza ponad 2 mln klientów

ESET UZNANY PRZEZ



ESET otrzymał nagrodę Business Security APPROVED od AV - Porównywarki w teście Business Security Test w grudniu 2022 roku.



ESET nieustannie zajmuje czołowe miejsca w rankingach globalnej platformy G2, a jego rozwiązania są doceniane przez klientów na całym świecie.



ESET po raz 4. został uznany za tzw. „Kluczowego gracza” w raporcie Radicati Advanced Persistent Threat (APT) Protection — Market Quadrant 2023.