# Europejskie przepisy dotyczące cyberbezpieczeństwa NIS2

**Bart Salaets**
EMEA Field CTO

# Wprowadzenie do dyrektywy NIS 2

Poprawa cyberbezpieczeństwa UE


- **Cel dyrektywy NIS 2:** zwiększenie bezpieczeństwa cybernetycznego UE poprzez przeciwdziałanie coraz bardziej wyrafinowanym i częstym zagrożeniom cybernetycznym.
- **Kontekst:** Reakcja na eskalację ataków cybernetycznych na usługi podstawowe (opieka zdrowotna, finanse, energetyka, transport).
- **Ograniczenia pierwotnej dyrektywy w sprawie bezpieczeństwa sieci i informacji**: Ograniczony zakres i zróżnicowane wdrażanie w poszczególnych państwach członkowskich UE.
- **Kluczowe cechy dyrektywy NIS 2:**
  - Rozszerzony zakres regulacyjny w celu objęcia większej liczby sektorów i usług cyfrowych.
  - Obowiązkowe zarządzanie ryzykiem i zgłaszanie incydentów dla administracji publicznej oraz średnich i dużych podmiotów w sektorach krytycznych.
- https://www.nis-2-directive.com/
- https://nis2directive.eu/

# Dyrektywa NIS 2 – cele i zastosowanie

**GŁÓWNE CELE**

Zobowiązanie rządów krajowych do zwrócenia należytej uwagi na cyberbezpieczeństwo.

Zacieśnienie europejskiej współpracy między organami ds. cyberbezpieczeństwa.

Zobowiązanie głównych operatorów w kluczowych branżach naszego społeczeństwa do podejmowania środków bezpieczeństwa i zgłaszania incydentów.

**DOTYCZY PODMIOTÓW W SEKTORACH O WYSOKIM ZNACZENIU KRYTYCZNYM**

Duży podmiot definiuje się jako przedsiębiorstwo zatrudniające minimum 250 pracowników lub którego roczny obrót wynosi co najmniej 50 mln euro, lub roczna suma bilansowa wynosi więcej niż 43 mln euro.

Średnie przedsiębiorstwo definiuje się jako przedsiębiorstwo zatrudniające od 50 pracowników lub o rocznym obrocie (lub sumie bilansowej) wynoszącym minimum10 mln euro.

