RAPORT BEST IN CLOUD 2024

COMPUTERWORLD

CZERWIEC 2024

BEST IN CLOUD

Chapter 2 dla chmury

KRZYSZTOF STUMPF

Cloud FinOps: co nowego i co dalej?

ERNEST ORŁOWSKI

ADAM PIECHURA

Chmura regulacji

SZYMON CIACH

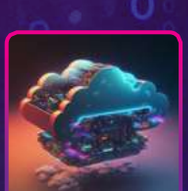
NORBERT LUTOWSKI

Huuuge Games: ponad 10 lat obecności w chmurze

MARCIN SAFRANOW

ExecutiveViewPoint: Zarządzanie ekspozycją w cyberbezpieczeństwie

BERNARD MONTEL



Chmura w 2024 roku

WIESŁAW PAWŁOWICZ

Wdrożenia chmurowe:
Polskie Sieci Elektroenergetyczne, PGZ Stocznia Wojenna, VULCAN

Produkty chmurowe w kategoriach:
Bezpieczna chmura, Dostawca chmury w modelu IaaS, Zabezpieczenie środowiska chmurowego, Produkt ERP/CRM, Najlepsza wydajność i integracja

WWW.COMPUTERWORLD.PL

Wstęp

Uczmy się na błędach poprzedników

Rodzime organizacje miały wystarczająco dużo czasu, aby czerpać wiedzę i doświadczenia chmury z bardziej dojrzałych rynków, głównie amerykańskiego. Dzisiaj popularyzacja chmury wkracza w drugi etap, który zachęca do poszukiwania efektywności. Firmy i instytucje publiczne muszą nauczyć się łączyć różne modele chmury, unikać uzależnienia od jednego dostawcy oraz proaktywnie zarządzać kosztami.

Na naszych oczach zmienia się także rynek dostawców, których portfolio obejmuje zestaw dobrze skrojonych produktów i usług chmurowych, spełniających specyficzne potrzeby klientów. Ich ogromna różnorodność, zaprezentowana na kolejnych stronach raportu i potwierdzona przykładami konkretnych wdrożeń, pozwala odkryć potencjał chmury. Firmy, które dopiero stawiają pierwsze kroki w chmurze, mogą uczyć się na błędach poprzedników.

Zapraszam do lektury.

Artur Pęczak
Redaktor prowadzący

Spis treści

COMPUTERWORLD

REDAKCJA
00-131 Warszawa, ul. Grzybowska 2/44
www.computerworld.pl

REDAKTOR NACZELNY
Grzegorz Stech

REDAKCJA
Ludwik Krakowiak
Daniel Olszewski
Grzegorz Kubera
Artur Pęczak
Janusz Chrustecki
Jan Mazurek

DYREKTOR DZIAŁU KONFERENCJI
Magdalena Szczodrońska

OPRACOWANIE GRAFICZNE, SKŁAD I ŁAMANIE
Małgorzata Majer-Tyc

BIURO REKLAMY
Daniel Malinowski +48 662 287 881
Anna Dubrawska +48 662 287 830
Elżbieta Olszewska +48 662 287 909
Agata Pranik +48 662 287 833
Monika Gałązka +48 662 287 871

Tekstów niezamówionych redakcja nie zwraca, zastrzegając sobie prawo ich skracania i opracowywania. Redakcja nie ponosi odpowiedzialności za treść reklam.

FOUNDRY
Formerly IDG Communications

WYDAWNICTWO
International Data Group Poland SA

PREZES ZARZĄDU
Jonas Triebel

KRZYSZTOF STUMPF
Head of Delivery Stream, Raiffeisen Tech

„Chapter 2", czyli kolejny krok w drodze do chmury

Firmy, skłonne do podążania za innowacjami technologicznymi, mamione są rozmaitymi nowinkami. Aktualne trendy napędza sztuczna inteligencja, ale historia sztucznego „hype" jest przebogata. Wystarczy wspomnieć o chmurze, która właśnie wkracza w drugi etap popularyzacji. Organizacje, które zwlekały z wprowadzeniem chmury, mogą od razu otworzyć „drugi rozdział", korzystając z dostępnych doświadczeń i kompetencji na rynku, ucząc się przy tym na błędach poprzedników.

Dostawcy technologii, jako zachętę do spróbowania i późniejszego zakupu, podsuwają nam nowinki w postaci bezpłatnych licencji, programów i innych promocyjnych pakietów. Sięganie po nowości stanowi ogromną wartość dla firm, bo buduje ich przewagę konkurencyjną oraz wspiera innowacje. Dzięki chmurze, która przecież jakiś czas temu również była trendem, firmy po raz pierwszy od długiego czasu mogły zająć się czymś innym, niż zapewnianiem wymaganej mocy obliczeniowej, przestrzeni na dane, backupem, wysoką dostępnością czy wsparciem dla rozwiązań Open Source. Zniknął problem z obsługą usług biurowych, takich jak systemy ERP i CRM czy poczta korporacyjna. W końcu pojawiła się całkowita transparentność kosztów, a działy IT przestały być „czarnymi dziurami" pochłaniającymi ogromne fundusze. Po pewnym czasie używania usług przyszedł czas na przemyślenia i rozdział drugi.

Chmura pozwoliła firmom zająć się czymś innym, niż zapewnianiem zasobów obliczeniowych, a działy IT przestały być „czarnymi dziurami" pochłaniającymi ogromne fundusze. Po pewnym czasie używania usług przyszedł czas na przemyślenia i rozdział drugi.

Chapter 2: bujać w obłokach bardzo, czy tylko trochę

Dostawcy chmurowi konkurują ze sobą kusząc klientów coraz bardziej łatwymi w użyciu i skalowalnymi usługami typu managed (zarządzanymi). To naturalna tendencja do rozszerzania oferty, budowania szerokiego zakresu szkoleń dla specjalistów i ścieżki certyfikacji dla nich.

Specjaliści IT bardzo chętnie sięgają po gotowe komponenty, używając ich w projektowanych rozwiązaniach. W ten sposób szybko się uczą i dopasowują do nich swoją ścieżkę rozwoju. Z kolei biznes najwięcej korzyści próbuje czerpać z rozwiązań chmurowych w modelu SaaS, bez czekania na efekty prac programistów. Firmy mogą włączać gotowe komponenty w procesy biznesowe lub samodzielnie budować aplikacje używając platform low-code.

W skomplikowanej sytuacji geopolitycznej zasadne staje się nakreślenie strategii wyjścia z chmury. Wśród zarządzających firmami pojawia się mocne wymaganie, aby z teoretycznych dokumentów kreślących tego typu scenariusze, tworzyć realne plany BCP.

W drodze na skróty musimy pamiętać, że w pewnym momencie stajemy się w pełni zależni od dostawcy chmury, a sam ten moment jest bardzo łatwo przegapić. Nie ma problemu, gdy kolejne granice zależności przekraczamy świadomie. Konsekwencje mogą być bolesne, gdy robimy to przypadkowo.

W skomplikowanej sytuacji geopolitycznej, zasadne staje się nakreślenie strategii wyjścia (exit strategy) z chmury. Wśród zarządzających firmami pojawia się mocne wymaganie, aby z teoretycznych dokumentów kreślących tego typu scenariusze tworzyć realne plany BCP.

Zadanie to wydaje się trudne, bowiem niektóre rozwiązania chmurowe SaaS są niedostępne w innych modelach, albo używają „pod spodem" zasobów jednego z trzech największych hiperskalerów. Wiele organizacji stawia sobie za cel mocną dywersyfikację pozyskiwanych zasobów w każdym obszarze zarządzania IT. Łatwo wyobrazić sobie scenariusz, w którym firma nakłada obowiązek, aby nawet najlepsze i najlepiej zintegrowane usługi oferowane przez dostawców mogły zostać zastąpione. Przykładem może być zamiana AWS KMS na wewnętrznie zarządzane repozytorium kluczy.

Sytuacja geopolityczna wymusza rewizję założeń, czy używanie jednego regionu dostawcy chmurowego jest wystarczające, aby zapewnić oczekiwany poziom nadmiarowości i zastępowalności. A może powinniśmy pomyśleć o dywersyfikacji między regionami, mimo dostępności systemów i danych w kilku Availability Zones.

Zmiana myślenia o zapewnieniu wysokiej dostępności nastąpiła wraz z szerszą popularyzacją chmury. Jeszcze kilka lat temu firmom wystarczało posiadanie zapasowego centrum danych w bliskiej odległości od tego głównego, a korzystanie z dwóch dostawców chmury wiązało się tylko z potrzebą dywersyfikacji dostawców (unikanie monopolu na usługi). Dzisiaj w kontekście strategicznym, aby rozproszyć geograficznie swoje systemy i dane, zasadne staje się używanie kilku regionów dostępności i sięganie po zasoby różnych dostawców chmury (multicloud).

Dla inżynierów chmurowych dywersyfikacja oznacza konieczność wejścia w inne chmury, a czasami nawet powrót, choć w nieco innej formie, do rozwiązań

lokalnych (on-premise). W tym miejscu pojawia się się lekki opór, a nawet zdziwienie, bo przecież jeszcze niedawno trendy w tym obszarze były zupełnie inne.

Głęboka znajomość nawet jednej chmury gwarantowała pewność zatrudnienia na rynku IT. To ogromne wyzwanie dla menedżerów, kiedy pokolenie Z chce działać tylko w najnowszych technologiach, pokolenie Y już ich używa i nie chce wracać do przestarzałych rozwiązań, a pokolenie X niebawem odejdzie z rynku, choć wszyscy życzymy sobie, aby zostało z nami jak najdłużej.

Porównywać jabłka do jabłek i gruszki do gruszek

Chmura zrewolucjonizowała podejście do kosztów IT przez promocję modelu „pay-as-you-go". W praktyce zmiana ta pozwoliła na przypisanie kosztu rozwiązania IT jako bezpośredniego kosztu danej linii biznesowej, a w końcu na policzenie P&L dla produktu bez karkołomnych kalkulacji współczynników, proporcji itd.

Podejście to wyeliminowało spekulacje na temat kogo i czego dotyczy dany koszt. Dzięki chmurze transparentność nakładów stała się tak duża, że osoby nietechniczne, np. w roli business ownerów, zyskały możliwość kontroli kosztów IT. Kiedy koszty wyszły ze „strefy cienia" pojawiła się nawet pokusa podważania zasadności niektórych kosztów przez osoby spoza działu IT.

Powszechnie wiadomo, że niektóre usługi chmurowe, np. AWS Cloudwatch czy Opensearch, są drogie. Wynika to z ich złożoności i skali zintegrowania z innymi rozwiązaniami. Naturalnym pomysłem w tej sytuacji staje się chęć rezygnacji z niektórych usług chmurowych na rzecz innych, tańszych, być może konkurencyjnych lub własnych. Prowadzi to do szeregu przeliczeń i porównywania bardzo klarownego kosztu usługi chmurowej z wielowymiarowymi modelami kosztów, gdzie wymiarami są ludzie, licencje lub ich brak (Open Source), amortyzacja i wiele innych. Na etapie analiz pojawiają się też koszty trudno policzalne, wynikające z kosztów aktualizacji czy integracji z innymi usługami chmurowymi. Zazwyczaj koszty te są zatem szacowane lub przypisywane odpowiednio wyliczonymi współczynnikami.

W rezultacie otrzymujemy zaledwie zestawienie realnych kosztów, z pewnymi przybliżeniami, a wynik tego porównania może prowadzić nas do błędnych decyzji. Trudno bowiem porównać namacalny koszt bezpośredni z kosztem alokowanym i podlegającym wpływowi wielu czynników, na które często nie mamy wpływu, albo wpływ ten jest ograniczony.

W kontekście strategicznym, aby rozproszyć geograficznie swoje systemy i dane, zasadne staje się używanie kilku regionów dostępności i sięganie po zasoby różnych dostawców chmury (multicloud).

Uczyć się na błędach (najlepiej cudzych)

Chapter 2 jest niczym innym jak kolejną fazą wdrożenia chmury w organizacji. Te, które przeszły przez chapter 1, na pewno popełniły kilka błędów i wiele się na nich nauczyły. To bezcenna wiedza, która będzie procentować. Jednocześnie firmy i instytucje publiczne, które zwlekały z wprowadzeniem chmury, mogą od razu otworzyć „drugi rozdział" korzystając z dostępnych doświadczeń i kompetencji na rynku, ucząc się przy tym na błędach poprzedników.

ERNEST ORŁOWSKI
Senior Manager
PwC Polska

ADAM PIECHURA
Specjalista Cloud FinOps
PwC Polska

Cloud FinOps: co nowego i co dalej?

SYSTEMATYCZNY WZROST KOSZTÓW CHMURY W OSTATNICH 2-3 LATACH WŚRÓD ORGANIZACJI, KTÓRE CORAZ SZERZEJ WYKORZYSTUJĄ CHMURĘ PUBLICZNĄ, SPOWODOWAŁ WYRAŹNE ZMIANY W PODEJŚCIU DO ZARZĄDZANIA WYDATKAMI W TYM OBSZARZE. WIODĄCĄ METODYKĄ PROAKTYWNEGO ZARZĄDZANIA KOSZTAMI CHMURY, BAZUJĄCĄ NA DOŚWIADCZENIACH INNYCH, STAŁ SIĘ FINOPS, CZĘSTO OKREŚLANY JAKO STWORZONY PRZEZ PRAKTYKÓW DLA PRAKTYKÓW.

Coraz częściej implementacja elementów FinOps planowana jest jako immanentna część strategii migracji do chmury obliczeniowej. Podejście to pozwala organizacjom od początku przygotować się na zmienny model kosztowy. W rozmowach z klientami coraz częściej pojawia się pojęcie „Cloud Smart", które zakłada łączenie potencjału technologicznego i biznesowego chmury publicznej wraz z zaplanowanym podejściem do efektywnego zarządzania nią, w tym z wykorzystaniem metodyki FinOps.

Dojrzałość FinOps w praktyce

FinOps definiuje trzy poziomy dojrzałości (ang. Maturity levels): Crawling (Pełzanie), Walking (Chodzenie) i Running (Bieganie). Poziom dojrzałości FinOps w firmach będących dużymi użytkownikami chmury publicznej w Polsce jest zróżnicowany, co odzwierciedla różne etapy wdrażania chmury i różne poziomy implementacji praktyk FinOps.

