enteo
CLOUDPOINT

DOKUMENTACJA HANDLOWA

Cloudpoint Opis usług

Infrastruktura chmurowa dla polskiego biznesu

- Charakterystyka
- Pełny zakres
- Metody rozliczeń
- Zakres odpowiedzialności

enteo.pl · dh@cloudpoint.pl

Wersja dokumentu: 31.08.2026

enteo
CLOUDPOINT

01

MODEL USŁUGI

IaaS*

Infrastructure as a Service — zasoby centrum danych Enteo Cloudpoint, gotowe do uruchomienia w kilka chwil.

ROZLICZENIE
Wedle zużycia per CPU i RAM

DOSTĘPNOŚĆ
Tier III · ISO 27001

LOKALIZACJA
Polskie centrum danych

Pełna kontrola nad środowiskiem · samodzielne zarządzanie przez portal

IaaS*

INFRASTRUCTURE AS A SERVICE

DLACZEGO IAAS

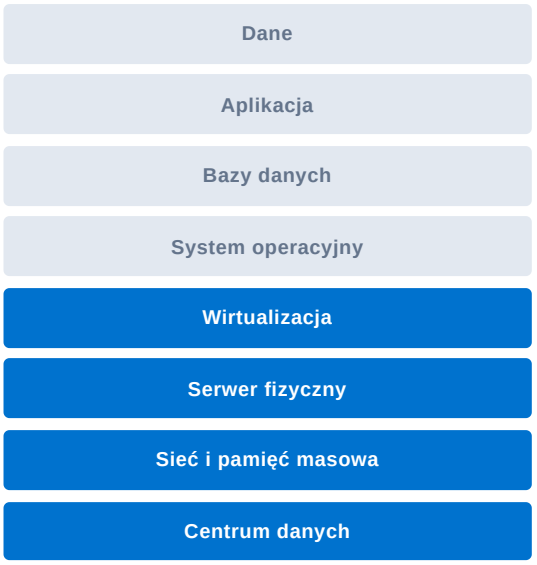
Profesjonalna infrastruktura bez własnej serwerowni

Systemy IT stanowią obecnie podstawę funkcjonowania znakomitej większości firm. Trudno wyobrazić sobie efektywny biznes bez dobrego systemu ERP, sprawnej komunikacji i wymiany dokumentów czy wydajnych systemów wspomagających np. logistykę czy produkcję. Aby systemy mogły efektywnie gwarantować ciągłość oraz bezpieczeństwo działania — kluczowa jest infrastruktura, na której są uruchomione.

Budowa i utrzymanie własnej profesjonalnej serwerowni są trudne i bardzo kosztowne. Własne środowisko jest mało elastyczne i często przysparza znacznych problemów, a jego odpowiednie zabezpieczenie wymaga trudno dostępnej specjalistycznej wiedzy.

> Odpowiedzią jest przygotowana przez Enteo Cloudpoint usługa IaaS — elastyczna, bezpieczna i w pełni zarządzana infrastruktura w polskim centrum danych.

ZAKRES ZARZĄDZANIA



Niebieski = zakres Enteo Cloudpoint

***** Usługa zawiera licencje oprogramowania Microsoft udostępniane w ramach programu Microsoft SPLA — warunki na stronie 14.

ZAKRES USŁUGI

Co wchodzi w skład usługi

- Moc obliczeniowa procesorów i pamięci RAM
- Przechowywanie danych na szybkiej i bezpiecznej pamięci masowej
- Komunikacja w ramach wysoko dostępnej sieci o przepustowości min. 10 Gbps
- Dostęp do systemu kopii zapasowych wykonywanych bezagentowo do odrębnego centrum danych na terenie Polski
- Licencje Windows Server wraz z CAL-ami w cenie usługi
- Dedykowany firewall z funkcją IPSec VPN w cenie usługi
- 1 publiczny adres IPv4 i 100 Mbps dostępu do Internetu bez limitu transferu (możliwość dokupienia dodatkowych IP i przepływności)

USŁUGI DODATKOWE

Istnieje możliwość zakupu dodatkowych produktów i usług w zakresie bezpieczeństwa i zarządzania jak systemy NG Firewall, WAF, AntySpam, NG-Endpoint, produkty Microsoft. Enteo Cloudpoint służy wsparciem w zakresie projektu, konfiguracji i zabezpieczenia rozwiązania bazując na inżynierach z doświadczeniem w dużych złożonych projektach dla największych polskich firm.

ROZLICZANIE

Model rozliczeniowy

Rozliczenie odbywa się miesięcznie zgodnie z zużyciem per instancja maszyny wirtualnej w oparciu o przypisane im zasoby CPU, RAM, storage dla maszyn wirtualnych, storage dla kopii zapasowych. Dodatkowe publiczne adresy IP i przepustowość Internetu rozliczane są zgodnie z zamówieniem.

CHARAKTERYSTYKA USŁUGI

Dostęp przez portal webowy HTML5. Środowisko jest w pełni odseparowane od innych klientów — wszystkie maszyny wirtualne, sieci i firewalle są dedykowane dla Klienta.

Całość przetwarzania odbywa się na terenie RP. Nasze centrum danych spełnia najwyższe standardy w zakresie dostępności potwierdzone certyfikacją **Tier III** i **ISO 27001**.

PROFIL KLIENTA

Firmy posiadające własne zasoby IT z kompetencjami w zarządzaniu systemami (ERP, MES, WMS, WorkFlow, B2B), które chcą wyeliminować problemy z utrzymaniem własnej infrastruktury. Usługa dostępna również dla Partnerów realizujących ją dla swoich Klientów.

