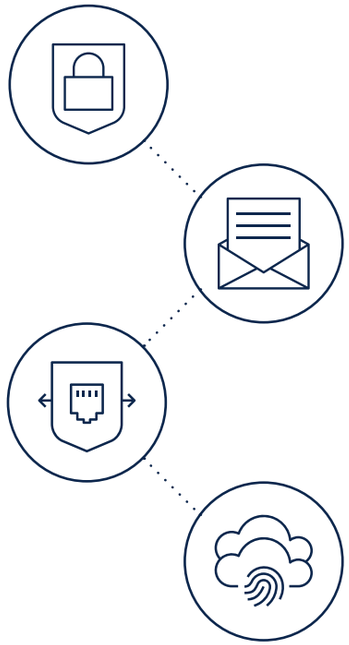
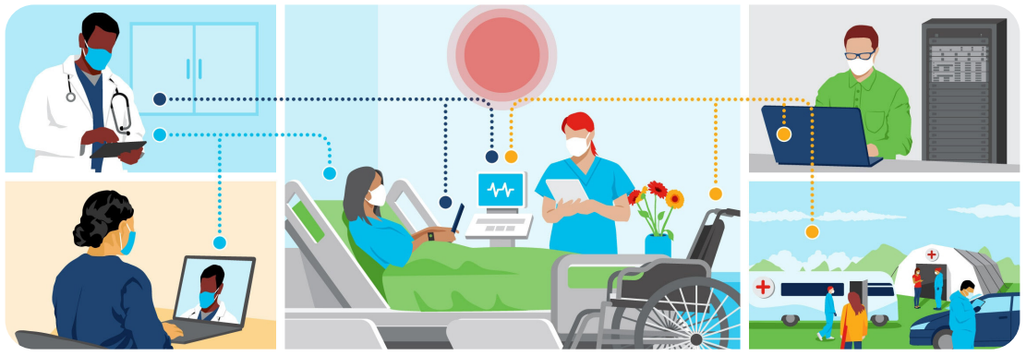
Czy wiesz, że...

21 maja 2022 r. weszło w życie **Zarządzenie nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia** w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych u świadczeniodawców.

Zarządzenie określa warunki przyznawania i rozliczania środków na finansowanie działań, które mogą podnieść poziom bezpieczeństwa posiadanych systemów.

W ofercie Cisco Systems znaleźć można konkretne rozwiązania spełniające wytyczne i wymagania funkcjonalne **Zarządzenia:**





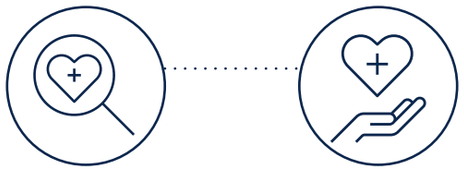
Rozwiązania Cisco spełniające wytyczne i wymagania funkcjonalne

Zarządzenia 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia.

1. Cisco Secure Endpoint

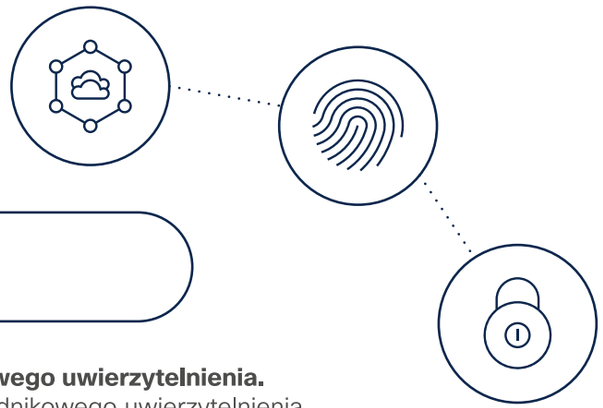
Cisco Secure Endpoint to rozwiązanie klasy EDR pozwalające efektywnie ochronić stację przed atakami, w tym atakami typu „zero day" oraz ransomware. Umożliwia precyzyjną analizę pełnego spektrum zachowań stacji, jej aplikacji oraz sprawdzenie, jak zachowanie procesów zmieniało się w czasie. Cisco Secure Endpoint zapewnia możliwość drobiazgowego, retrospektywnego prześledzenia prób ingerencji złośliwego oprogramowania w systemy i wykrycie tzw. „pacjentów zero". Podstawą działania Cisco Secure Endpoint jest śledzenie ruchu z dokładnością do procesu. Dzięki natywnej integracji z bezpłatną platformą Cisco SecureX rozwiązanie jest w stanie zapewnić funkcjonalności systemu XDR. Warto podkreślić, że Cisco Secure Endpoint jest bardzo prosty we wdrożeniu i utrzymaniu, nawet w dużym środowisku. Rozwiązanie jest licencjonowane na liczbę stacji chronionych.