Większość firm korzystających z usług chmury publicznej zidentyfikowała już potrzebę wdrażania i zwiększania dojrzałości FinOps. W poszczególnych obszarach prowadzone są działania mające na celu podniesienie tej dojrzałości, które obejmują:

- wdrożenie narzędzi analitycznych - firmy inwestują w zaawansowane narzędzia, które umożliwiają monitorowanie i analizę kosztów związanych z korzystaniem z chmury. Narzędzia te pomagają w identyfikacji nieefektywności i optymalizacji wydatków.
- powołanie zespołów FinOps - tworzenie dedykowanych zespołów FinOps, które zajmują się zarządzaniem finansami w kontekście chmury. Zespoły te składają się z ekspertów IT, finansów i operacji, którzy współpracują nad optymalizacją kosztów i wydajności chmury.
- modyfikacja procesów - adaptacja i zmiana istniejących procesów biznesowych w celu lepszego zarządzania zasobami chmurowymi. Firmy wprowadzają nowe procedury i polityki, które promują oszczędność i efektywność.
- szkolenia i edukacja - inwestowanie w szkolenia dla pracowników, aby zrozumieli zasady i praktyki FinOps. Świadomość i wiedza na temat zarządzania kosztami chmury są kluczowe dla skutecznego wdrożenia FinOps.

- automatyzacja - wykorzystanie narzędzi automatyzujących procesy związane z zarządzaniem kosztami chmury. Automatyzacja pomaga w szybkim zidentyfikowaniu i reagowaniu na zmieniające się koszty, co jest szczególnie ważne na wyższych poziomach dojrzałości FinOps.

Wiele do zrobienia

Niestety, wspomniane działania często prowadzone są punktowo, co powoduje duże dysproporcje w poziomach dojrzałości FinOps w różnych obszarach. Przykładem mogą być klienci, którzy osiągnęli wysoki poziom transparentności kosztów chmury (ang. cloud cost transparency) i wdrożyli zaawansowane narzędzia analityczne do bieżącej analizy kosztów chmurowych, ale jednocześnie nie zoptymalizowali kosztów na poziomie zasobów chmurowych. Nie mają też strategii dla rezerwacji zasobów i w konsekwencji nie wykorzystują tej metody optymalizacji kosztowej.

Punktowe podejście prowadzi do sytuacji, w której organizacje nadal „przepalają" nawet kilkadziesiąt procent kosztów chmury publicznej, mimo że miesięczne faktury za usługi chmurowe sięgają sześciocyfrowych kwot. Jako PwC dostrzegamy typowe schematy i wzorce przyczynowo-skutkowe, które powodują marnotrawienie zasobów i kosztów chmury publicznej u klientów.

FinOps może w tym pomóc

Zwiększanie dojrzałości obszaru FinOps w organizacji to ciągły proces, a nie jednorazowe działanie. Wynika to z dwóch głównych powodów: rosnącej popularyzacji chmury i dynamicznego rozwoju metodyki FinOps. W miarę jak organizacje coraz bardziej polegają na chmurze, pojawiają się nowe wyzwania związane z zarządzaniem kosztami, które wymagają bieżącej optymalizacji.

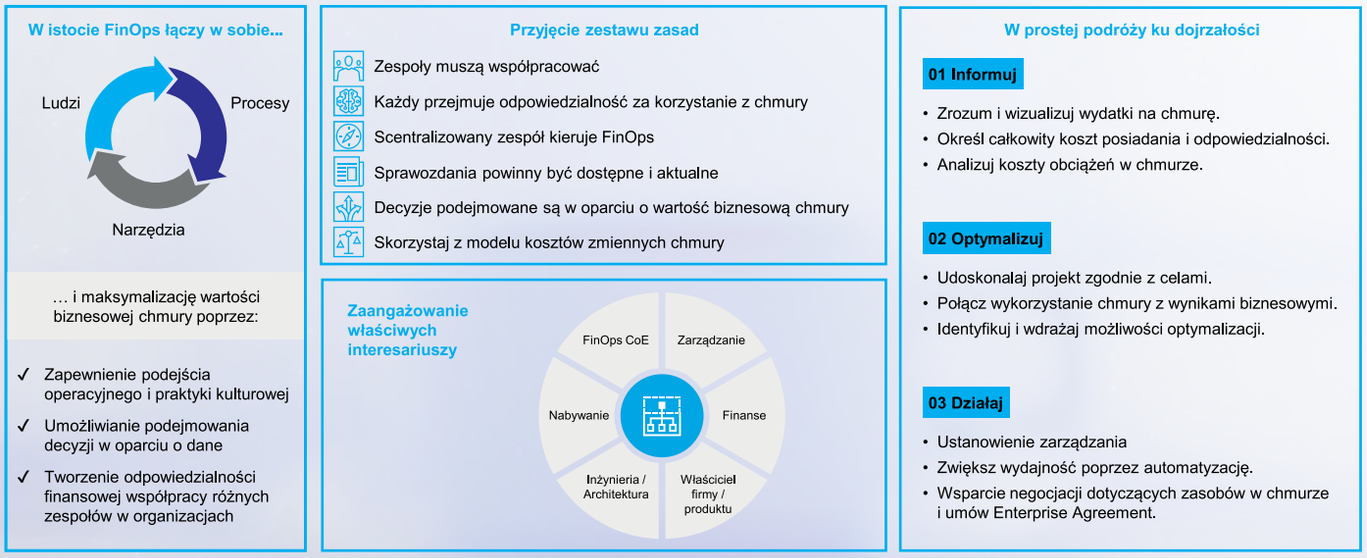
Stały rozwój FinOps wprowadza nowe narzędzia i strategie, które pomagają firmom lepiej kontrolować wydatki. Dzięki temu organizacje mogą skuteczniej zarządzać zasobami i optymalizować koszty, co jest kluczowe w kontekście rosnących wydatków na usługi chmurowe. Firmy, które systematycznie podnoszą dojrzałość FinOps, zyskują lepszą kontrolę nad budżetem IT i mogą efektywniej reagować na zmieniające się warunki rynkowe.

Nowości w FinOps

Jednym z najnowszych kamieni milowych rozwoju metodyki FinOps jest FOCUS, czyli schemat pozwalający w spójny sposób analizować i porównywać koszty cloud wielu dostawców (multicloud). Zgodnie z definicją, FOCUS (ang. The FinOps Cost and Usage Specification) to specyfikacja typu open-source, która definiuje jasne wymagania dla dostawców usług w chmurze w zakresie tworzenia spójnych zestawów danych dotyczących kosztów i wykorzystania. Wspierany przez FinOps Foundation, FOCUS ma na celu zmniejszenie złożoności dla praktyków FinOps, aby mogli oni podejmować decyzje oparte na danych i maksymalizować wartość biznesową chmury, jednocześnie sprawiając, że ich umiejętności są bardziej przenoszalne między chmurami, narzędziami i organizacjami.

Wzorzec	Powód
„Over-provisioning" zasobów w chmurze	• Brak precyzyjnego prognozowania i mentalność on-prem „na wszelki wypadek".
Niewykorzystane lub bezczynne zasoby chmury	• Środowiska programistyczne i testowe pozostają uruchomione, duże instancje są używane do małych zadań.
Osierocone zasoby w chmurze	• Wolumeny pamięci lub kopie danych pozostawione po wyłączeniu VM lub zakończeniu migracji do chmury opartej na odtwarzaniu kopii zapasowej.
Nieużywane/niewykorzystane instancje zarezerwowane	• Słabe prognozowanie: nieprawidłowe przewidywanie zapotrzebowania na zasoby. • Zmiana obciążeń: Obciążenia zmieniają się po zakupie wystąpień zarezerwowanych. Wdrażanie typów instancji innych niż zarezerwowane.
Nieefektywne rozwiązania pamięci masowej	• Brak optymalizacji warstw pamięci masowej (np. używanie dysków SSD do przechowywania danych, które można przechowywać na dyskach mniejszej wydajności), wykorzystywanie pamięci masowej o wysokiej wydajności w przypadku rzadko używanych danych.
Nieoptymalne typy instancji	• Instancje ogólnego przeznaczenia dla konkretnych potrzeb. • Niewłaściwa alokacja zasobów: instancje z niedopasowanym procesorem, pamięcią i pamięcią masową.
Nadmierna redundancja	• Nadmiernie ostrożna wysoka dostępność: replikacja danych w zbyt wielu regionach lub utrzymywanie zbyt wielu kopii zapasowych. • Przesada w zakresie odzyskiwania po awarii: Nadmierna konfiguracja odzyskiwania po awarii wykraczająca poza potrzeby biznesowe.

Wzorce, jakie PwC Polska obserwuje u różnych klientów w obszarze Cloud FinOps *Źródło: PwC Polska*



Wysokopoziomowe spojrzenie na podejście Cloud FinOps

Źródło: PwC Polska

Zespoły, specjaliści i analitycy FinOps będą mogli zgłaszać prośby o eksport danych kosztowych w schemacie FOCUS, co wyeliminuje potrzebę dalszej analizy i dekodowania danych dotyczących zużycia i stawek zasobów chmurowych.

Kolejnym trendem rozwoju FinOps będzie szersze wykorzystanie AI i ML do wsparcia w analizie ogromnej ilości danych i wychwytywania oraz wczesnej interpretacji anomalii kosztowych w obszarze cloud.

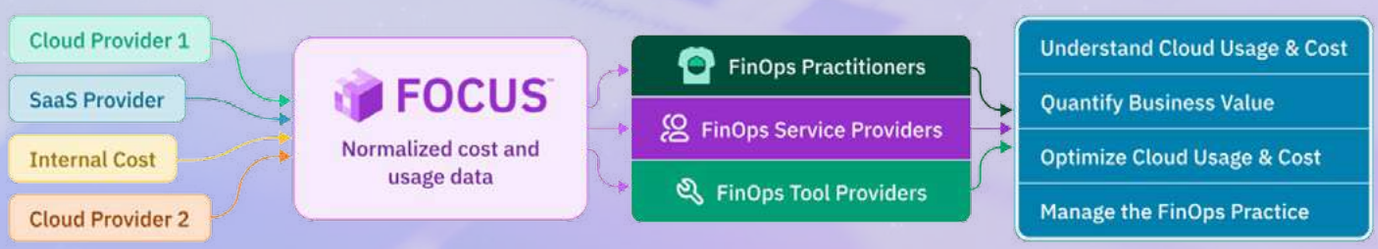
W kierunku kompleksowego zarządzania kosztami IT

Celem, do którego firmy powinny strategicznie dążyć w obszarze FinOps, jest wysoka dojrzałość pozwalająca adresować całe spektrum zagadnień FinOps niewielkim dedykowanym zespołem. W tym kontekście kluczowe staje się zatem szerokie wykorzystanie analityki danych, narzędzi wspierających oraz integracji i automatyzacji. Pozwoli to przedsiębiorstwom na dalsze skalowanie zasobów w chmurze, bez konieczności zwiększania składu osobowego w zespole FinOps.

FinOps pozwolił wielu organizacjom uzyskać transparentność kosztów i biznesową higienę proaktywnego zarządzania finansowego. Metodyka zauważona została na szczeblu zarządów firm, rozbudzając apetyt na zastosowanie podobnego podejścia do obszaru kosztów on-premises.

Dlatego kolejnym wyzwaniem dla wielu organizacji, po wdrożonym z sukcesem FinOps, będzie podjęcie kolejnej próby efektywnego zarządzania zasobami i kosztami IT w sposób kompleksowy. Odpowiedzią na to wyzwanie jest framework TBM (Technology Business Management). TBM oraz FinOps mają wspólny cel: zarządzanie wydatkami na technologię w sposób transparentny i zgodny z celami biznesowymi.

TBM obejmuje ogólną strategię, podczas gdy FinOps skupia się na kosztach związanych z chmurą. Obie te dziedziny są ważne dla efektywnego zarządzania technologią i finansami w dużych organizacjach IT.



Wizualizacja wartości dodanej jaką zapewnia FOCUS - uproszczenie danych kosztowych

Źródło: Flexera, Title: Flexera 2023 State of the Cloud Report, Publication date: 2023

Chmura regulacji

Trendy regulacyjne dla usług przetwarzania danych

SZYMON CIACH
Counsel w Osborne Clarke
NORBERT LUTOWSKI
Junior Associate w Osborne Clarke

Fot.: Freepik

Zastosowanie chmury w biznesie przestało być nowinką, a zaczęło być codziennością. Prawo, które zawsze podąża w pewnej odległości za rozwojem technicznym, wypracowało już swoją odpowiedź na tę technologię. Jej przejawem w Polsce jest przede wszystkim Komunikat Chmurowy UKNF - najbardziej znana regulacja dedykowana chmurze obliczeniowej. Usługi finansowe, obok sektora medycznego i publicznego, to obszar szczególnie uregulowany pod kątem ochrony danych, co przekłada się na liczne wymagania i ograniczenia w korzystaniu z chmury. Ta stała się obecnie ważną, ale jednak jedynie częścią prawnej układanki świata IT.

Szymon Ciach
Counsel w Osborne Clarke

Gdzie jesteśmy?

Niewątpliwie możemy zaobserwować, że regulowanie spraw powiązanych z technologiami informacyjnymi jest dziś na wysokim priorytecie ustawodawcy, zwłaszcza unijnego. W poczet „regulacji IT", czyli aktów prawnych poświęconych w istotnym zakresie technologiom informacyjnym, zaliczamy już kilkadziesiąt pozycji. Wiele z nich to produkty z ostatnich lat, choć niektóre wciąż są w toku prac legislacyjnych.

Przykładowe obszary tych regulacji dotyczą sektora finansowego, w którym regulowane są takie aspekty jak cyfrowa odporność operacyjna (rozporządzenie DORA), kryptoaktywa (rozporządzenie ds. rynków kryptoaktywów), bezpieczeństwo zarówno w sferze cybernetycznej (dyrektywa NIS2) i fizycznej (dyrektywa RCE), dane, a więc RODO oraz powstające regulacje dot. danych nieosobowych (rozporządzenie Data Act), platformy i usługi cyfrowe oraz sztuczna inteligencja. Dokładając do tego regulacje sektorowe dotyczące ochrony danych, możemy śmiało stwierdzić, że działalność w obszarze IT, a zwłaszcza świadczenie usług przetwarzania danych, staje się działalnością regulowaną. W natłoku zmian prawnych warto się przyjrzeć kluczowym trendom, jakie z nich wynikają.

W sektorze finansowym regulowane są takie aspekty jak cyfrowa odporność operacyjna, kryptoaktywa, bezpieczeństwo, dane, platformy i usługi cyfrowe oraz sztuczna inteligencja. Dokładając do tego regulacje sektorowe dotyczące ochrony danych, możemy śmiało stwierdzić, że działalność w obszarze IT, a zwłaszcza świadczenie usług przetwarzania danych, staje się działalnością regulowaną.

Dokąd idziemy?