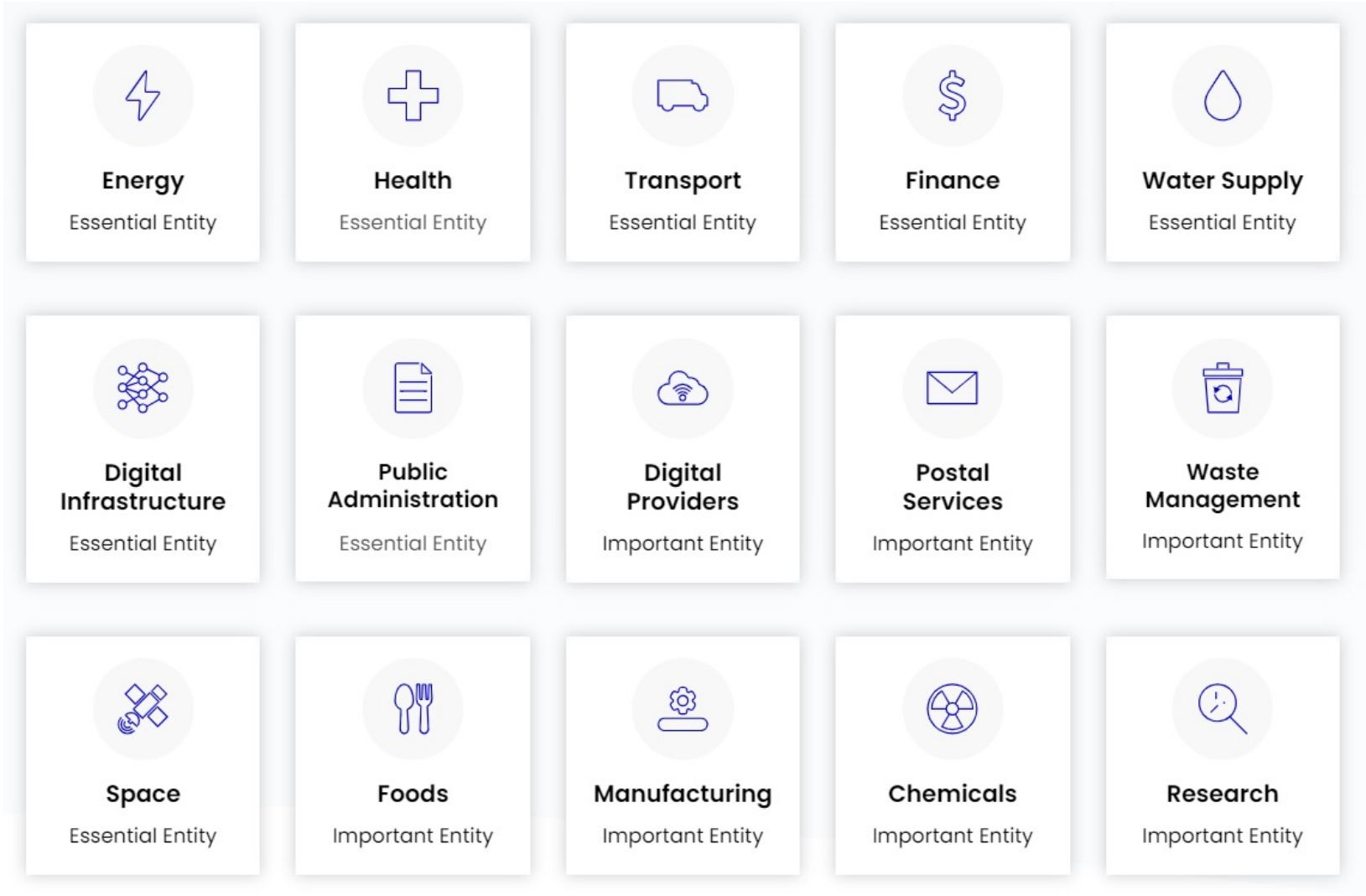
Szacuje się, że NIS 2 dotknie 160 000 firm.

**TERMIN WDROŻENIA**

17 października 2024 r

# NIS 2 – Sektory krytyczne podzielone na dwie listy

## Podmioty niezbędne i ważne



# NIS 2 – Środki zarządzania ryzykiem w cyberprzestrzeni

| | | | | |
|---|---|---|---|---|
| **01** Polityki dotyczące bezpieczeństwa informacji i zarządzania ryzykiem | **02** Zarządzanie incydentami i ich raportowanie | **03** Ciągłość działania biznesu i odzyskiwanie po katastrofie | **04** Zarządzanie bezpieczeństwem dostawców zewnętrznych / łańcucha dostaw | **05** Bezpieczeństwo sieci i systemów informatycznych, nabywanie, rozwój i utrzymanie oraz zarządzanie podatnościami |
| **06** Wewnętrzny audyt bezpieczeństwa informacji | **07** Szkolenia i świadomość dotycząca cyberbezpieczeństwa | **08** Polityka dotycząca stosowania kryptografii | **09** Polityki dotyczące bezpieczeństwa zasobów ludzkich, dostępu i zarządzania zasobami | **10** Polityka dotycząca stosowania uwierzytelniania wieloskładnikowego |

# Twoje aplikacje : Rozszerzony obszar podatny na ataki

# Nowoczesne cyberbezpieczeństwo – Rozległy i złożony ekosystem

Podziel strukturę zarządzania ryzykiem na łatwe do zarządzania bloki

# Rozszerzający się krajobraz zagrożeń dla aplikacji

Odmowa usługi, ataki typu zero day, przejęcia kont, naruszenia API, ...

## Hackers Target New NATO Member Sweden with Surge of DDoS Attacks

Trends, Reports, Analysis • May 02, 2024 • Infosecurity Magazine

## TICKETMASTER CONFIRMS DATA BREACH IMPACTING 560 MILLION CUSTOMERS

2024

## Account takeover attacks - the number one threat?

83% of organizations have experienced at least one account takeover in the last year; security leaders lack confidence in their current defenses to protect against this threat.

