CTI Telekom Sp. z o.o.
02-389 Warszawa
al. Bohaterów Września 9
NIP: 5262666398
tel. +4822 398 89 00

Dane aktualne na dzień: 21-05-2026 09:33

Link do produktu: https://www.ctistore.pl/cisco-sec-ea-20-choice-amp-endpoints-essentials-10pk-p-293098.html

CISCO Sec EA 2.0 Choice AMP Endpoints Essentials 10pk

Cena brutto	**194,10 zł**
Cena netto	**157,80 zł**
Dostępność	**Dostępny**
Czas wysyłki	**1-3 dni**
Numer katalogowy	**4374951**
Kod producenta	**E2SF-P-AMP-EP-10**

Opis produktu

Opis
Cisco Advanced Malware Protection (AMP) for Endpoint oferuje jedyny zaawansowany system ochrony przed złośliwym oprogramowaniem, który obejmuje całe kontinuum ataku - przed, w trakcie i po ataku. Zapewnia ciągłą analizę i zaawansowaną analitykę, które wspierają retrospektywne możliwości bezpieczeństwa Cisco. Bezpieczeństwo retrospektywne to możliwość spojrzenia wstecz w czasie i śledzenia procesów, działań na plikach i komunikacji w celu zrozumienia pełnego zakresu infekcji, ustalenia pierwotnej przyczyny i przeprowadzenia działań naprawczych. Potrzeba zabezpieczenia retrospektywnego pojawia się, gdy wystąpią jakiekolwiek oznaki naruszenia bezpieczeństwa, takie jak wyzwalacz zdarzenia, zmiana w dyspozycji pliku lub wyzwalacz wskazujący na naruszenie bezpieczeństwa (IoC). Zabezpieczenia retrospektywne pozwalają menedżerom cofnąć się w czasie w celu zbadania zagrożeń w ich systemach. Narzędzia takie jak retrospekcja, korelacja łańcucha ataków, behawioralne IoC, trajektoria i wyszukiwanie naruszeń pozwalają specjalistom ds. bezpieczeństwa ustalić zakres, widoczność i kontrolę w przypadku naruszenia. Ta zdolność pomaga zespołowi ds. bezpieczeństwa szybko i skutecznie zaradzić wszystkim zagrożeniom w środowisku, zanim będzie za późno.

- **Ciągła analiza**
  AMP for Endpoint wykorzystuje opartą na chmurze analizę dużych zbiorów danych, aby wykraczać poza wykrywanie punktowe w czasie, stale ponownie oceniając nowe i historyczne dane gromadzone w czasie w celu wykrywania ukrytych ataków.
- **Kontrola epidemii**
  AMP for Endpoint zapewnia możliwości wykrywania i kontrolowania podejrzanych plików na punktach końcowych zarówno pod kątem przyszłych, jak i przeszłych zagrożeń. Kontrola epidemii jest jedną z kluczowych funkcji, które pomagają szybko powstrzymać rozprzestrzenianie się złośliwego oprogramowania w środowisku.
- **IoCs**
  AMP for Endpoint automatycznie koreluje dane o zdarzeniach bezpieczeństwa z wielu źródeł, takich jak włamania i złośliwe oprogramowanie, aby pomóc zespołom ds. bezpieczeństwa połączyć zdarzenia z większymi, skoordynowanymi atakami.
- **Reputacja plików**
  Wykorzystuje zaawansowaną analitykę i zbiorową inteligencję, aby określić, czy plik jest czysty, czy złośliwy, poprawiając dokładność wykrywania.
- **Analiza plików i sandboxing**
  Wykorzystuje wysoce bezpieczne środowisko do wykonywania, analizowania i testowania zachowania złośliwego oprogramowania, pomagając odkryć nieznane wcześniej zagrożenia typu zero-day.
- **Trajektoria pliku**
  Śledzi rozprzestrzenianie się plików w środowisku w czasie, dzięki czemu można zminimalizować czas wymagany do wykrycia naruszenia złośliwego oprogramowania.
- **Trajektoria urządzenia**
  Śledzi aktywność i komunikację na poziomie systemu w czasie, umożliwiając szybkie zrozumienie głównych przyczyn i historii zdarzeń prowadzących do i po naruszeniu bezpieczeństwa.
- **Elastyczne wyszukiwanie**
  Zapewnia proste, nieograniczone wyszukiwanie w plikach, telemetrii i zbiorowych danych analitycznych dotyczących bezpieczeństwa, pomagając połączyć kontekst i zakres ekspozycji na IoC lub złośliwą aplikację.
- **Ochrona wykraczająca poza punkt w czasie**
  AMP for Endpoint stosuje retrospektywne podejście bezpieczeństwa do tradycyjnego wykrywania, pomagając obronie