Cyberbezpieczeństwo

Zabezpieczenie infrastruktury ICT oraz cyfrowych elementów produktów fizycznych stanowi jedno z centrów ostatniej aktywności legislacyjnej Unii Europejskiej. W zakresie sektora finansowego Komunikat Chmurowy zostanie w praktyce zastąpiony przez rozporządzenie DORA, czyli rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego. DORA, której centrum zainteresowania stanowi cyfrowa odporność operacyjna, określa m.in. nowe, wysokie standardy zawierania umów z dostawcami usług ICT, w tym chmurowych. Poza tym, dostawcy tych rozwiązań, będą musieli zaadaptować się do polityk zarządzania zewnętrznymi dostawcami usług ICT. Jedną z konsekwencji wprowadzenia DORA będzie w szczególności konieczność zapewnienia zaawansowanych rozwiązań bezpieczeństwa, które powinny być cyklicznie aktualizowane w ramach potrzeb i rozwoju technologicznego. Jednocześnie należy pamiętać, że DORA stanowi wyłącznie uszczegółowienie dyrektywy NIS 2, dedykowane tylko sektorowi finansowemu.

NIS 2 to skrótowa nazwa dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii. Diametralnie rozszerza ona zakres podmiotów zobowiązanych do posiadania systemu ochrony informacji, pierwotnie określony przez dyrektywę NIS 1. Jednymi

z głównych zmian są wymagany „bazowy poziom cyberbezpieczeństwa", związany z higieną cyfrową wewnątrz organizacji danego podmiotu oraz – ponownie - nowe zasady zarządzania dostawcami ICT. Pierwsza z powyższych przekłada się na obowiązkowe zwiększanie świadomości każdego pracownika i współpracownika wobec przyjętych rozwiązań, w tym funkcji związanych z bezpieczeństwem chmury. Natomiast nowe standardy zarządzania dostawcami ICT efektywnie rozszerzają potrzebę całościowego zwiększenia bezpieczeństwa rozwiązań chmurowych na produkty oferowane podmiotom regulowanym przez NIS 2. Oprócz tego, że nowe regulacje zawierają istotne sankcje za niestosowanie się do nich (kary administracyjne), znacząco zwiększają nadzór organów administracji nad dostawcami usług ICT, w tym dostawcami usług chmurowych.

NIS 2 diametralnie rozszerza zakres podmiotów zobowiązanych do posiadania systemu ochrony. Jednymi z głównych zmian są wymagany „bazowy poziom cyberbezpieczeństwa", związany z higieną cyfrową wewnątrz organizacji danego podmiotu oraz nowe zasady zarządzania dostawcami ICT.

Sztuczna inteligencja

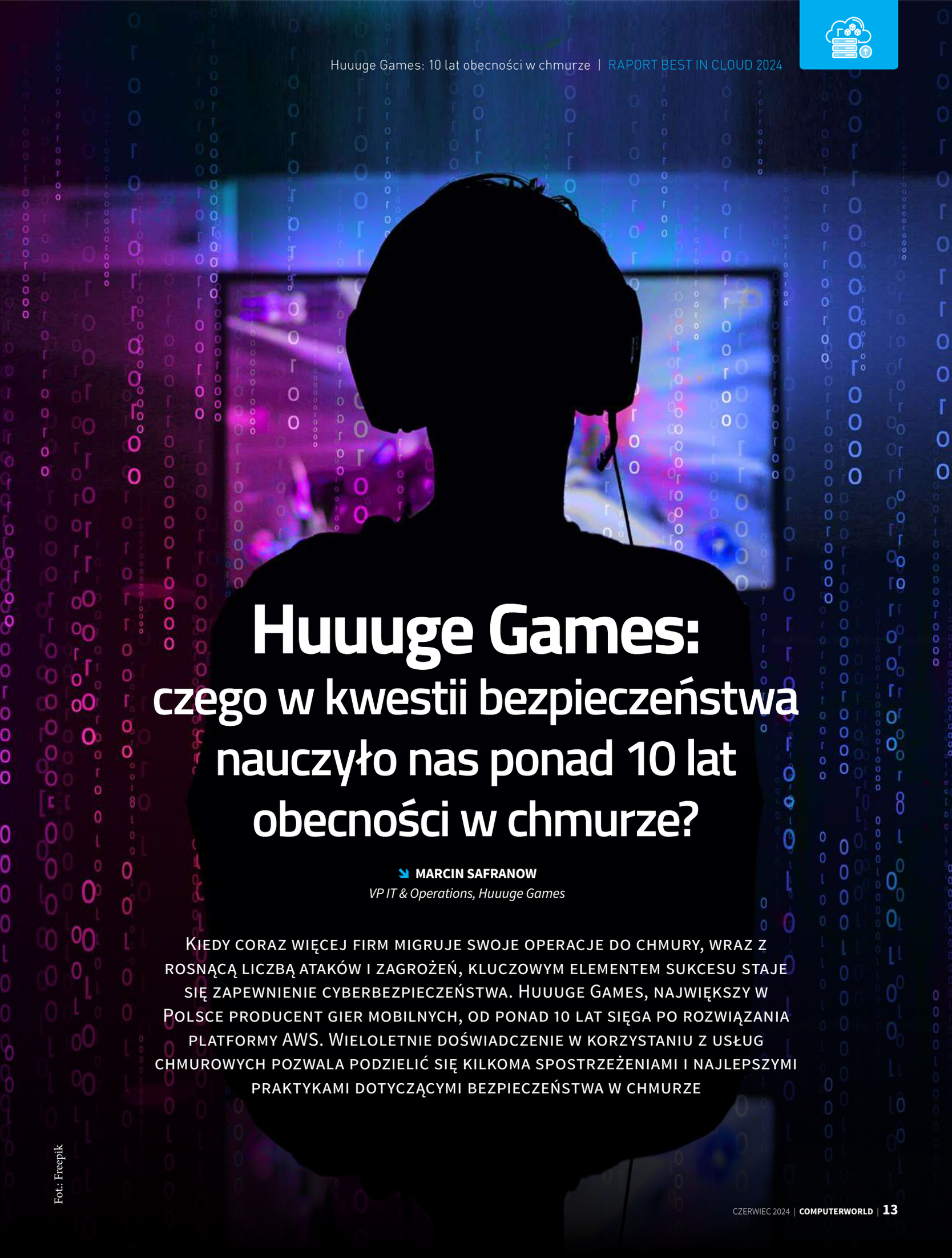
Rozpowszechnienie AI na wszystkie dziedziny życia, w tym przede wszystkim na gospodarkę, często określa się jako największą zmianę od czasów rewolucji przemysłowej. Nietrudno dostrzec wiele wyzwań wiążących się z jej rozwojem. Unia Europejska odpowiedziała na te wyzwania wydając tzw. „AI Act", czyli rozporządzenia ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji. Obowiązki wprowadzone przez to prawo niejednokrotnie będą wpływały na wykorzystanie chmury przez podmioty korzystające z lub tworzące AI. Dane przechowywane w chmurze, w tym przede wszystkim logi funkcjonowania rozwiązań uczenia maszynowego, czy zbiory danych krytyczne dla ich treningu, nabędą bardzo istotnego znaczenia, zwłaszcza w kontekście wymaganych procesów zarządzania danymi. Sam sposób dystrybucji AI, gdzie najpopularniejszym rozwiązaniem jest AIaaS, wiąże się z ryzykiem wobec danych przechowywanych w chmurze, czego świetnym przykładem jest zagadnienie ekstrakcji danych treningowych z dużych modeli językowych. Tym samym, bezpieczeństwo związane z samą chmurą staje się kluczowym aspektem jej zastosowania z punktu widzenia prawa i AI.

W polityce unijnej, a w ślad za nią w regulacjach, widoczne jest dążenie do budowania gospodarki opartej o dane. W tym celu identyfikowane są obszary gospodarki i grupy podmiotów, które gromadzą duże zasoby wartościowych danych oraz określane zasady dostępu dla tych danych.

Ekonomia danych

W polityce unijnej, a w ślad za nią w regulacjach, widoczne jest dążenie do budowania gospodarki opartej o dane. W tym celu identyfikowane są obszary gospodarki i grupy podmiotów, które gromadzą duże zasoby wartościowych danych. Opracowywane są zatem reguły ich współdzielenia. Zasady te określają kto i na jakich warunkach uprawniony jest do dostępu dla tych danych. Koncepcja ta została wypróbowana w sektorze bankowym, gdzie na gruncie dyrektywy PSD 2 umożliwiono innym podmiotom dostęp do wybranych danych bankowych, tzw. open banking. Koncepcja ta jest rozszerzana obecnie na kolejne branże sektora finansowego (projekt rozporządzenia FIDA) oraz na obszar Internetu rzeczy (Internet of Things, IoT). W tym zakresie dostawcy usług chmurowych powinni mieć „na radarze" w szczególności projekt rozporządzenia Data Act. Regulacja ta ustanowi prawo do danych nieosobowych, jakie będzie miał użytkownik urządzenia generującego dane, a także określi zasady na jakich producent takiego urządzenia będzie musiał udostępniać te dane innym podmiotom. Użytkownik będzie mógł, np. sprzedawać dane, jakie gromadzą na jego temat urządzenia za pośrednictwem marketplace'ów danych. W Data Act przewiduje się ponadto standardowe klauzule umowne dla umów na świadczenie usług chmurowych oraz przeciwdziałanie chmurowemu vendor lock-in. Dostawcy nie będą mogli kształtować swoich usług w sposób utrudniający klientowi przeniesienie się do innego dostawcy, co ma zapewniać lepszą interoperacyjność systemów IT w Unii.

W ślad za dynamicznie rozwijającymi się technologiami informacyjnymi tworzone są dotyczące ich regulacje. Mimo, że w praktyce trudno nadążyć na tymi zmianami, zawsze warto próbować to robić. Regulacje to nie tylko ryzyko kar i koszty. Rozumiejąc wpływ nadchodzących regulacji na organizację można określić nowe modele biznesowe i zbudować przewagi konkurencyjne na przyszłość.

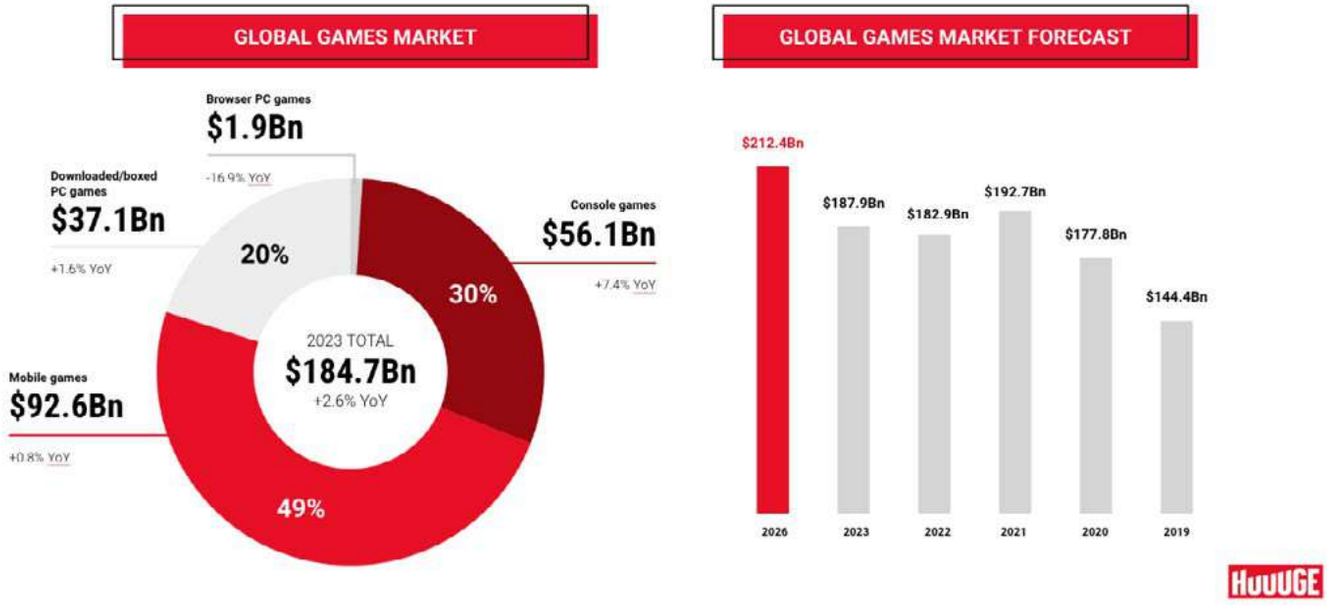


Huuuge Games: czego w kwestii bezpieczeństwa nauczyło nas ponad 10 lat obecności w chmurze?

MARCIN SAFRANOW
VP IT & Operations, Huuuge Games

Kiedy coraz więcej firm migruje swoje operacje do chmury, wraz z rosnącą liczbą ataków i zagrożeń, kluczowym elementem sukcesu staje się zapewnienie cyberbezpieczeństwa. Huuuge Games, największy w Polsce producent gier mobilnych, od ponad 10 lat sięga po rozwiązania platformy AWS. Wieloletnie doświadczenie w korzystaniu z usług chmurowych pozwala podzielić się kilkoma spostrzeżeniami i najlepszymi praktykami dotyczącymi bezpieczeństwa w chmurze

Fot.: Freepik



Huuuge Games działa na rynku gier mobilnych, który jest jednym z najszybciej rozwijających się segmentów rynku gier. Z prognoz wynika, że globalny rynek gier zbliża się do wartości 200 miliardów dolarów rocznie, a gry mobilne, z przychodami sięgającymi 92,6 miliardów dolarów w 2023 roku, stanowią obecnie jego największy segment. Ten dynamiczny wzrost popytu na gry mobilne wymaga od dostawców nie tylko zaawansowanej technologii, ale również solidnych zabezpieczeń, które chronią dane użytkowników oraz integralność systemów.

W gry Huuuge Games, głównie Huuuge Casino i Billioner Casino, grają miliony graczy miesięcznie. Nierzadko liczba jednoczesnych graczy sięga 20 tysięcy. Infrastruktura firmy rozproszona jest na tysiące kontenerów, które generują 10 miliardów wpisów do logów miesięcznie i przetwarzają ponad 2 petabajty danych. Firma zatrudnia blisko 500 osób, z czego połowa to inżynierowie, którzy pracują nad rozwojem gier. W środowisku, gdzie skala i złożoność są ogromne, bezpieczeństwo musi być priorytetem.

Wraz z popularyzacją pracy zdalnej i migracją aplikacji do chmury, tradycyjne granice bezpieczeństwa przestają istnieć. Tradycyjne metody zabezpieczeń, takie jak firewall czy VPN, nie są już wystarczające. Organizacje muszą wdrażać bardziej zaawansowane strategie, które chronią dane i aplikacje w rozproszonym środowisku.

Zmieniający się krajobraz bezpieczeństwa

Wraz z popularyzacją pracy zdalnej i migracją aplikacji oraz danych do chmury tradycyjne granice bezpieczeństwa przestają istnieć. Dzisiaj, aktywa cyfrowe i pracownicy firmy rozproszeni są na całym świecie, co wymaga nowego podejścia do zabezpieczeń. Tradycyjne metody zabezpieczeń, takie jak firewall czy VPN, nie są już wystarczające. Organizacje muszą wdrażać bardziej zaawansowane strategie, które chronią dane i aplikacje w rozproszonym środowisku.