Sunday, 9th June 2024 Posted 1 week ago in Tech & Trends by Phil Alsop

## T-Mobile Says Hackers Used API to Steal Data on 37 Million Accounts

disclosed another massive data breach affecting approximately 37 million customer accounts.

CYBERCRIME

## Millions of User Records Stolen From 65 Websites via SQL Injection Attacks

The ResumeLooters hackers compromise recruitment and retail websites using SQL injection and XSS attacks.

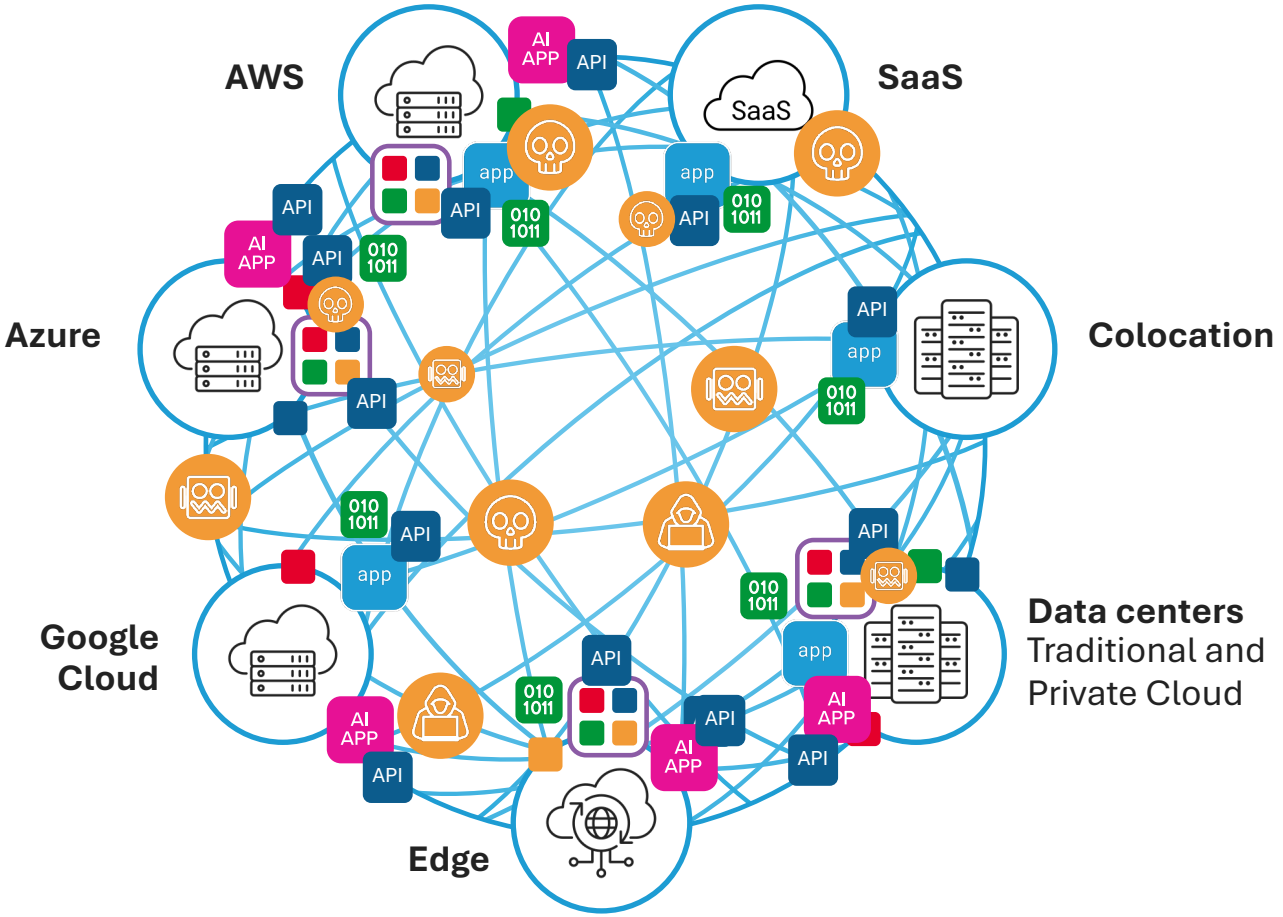
## The Log4j security flaw could impact the entire internet. Here's what you should know