SZCZEGÓŁOWY PODZIAŁ ODPOWIEDZIALNOŚCI

Wyłączna odpowiedzialność techniczna Enteo	Odpowiedzialność Klienta
• Dostępność i wydajność zasobów: CPU, RAM, Storage, sieć, Internet • Utrzymanie portalu zarządzającego i warstwy wirtualizacji • Dostępność centrum danych i infrastruktury fizycznej • Techniczne reagowanie na awarie w zakresie infrastruktury	• Wdrożenie systemów operacyjnych i konfigurację środowiska • Samodzielne tworzenie serwerów, sieci, dysków i firewalli w portalu • Zarządzanie i bezpieczeństwo systemów oraz aplikacji • Dane, wymagania zasobowe i decyzje biznesowe

enteo
CLOUDPOINT

02

MODEL USŁUGI

PaaS*

Platform as a Service — gotowa platforma systemowa, w pełni zarządzana przez inżynierów Enteo Cloudpoint.

ROZLICZENIE	ZARZĄDZANIE	DR
Per instancja VM (CMI)	**Do poziomu systemu OS**	**Opcjonalne, w centrum w RP**

Wszystkie cechy IaaS bez konieczności samodzielnego zarządzania środowiskiem

PaaS*

PLATFORM AS A SERVICE

DLACZEGO PAAS

Zarządzana platforma bez kompetencji infrastrukturowych

Zarządzanie chmurą od strony portalu, zarządzanie bezpieczeństwem i efektywne zarządzanie systemami operacyjnymi wymaga sporej wiedzy z zakresu infrastruktury IT, sieci i bezpieczeństwa.

Z doświadczenia Enteo Cloudpoint wynika, że infrastruktura przygotowana i zarządzana przez specjalistów znacząco podnosi jakość działania systemów IT, a zwłaszcza bezpieczeństwo danych. Klient otrzymuje gotową platformę systemową do wdrożenia i utrzymania kluczowych dla jego biznesu aplikacji.

> Usługa zawiera wszystkie cechy IaaS, z wyjątkiem zarządzania przez Klienta poprzez portal — wszystkim zajmuje się zespół Enteo Cloudpoint.

ZAKRES ZARZĄDZANIA

- Dane
- Aplikacja
- **Bazy danych**
- **System operacyjny**
- **Wirtualizacja**
- **Serwer fizyczny**
- **Sieć i pamięć masowa**
- **Centrum danych**

Niebieski = zakres Enteo Cloudpoint

***** Usługa zawiera licencje oprogramowania Microsoft udostępniane w ramach programu Microsoft SPLA — warunki na stronie 14.

CO ZAWIERA USŁUGA

Pełny zakres Cloudpoint Managed Instances

- Przechowywanie maszyn wirtualnych na szybkiej i bezpiecznej pamięci masowej
- Komunikacja w ramach wysoko dostępnej sieci o przepustowości min. 10 Gbps
- Kopie zapasowe wykonywane zgodnie z indywidualnym harmonogramem do odrębnego centrum danych na terenie Polski
- W pełni zarządzany firewall brzegowy z możliwością zestawienia dowolnej liczby tuneli IPSec VPN
- Firewall dystrybuowany realizujący mikrosegmentację — dopuszczenie tylko niezbędnych przepływów sieciowych
- Licencje Windows Server wraz z CAL-ami w cenie usługi
- 1 publiczny adres IPv4 i 100 Mbps dostępu do Internetu bez limitu transferu
- Możliwość uruchomienia usługi DR do odrębnego centrum danych na terenie Polski

ZARZĄDZANIE OPERACYJNE

Bieżąca obsługa techniczna

- Bieżąca konfiguracja i monitorowanie pracy maszyn wirtualnych
- Monitorowanie funkcjonowania i wydajności systemów Windows i Linux
- Aktualizacja systemów operacyjnych zgodnie z harmonogramem
- Monitorowanie poprawności wykonywania kopii zapasowych
- Odzyskiwanie danych na życzenie Klienta lub w wypadku awarii
- Reagowanie na usterki, awarie i problemy wydajnościowe
- Pełne zarządzanie ochroną EDR — w tym sam system EDR oraz obsługa incydentów bezpieczeństwa

ROZLICZENIE

Rozliczenie miesięcznie per instancja maszyny wirtualnej z predefiniowaną konfiguracją CPU i RAM. Storage rozliczany miesięcznie zgodnie ze zużyciem. Enteo Cloudpoint automatycznie monitoruje i zwiększa storage w miarę rosnących potrzeb.

CHARAKTERYSTYKA

Indywidualnie projektowane środowisko

Usługa jest zawsze projektowana dla konkretnego Klienta przez inżynierów Enteo Cloudpoint zgodnie z jego wymaganiami i najwyższymi standardami dostępności, wydajności i bezpieczeństwa. Środowisko jest w pełni odseparowane — wszystkie maszyny wirtualne, sieci i firewalle są dedykowane.

Całość przetwarzania, zarówno w podstawowym centrum danych jak i centrum DR, odbywa się na terenie RP. Centrum danych posiada certyfikację **Tier III** i **ISO 27001**. Komunikacja przez system zgłoszeń **support@cloudpoint.pl**.

PRZYKŁADY PODZIAŁU

Scenariusze odpowiedzialności

Windows z AD i serwerem plików

Enteo Cloudpoint: utrzymanie serwera, konfiguracja AD i serwera plików, poprawki bezpieczeństwa. Klient: żądania zmian (udziały, użytkownicy AD), aktualizacje pozabezpieczeństwowe.

Linux / Windows z serwerem WWW lub DB

Enteo Cloudpoint: utrzymanie i dostępność serwera, poprawki bezpieczeństwa. Klient: konfiguracja i instalacja serwera WWW/DB, aktualizacje pozabezpieczeństwowe.

Windows z usługą terminalową

Enteo Cloudpoint: utrzymanie serwera, konfiguracja usług terminalowych, poprawki. Klient: instalacja aplikacji (ERP, Płatnik, podpis elektroniczny).