Cisco Secure Endpoint spełnia wytyczne i funkcjonalne Zarządzenia 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia w zakresie § 3. 1. 1. b) systemów antywirusowych dla stacji roboczych i serwerów – centralnie zarządzanych, systemów klasy Endpoint Detection and Response (EDR)



2. Cisco Cloud Email Security

w zakresie bezpiecznego systemu **poczty elektronicznej.**
Cisco Cloud Email Security jest wiodącym na rynku rozwiązaniem zapewniającym ochronę poczty elektronicznej. Z uwagi na popularność ataków przez pocztę elektroniczną, zabezpieczenie tej usługi jest krytyczne. Rozwiązanie umożliwia bezpieczną komunikację poprzez email. Skutecznie chroni przed zagrożeniami, zarówno malware jak i ransomware, pozwala na efektywne blokowanie SPAM, zapewnia klasyfikacje maili, ma wbudowany silnik DLP oraz integruje rozwiązanie sandbox Cisco ThreatGrid. Rozwiązanie jest licencjonowane na liczbę chronionych skrzynek email.



3. Cisco DUO

w zakresie systemów **wieloskładnikowego uwierzytelnienia.**
Cisco Duo jest rozwiązaniem wieloskładnikowego uwierzytelnienia (MFA). Jest to jedno z najprostszych rozwiązań MFA na rynku. Pozwala ono w szybki i prosty sposób uzyskać bezpieczny dostęp do wszystkich aplikacji oraz innych systemów np. VPN. Cisco DUO jest fundamentem architektury Zero Trust. Rozwiązanie jest licencjonowane na liczbę użytkowników korzystających z rozwiązania.

Cisco Cloud Email Security oraz **Cisco DUO** spełniają wytyczne i funkcjonalne Zarządzenia 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia w zakresie § 3. 1. 1. e) systemów zapewniających bezpieczny system poczty elektronicznej, włączając w to systemy weryfikacji załączników i treści korespondencji oraz systemy wieloskładnikowego uwierzytelniania.

4. Cisco Umbrella

Cisco Umbrella to chmurowa platforma bezpieczeństwa, która pełni rolę pierwszej linii obrony przed zagrożeniami. Cisco Umbrella chroni w czasie rzeczywistym każdą komunikację DNS ze stacji końcowej, a więc potrafi automatycznie zablokować zagrożenie zanim dotrze do sieci, czy urządzenia końcowego pracownika. Rozwiązanie jest podstawowym, prostym i efektywnym mechanizmem ochrony przed zagrożeniami takimi jak ransomware. Cisco Umbrella pełni ponadto rolę pełnego web proxy z elementami inspekcji plików, dekrypcji SSL czy DLP. Posiada również funkcjonalności takie jak CDFW (Cloud Delivered Firewall) oraz CASB (Cloud Access Security Broker). Umbrella to podstawowy element architektury bezpieczeństwa SASE (Secure Access Service Edge). Rozwiązanie jest licencjonowane na liczbę użytkowników chronionych w sieci.

Cisco Umbrella spełnia wytyczne i funkcjonalne Zarządzenia 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia w zakresie § 3. 1. 1. f) rozwiąza zapewniających ochron DNS (DNS Protection) z użyciem systemów lokalnych (licencja oraz wsparcie w okresie do dnia 31 grudnia 2022 r.),

Powyższe rozwiązania spełniają wytyczne i wymagania funkcjonalne zarządzenia 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia

W przypadku pytań zapraszamy do kontaktu email:
Joanna Gustyn, **jgustyn@cisco.com**