By Jennifer Korn

4 minute read · Updated 9:33 AM EST, Thu December 16, 2021

# Ochrona aplikacji w środowisku wielochmurowym jest złożona

Zwiększa zapotrzebowanie na scentralizowane operacje i widoczność




- **Multicloud**
- **Microservices**
- **API**
- **AI**
- **Edge Computing**
- **Data Sovereignty**

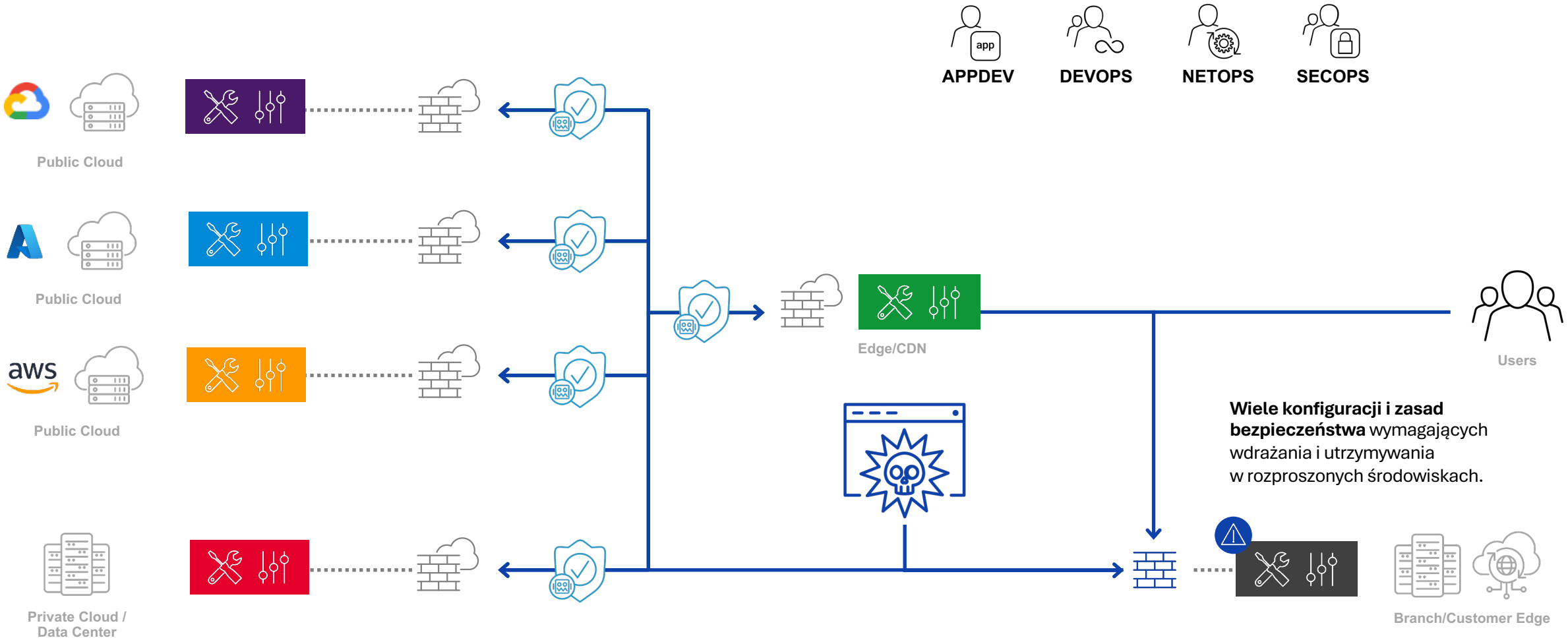
# Jak F5 może pomóc

# Zgodność z przepisami a ochrona

# Bezpieczeństwo aplikacji wielochmurowych — trudna droga

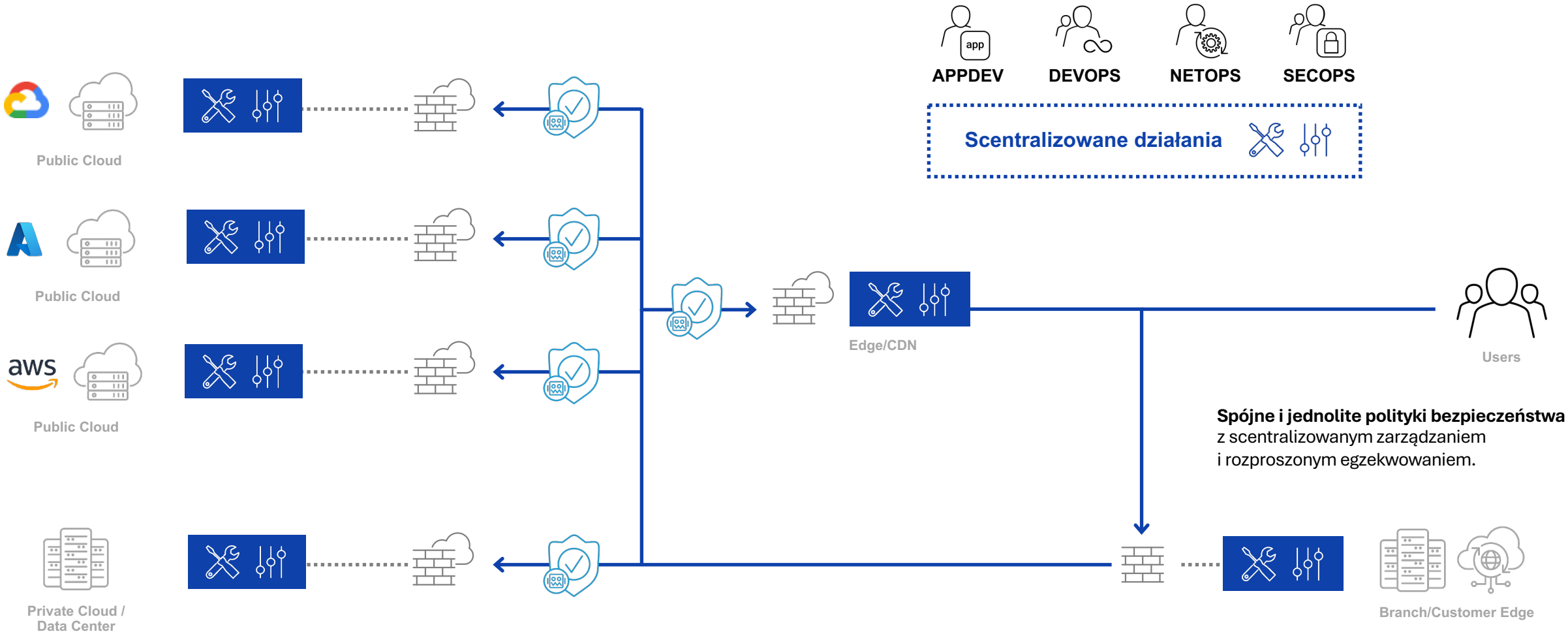
Różne produkty, odmienne platformy zarządzania, chaotyczne raportowanie