SZCZEGÓŁOWY PODZIAŁ ODPOWIEDZIALNOŚCI — C-SUPPORT-GOLD / PAAS

Wyłączna odpowiedzialność techniczna Enteo	Odpowiedzialność Klienta
• Infrastruktura fizyczna, wirtualizacja i sieć • Systemy operacyjne i powszechne usługi systemowe • Bezpieczeństwo platformy i aktualizacje bezpieczeństwa • Backup zgodnie z zamówieniem i techniczne reagowanie na awarie	• Aplikacje biznesowe i ich konfiguracja merytoryczna • Dane oraz współpraca z dostawcami tych aplikacji • Wymagania RPO/RTO oraz potrzeby zasobowe • Decyzje biznesowe i akceptacja ryzyka

Zakres odpowiedzialności Enteo Cloudpoint kończy się na poziomie systemu operacyjnego i powszechnych usług. Klient zgłasza osoby, które mają uzyskać prawa administratora lokalnego.

C-SUPPORT-PLATINUM

DODATEK DO PAAS — ZARZĄDZANIE APLIKACJAMI, DR I AUDYT

ROZSZERZENIE USŁUGI PAAS

Zaawansowane wsparcie aplikacji, ciągłości i bezpieczeństwa

C-SUPPORT-PLATINUM to opcjonalny dodatek dokupywany do usługi PaaS (Cloudpoint Managed Instances), rozszerzający zakres o pełne zarządzanie aplikacjami firm trzecich oraz regularne testy odtworzenia i coroczny audyt bezpieczeństwa.

> Dodatek dostępny wyłącznie do aktywnej usługi **PaaS**. Rozliczany **per CMI** (per instancja Cloudpoint Managed Instances), analogicznie do usługi PaaS.

ZARZĄDZANIE APLIKACJAMI

- Pełna administracja aplikacjami biznesowymi: enova365, Microsoft Exchange, WordPress, SQL Server, PostgreSQL, Nextcloud, Jira i inne
- Zarządzanie strukturą instancji, konfiguracją usług, kontami i uprawnieniami
- Monitoring dostępności i responsywności aplikacji, powiadomienia o błędach i przekroczeniach zasobów
- Planowanie i bezpieczne wdrażanie aktualizacji (core, pluginy, zależności, silniki DB)
- Zarządzanie kopiami zapasowymi danych aplikacyjnych

Zakres zarządzania aplikacjami odpowiada usłudze T-SUPPORT-SERVER-APP-AddOn w ofercie enteo Technologie. Usługa nie obejmuje zakresu merytorycznego (np. konfiguracji funkcji biznesowych ERP).

TESTY ODTWORZENIA I DISASTER RECOVERY

- Regularny test odtworzenia kopii zapasowych i DR — nie rzadziej niż 2 razy w roku
- Weryfikacja poprawności i kompletności odtwarzanych danych
- Potwierdzenie gotowości środowiska zapasowego i zgodności z założeniami RPO/RTO

COROCZNY AUDYT BEZPIECZEŃSTWA

Raz w roku przeprowadzany audyt obejmujący:

- Weryfikację aktualizacji i hardeningu systemów
- Poprawność konfiguracji oraz segmentacji sieci
- Szczegółowość i zasadność reguł firewall
- Kompletność dokumentacji technicznej
- Przegląd uprawnień i dostępów

ROZLICZENIE

Dodatek rozliczany miesięcznie per CMI, dokupywany do aktywnej usługi PaaS. Nie może być zamawiany samodzielnie.

SZCZEGÓŁOWY PODZIAŁ ODPOWIEDZIALNOŚCI

Wyłączna odpowiedzialność techniczna Enteo	Odpowiedzialność Klienta
• Administracja aplikacjami (usługi, konfiguracje, dostęp) • Diagnostyka, rozwiązywanie problemów i aktualizacje • Backup danych aplikacyjnych • Przeprowadzanie testów odtworzenia i Disaster Recovery • Przeprowadzanie corocznego audytu bezpieczeństwa i raportowanie wyników	• Zgłaszanie potrzeb funkcjonalnych (role, konta, funkcjonalności) • Udział w decyzjach biznesowych przy wdrożeniach • Współpraca z firmami wdrożeniowymi • Wdrażanie rekomendacji poaudytowych • Decyzje biznesowe i akceptacja ryzyka

enteo
CLOUDPOINT

03

MODEL USŁUGI

SaaS*

Software as a Service — kompletna platforma biznesowa, w pełni przygotowana i utrzymywana przez Enteo Cloudpoint.

WARIANTY
Terminal · Db · Enova365Web

ROZLICZENIE
Per użytkownik / instancja

TECHNOLOGIA
Kubernetes · Microsoft

Dla firm o prostej strukturze IT — handel, biura rachunkowe, organizacje z 1–2 systemami

SaaS*

SOFTWARE AS A SERVICE — TERMINAL

DLACZEGO SAAS

Chmura dla firm z prostym środowiskiem IT

Wiele firm posiada proste środowisko IT złożone z jednej lub dwóch aplikacji — np. systemu ERP wymagającego bazy danych i stacji roboczej. Firmy te chcą skorzystać z zalet chmury (elastyczność, obniżenie kosztów, bezpieczeństwo), ale budowa złożonego środowiska chmurowego jest biznesowo nieopłacalna.

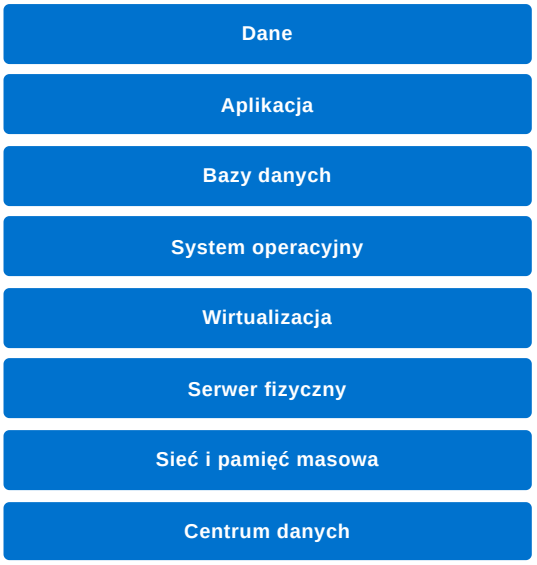
SaaS Cloudpoint to odpowiedź — przygotowana i w pełni utrzymywana usługa dopasowana do potrzeb małych i średnich firm.