Kluczowe zasady bezpieczeństwa

1. Ciągła weryfikacja tożsamości

Mimo, że zarządzanie tożsamością i dostępem (IAM) zawsze było fundamentem bezpieczeństwa, w chmurze nabrało jeszcze większego znaczenia. Bardzo szczegółowe zarządzanie uprawnieniami umożliwia przypisywanie ról użytkownikom i usługom, co jest kluczowe w dynamicznych środowiskach chmurowych. Tworzenie polityk IAM i zarządzanie nimi może być skomplikowane i podatne na błędy, zwłaszcza gdy zarządza się uprawnieniami na dużą skalę. Dynamiczny

i elastyczny charakter zasobów w chmurze oznacza, że często są one efemeryczne, co dodaje dodatkowej warstwy złożoności.
Bez dobrego narzędzia firmy nie są w stanie skutecznie podejść do zagadnień IAM. Huuuge Games inwestuje w Cloud Infrastructure Entitlement Management (CIEM), które koncentruje się na zarządzaniu uprawnieniami i uprawnieniami w środowiskach chmurowych. Przykładem rozwiązania, które częściowo realizuje funkcje CIEM jest AWS IAM Access Analyzer.

2. Automatyzacja konfiguracji chmury

Według ekspertów, ponad 99% naruszeń bezpieczeństwa w chmurze wynika z błędnych konfiguracji. Kluczowa jest automatyzacja, aby zminimalizować ryzyko ludzkich błędów. Huuuge Games używa AWS Control Tower i Account Factory for Terraform, aby zarządzać wszystkimi kontami AWS w organizacji oraz wdrażać zasoby AWS w sposób zautomatyzowany. AWS Service Control Policies pomagają firmie chronić zarządzane zasoby AWS przed nieautoryzowanymi modyfikacjami lub usunięciami, a także ograniczają użycie nieautoryzowanych regionów i typów zasobów.

99% naruszeń bezpieczeństwa w chmurze wynika z błędnych konfiguracji. Kluczowa jest automatyzacja, aby zminimalizować ryzyko ludzkich błędów.

3. Monitorowanie i logowanie

Bieżące monitorowanie i logowanie wszystkich aktywności sieciowych jest niezbędne do szybkiego wykrywania anomalii i potencjalnych incydentów bezpieczeństwa. Huuuge Games inwestuje w narzędzia Cloud Security Posture Management (CSPM), które skupiają się na monitorowaniu postury bezpieczeństwa środowisk chmurowych i zarządzaniu nią. Kluczowe funkcje tych narzędzi to automatyczne audyty, monitorowanie w czasie rzeczywistym, sprawdzanie zgodności, alarmowanie i raportowanie, a także automatyczne działania naprawcze.

Huuuge Games wykorzystuje usługi dostarczane przez dostawcę chmury, takie jak AWS Systems Manager, AWS Config, AWS CloudTrail i AWS Inspector oraz wspiera się dodatkowym narzędziem o nazwie Lacework. Inne chmury, takie jak Azure czy Google mają odpowiedniki wymienionych tutaj rozwiązań. W środowiskach wielochmurowych poleganie na zewnętrznym CSPM może być lepszą opcją, gdyż znacznie ułatwia zarządzanie, centralizując operacje w jednym miejscu.

4. Zabezpieczenia kontenerów

Kluczowym elementem architektury oprogramowania Huuuge Games są kontenery. Huuuge Games wykorzystuje dedykowane systemy operacyjne, takie jak Flatcar, skanuje obrazy kontenerów i sięga po narzędzia zarządzania lukami w zabezpieczeniach kontenerów. Ważne jest, aby grupować kontenery według ich przeznaczenia i stosować odpowiednie zabezpieczenia działających już workloadów. Narzędzie Lacework używane jest do wykrywania nieautoryzowanego dostępu sieciowego lub uruchamiania procesów, inspekcji pakietów oraz skanowania podatności.

Bieżące monitorowanie i logowanie wszystkich aktywności sieciowych jest niezbędne do szybkiego wykrywania anomalii i potencjalnych incydentów bezpieczeństwa.

5. Dystrybucja odpowiedzialności za bezpieczeństwo

W organizacjach, w których zespół ds. bezpieczeństwa ma wyłączną odpowiedzialność za bezpieczeństwo chmury i aplikacji, skuteczność działań jest często niższa. Ważne jest, aby zespoły deweloperskie i operacyjne również angażowały się w procesy bezpieczeństwa. Huuuge Games stosuje podejście „shift left", gdzie zespoły deweloperskie są również odpowiedzialne za bezpieczeństwo swojego kodu od samego początku. Huuuge Games ma w zespołach deweloperskich architektów oraz „championów bezpieczeństwa", którzy dbają o zgodność z najlepszymi praktykami ochrony aplikacji i danych.

W organizacjach, w których zespół ds. bezpieczeństwa ma wyłączną odpowiedzialność za zarządzanie chmurą, skuteczność jest często niższa. Ważne jest, aby zespoły deweloperskie i operacyjne również angażowały się w procesy bezpieczeństwa.

Praktyczne wdrożenia w Huuuge Games

Huuuge Games wdrożyło szereg narzędzi i procesów, które pomagają utrzymać wysoki poziom bezpieczeństwa w chmurze:

- AWS Control Tower i Account Factory for Terraform do zarządzania wszystkimi kontami AWS w organizacji oraz wdrażania zasobów w sposób zautomatyzowany,
- AWS Service Control Policies do ochrony zarządzanych zasobów AWS przed nieautoryzowanymi modyfikacjami lub usunięciami,
- AWS Config do śledzenia zmian konfiguracji wszystkich zasobów AWS oraz monitorowania niezgodnych konfiguracji,
- Lacework do wykrywania nieautoryzowanego dostępu sieciowego i procesów na instancjach EC2 oraz skanowania podatności,
- AWS Inspector do monitorowania i skanowania funkcji AWS Lambda pod kątem podatności,
- AWS CloudTrail do wykrywania anomalii w wywołaniach API.

Kluczowe wnioski

Firmy nie powinny lekceważyć zarządzania tożsamością, ponieważ stanowi to fundament bezpiecznego środowiska chmurowego. Dokładne poznanie swojej chmury jest kluczowe, gdyż błędne konfiguracje są najczęstszą przyczyną naruszeń bezpieczeństwa. Istotne staje się eksplorowanie narzędzi CSPM i CIEM. Inwestowanie w narzędzia do zarządzania posturą bezpieczeństwa chmury i zarządzania uprawnieniami infrastruktury chmurowej może znacznie poprawić poziom bezpieczeństwa.

Zrozumienie zagrożeń związanych z kontenerami i Kubernetes jest niezbędne, bowiem środowiska budowane na ich bazie wymagają specjalistycznych zabezpieczeń. W końcu dystrybucja odpowiedzialności za bezpieczeństwo w organizacji jest kluczowa, ponieważ zespoły deweloperskie i operacyjne powinny być aktywnie zaangażowane w procesy ochrony systemów i danych.

Doświadczenia Huuuge Games pokazują, że tak kompleksowe podejście do bezpieczeństwa nie tylko zwiększa poziom ochrony, ale wpiera rozwój firmy i pozwala na szybszą adaptację procesów do zmieniających się warunków.

PODCASTY

COMPUTERWORLD

LUDZIE. BIZNES. TECHNOLOGIA.

TECH TRENDS

SŁUCHAJ NAS NA:

EXECUTIVE VIEWPOINT | TENABLE

Bernard Montel

ZARZĄDZANIE EKSPOZYCJĄ W CYBERBEZPIECZEŃSTWIE

ORGANIZACJE, ABY UCHWYCIĆ SENS I KRAJOBRAZ ZAGROŻEŃ MUSZĄ ZROZUMIEĆ GLOBALNY KONTEKST WOKÓŁ – POŁĄCZENIE ROZCHWIANEJ GOSPODARKI, AKTYWIZMU I NAPIĘĆ GEOPOLITYCZNYCH. HOLISTYCZNE SPOJRZENIE NA TE KWESTIE, WYKRACZAJĄCE DALEKO POZA OBSZAR TECHNOLOGII, JEST ABSOLUTNIE KLUCZOWE DLA POZYSKANIA WIEDZY, KTÓRE DRZWI I OKNA SĄ SZEROKO OTWARTE, A KTÓRE TRZEBA ZAMKNĄĆ W PIERWSZEJ KOLEJNOŚCI – mówi w rozmowie z Computerworld Bernard Montel, Dyrektor Techniczny EMEA i Strateg ds. Bezpieczeństwa w Tenable

Computerworld: Jak zmienił się krajobraz cyberbezpieczeństwa w ostatnich pięciu latach?

Bernard Montel: Globalna pandemia dramatycznie zmieniła sposób, w jaki pracujemy. Dla niektórych organizacji zmiana ta nastąpiła praktycznie z dnia na dzień. Zamiast podróżować do biur lub innych miejsc pracy, łączyliśmy się z systemami i zasobami zdalnie. Z punktu widzenia cyberbezpieczeństwa miało to ogromny wpływ na sposób myślenia o bezpieczeństwie.

Computerworld: Jakie były największe wyzwania związane z tą zmianą?

Bernard Montel: Sieć domowa, która nigdy wcześniej nie była zabezpieczona, nagle stała się przedłużeniem sieci korporacyjnej. Domowe routery stały się jedynym sposobem, w jaki pracownicy mogli uzyskać dostęp do zasobów, co znacznie rozszerzyło powierzchnię ataku. Korzystanie z sieci prywatnych (VPN) i uwierzytelniania wieloskładnikowego (MFA) było jedynym sposobem na zabezpieczenie tych połączeń. Przeniesienie zasobów do chmury wyeliminowało konieczność zestawiania łączy VPN, co bardzo ułatwiło życie pracownikom zdalnym, zapewniając jednocześnie dodatkową warstwę zabezpieczenia firmowych systemów i danych.

„Twierdza" reprezentowana przez sieć korporacyjną jest teraz rozproszona, co powoduje, że powierzchnia ataku nigdy wcześniej nie była tak duża, ani bardziej dynamiczna, niż obecnie.

Computerworld: Jakie najważniejsze doświadczenie pozostawiła pandemia COVID-19?

Bernard Montel: Jeśli moglibyśmy zachować jedną zmianę po pandemii, byłoby to przyspieszenie wdrażania usług chmurowych w każdym z modeli: Software as a Service (SaaS),

Platform as a Service (PaaS) czy Infrastructure as a Service (IaaS). Chmura zmieniła sposób, w jaki dziś pracujemy, eliminując potrzebę fizycznych maszyn, które były dostępnie jedynie zdalnie. W mojej opinii nie ma potrzeby być bezpośrednio podłączonym do sieci korporacyjnej, aby pozostawać bezpiecznym. Oczywiście nadal mamy wdrożone i używane pewne rozwiązania on-premise, jednak większość organizacji działa w środowisku hybrydowym, łącząc publiczną chmurę z zasobami obsługiwanymi lokalnie. Dzisiejsza „nowa normalność" oznacza, że „twierdza" reprezentowana przez sieć korporacyjną jest teraz rozproszona, co powoduje, że powierzchnia ataku nigdy wcześniej nie była tak duża, ani bardziej dynamiczna, niż obecnie.

Computerworld: Zatem, jak w kontekście nowych płaszczyzn ataku kształtują się obecnie trendy w dziedzinie cyberbezpieczeństwa?

Bernard Montel: Największym zagrożeniem nadal pozostaje ransomware. Liczba ataków, z którymi borykają się organizacje wyraźnie rośnie. Każdego dnia padają kolejne rekordy pod względem liczby naruszonych rekordów lub ilości wykradzionych danych. Bezpieczeństwo chmury to dzisiaj realny problem dla wszystkich organizacji. Przejście na zasoby chmurowe zmusza zespoły bezpieczeństwa do przemyślenia sposobu, w jaki zarządzają bezpieczeństwem. Tradycyjne podejście perymetryczne z punktem końcowym i/lub serwerem jako głównym obiektem praktyk bezpieczeństwa jest prawie bezużyteczne w przypadku mikroserwisów i kontenerów.

Computerworld: Najsłabszym ogniwem w ekosystemie cyberbezpieczeństwa pozostaje człowiek. Wszystko zaczyna się od wykradzionych haseł...

Bernard Montel: Zarządzanie tożsamością zawsze było kluczowe w zapewnieniu bezpieczeństwa danych. W ostatnich dwóch dekadach wyzwania te adresowane były poprzez stosowanie systemów klasy Identity and Access Management (IAM). Dzisiaj problemy związane z zarządzaniem tożsamością są nadal widoczne, ale obszary i metody ochrony stały już znacznie bardziej złożone. Mam tutaj na myśli konieczność stosowania federacyjnych tożsamości, MFA, Active Directory i EntraID w połączeniu z tożsamościami chmurowymi (AWS, Azure, GCP).

Kolejnym obszarem zainteresowania w obszarze cyberbezpieczeństwa, podobnie jak w innych technologiach, staje się sztuczna inteligencja. Atakujący dopiero zaczynają zdawać sobie sprawę z możliwości jakie oferuje AI. Jednocześnie my jako obrońcy, atakowani musimy określić jak wykorzystać tę technologię do ochrony. Wykorzystanie mocy i szybkości generatywnej AI, takiej jak Google Virtex AI, OpenAI GPT-4 czy LangChain, umożliwia uzyskiwanie nowych, inteligentnych informacji w ciągu minut. Może to przyspieszyć cykle badań i rozwoju w dziedzinie cyberbezpieczeństwa, poszukiwanie wzorców i wyjaśnianie tego, co zostało znalezione, w możliwie najprostszy sposób. Wykorzystanie mocy AI pozwala zespołom bezpieczeństwa szybciej pracować, szukać i analizować, a ostatecznie podejmować właściwe decyzje.

Wykorzystanie mocy i szybkości generatywnej AI umożliwia uzyskiwanie nowych, inteligentnych informacji w ciągu minut. Może to przyspieszyć cykle badań i rozwoju w dziedzinie cyberbezpieczeństwa, poszukiwanie wzorców i wyjaśnianie tego, co zostało znalezione

Computerworld: Jaki tok myślowy powinny przyjąć organizacje w kwestii zagrożeń bezpieczeństwa?

Bernard Montel: W większości przypadków to znana, opublikowana luka (vulnerability) umożliwia cyberprzestępcom dostanie się do infrastruktury organizacji. Po uzyskaniu dostępu, atakujący dążą do dalszej infiltracji organizacji w celu kradzieży danych, szyfrowania systemów lub innych złowrogich działań. Otwarte drzwi dla atakujących stanowią również, z pozoru nieszkodliwe, błędy konfiguracyjne, czyli podstawowe błędy ludzkie - od pozostawionych „domyślnie" ustawień aż do błędów programistów, którzy przesyłają niesprawdzony kod w szybkim cyklu DevOps.