**Wiele konfiguracji i zasad bezpieczeństwa** wymagających wdrażania i utrzymywania w rozproszonych środowiskach.

**Zwiększone ryzyko zagrożeń** wynikające z błędnych konfiguracji i niespójnych polityk bezpieczeństwa

# F5 and multicloud – Consistent policies & Centralized reporting




**Spójne i jednolite polityki bezpieczeństwa** z scentralizowanym zarządzaniem i rozproszonym egzekwowaniem.

**Zmniejszona podatność na ataki** dzięki centralnemu punktowi konfiguracji i możliwości monitorowania

# Funkcje zabezpieczeń aplikacji internetowej F5 i interfejsu API

Rozwiązywanie problemów związanych z bezpieczeństwem aplikacji wielochmurowych

| | | |
|---|---|---|
| **Zapora sieciowa aplikacji** | **Identyfikacja oparta na podpisie** | **Identyfikacja zagrożeń i fałszywych alarmów oparta na analizie zachowania jednostek** |
| **Ograniczanie ataków DDoS** | **Atak Wolumetryczny DDoS na warstwie sieciowej (L4)** | **Atak DDoS na poziomie aplikacji (warstwa L7)** |
| **Obrona przed botami** | **Wykrywanie i łagodzenie skutków ataków botów: Identyfikacja automatycznych ataków, które mogą przeciążyć infrastrukturę cyfrową** | |
| **Ochrona API** | **Wykrywanie API i bezpieczeństwo: Prosta identyfikacja wszystkich punktów końcowych API przypisanych do aplikacji oraz wykrywanie anomalii.** | |

# Uzyskaj zgodność i wzmocnij stan zabezpieczeń aplikacji za pomocą F5

| Oferty F5 | NIS 2 | DORA |
|---|---|---|
| **Zarządzanie ryzykiem: ochrona portfolio aplikacji wielochmurowych przed najbardziej wyrafinowanymi atakami**<br>Zapora aplikacji internetowej w chmurze rozproszonej, łagodzenie ataków DDOS, zabezpieczenia przed botami i rozwiązania chroniące interfejsy API | X | X |
| **Zgłaszanie incydentów w przypadku ataków i naruszeń zabezpieczeń aplikacji**<br>Lepszy wgląd w ataki na aplikacje dzięki F5 Distributed Cloud Console | X | X |
| **Oceny podatności, skany i testy penetracyjne**<br>Skanowanie i testowanie aplikacji i interfejsów API pod kątem luk w zabezpieczeniach za pomocą F5 Rozproszone skanowanie aplikacji internetowych w chmurze | | X |
| **Odporność operacyjna dzięki środowisku wielochmurowemu**<br>Uproszczone dostarczanie i zabezpieczanie aplikacji w środowiskach wielochmurowych dzięki F5 Distributed Cloud, sieci wielochmurowej i WAAP | | X |
| **Kryptografia**<br>Silne możliwości SSL/TLS do szyfrowania end-to-end i mapy drogowej w kierunku postkwantowych kryptowalut dzięki rozwiązaniom F5 | | X |

# F5 może pomóc w osiągnięciu zgodności z NIS2

Rozwiązywanie problemów związanych z ograniczaniem ryzyka i raportowaniem zabezpieczeń aplikacji

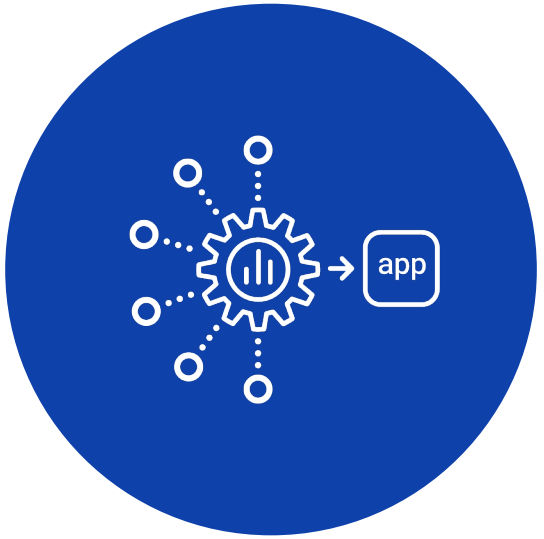
## WZMACNIANIE BEZPIECZEŃSTWA APLIKACJI

**Skonsolidowane rozwiązania WAAP oparte na sztucznej inteligencji i uczeniu maszynowym w bezpieczeństwie aplikacji internetowych i interfejsów API**

## UŁATWIENIE PRACY W CHMURZE

**Spójne zasady dostarczania aplikacji, bezpieczeństwa i sieci w centrach danych, chmurze i na brzegu sieci.**

## UPROSZCZENIE OPERACJI




**Scentralizowane operacje dla uproszczonej konfiguracji zasad i raportowania z bogatą analityką**