SAAS-TERMINAL

Desktop Windows w chmurze

- Wszystkie wymagane licencje Microsoft zawarte w cenie
- Dostęp przez RDP Gateway (SSL VPN w kliencie RDP) — terminale nie są publikowane w Internecie
- Pełne zarządzanie; zasoby dostosowywane do obciążenia bez dodatkowych kosztów
- Regularne aktualizacje luk bezpieczeństwa
- Uprawnienia administratora lokalnego dla wskazanych użytkowników
- Kopie zapasowe nie rzadziej niż raz na 24h
- Kompleksowy system ochrony przed wirusami i atakami
- Możliwość jednego dostępu administracyjnego w obniżonej cenie

ZAKRES ZARZĄDZANIA



Niebieski = zakres Enteo Cloudpoint

* Usługa zawiera licencje oprogramowania Microsoft udostępniane w ramach programu Microsoft SPLA — warunki na stronie 14.

SAAS-DB

Dedykowany serwer bazodanowy MS SQL

- Kopie zapasowe zależne od wersji usługi (Silver, Gold, Platinum) — 1, 2 lub 3 razy dziennie
- Regularne aktualizacje luk bezpieczeństwa
- Nielimitowana ilość baz danych
- Nielimitowana rozbudowa powierzchni danych, niezależnie od wariantu
- Obsługa nawet kilkuset jednoczesnych użytkowników (najwyższy wariant)
- Dostęp administracyjny przez Internet z usługą SaaS-VPN
- Dostęp do kopii zapasowych bezpośrednio z SQL Server Management Studio

SAAS-ENOVA365WEB

Dedykowany serwer Enova365 Web

- Aktualizacje na zgłoszenie, w uzgodnionym terminie, bez dodatkowych kosztów
- Możliwość rozbudowy o Harmonogram Zadań, TeleKey, WebApi
- Dostęp domyślnie zabezpieczony usługą CDN i WAF Cloudflare — serwery publikowane przez globalną sieć pośredniczącą
- Dedykowany serwer plików na przechowywanie załączników

TECHNOLOGIA I CERTYFIKATY

Sprawdzone fundamenty bezpieczeństwa

SaaS-Db i SaaS-Enova365 pracują pod kontrolą Linux z konteneryzacją Kubernetes (K8S), na wirtualizacji Microsoft Hyper-V zabezpieczonej zgodnie z normą **ISO 27001** oraz standardami **NIS2, CIS, STIG**.

Całość przetwarzania na terenie RP. Centrum danych z certyfikacją **Tier III**. SaaS-VPN umożliwia bezpieczny dostęp zdalny do zasobów Cloudpoint (IaaS, PaaS) oraz administracji SaaS-Db.

ROZLICZENIE

SaaS-Terminal: per nazwany użytkownik. **SaaS-Db / Enova365Web:** per instancja serwera zgodnie z wersją.

PROFIL KLIENTA

Firmy handlowe, biura rachunkowe — prosta struktura IT oparta na jednym/dwóch systemach branżowych, bez kompetencji infrastrukturowych, z potrzebą elastycznego dostępu z dowolnego miejsca.

PODZIAŁ ODPOWIEDZIALNOŚCI

Enteo Cloudpoint: pełne zarządzanie usługami SaaS do poziomu systemu i platformy, utrzymanie serwerów, backupów, bezpieczeństwa i dostępności. **Klient:** instalacja aplikacji na terminalu, konfiguracja merytoryczna Enova365 i konwersja bazy przy aktualizacji, dane oraz wymagania biznesowe.

***** Usługa zawiera licencje oprogramowania Microsoft udostępniane w ramach programu Microsoft SPLA — warunki na stronie 14.
******* Usługa wykorzystuje technologię Cloudflare (DNS / CDN / WAF) — warunki na stronie 16.

enteo
CLOUDPOINT

04

KATEGORIA USŁUG · SECAAS

Bezpieczeństwo

Security as a Service — usługi bezpieczeństwa Enteo Cloudpoint: ochrona danych, ochrona urządzeń, ochrona aplikacji webowych, logowanie zdarzeń i bezpieczny dostęp.

OCHRONA DANYCH

BaaS · DRaaS

OCHRONA WWW

C-WAF · C-CDN

DOSTĘP I LOGI

C-VPN · C-LOG

Oparte o tenant Acronis Cyber Cloud w polskim centrum danych oraz technologię Cloudflare

BaaS / DRaaS**

BACKUP & DISASTER RECOVERY AS A SERVICE

OCHRONA DANYCH — ACRONIS CYBER CLOUD

Kopie zapasowe i odtwarzanie w polskim centrum danych

BaaS i DRaaS bazują na udostępnianym przez Enteo Cloudpoint tenancie **Acronis Cyber Cloud**, działającym w centrum danych na terenie Polski. Usługa chroni środowiska fizyczne, wirtualne, chmurowe oraz Microsoft 365, z rozliczeniem według zużycia lub per obciążenie (workload) i storage.

BaaS zapewnia kopie zapasowe z harmonogramem definiowanym w portalu, ochroną przed ransomware i odtwarzaniem na żądanie. **DRaaS** rozszerza ochronę o replikację środowisk i failover do zapasowej lokalizacji w chmurze Enteo Cloudpoint, zgodnie z parametrami RPO/RTO.

> W modelach IaaS / PaaS / SaaS backup i DR są opcją wbudowaną w usługę i obsługiwaną z naszego portalu. BaaS / DRaaS to usługi samodzielne — tenant Acronis udostępniany bezpośrednio Klientowi.