Computerworld: Czy mniejsze firmy również narażone są na te zagrożenia?

Bernard Montel: Często istnieje przekonanie, że małe firmy, z uwagi na swój rozmiar, nie stanowią atrakcyjnego celu dla atakujących. Nic bardziej mylnego. Oczywiście zgadzam się, że to zazwyczaj duże i znane firmy trafiają na nagłówki gazet. Cyberprzestępcy zdają sobie jednak sprawę, że mniejsze organizacje, będące częścią łańcucha dostaw, również mogą być celem, otwierając drzwi do większych firm.

EXECUTIVE VIEWPOINT | TENABLE

Computerworld: Wróćmy jeszcze na chwilę do ataków ransomware jako tych, których skutki mogą być naprawdę bolesne dla firmy. Jak ewoluowały ataki tego typu w ostatnich latach?

Bernard Montel: Dziesięć lat temu atak ransomware był łatwo zauważalny. Nikt nie miał wątpliwości co się stało, gdy komputer stawał się bezużyteczny po jego zablokowaniu komunikatem żądania okupu wyświetlanym na ekranie. Dzisiaj ataki stają się mniej oczywiste i mogą pozostawać niewykryte przez kilka tygodni. Cyberprzestępcy starają się ukryć swoją obecność, aby móc poruszać się po infrastrukturze w celu wykonywania innych złowrogich działań. Co więcej, grupy zajmujące się wymuszeniami przez ransomware stosują metodę podwójnego wymuszenia, która łączy taktykę szyfrowania z dodaniem kolejnego elementu. Jeszcze przed zaszyfrowaniem plików, przestępcy kradną je i grożą opublikowaniem ich w dark webie, jeśli okup nie zostanie zapłacony. Dodatkowa presja, wynikająca z tego rodzaju wymuszenia sprawia, że ataki ransomware są tak skuteczne.

Dzisiaj ataki ransomware stają się mniej oczywiste i mogą pozostawać niewykryte przez kilka tygodni. Cyberprzestępcy starają się ukryć swoją obecność, aby móc poruszać się po infrastrukturze w celu wykonywania innych złowrogich działań.

Computerworld: Na koniec spróbujmy zastanowić się jakie podejście powinny przyjąć organizacje, aby skutecznie zarządzać ryzykiem?

Bernard Montel: Przedsiębiorstwa i instytucje publiczne, aby uchwycić sens i krajobraz zagrożeń, muszą zrozumieć globalny kontekst wokół — połączenie rozchwianej gospodarki, aktywizmu i napięć geopolitycznych. Skupienie się tylko na „technologicznym" aspekcie cyberzagrożeń nie wystarczy, aby zredukować ryzyko. Kluczowe dla jego ograniczenia jest proaktywne podejście prewencyjne. Holistyczne spojrzenie na kwestie zarządzania ryzykiem, wykraczające daleko poza obszar technologii, jest absolutnie kluczowe dla pozyskania wiedzy, które drzwi i okna są szeroko otwarte, a które trzeba zamknąć w pierwszej kolejności. Podejście to nazywamy zarządzaniem ekspozycją.

Wyniki XII konkursu **Computerworld Best in Cloud**

Fot.: Freepik

Najlepsze wdrożenie usługi chmurowej w ostatnich 12 miesiącach

Polskie Sieci Elektroenergetyczne / Asseco Poland (s. 27) – 1. miejsce
za wykorzystanie chmury Amazon do udostępnienia
Narzędzia Migracji Danych inicjalnych systemu CSIRE

Najlepsze produkty i dostawcy rozwiązań chmurowych

Bezpieczna chmura

Integrated Solutions - Integrated Computing (s. 36) - 1. miejsce
Platforma OChK (s. 40) – 2. miejsce
Oktawave (s. 42) – 3. miejsce

Najlepszy dostawca chmury w modelu IaaS

SUPREMIS (s. 44) – 1. miejsce ex aequo
Integrated Solutions (s. 36) – 1. miejsce ex aequo

Najlepszy produkt zintegrowanej komunikacji (Unified Communications)

Symfonia eBiuro (s. 60) – wyróżnienie

Zabezpieczenie środowiska chmurowego

Tenable Cloud Security (s. 52) – 1. miejsce ex aequo
Perceptus perc.pass (s. 54) - 1. miejsce ex aequo

Najlepszy produkt ERP/CRM

Symfonia Obieg Dokumentów (s. 56) – 1. miejsce
Soneta TRIVA ERP (s. 58) - wyróżnienie

Najlepsza wydajność i integracja

Integrated Solutions - Integrated Computing (s. 36) – 1. miejsce

Wyniki XII konkursu Computerworld Best in Cloud

Na dorocznej konferencji Computerworld Best in Cloud 2024 poznaliśmy wyniki konkursu na najlepsze wdrożenie usługi chmurowej w ostatnich 12 miesiącach oraz konkursu na najciekawsze i najbardziej innowacyjne rozwiązania chmurowe. Wyniki konkursu ogłosił, pełen zachwytu nad dojrzałością i unikalnością produktów chmurowych, Grzegorz Stech, redaktor naczelny „Computerworld" i przewodniczący jury konkursu „Best in Cloud".

Najlepsze wdrożenie usługi chmurowej w ostatnich 12 miesiącach

O wyniku konkursu dla organizacji, które w ostatnich miesiącach wdrożyły rozwiązania chmurowe, decydowały oryginalność i innowacyjność projektu oraz potencjał jego oddziaływania na biznes. Pierwsze miejsce jury konkursu przyznało spółce Polskie Sieci Elektroenergetyczne (PSE), która wykorzystała zasoby chmury Amazon do udostępnienia Narzędzia Migracji Danych inicjalnych systemu CSIRE około 300 sprzedawcom i dystrybutorom energii elektrycznej.

Centralny System Informacji Rynku Energii (CSIRE) będzie gromadzić informacje z ponad 19 mln punktów pomiaru energii elektrycznej. Obecnie dane te znajdują się w systemach sprzedawców i dystrybutorów energii elektrycznej. Firma Asseco Poland, na zlecenie PSE, stworzyła i udostępniła narzędzie, które pozwoli uczestnikom rynku na przygotowanie zbioru danych inicjalnych i przekazanie ich do centralnego rejestru.

Wykorzystanie chmury w projekcie przyczyniło się do istotnego ograniczenia wydatków CAPEX, co okazało się niezwykle ważne z uwagi na ograniczony okres użytkowania narzędzia. Brak konieczności zapewniania własnej infrastruktury fizycznej przełożył się na skrócony czas uruchomienia systemu, przy zagwarantowaniu bardzo dużej dostępności, skalowalności i stabilności rozwiązania.

Najlepsze produkty i dostawcy rozwiązań chmurowych

W konkursie na najciekawsze i najbardziej innowacyjne rozwiązania chmurowe nagrody przyznano w 6 kategoriach produktowych. Największym wygranym plebiscytu okazała się spółka Integrated Solutions, której usługi chmury Integrated Computing zostały nagrodzone aż w trzech kategoriach: Bezpieczna chmura, Najlepszy dostawca chmury w modelu IaaS oraz Najlepsza wydajność i integracja.

Bezpieczna chmura

Tytuł zwycięzcy w kategorii Bezpieczna chmura przypadł spółce Integrated Solutions, która w ramach chmury Integrated Computing dostarcza gotowe do użycia platformy według ustandaryzowanego katalogu usług. Na życzenie klienta oferuje możliwość zbudowania i wdrożenia indywidualnego, współdzielonego lub dedykowanego środowiska obliczeniowego. Szerokie portfolio dostawcy obejmuje usługi zapasowego centrum danych (Disaster Recovery), wirtualizacji baz danych Oracle oraz wdrażania dedykowanych chmur prywatnych. Usługi chmurowe świadczone są z centrów danych Orange zlokalizowanych w Polsce.

Dwa pozostałe miejsca na podium w kategorii Bezpieczna chmura przypadły Platformie OChK (2. miejsce) oraz chmurze publicznej Oktawave (3. miejsce). Platforma OChK pozwala na budowanie całej gamy rozwiązań – od chmury publicznej, przez środowiska hybrydowe i wielochmurowe (multicloud), po chmurę prywatną. Platforma OChK zbudowana została od podstaw i zarządzana jest przez zespół wewnętrznych ekspertów firmy w modelu security by design. Jej elastyczna architektura umożliwia dostosowywanie oferowanych usług do niestandardowych projektów oraz specyficznych wymagań klientów. Dostawca zapewnia indywidualną konfigurację usług, bardziej spersonalizowaną, niż w przypadku rozwiązań hiperskalerów.

Oktawave to polska publiczna chmura obliczeniowa zapewniająca dostęp do rozwiązań o dużej skalowalności i wysokiej dostępności, uruchamianych w trzech certyfikowanych centrach w Polsce. Geograficzne rozproszenie miejsc przetwarzania danych gwarantuje wysoką dostępność, skalowalność i bezpieczeństwo dostarczanych usług IaaS/PaaS. W ramach chmury Oktawave możliwe jest uruchamianie, przetwarzanie i przechowywanie dowolnych zasobów w postaci serwisów e-commerce, aplikacji biznesowych, rozwiązań korporacyjnych czy systemów IT.

Najlepszy dostawca chmury w modelu IaaS

W tym roku za najlepszego dostawcę chmury w modelu IaaS jury konkursowe uznało ex aequo firmy SUPREMIS oraz Integrated Solutions. SUPREMIS specjalizuje się w dostarczaniu infrastruktury dla systemów ERP, takich jak SAP, oraz obsługi wysokowydajnych baz danych. Flagowa usługa firmy, SUPREMIS Cloud Platform, to skalowalne, certyfikowane przez SAP, środowisko chmurowe do obsługi najbardziej wymagających obciążeń biznesowych. Platforma wyróżnia się niezawodnością, wydajnością i bezpieczeństwem danych, pozwalając klientom zrealizować dowolny scenariusz biznesowy – samodzielnie lub ze wsparciem wykwalifikowanych inżynierów. Oferuje ciągłość pracy dzięki wielowarstwowej redundancji elementów środowiska fizycznego.

Najlepszy produkt zintegrowanej komunikacji (Unified Communications)

W kategorii Najlepszy produkt zintegrowanej komunikacji (Unified Communications) jury konkursowe przyznało wyróżnienie oprogramowaniu Symfonia eBiuro. To chmurowa aplikacja dla biur rachunkowych i jednoosobowych działalności gospodarczych, która pozwala sprawnie zarządzać uproszczoną księgowością, magazynem oraz sprawami kadrowo-płacowymi. Platforma umożliwia wygodne wprowadzanie dokumentów sprzedażowych i kosztowych oraz usprawnia kontakty z klientami. Elektroniczny obieg dokumentów, wspierany przez zaawansowane rozwiązanie OCR, zintegrowany został z około 20 systemami finansowo-księgowymi. Na tle konkurencyjnych rozwiązań Symfonia eBiuro wyróżnia się pracą w chmurze, aplikacją mobilną oraz dedykowaną platformą komunikacji z partnerami.

Zabezpieczenie środowiska chmurowego

W nowej kategorii Zabezpieczenie środowiska chmurowego jury konkursowe przyznało ex aequo dwa pierwsze miejsca platformie zabezpieczania chmury Tenable Cloud Security oraz menedżerowi haseł perc. pass firmy Perceptus.

Tenable Cloud Security to zaawansowana platforma ochrony środowisk chmurowych (CNAPP), która zapewnia kompleksowe zabezpieczenie infrastruktury, tożsamości i korzystania z zasobów w środowiskach chmurowych. Rozwiązanie upraszcza identyfikację i korygowanie ryzyka w środowiskach wielochmurowych, zmniejszając płaszczyzny ataku lub wycieku danych, przy jednoczesnej poprawie produktywności. Rozwiązanie adresuje wyzwania związane z rosnącą złożonością i rozproszonym charakterem nowoczesnych środowisk chmurowych, oferując zintegrowane podejście do zabezpieczeń.

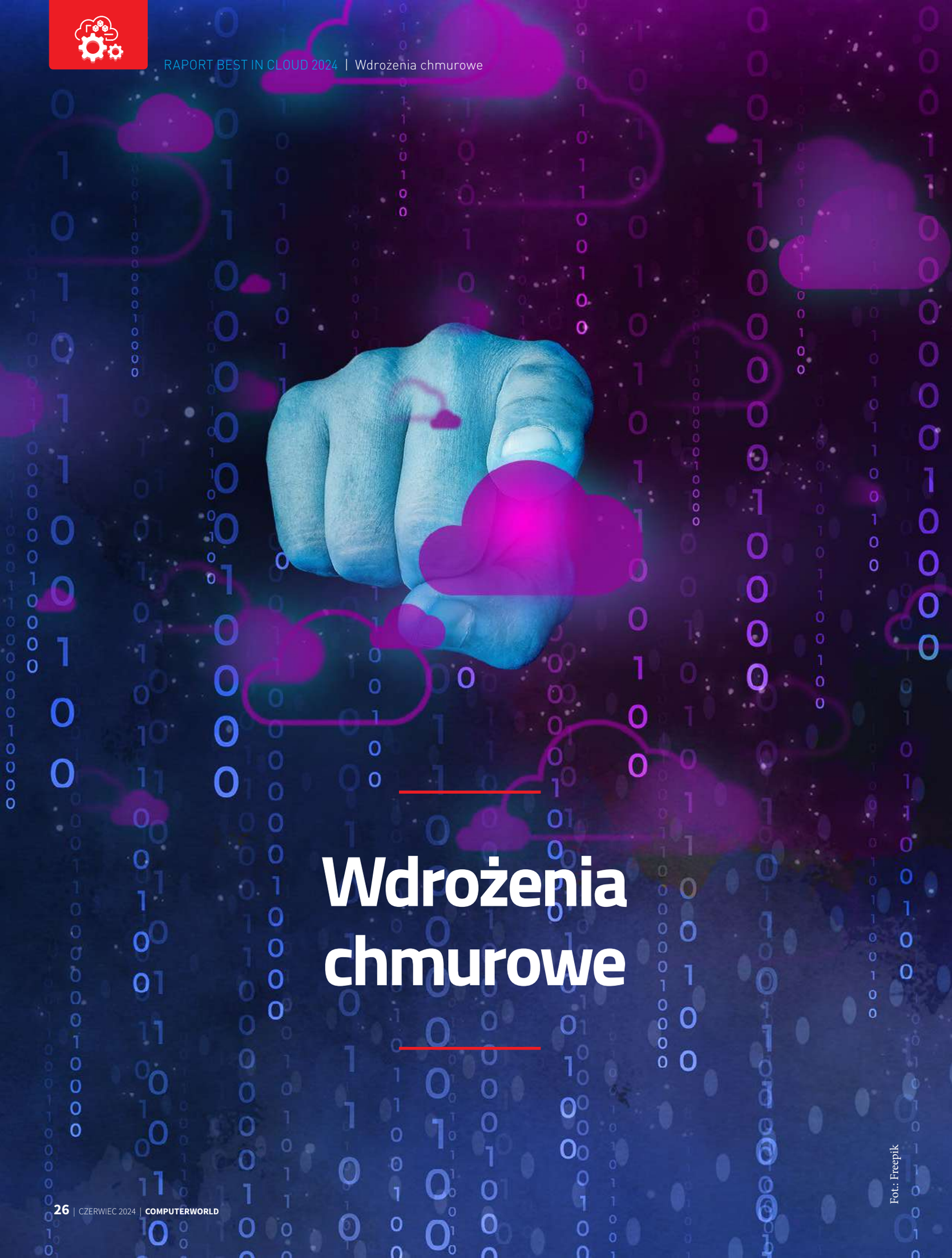
Z kolei perc.pass to pierwszy polski menedżer haseł zaprojektowany dla zespołów, które mogą dzięki niemu szybko dzielić się dostępem do różnych systemów, aplikacji oraz stron webowych. Menedżer oferuje innowacyjną metodę szyfrowania zero-knowledge, która w połączeniu z dwuskładnikowym uwierzytelnianiem oraz szyfrowaniem danych w spoczynku z wykorzystaniem HSM zapewnia użytkownikom maksymalne bezpieczeństwo. Wrażliwe dane przechowywane i przetwarzane są na terytorium Polski, co czyni ją unikalnym rozwiązaniem na rynku.