poprawić możliwości punktowe w czasie i stać się bardziej skutecznym, wydajnym i wszechobecnym.

- **Widoczność łańcucha ataków**
  AMP for Endpoint to coś więcej niż retrospekcja. Wprowadza nowy poziom inteligencji, łącząc i korelując różne formy retrospekcji w linię aktywności dostępną do analizy w czasie rzeczywistym. Następnie wyszukuje wzorce złośliwego zachowania na pojedynczym punkcie końcowym lub w całym środowisku punktów końcowych.
- **Zaawansowana analiza**
  AMP for Endpoint zapewnia zautomatyzowane, zaawansowane funkcje wykrywania zachowań, które zapewniają priorytetowy i zestawiony widok najważniejszych obszarów naruszeń i ryzyka.
- **Dochodzenie, które zmienia łowcę w myśliwego**
  AMP for Endpoint przenosi działania śledcze poza poszukiwanie faktów i wskazówek na ukierunkowane polowanie na naruszenia oparte na rzeczywistych zdarzeniach, takich jak wykrycia złośliwego oprogramowania i behawioralne IoC.
- **Uproszczone powstrzymywanie**
  AMP for Endpoint zapewnia wgląd w łańcuch zdarzeń i kontekst, który uzupełnia pulpity nawigacyjne i widoki trajektorii. AMP for Endpoint umożliwia ukierunkowanie na określone aplikacje, pliki, złośliwe oprogramowanie i inne przyczyny źródłowe, dzięki czemu przerwanie łańcucha ataków jest szybkie, łatwe i proste.
- **Przydatne, kontekstowe pulpity nawigacyjne**
  Raporty nie ograniczają się do wyliczania i agregacji zdarzeń. Raportowanie AMP for Endpoint obejmuje praktyczne pulpity nawigacyjne i trendy, które podkreślają znaczenie biznesowe i wpływ z perspektywy ryzyka.
- **Ściśle zintegrowane platformy**
  AMP można aktywować w rozwiązaniach Cisco Email i Web Security za pomocą jednego przełącznika. Aby zapewnić lepszą widoczność i kontrolę, AMP można wdrożyć inline jako dedykowane urządzenie sieciowe oraz w punkcie końcowym jako lekki łącznik.

Produkt:

Nazwa:	CISCO Sec EA 2.0 Choice AMP Endpoints Essentials 10pk
Opis:	Cisco Advanced Malware Protection for Endpoints - Licencja - liczba licencji — 10 - Security Enterprise Licensing Agreement (ELA) 2.0 - Win, Android, Mac
EAN:	
Reklamacje:	Brak gwarancji
Ogólne	
Kategoria:	Usługi online i narzędziowe - narzędzia do usuwania oprogramowania i reklam
Typ produktu:	Licencja
Platforma:	Windows, Android, MacOS
Licencje	
Ilość licencji:	Liczba licencji — 10
Program licencjonowania:	Security Enterprise Licensing Agreement (ELA) 2.0

Dane techniczne przekazywane nam są przez firmy trzecie do celów informacyjnych. Nie ponosimy żadnej odpowiedzialności za zawarte w nich ewentualne błędy.