MODEL ŚWIADCZENIA

Tenant zarządzany przez Klienta

Klient otrzymuje dostęp do własnego tenanta i może samodzielnie konfigurować plany ochrony, a Enteo Tech świadczy wsparcie.

Tenant bez dostępu Enteo

Opcjonalnie tworzymy tenant bez naszego dostępu — wsparcie jest wówczas ograniczone.

Zarządzanie w ramach usług Tech

Możemy też zarządzać usługami w ramach enteo Technologie — zakres opisują wtedy usługi Tech.

SZCZEGÓŁOWY PODZIAŁ ODPOWIEDZIALNOŚCI

Wyłączna odpowiedzialność techniczna Enteo	Odpowiedzialność Klienta
• Udostępnienie i utrzymanie tenanta Acronis w centrum danych w Polsce • Dostarczenie wymaganych licencji i funkcjonalności • Wsparcie techniczne w zakresie wynikającym z wybranego modelu • Opcjonalnie: pełna konfiguracja i zarządzanie planami (w ramach usług Tech)	• Samodzielna konfiguracja planów ochrony i harmonogramów (model self-service) • Zapewnienie warunków technicznych chronionych systemów i łączności • Definiowanie wymagań RPO/RTO i testowanie odtwarzania • Dane oraz decyzje o zakresie chronionych zasobów

Udostępnienie funkcjonalności ochrony danych nie jest gwarancją odtworzenia wszystkich danych ani parametrów RPO/RTO, o ile nie zagwarantowano ich w Umowie.

** Usługa wykorzystuje oprogramowanie i usługi Acronis — warunki na stronie 15.

EDR · RMM · Email Security**

OCHRONA URZĄDZEŃ KOŃCOWYCH

EDR z antywirusem oraz zdalne zarządzanie

W ramach tenanta Acronis Cyber Cloud dostępne są funkcjonalności bezpieczeństwa i zarządzania urządzeniami, wykorzystywane również w usługach enteo Technologie (T-SUPPORT-USER, T-SUPPORT-SECURITY-USER, T-SUPPORT-SERVER).

EDR + AV

- Ochrona klasy Endpoint Detection and Response z wbudowanym antywirusem
- Wykrywanie, analiza i blokowanie zagrożeń, ochrona przed ransomware
- Reagowanie na incydenty i izolacja zagrożonych urządzeń

RMM — zdalne zarządzanie

- Zdalne monitorowanie i zarządzanie stacjami i serwerami
- Inwentaryzacja, zarządzanie aktualizacjami i konfiguracją
- Automatyzacja zadań administracyjnych

OCHRONA POCZTY

Email Security oparte o Perception Point

- Zaawansowana ochrona poczty elektronicznej (Acronis Advanced Email Security)
- Ograniczanie zagrożeń: phishing, złośliwe oprogramowanie, niebezpieczne załączniki i odnośniki
- Technologia dostarczana przez Perception Point Ltd.

> Mechanizmy ochrony poczty ograniczają zagrożenia, lecz nie gwarantują wykrycia lub zablokowania wszystkich niepożądanych wiadomości ani zagrożeń.

ROZLICZENIE

Rozliczenie per urządzenie / skrzynkę zgodnie z wybranymi funkcjonalnościami. Komponenty EDR/AV i RMM są wymagane w ramach usług Tech i rozliczane oddzielnie per urządzenie.

ZARZĄDZANIE

Dostępne w modelu self-service (tenant Klienta) lub jako usługa zarządzana w ramach enteo Technologie.

** Usługa wykorzystuje oprogramowanie i usługi Acronis — warunki na stronie 15.

C-WAF / C-CDN***

OCHRONA APLIKACJI WEBOWYCH — CLOUDFLARE

WAF i CDN
w całości wbudowane w portal

Usługi ochrony aplikacji webowych oparte są o technologię **Cloudflare** i w całości obsługiwane z portalu Enteo Cloudpoint. Cloudflare działa jako reverse proxy: filtruje ruch HTTP/HTTPS, buforuje treści w globalnej sieci CDN, terminuje TLS i ukrywa adres serwera źródłowego.

C-CDN

- Dystrybucja i buforowanie treści w globalnej sieci brzegowej
- Przyspieszenie ładowania i odciążenie serwera źródłowego
- Terminacja TLS i ochrona przed atakami wolumetrycznymi

C-WAF-BASE

- Publikacja rekordu tunelem lub przez proxy w portalu, w naszej domenie **cloudpoint.pl**
- Filtrowanie ruchu i ochrona aplikacji regułami WAF
- Bez konieczności przenoszenia domeny Klienta

C-WAF-ADVANCED

- Publikacja w domenie Klienta (jak wyżej, we własnej domenie)
- Pełna kontrola reguł i polityk WAF dla aplikacji Klienta

CHARAKTERYSTYKA

Wszystko
z poziomu portalu

Konfiguracja DNS, CDN i reguł WAF odbywa się w portalu Enteo Cloudpoint. W modelu tunelu/proxy ruch kierowany jest przez sieć Cloudflare, bez publikowania adresu serwera źródłowego w Internecie.

> Mechanizmy WAF ograniczają zagrożenia, lecz nie gwarantują wykrycia i zablokowania wszystkich zagrożeń. Usługa nie zastępuje obowiązku utrzymywania bezpieczeństwa aplikacji i infrastruktury źródłowej.

ROZLICZENIE

C-CDN, **C-WAF-BASE** i **C-WAF-ADVANCED** rozliczane zgodnie z wybraną opcją i konfiguracją. Usługa WAF/CDN Cloudflare jest domyślnie wbudowana w usługę SaaS-Enova365.

PROFIL KLIENTA

Organizacje publikujące aplikacje i serwisy webowe, które chcą przyspieszyć ich działanie oraz zabezpieczyć je bez budowania własnej infrastruktury ochronnej.