Najlepszy produkt ERP/CRM

W konkursie Best in Cloud 2024 najlepszym produktem klasy ERP/CRM została Symfonia Obieg Dokumentów. Jednocześnie jury konkursu przyznało wyróżnienie w tej kategorii systemowi Soneta TRIVA ERP.

Symfonia Obieg Dokumentów to chmurowa platforma łącząca rozwiązanie ECM z elementami pracy grupowej i systemu ERP, która agreguje funkcje biznesowe w jednym, spójnym interfejsie okienkowym. Oprogramowanie odpowiada na potrzebę tworzenia cyfrowych miejsc pracy, tzw. digital workplace. Łączą one ludzi z informacjami i procesami, aby zapewniać efektywną komunikację i nowoczesne metody zarządzania firmą. Platforma oferuje kilkadziesiąt obszarów zastosowań, z których najczęściej wykorzystywane są funkcje obiegu dokumentów, w szczególności związane z fakturami zakupu i procesami zakupowymi.

Z kolei Soneta TRIVA ERP jest nowoczesnym systemem ERP stworzonym dla średnich i dużych firm, umożliwiającym organizację przepływu pracy i informacji oraz pomagającym użytkownikom efektywnie pracować, zarządzać zmianami i konkurować na rynku. TRIVA automatyzuje i ujednolica analizę biznesową oraz finansową, a także pomaga nadzorować procesy w firmie. Każdy z tych obszarów jest wspierany natywnie przez moduły Business Intelligence (BI) oraz Automatyzacja procesów biznesowych (Workflow). Produkt może zostać dopasowany do dowolnej branży i niemal każdej specyfiki działania firmy. Umożliwia organizację pracy zdalnej.



Wdrożenia chmurowe

Fot.: Freepik

Polskie Sieci Elektroenergetyczne

Polskie Sieci Elektroenergetyczne wykorzystały zasoby chmury Amazon do udostępnienia Narzędzia Migracji Danych inicjalnych systemu CSIRE około 300 sprzedawcom i dystrybutorom energii elektrycznej

Polskie Sieci Elektroenergetyczne wdrożyły Narzędzie Migracji Danych w chmurze na potrzeby inicjalnego zasilenia danymi Centralnego Systemu Informacji Rynku Energii (CSIRE). Narzędzie migracji danych, zbudowane na bazie usług Amazon Web Services, udostępniono uczestnikom migracji w kwietniu 2023 roku.

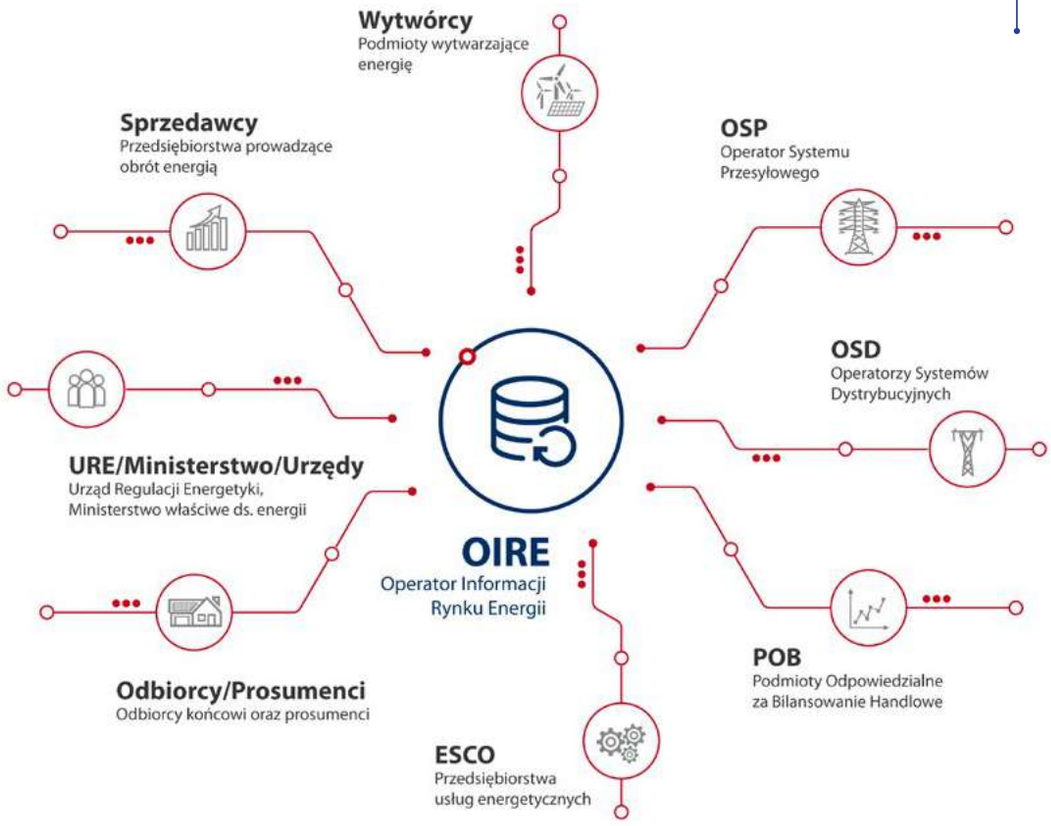
Polskie Sieci Elektroenergetyczne S.A. są operatorem elektroenergetycznego systemu przesyłowego w Polsce. Zadaniem PSE jest bilansowanie systemu elektroenergetycznego, czyli dbanie, by energia elektryczna, potrzebna odbiorcom w całym kraju, została im dostarczona, bez względu na porę dnia i roku. Spółka zarządza siecią przesyłową linii najwyższych napięć 400 kV oraz 220 kV o łącznej długości ponad 16 tysięcy kilometrów oraz posiada 109 stacji elektroenergetycznych. Dzięki liniom najwyższych napięć, energia elektryczna wytworzona w krajowym systemie elektroenergetycznym trafia do sieci lokalnych dystrybutorów, a za ich pośrednictwem do przedsiębiorstw i gospodarstw domowych.

Od lipca 2021 roku PSE pełnią funkcję Operatora Informacji Rynku Energii (OIRE), którego zadaniem jest wdrożenie Centralnego Systemu Informacji Rynku Energii (CSIRE), a następnie administrowanie nim. W bazie gromadzone będą dane z ponad 19 mln punktów pomiaru energii elektrycznej. Z systemu będzie mogło korzystać około 500 aktywnych użytkowników profesjonalnych i prawie 17,5 mln odbiorców końcowych energii elektrycznej, w tym ponad 15 mln gospodarstw domowych. Dzięki CSIRE ujednolicone zostaną także standardy wymiany informacji. Procesy zachodzące na detalicznym rynku energii elektrycznej będą zaś znacznie usprawnione i przyspieszone.

Narzędzie migracji danych umożliwia zebranie i odpowiednie przygotowanie danych pochodzących od około 300 podmiotów: sprzedawców i dystrybutorów energii elektrycznej

Narzędzie Migracji Inicjalnej

Proces Migracji Inicjalnej ma na celu przygotowanie zbioru danych inicjalnych niezbędnych do uruchomienia CSIRE, które obecnie znajdują się w systemach sprzedawców i dystrybutorów energii elektrycznej. Aby sprostać temu wyzwaniu, zdecydowano się na opracowanie narzędzia informatycznego, które umożliwia zebranie i odpowiednie przygotowanie danych pochodzących od około 300 podmiotów. Narzędzie migracji danych, na zlecenie PSE, zbudowało Asseco Poland. To rozwiązanie chmurowe, oparte o Amazon Web Services, które



udostępniono uczestnikom migracji w kwietniu 2023 roku.

W ramach procesu uczestnicy migracji (UM) przygotowują dane źródłowe oraz weryfikują zgodność danych z wymaganiami zawartymi w dokumencie Zakres Danych Migracji CSIRE. Przeprowadzana jest walidacja zgodności danych pomiędzy różnymi uczestnikami migracji. Sam proces migracji ma także na celu ujednolicenie danych funkcjonujących na detalicznym rynku energii elektrycznej, podniesienie jakości tych informacji i budowanie świadomości przyszłej współpracy z CSIRE. OIRE zarządza przebiegiem tego przedsięwzięcia, udziela wsparcia uczestnikom migracji w zakresie przygotowania danych migracyjnych oraz zbudowania zbioru danych inicjalnych niezbędnych do uruchomienia CSIRE.

Wykorzystana w projekcie infrastruktura pozwala na sprawną obsługę dużych ilości danych, przy oszczędności zasobów w okresach, kiedy potrzeby biznesowe są minimalne

Architektura rozwiązania

Całość rozwiązania została posadowiona w chmurze Amazon Web Services. Procesy biznesowe zostały zaimplementowane w sposób rozproszony – zrównoleglony z użyciem technologii AWS Glue/Spark. Wykorzystano usługi w modelu serverless na poziomie logiki procesowej oraz baz danych. W projekcie wykorzystano relacyjne bazy danych (PostgreSQL) oraz bazy NoSQL (MongoDB). Interfejsem dla uczestnika migracji oraz pracowników wsparcia OIRE jest aplikacja webowa z przyjaznym interfejsem użytkownika, stworzona w Angular z wykorzystaniem technik konteneryzacji Kubernetes. Narzędzie zapewnia bardzo wysoki poziom bezpieczeństwa, dzięki wykorzystaniu protokołu autoryzacji OpenID Connect opartego

o framework OAuth 2.0. Architektura rozwiązania zaprojektowana została zgodnie z zasadą minimalnych uprawnień.

Korzyści z wykorzystania chmury

Wykorzystanie chmury w projekcie wdrożenia i udostępnienia Narzędzia Migracji Danych przyczyniło się do istotnego ograniczenia wydatków CAPEX, co ma szczególne znaczenie przy założeniu ograniczonego (skończonego) okresu użytkowania narzędzia. Brak konieczności zapewniania własnej infrastruktury fizycznej przełożył się na skrócony czas uruchomienia rozwiązania. Jednocześnie infrastruktura chmury gwarantuje bardzo dużą dostępność i stabilność rozwiązania, co pozostaje w zgodzie z koniecznością zapewnienia ciągłości biznesu.

Chmura obliczeniowa zapewnia bardzo wysoką wydajność przetwarzania oraz skalowalność. W obecnym stadium całość przetwarzania biznesowego zajmuje około 20% limitu czasu przetwarzania założonego przy specyfikowaniu wymagań do projektu. Wykorzystywana infrastruktura pozwala na sprawną obsługę dużych ilości danych, przy oszczędności zasobów w okresach, kiedy potrzeby biznesowe są minimalne.

Zaprojektowane rozwiązanie zapewnia zgodność z wymogami RODO i założeniami projektowymi przyjętymi na tym polu. System gwarantuje, że dane nie zostaną przeniesione poza EOG/UE a logowanie do aplikacji jest możliwe tylko z tego obszaru.