*** Usługa wykorzystuje technologię Cloudflare (DNS / CDN / WAF) — warunki na stronie 16.

C-LOG / T-LOG · C-VPN

CENTRALNE GROMADZENIE LOGÓW

C-LOG i T-LOG
logi w naszym systemie

Usługa centralnego gromadzenia logów zdarzeń, utrzymywanych w systemie Enteo Cloudpoint. Rozliczana per endpoint oraz ilość storage.

- **C-LOG** — dla systemów w modelu PaaS Cloudpoint
- **T-LOG** — dla urządzeń w ramach usług enteo Technologie

Okresy retencji

- T-LOG: 7 dni (w pakiecie dla T-SUPPORT-SECURITY-DEVICE)
- Opcje rozszerzone: 1 miesiąc, 3 miesiące, 6 i 12 miesięcy

> Logi przechowywane są w systemie Enteo Cloudpoint. Zakres i okres retencji dobierany jest do potrzeb Klienta oraz wymogów zgodności.

BEZPIECZNY DOSTĘP ZDALNY

C-VPN
dostęp oparty o certyfikaty

C-VPN to VPN typu dial-up z uwierzytelnianiem opartym o certyfikaty. Służy do bezpiecznego dostępu do usług **PaaS** oraz do usługi **SaaS-Db**. Rozliczany per użytkownik.

- Uwierzytelnianie certyfikatami — bez haseł współdzielonych
- Dostęp do zasobów PaaS oraz administracji SaaS-Db
- Szyfrowany tunel inicjowany przez użytkownika (dial-up)

ROZLICZENIE

C-LOG / T-LOG: per endpoint + ilość storage, zależnie od okresu retencji. **C-VPN:** per użytkownik.

PROFIL KLIENTA

Organizacje wymagające centralizacji logów na potrzeby bezpieczeństwa i zgodności oraz bezpiecznego, imiennego dostępu zdalnego do zasobów chmurowych.

Licencje Microsoft

Warunki korzystania z oprogramowania Microsoft (Microsoft End User License Terms). Niniejsze warunki mają zastosowanie do wszystkich usług oznaczonych symbolem „*", w ramach których Enteo Tech Sp. z o.o. („Usługodawca") udostępnia Klientowi oprogramowanie Microsoft na podstawie programu Microsoft Services Provider License Agreement (SPLA). Akceptując Umowę oraz niniejszy dokument, Klient potwierdza, że zapoznał się z niniejszymi warunkami i zobowiązuje się do ich przestrzegania.

1. Zakres stosowania

Warunki obejmują wszystkie usługi oznaczone symbolem „*", w których Usługodawca udostępnia oprogramowanie Microsoft na podstawie programu SPLA.

2. Licencjonowanie oprogramowania

Oprogramowanie Microsoft udostępniane Klientowi pozostaje własnością Microsoft Corporation lub jej podmiotów powiązanych. Klient nie nabywa prawa własności ani odrębnej licencji. Klient uzyskuje wyłącznie niewyłączne, niezbywalne prawo do korzystania z oprogramowania w zakresie niezbędnym do korzystania z usług Usługodawcy.

3. Dozwolone korzystanie

Klient może korzystać z oprogramowania Microsoft wyłącznie w ramach usług świadczonych przez Usługodawcę, zgodnie z zawartą Umową oraz niniejszymi Warunkami. Jakiekolwiek wykorzystanie poza zakresem świadczonych usług jest niedozwolone.

4. Ograniczenia

Bez uprzedniej pisemnej zgody Usługodawcy oraz Microsoft Klient nie jest uprawniony do:

- kopiowania oprogramowania,
- odsprzedaży lub dalszego udostępniania oprogramowania osobom trzecim,
- udzielania sublicencji,
- wynajmowania, dzierżawy lub użyczania oprogramowania,
- modyfikowania oprogramowania,
- dekompilowania,
- odtwarzania kodu źródłowego (reverse engineering),
- obchodzenia zabezpieczeń technicznych.

Ograniczenia obowiązują w zakresie dopuszczalnym przez obowiązujące przepisy prawa.

5. Własność intelektualna

Wszelkie prawa autorskie, prawa własności intelektualnej oraz prawa do znaków towarowych związanych z oprogramowaniem Microsoft pozostają własnością Microsoft Corporation lub jej dostawców. Żadne postanowienie Umowy nie przenosi tych praw na Klienta.

6. Wsparcie techniczne

Wsparcie techniczne dotyczące usług świadczone jest przez Usługodawcę. Microsoft nie świadczy bezpośrednio na rzecz Klienta wsparcia technicznego ani usług serwisowych wynikających z korzystania z usług Usługodawcy.

7. Ograniczenie odpowiedzialności Microsoft

W zakresie dopuszczalnym przez prawo Microsoft nie ponosi wobec Klienta odpowiedzialności za szkody wynikające z korzystania z usług Usługodawcy. Za realizację usług wobec Klienta odpowiada wyłącznie Usługodawca.

8. Ograniczenia eksportowe

Klient zobowiązuje się do przestrzegania wszystkich obowiązujących przepisów dotyczących kontroli eksportu, sankcji gospodarczych oraz ograniczeń w zakresie eksportu technologii mających zastosowanie do udostępnionego oprogramowania Microsoft.

9. Naruszenie Warunków

Naruszenie niniejszych Warunków stanowi naruszenie Umowy z Usługodawcą. W przypadku naruszenia Usługodawca może — zgodnie z Umową oraz Regulaminem — zawiesić świadczenie usług, ograniczyć dostęp do oprogramowania lub rozwiązać Umowę ze skutkiem natychmiastowym.

10. Kontrola zgodności

Klient zobowiązuje się udzielać Usługodawcy informacji niezbędnych do wykazania zgodności korzystania z oprogramowania Microsoft z obowiązującymi warunkami licencyjnymi, jeżeli obowiązek taki wynika z umowy pomiędzy Usługodawcą a Microsoft. Microsoft jest uprawniony do egzekwowania wobec Klienta postanowień niniejszych Warunków w zakresie wynikającym z programu SPLA.

11. Postanowienia końcowe

Niniejsze Warunki stanowią integralną część dokumentu „Opis usług Cloudpoint" oraz Umowy. W zakresie nieuregulowanym stosuje się Umowę, Regulamin i przepisy prawa.

Warunki Acronis

ACRONIS END USER TERMS

Warunki korzystania z oprogramowania i usług Acronis (Acronis End User Terms). Mają zastosowanie do usług oznaczonych symbolem „**", w ramach których Enteo Tech Sp. z o.o. („Usługodawca") udostępnia Klientowi oprogramowanie lub funkcjonalności usług Acronis na podstawie uprawnień uzyskanych od producenta lub jego autoryzowanego dystrybutora.

1. Zakres stosowania

Warunki obejmują usługi świadczone z wykorzystaniem produktów: Acronis Cyber Protect Cloud, Acronis Disaster Recovery (Advanced Disaster Recovery) oraz Acronis Advanced Email Security. Warunki nie obejmują pozostałych produktów Acronis nieudostępnionych Klientowi.

2. Licencjonowanie oprogramowania

Oprogramowanie i usługi Acronis pozostają własnością Acronis International GmbH, jej podmiotów powiązanych lub licencjodawców. Klient uzyskuje ograniczone, niewyłączne i niezbywalne prawo do korzystania w zakresie niezbędnym do korzystania z usług Usługodawcy. Korzystanie podlega warunkom Acronis EULA.

3. Dozwolone korzystanie

Klient może korzystać z oprogramowania i usług Acronis wyłącznie w ramach usług Usługodawcy, zgodnie z Umową, dokumentacją i warunkami licencyjnymi. Wykorzystanie poza zakresem usług jest niedozwolone, chyba że Klient posiada odrębne uprawnienia licencyjne.

4. Ograniczenia

Bez zgody uprawnionego podmiotu Klient nie jest uprawniony do:

- kopiowania lub rozpowszechniania oprogramowania poza zakresem licencji,
- odsprzedaży, sublicencjonowania lub udostępniania osobom trzecim,
- wynajmowania, dzierżawy lub użyczania oprogramowania,
- modyfikowania lub tworzenia opracowań oprogramowania,
- dekompilowania lub odtwarzania kodu źródłowego,
- obchodzenia zabezpieczeń technicznych i mechanizmów licencyjnych,
- wykorzystywania w sposób naruszający prawa producenta lub bezpieczeństwo usług.

5. Własność intelektualna

Prawa autorskie, własności intelektualnej oraz do znaków towarowych związanych z Acronis pozostają własnością Acronis lub podmiotów uprawnionych. Żadne postanowienie nie przenosi tych praw na Klienta.

6. Korzystanie z usług ochrony danych

Usługi Cyber Protect Cloud i Disaster Recovery służą ochronie danych i wspomaganiu ich odzyskiwania zgodnie z wykupionymi funkcjonalnościami. Klient zapewnia warunki techniczne po jego stronie. Udostępnienie funkcjonalności nie stanowi gwarancji odtworzenia wszystkich danych ani parametrów RPO/RTO, o ile nie zagwarantowano ich w Umowie.

7. Korzystanie z usług Email Security

Acronis Advanced Email Security wykorzystuje technologie Perception Point Ltd.; korzystanie podlega również warunkom tego dostawcy. Mechanizmy ochrony poczty nie gwarantują wykrycia lub zablokowania wszystkich zagrożeń.

8. Ochrona danych osobowych

Dane osobowe mogą być przetwarzane przez Acronis i dostawców technologii w zakresie świadczenia i zabezpieczenia usług. Zasady określa Acronis Customer Privacy Statement. Warunki nie zastępują umowy powierzenia.

9. Wsparcie techniczne

Wsparcie świadczy Usługodawca. Acronis nie jest stroną Umowy między Klientem a Usługodawcą. Usługodawca może korzystać ze wsparcia producenta lub dystrybutora.

10. Ograniczenie odpowiedzialności producenta

Odpowiedzialność Acronis i dostawców technologii określają ich warunki licencyjne i warunki świadczenia usług. Za realizację Umowy wobec Klienta odpowiada Usługodawca.

11. Ograniczenia eksportowe

Klient przestrzega przepisów o kontroli eksportu, sankcjach i ograniczeniach udostępniania technologii mających zastosowanie do oprogramowania i usług Acronis.

12. Naruszenie Warunków

Naruszenie Warunków stanowi naruszenie Umowy. Usługodawca może zawiesić usługi, ograniczyć dostęp lub rozwiązać Umowę zgodnie z Umową i Regulaminem.

13. Kontrola zgodności

Klient udziela informacji niezbędnych do wykazania zgodności z warunkami licencyjnymi (zakres wykorzystania licencji, liczba chronionych zasobów).

14. Warunki producenta

Korzystanie podlega również warunkom producenta: Acronis EULA (acronis.com/en/support/eula/), Acronis Platform Terms and Conditions oraz Acronis Customer Privacy Statement.

15. Postanowienia końcowe

Warunki stanowią integralną część dokumentu „Opis usług Cloudpoint" oraz Umowy. Warunki nie zastępują warunków licencyjnych producenta ani umów o przetwarzanie danych osobowych.

enteo CLOUDPOINT

Warunki Cloudflare

DNS · CDN · WAF — TECHNOLOGIA CLOUDFLARE

Warunki korzystania z usług DNS, CDN i WAF opartych na technologii Cloudflare. Mają zastosowanie do usług oznaczonych symbolem „***", w ramach których Enteo Tech Sp. z o.o. („Usługodawca") świadczy na rzecz Klienta usługi DNS, CDN oraz WAF z wykorzystaniem infrastruktury i technologii Cloudflare („Dostawca Technologii").