Firma:
Polskie Sieci Elektroenergetyczne

Profil działalności firmy:
Operator Systemu Przesyłowego w Polsce oraz Operator Informacji Rynku Energii

Wykorzystana chmura: Amazon Web Services

Integrator: Asseco Poland

PGZ Stocznia Wojenna wykorzystuje Platformę OChK jako środowisko do projektowania fregat Miecznik

we know the cloud

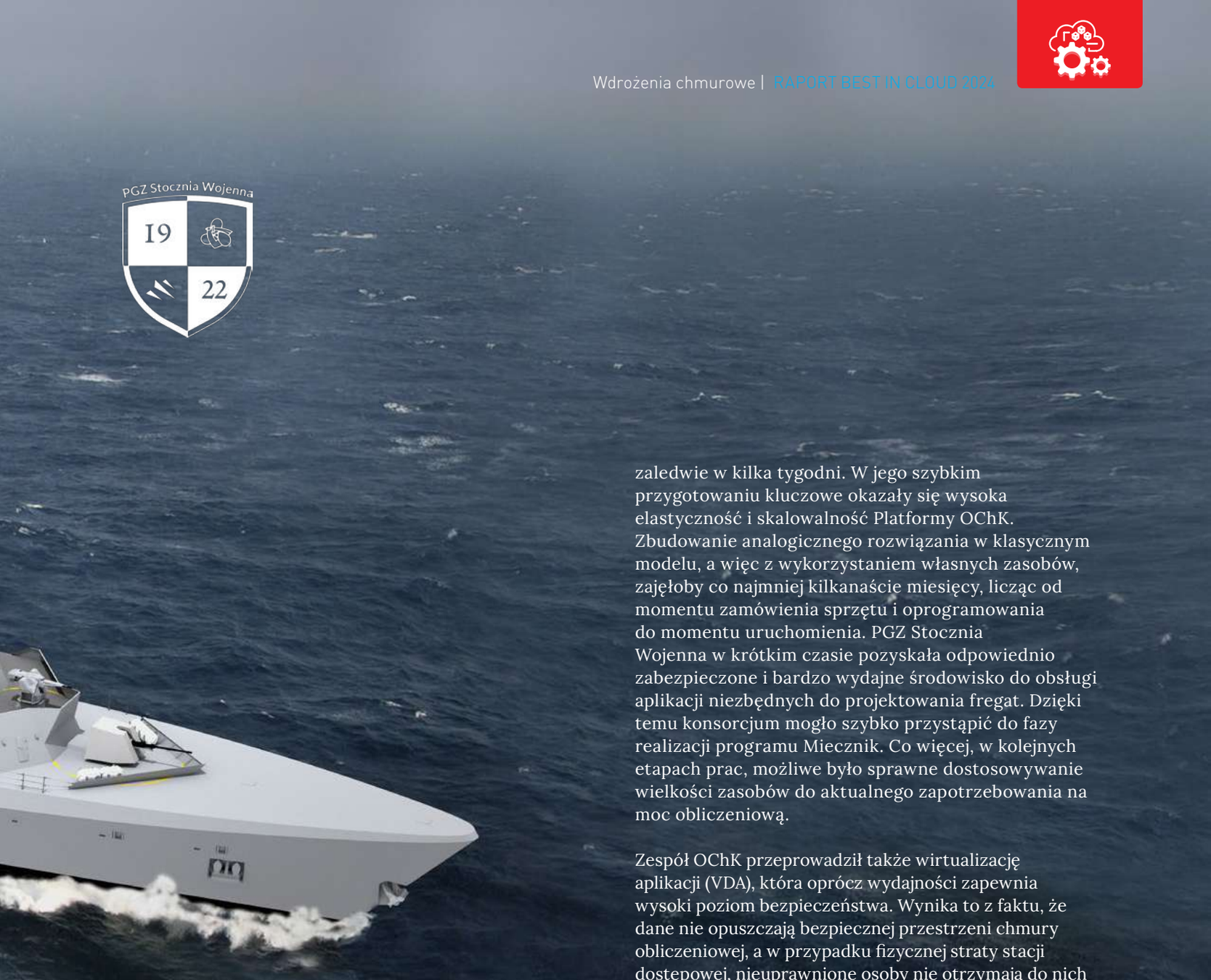
Platforma OChK pozwoliła na zbudowanie i szybkie uruchomienie aplikacji potrzebnych do projektowania fregat Miecznik. Dzięki temu PGZ Stocznia Wojenna uzyskała dostęp do bardzo dużej mocy obliczeniowej, którą może elastycznie dopasowywać do aktualnych potrzeb, na każdym etapie realizacji tego kluczowego dla jej rozwoju projektu.

PGZ Stocznia Wojenna zajmuje się projektowaniem, budową, remontowaniem i modernizacją okrętów wojennych oraz jednostek dla innych służb mundurowych i państwowych. Jest najstarszą polską stocznią – działa od 1922 roku, kontynuując tradycję Stoczni Marynarki Wojennej oraz Warsztatów Portowych Marynarki Wojennej, utworzonych jeszcze przed II wojną światową w Pucku, a następnie przeniesionych do Gdyni. Obecnie stanowi część Polskiej Grupy Zbrojeniowej, jednego z największych koncernów zbrojeniowych w Europie Środkowo-Wschodniej. PGZ Stocznia Wojenna jest głównym wykonawcą konsorcjum realizującego program „Miecznik", którego celem jest dostarczenie Marynarce Wojennej RP trzech nowoczesnych okrętów klasy fregata.

Decyzja o wykorzystaniu chmury podyktowana była chęcią znalezienia skalowalnego rozwiązania, dzięki któremu zmienne zapotrzebowanie na zasoby IT nie generowałoby zbędnych kosztów

Wyzwania i potrzeby

Na początkowym etapie prac głównym wyzwaniem dla PGZ Stoczni Wojennej było szybkie uruchomienie procesu projektowania i budowy fregat. Ze względu na szeroką skalę przedsięwzięcia, wykorzystywane wówczas w projekcie specjalistyczne oprogramowanie CAD wymagało dużej mocy obliczeniowej, a tym samym znacznej rozbudowy wykorzystywanego lokalnego środowiska informatycznego. Dodatkową kwestią, którą należało



wziąć pod uwagę, było nierównomierne rozłożenie zapotrzebowania na zasoby IT na różnych etapach projektu.

Biorąc pod uwagę wszystkie czynniki, PGZ Stocznia Wojenna podjęła decyzję o wykorzystaniu technologii chmury obliczeniowej. Podyktowana była ona przede wszystkim chęcią znalezienia skalowalnego rozwiązania, dzięki któremu zmienne zapotrzebowanie na zasoby IT nie generowałoby zbędnych, dodatkowych kosztów. Nie bez znaczenia była także możliwość automatyzacji powtarzalnych procesów, co w istotny sposób przyspiesza realizację prac.

Platforma OChK w PGZ SW

Gotowe środowisko IT zostało przy pomocy ekspertów z OChK skonfigurowane i uruchomione zaledwie w kilka tygodni. W jego szybkim przygotowaniu kluczowe okazały się wysoka elastyczność i skalowalność Platformy OChK. Zbudowanie analogicznego rozwiązania w klasycznym modelu, a więc z wykorzystaniem własnych zasobów, zajęłoby co najmniej kilkanaście miesięcy, licząc od momentu zamówienia sprzętu i oprogramowania do momentu uruchomienia. PGZ Stocznia Wojenna w krótkim czasie pozyskała odpowiednio zabezpieczone i bardzo wydajne środowisko do obsługi aplikacji niezbędnych do projektowania fregat. Dzięki temu konsorcjum mogło szybko przystąpić do fazy realizacji programu Miecznik. Co więcej, w kolejnych etapach prac, możliwe było sprawne dostosowywanie wielkości zasobów do aktualnego zapotrzebowania na moc obliczeniową.

Zespół OChK przeprowadził także wirtualizację aplikacji (VDA), która oprócz wydajności zapewnia wysoki poziom bezpieczeństwa. Wynika to z faktu, że dane nie opuszczają bezpiecznej przestrzeni chmury obliczeniowej, a w przypadku fizycznej straty stacji dostępowej, nieuprawnione osoby nie otrzymają do nich dostępu.

Wszystkie usługi Platformy OChK uruchamiane są na serwerach zlokalizowanych w Polsce, co daje gwarancję lokalnej rezydencji danych, a także właściwej redundantności. Platforma uwzględnia także zasady compliance i zapewnia pełną zgodność z polskimi regulacjami

Zespół OChK nie tylko zaprojektował i wdrożył architekturę bezpieczeństwa całości rozwiązania, ale także całodobowo monitoruje zbudowane środowisko IT w ramach usługi SOC (Security Operations Center), świadczonej przez certyfikowany zespół ekspertów. OChK zapewnia także usługi wsparcia, które gwarantują m.in. wysoki poziom dostępności środowiska (SLA) dla końcowego użytkownika.

Technologie chmurowe w projekcie

Dobranie odpowiedniej technologii w projekcie było istotne nie tylko ze względu na jego sprawną realizację, ale także zapewnienie możliwie najwyższego poziomu bezpieczeństwa. PGZ Stocznia Wojenna jest podmiotem,

który działa w sektorze obronnym, a wykorzystywane przez nią narzędzia IT muszą spełniać najwyższe wymogi dotyczące ochrony i poufności przetwarzanych danych. Aby im sprostać, wybrano technologię Platformy OChK w modelu chmury prywatnej. Wszystkie usługi Platformy OChK uruchamiane są na serwerach zlokalizowanych w Polsce, co daje gwarancję lokalnej rezydencji danych, a także właściwej redundantności. Platforma uwzględnia także zasady compliance i zapewnia pełną zgodność z polskimi regulacjami m.in. ochrony danych osobowych, bezpieczeństwa informacji i cyberbezpieczeństwa. Infrastruktura dla PGZ Stoczni Wojennej została rozlokowana w dwóch odseparowanych, niezależnych centrach danych OChK, na których zainstalowane zostały komponenty aplikacji CAD. Dodatkowym atutem architektury Platformy OChK są stosowane w niej mechanizmy bezpieczeństwa, w tym pełna separacja danych, zarządzanie tożsamością, szyfrowanie danych kluczami klienta czy złota kopia (Golden Copy), które razem zapewniają kompleksową ochronę przechowywanych danych i zwiększają odporność na nieprzewidziane zdarzenia.

Zaimplementowane środowisko pracy wykorzystuje także technologię zwirtualizowanego pulpitu (VDI) i jest wyposażone w wysokowydajne karty graficzne (GPU). Zastosowanie obu rozwiązań istotnie przyspiesza proces projektowania fregat oraz zapewnia każdej zaangażowanej w niego osobie dostęp do mocy obliczeniowej niezbędnej do pracy na dużych modelach projektowych. Jednocześnie wszystkie dane znajdują się w zabezpieczonej chmurze i nie są przetwarzane lokalnie na urządzeniach użytkowników końcowych.

Korzyści z wdrożenia

Zbudowanie środowiska IT na Platformie OChK pozwoliło PGZ Stoczni Wojennej znacznie szybciej rozpocząć realizację programu „Miecznik” poprzez sprawne uruchomienie aplikacji niezbędnych do projektowania okrętów. Wykorzystanie technologii chmury obliczeniowej nie tylko przyspiesza i unowocześnia proces, ale również usprawnia i ułatwia codzienną pracę osób zaangażowanych w projekt.

PGZ Stocznia Wojenna uzyskała dostęp do bardzo dużej mocy obliczeniowej, którą może elastycznie dopasowywać do bieżących potrzeb. Środowisko pracy projektantów jest odpowiednio zabezpieczone, wysoko dostępne i odporne na awarie. Zainstalowane na wydzielonej części Platformy OChK karty graficzne zagwarantowały projektantom bardzo wysoką wydajność. Wykorzystana zaś technologia wirtualizacji pulpitów pozwoliła współdzielić zasoby między projektantami i usprawnić ich pracę, przy równoczesnym zachowaniu odpowiednich standardów bezpieczeństwa.

PGZ Stocznia Wojenna uzyskała dostęp do bardzo dużej mocy obliczeniowej, którą może elastycznie dopasowywać do bieżących potrzeb. Środowisko pracy projektantów jest odpowiednio zabezpieczone, wysoko dostępne i odporne na awarie

Dzięki rozwiązaniom, takim jak Platforma OChK, firmy które działają w branży przemysłu ciężkiego, mogą sięgać po nowoczesne cyfrowe narzędzia, aby zwiększać efektywność pracy, poprawiać jakość wytwarzanych produktów oraz szybciej realizować założone cele.

Wspólna realizacja projektu nie zakończyła się na uruchomieniu środowiska. W kolejnych krokach zaplanowana została integracja aplikacji projektowej z innymi systemami działającymi w organizacji, m.in. z obrabiarkami CNC (będą one wytwarzać poszczególne elementy fregat bezpośrednio z dokumentacji projektowej) czy też z systemem ERP, co ułatwi zarządzanie całością produkcji, w tym łańcuchami dostaw.

Firma:
PGZ Stocznia Wojenna

Profil działalności firmy:
projektowanie, remonty, modernizacje i budowa okrętów

Wykorzystana chmura: Platforma OChK

Integrator: OChK

Nowoczesna technologia pomaga firmie VULCAN dostarczać usługi w modelu SaaS

Firma VULCAN, dostarczająca nowoczesne aplikacje w modelu SaaS dla sektora publicznego oraz edukacyjnego, wdrożyła rozwiązanie SigNoz do monitorowania poprawności działania usług oraz gromadzenia danych. Rozwiązanie korzysta z wysoko skalowalnego klastra Kubernetes, działającego na chmurze prywatnej Play Rozwiązania dla Biznesu, udostępnionej w ramach infrastruktury 3S Data Center – spółki należącej do Grupy Play.

VULCAN od ponad 35 lat dostarcza klientom z sektora edukacyjnego i publicznego nowoczesne rozwiązania, które sprawiają, że edukacja jest prostsza i przyjemniejsza, a szkoły nowoczesne i mądrze zarządzane. Bogate portfolio firmy wspiera procesy administracyjne, zarządcze, organizacyjne oraz finansowe, w tym budżetowe i kadrowo-płacowe. Zintegrowane środowisko pracy, łączące rozwiązania oferowane szkołom, samorządom czy centrom usług wspólnych, umożliwia swobodny przepływ danych pomiędzy nimi. Aplikacje skierowane do uczniów i ich rodziców pomagają zaś budować relację ze szkołą oraz śledzić postępy dzieci w nauce.

Cele wdrożenia

Projekt został powołany do życia z uwagi na chęć podniesienia SLA obsługi klientów, co było możliwe wyłącznie przez wdrożenie odpowiedniego narzędzia do monitorowania logów, metryk, trace'ów oraz identyfikacji błędów i awarii. Firma VULCAN potrzebowała narzędzia, które będzie potrafiło w skalowalnym środowisku analizować i prezentować ogromne ilości danych dochodzące do kilku milionów logów na minutę. Dotychczas stosowane rozwiązania nie zapewniały wystarczającej funkcjonalności i skalowalności. Co więcej, z uwagi na przetwarzanie dużej ilości danych, zasadne było podjęcie działań, których celem była optymalizacja wykorzystania zasobów pamięci masowej (storage), a w efekcie obniżenie kosztów utrzymywania usług. Graficzne panele podsumowań (dashboards), dzięki lepszej wizualizacji danych, miały zaś zapewnić administratorom przekrojowy, czytelny wgląd we wszystkie parametry działania usług.

Monitorowanie aplikacji z SigNoz

Do monitorowania poprawności działania aplikacji obsługiwanych w modelu SaaS wybrano system SigNoz. Narzędzie umożliwia identyfikację błędów oraz awarii przez pozyskiwanie metryk oraz trace'ów. Zebrane dane są przetwarzane, analizowane, porównywane i udostępniane w ramach jednego panelu webowego.

Aby zapewnić oczekiwaną wydajność i niezawodność, oprogramowanie wdrożone zostało na wysoce skalowalnym klastrze K8s Rancher SUSE z wykorzystaniem georedundantnej, chmurowej infrastruktury Play Rozwiązania dla Biznesu w ramach ośrodków 3S Data Center, będących częścią Grupy Play. Do 3S Data Center należy 6 rozproszonych geograficznie ośrodków przetwarzania danych.

Jacek Chylak
Dyrektor Handlowy, Play Rozwiązania dla Biznesu

Tak zaprojektowana infrastruktura pozwala firmie VULCAN bardzo dokładnie analizować przyczyny problemów w swoich aplikacjach, agregować dane śledzenia, filtrować logi i zapisy dzienników oraz tworzyć pulpity nawigacyjne powiązane z alertami w oparciu o atrybuty zawarte w rejestrach zdarzeń.