1. Zakres stosowania

Warunki obejmują usługi świadczone z wykorzystaniem funkcjonalności: **DNS** (obsługa i zarządzanie strefami DNS), **CDN** (dystrybucja i buforowanie treści) oraz **WAF** (analiza i filtrowanie ruchu HTTP/HTTPS oraz ochrona aplikacji). Warunki nie obejmują innych produktów Cloudflare nieudostępnionych Klientowi.

2. Zasady świadczenia i udostępniania

Usługi świadczone są z wykorzystaniem infrastruktury Cloudflare, w ramach konta administracyjnego zarządzanego przez Usługodawcę. Usługodawca może obsługiwać w ramach wspólnego konta domeny, strefy DNS i usługi wielu Klientów, z zachowaniem logicznej separacji konfiguracji. Klient nie uzyskuje bezpośredniego dostępu do konta Cloudflare Usługodawcy, chyba że Umowa stanowi inaczej. Korzystanie nie oznacza nabycia licencji ani nawiązania bezpośredniego stosunku umownego z Cloudflare.

3. Dozwolone korzystanie

Klient korzysta z usług zgodnie z ich przeznaczeniem, Umową, dokumentacją i prawem, wyłącznie w odniesieniu do domen, aplikacji i zasobów, do których posiada prawa lub upoważnienia.

4. Ograniczenia

Bez zgody uprawnionego podmiotu Klient nie jest uprawniony do:

- odsprzedaży, sublicencjonowania lub udostępniania usług poza zakresem Umowy,
- obchodzenia ograniczeń technicznych, zabezpieczeń lub kontroli dostępu,
- wykorzystywania usług do działań niezgodnych z prawem,
- celowego generowania ruchu zakłócającego infrastrukturę Cloudflare lub innych użytkowników,
- nieautoryzowanego testowania lub naruszania bezpieczeństwa infrastruktury,
- naruszania limitów technicznych lub zasad dopuszczalnego użytkowania.

5. Własność intelektualna

Prawa związane z platformą Cloudflare pozostają własnością Cloudflare lub podmiotów uprawnionych. Prawa Klienta do jego domen, treści, aplikacji i danych pozostają nienaruszone.

6. Usługi DNS

Usługa DNS umożliwia obsługę i publikację rekordów DNS dla domen objętych usługą. Klient odpowiada za prawa do domen i prawidłowe dane konfiguracyjne. Zmiany mogą wymagać czasu na propagację. Usługa nie obejmuje rejestracji ani odnawiania domen, chyba że Umowa stanowi inaczej.

7. Usługi CDN

Usługa CDN umożliwia dystrybucję i buforowanie treści z wykorzystaniem infrastruktury Cloudflare. Klient zapewnia prawa do treści. Usługodawca nie gwarantuje buforowania wszystkich treści ani dostarczania z najbliższego węzła. Usługa nie zastępuje kopii zapasowych ani archiwizacji.

8. Usługi WAF

Usługa WAF ogranicza zagrożenia w ruchu HTTP/HTTPS przez analizę i filtrowanie żądań (blokowanie, ograniczanie, weryfikowanie ruchu). Klient przyjmuje do wiadomości, że WAF nie gwarantuje wykrycia wszystkich zagrożeń, prawidłowy ruch może zostać błędnie zakwalifikowany, a skuteczność zależy od konfiguracji i charakteru zagrożeń. Usługa nie zastępuje obowiązku utrzymywania bezpieczeństwa aplikacji, systemów i infrastruktury źródłowej.

9. Ochrona danych osobowych

Dane techniczne i dane o ruchu (adresy IP, informacje o żądaniach HTTP/HTTPS, zdarzeniach bezpieczeństwa) mogą być przetwarzane przez Cloudflare w zakresie realizacji usług, z wykorzystaniem rozproszonej geograficznie infrastruktury. Klient pozostaje odpowiedzialny za zgodność przetwarzania we własnych aplikacjach. Warunki nie zastępują umowy powierzenia.

10. Wsparcie techniczne

Wsparcie świadczy Usługodawca. Cloudflare nie jest stroną Umowy między Klientem a Usługodawcą.

11. Dostępność i ograniczenia techniczne

Dostępność zależy od infrastruktury Cloudflare i łączności. Usługodawca nie gwarantuje nieprzerwanego działania infrastruktury ani całkowitej eliminacji zagrożeń. Parametry SLA określa Umowa.

12. Ograniczenie odpowiedzialności Dostawcy

Odpowiedzialność Cloudflare określają właściwe warunki świadczenia usług Dostawcy. Za realizację zobowiązań z Umowy odpowiada Usługodawca.

13. Ograniczenia eksportowe i zgodność

Klient przestrzega przepisów o kontroli eksportu, sankcjach i ograniczeniach korzystania z technologii Cloudflare.

14. Naruszenie Warunków

Naruszenie Warunków stanowi naruszenie Umowy. Usługodawca może ograniczyć dostęp, zawiesić usługi lub rozwiązać Umowę zgodnie z Umową i Regulaminem.

15. Warunki Dostawcy Technologii

Zastosowanie mają: Terms of Service (cloudflare.com/terms/), Service-Specific Terms, Acceptable Use Policy, Privacy Policy oraz Data Processing Addendum. Wskazanie tych dokumentów nie czyni Klienta stroną umowy między Usługodawcą a Cloudflare.

16. Postanowienia końcowe

Warunki stanowią integralną część dokumentu „Opis usług Cloudpoint" oraz Umowy. Warunki nie zastępują warunków Dostawcy Technologii ani umów o przetwarzanie danych osobowych.

enteo
CLOUDPOINT

Dziękujemy za uwagę!

Enteo Tech Sp. z o.o.

www.enteo.pl

dział handlowy:
dh@cloudpoint.pl

Wersja dokumentu: 31.08.2026