Architektura rozwiązania

Wdrożony system SigNoz składa się z następujących komponentów:

- wysokowydajnej, kolumnowej bazy danych OLAP ClickHouse, przeznaczonej do szybkiego przetwarzania ogromnych ilości danych,
- dedykowanego kolektora danych, przygotowanego przez producenta w oparciu o OpenTelemetry Collector, służącego do odbierania danych, parsowania oraz zapisywania ich w bazie ClickHouse,
- interfejsu Query Service między bazą danych a frontendem, odpowiedzialnego za wykonywanie zapytań generowanych przez użytkowników,

Krzysztof Mazurkiewicz
Dyrektor Pionu Produkcji, VULCAN

- interfejsu użytkownika zbudowanego w oparciu o ReactJS i Typescript, umożliwiającego przeglądanie i filtrowanie danych,
- menedżera alertów generującego ostrzeżenia wysyłane do użytkowników w zależności od zdefiniowanych reguł.

Dodatkowo, w rozwiązaniu SigNoz wdrożonym w modelu K8s uwzględnione zostały elementy pomocnicze: ClickHouse Operator, Zookeeper, OpenTelemetry Collector Metrics do zbierania metryk środowiska Kubernetes czy Schema Migrator, wykonującego niezbędne modyfikacje struktury bazy danych wraz z aktualizacjami system SigNoz.

System SigNoz uruchomiony został na wysoko skalowalnym rozwiązaniu opartym o klaster Kubernetes z wykorzystaniem RKE2. Klaster składa się z dwóch, odseparowanych od siebie środowisk: deweloperskiego oraz produkcyjnego.

W skład każdego klastra wchodzą role: control plane (host zarządzający pracą klastra), worker (hosty, na których deployowane są aplikacje) oraz rancher (zarządzanie klastrem z poziomu graficznego interfejsu). Za balansowanie ruchu HTTPS, kierowanie ruchu do aplikacji webowych rancher i do frontendu SigNoz oraz zapewnienie wysokiej dostępności odpowiada narzędzie HAProxy.

Dodatkowo, w ramach środowiska produkcyjnego dostępne są maszyny pomocnicze: Nagios do monitoringu elementów klastra oraz system kontroli wersji dla konfiguracji aplikacji znajdujących się na klastrach Gitea.

Dane aplikacji SigNoz w środowiskach deweloperskim i produkcyjnym zapisywane są w dedykowanym środowisku chmurowym firmy VULCAN, zlokalizowanym w georedundantnych ośrodkach data center, posiadających Certyfikaty ISO/IEC 27001:2022, 27017:2015 oraz 27018:2019.

Korzyści z wdrożenia

Dzięki wykorzystaniu skalowalnego środowiska opartego o K8s firmie VULCAN udało się stworzyć wysokodostępną platformę chmurową, korzystającą z rozproszonych geograficznie ośrodków przetwarzania danych. Zaprojektowana architektura gwarantuje wysoką dostępność i bezpieczeństwo, przy zachowaniu łatwości obsługi aplikacji po stronie deweloperów.

Z perspektywy technicznej, wykorzystanie hurtowni danych ClickHouse przyniosło mniejszą ilość danych zapisywanych w pamięci masowej przy uzyskaniu oczekiwanej, wysokiej wydajności. System SigNoz oferuje doskonałą funkcjonalność oraz szybkie generowanie raportów ad hoc na podstawie bardzo dużej ilości danych. Wysokiej jakości panele podsumowań (dashboards) ułatwiają zobrazowanie zachodzących procesów analitycznych. Wdrożone rozwiązanie zapewnia dużą ilość danych do obróbki analitycznej i informatyki „po awarii" przy zachowaniu niskiego kosztu utrzymania aplikacji (rozwiązanie open source).

Do głównych korzyści biznesowych zaliczyć można szybkość wykrywania anomalii i wąskich gardeł w aplikacjach, łatwość identyfikacji zagrożenia i awarii oraz możliwość analizy i monitorowania wydajności usług webowych w czasie rzeczywistym. Wdrożenie systemu SigNoz przyczyniło się do poprawy parametrów SLA dostarczanych aplikacji. Menedżerowie mają dostęp do analiz danych historycznych, które mogą wykorzystywać do analizy błędów i ciągłego rozwoju usług SaaS dostarczanych klientom końcowym.

Rozwiązanie zastosowane w firmie VULCAN to najprawdopodobniej pierwsze wdrożenie aplikacji SigNoz w Polsce z wykorzystaniem klastra K8s od SUSE Rancher, obsługiwanego w wielu ośrodkach przetwarzania danych w dedykowanej chmurze prywatnej Klienta.

Play Rozwiązania dla Biznesu zaoferowało firmie VULCAN oczekiwaną funkcjonalność i wydajność rozwiązania, które nie były osiągalne przez inne tego typu znane aplikacje przy założonym poziomie kosztów. Klaster K8s Rancher SUSE zapewnia ciągłość działania aplikacji oraz autoskalowanie zasobów w przypadku lawinowego zwiększania ilości logów w trakcie produkcyjnego dostarczania aplikacji w modelu SaaS.

Firma: VULCAN

Profil działalności firmy:
producent oprogramowania dla oświaty

Wykorzystana chmura: Play Rozwiązania dla Biznesu

Integrator: 3S Data Center

Katalog produktów chmurowych

Fot.: Freepik

Integrated Computing

Produkt: usługi chmury infrastrukturalnej

Dostawca/Producent: Integrated Solutions

Informacje: integratedsolutions.pl

Integrated Computing to chmura obliczeniowa zbudowana z wykorzystaniem najwyższej jakości infrastruktury IT i wirtualizacji klasy korporacyjnej. Dostawca oferuje klientom kompleksowe wsparcie integracyjne z naciskiem na zapewnienie najwyższego poziomu bezpieczeństwa. W portfolio firmy znajdują się usługi zapasowego centrum danych (Disaster Recovery), wirtualizacji baz danych Oracle oraz wdrażania dedykowanych chmur prywatnych.

W ramach chmury Integrated Computing dostarczane są gotowe do użycia platformy według ustandaryzowanego katalogu usług. Na życzenie klienta istnieje możliwość zbudowania i wdrożenia indywidualnego, współdzielonego lub dedykowanego środowiska obliczeniowego. Usługa świadczona jest z centrów danych Orange zlokalizowanych w Polsce.

Dostawca realizuje projekty hybrydowe będące połączeniem Integrated Computing z chmurą prywatną (w lokalizacji klienta lub Data Center Orange), a także z chmurami publicznymi (GCP, AWS, MS Azure). Zapewnia integrację z operatorskimi usługami z zakresu cyberbezpieczeństwa (DDoS Protection oparty na routerach sieci szkieletowej, WAF, SOC/SIEM) oraz łączności (Internet, MPLS, APN w sieci mobilnej, dedykowane łącza). Bogaty katalog usług i funkcjonalności (wirtualne sieci i routery, dyski wirtualne o różnych profilach wydajności, backup, monitoring, DRaaS) dostępny jest z jednej konsoli administracyjnej.

Bezpieczna chmura

Integrated Solutions zapewnia bezpieczeństwo i ciągłość działania zasobów uruchamianych w chmurze dzięki zaangażowaniu własnych zespołów CERT i SOC oraz integracji wdrażanych rozwiązań z sieciowymi usługami cyberbezpieczeństwa, w tym DDoS Protection na poziomie sieci szkieletowej.

Bezpieczeństwo i poufność danych klientów gwarantuje szyfrowanie sprzętowe danych na poziomie macierzy, zintegrowany system backupu oraz możliwość powołania zapasowego centrum danych (DRaaS). Usługi chmurowe oferowane przez Integrated Solutions zapewniają zgodność z wymaganiami RODO w chmurze oraz objęte są certyfikacjami ISO 27018 Ochrona Danych Osobowych w Chmurze, ISO 27001 System Zarządzania Bezpieczeństwem Informacji, ISO 22301 Zarządzanie Ciągłością Działania oraz FIPS 140-2.

Podstawowe usługi chmury infrastrukturalnej (IaaS) Integrated Computing uzupełnione zostały o katalog preinstalowanych systemów operacyjnych, gotowe rozwiązanie Disaster Recovery (DRaaS), mechanizmy automatycznej kopii zapasowej oraz wsparcie dla baz danych Oracle. Integrated Solutions dostarcza licencje firm Microsoft, SUSE, RedHat, Oracle, MicroFocus.

Jednocześnie, w ramach usług chmury infrastrukturalnej (IaaS), bez dodatkowych opłat dostępne są:

- transfer danych do/z internetu,
- zestaw narzędzi sieciowych (takich jak VPN IPSec),
- monitoring zasobów chmurowych z gotowym zestawieniem wykresów.

Poza abonamentowym modelem rozliczeń, klientom oferowany jest model Pay-as-You-Go, w którym nie tworząc zasobów, nie ponosi się żadnych opłat.

Usługi wspomagane są wysokimi kompetencjami integratorskimi w ramach centrów kompetencji IT (infrastruktura, chmura, bezpieczeństwo). Dostawca zapewnia wsparcie dla aktywacji, migracji, utrzymania rozwiązań zapewniających ciągłość działania. Prowadzi też program edukacyjny (webinaria, wideo przewodnik, artykuły, seria wideocastów

„Porozmawiajmy o chmurze") mający na celu podnoszenie wiedzy i umiejętności administratorów.

Skalowalna infrastruktura

Usługi chmurowe dostarczane są z centrum danych Orange. Firma wspiera się dojrzałymi, wiodącymi na świecie technologiami: VMware Cloud Director w obszarze wirtualizacji, platformą sprzętową opartą o serwery HPE Synergy, procesorami Intel Platinum i macierzami HPE 3PAR oraz najnowocześniejszymi rozwiązaniami umożliwiającymi działanie według idei Software Defined Data Center. W ramach centrum danych wdrożone zostały i rozwijane są najlepsze praktyki związane z architekturą i zarządzaniem rozwiązaniami typu multi-tenant.

Usługa zrealizowana jest w oparciu o serwery typy blade i hybrydowe macierze blokowe o wysokiej wydajności. Rozwiązanie ma zdolność do szybkiego uruchamiania projektów o bardzo dużej skali zasobów IT rzędu dziesiątek tysięcy vCPU, dziesiątek TB pamięci operacyjnej i petabajtów storage'u. Chmura Integrated Computing wspiera skalowanie wzwyż (CPU/RAM/storage Hot-Add, bardzo wysokie maksymalne rozmiary VM) i wszerz (model Pay as You Go, zarządzanie szablonami VM).

Zasoby dyskowe zapewniają wydajność oczekiwaną przez najbardziej wymagające systemy, do ponad 100k IOPS. Zastosowana infrastruktura umożliwia płynne skalowanie zasobów maszyn wirtualnych (do 128 vCPU i 1500 GB RAM w jednej maszynie), rezerwację pełnej mocy procesora dla klienta (dedykowany CPU bez współdzielenia) czy uruchomienie dedykowanej infrastruktury dla baz danych Oracle, spełniającej warunki licencji on-premise.

W zakresie ochrony danych stosowane są najwyższej klasy systemy kopii zapasowej wykorzystujące zaawansowane rozwiązania do deduplikacji danych.

Dostawca oferuje wsparcie przy wdrażaniu najnowszych technik automatyzacji IT (DevOps) i konteneryzacji (Kubernetes) u klienta, aby wykorzystać pełnię możliwości chmury.

Chmura Integrated Computing jest częścią kompleksowych usług dostarczanych przez Integrated Solutions. W wersji standardowej zasoby chmury dostępne są natychmiast, choć istnieje możliwość zaprojektowania i udostępnienia rozwiązania ściśle dopasowanego do potrzeb klienta.

Chmura zapewnia pełną interoperacyjność z innymi usługami infrastrukturalnymi i sieciowymi (kolokacja, sieci WAN, łącza transmisyjne, Internet, usługi cyberbezpieczeństwa). Orange posiada najbardziej rozbudowaną, stale rozwijaną sieć dostępową w Polsce, co pozwala dotrzeć z usługami do większości firm w kraju. Chmura Integrated Computing działa bezawaryjnie od 2012 roku, a kompleksowe podejście do jej świadczenia spowodowało, że większość klientów decyduje się na kontrakty powyżej 3 lat.

Kluczowe cechy:

- bogaty katalog usług i funkcjonalności dostępny z jednej konsoli administracyjnej,
- wysoka wydajność platformy sprzętowej ze skalowaniem wzwyż i wszerz,
- lokalizacja danych w Polsce,
- SLA na poziomie 99,95%,
- zespoły CERT i SOC dbające o bezpieczeństwo danych,
- brak opłat za transfer danych z/do chmury,
- certyfikaty ISO 27001, 27018, 22301,
- dedykowane środowisko dla baz danych Oracle,
- aktualność środowiska (VMware Cloud Director 10).

Klienci i wdrożenia: Rida Software, Alsseco, Femion, Bunasta, SDT, polski oddział Grupy Van Der Vlist, Silekol, Winezja, Tous Poland.

Dla firm

orange™

tu jest

Zatrudnij naszą chmurę

w swojej firmie

INTEGRATED SOLUTIONS

Twoje aplikacje w bezpiecznym środowisku wirtualnym Integrated Computing

- Data Center klasy Tier III+ zlokalizowane w Polsce.
- Wsparcie ekspertów w projektach – architektura, migracja, automatyzacja.
- VMware Cloud Director – czołowa platforma i pionier wirtualizacji.
- Własne zespoły CERT i SOC dbające o bezpieczeństwo danych.
- Chmura odpowiednia do przetwarzania danych osobowych – zgodna z ISO 27018.
- Integracja z usługami IP VPN/MPLS.
- Bezpłatny transfer danych do internetu.

Zapraszamy do kontaktu

Zeskanuj nasz kod QR i dowiedz się więcej o usłudze

orange.pl/duze-firmy/cloud

Platforma OChK

Produkt: usługi chmury infrastrukturalnej

Dostawca/Producent: OChK

Informacje: platformaochk.pl

Platforma OChK to chmura publiczna zbudowana od podstaw i zarządzana przez zespół wewnętrznych ekspertów firmy w modelu security by design. Jej elastyczna architektura umożliwia dostosowywanie oferowanych usług do niestandardowych projektów oraz specyficznych wymogów organizacji. Zapewnia kompleksowe bezpieczeństwo danych i pełną geograficzną redundancję zasobów, a także umożliwia automatyzację zarządzania zasobami z kodu (IaC), wspomagając procesy DevOps. Jej użytkownicy mają zapewnione wsparcie zespołu OChK w trybie 24/7, wraz z monitoringiem bezpieczeństwa (SOC).

Platforma OChK pozwala na budowanie całej gamy rozwiązań – od chmury publicznej przez środowiska hybrydowe i wielochmurowe (multicloud) po chmurę prywatną. Sposób jej wykorzystania w dużej mierze zależy od specyfiki realizowanych projektów. Niezależnie od wybranego modelu, umożliwia ona skalowanie biznesu, maksymalizację efektywności środowiska IT oraz optymalizację kosztów. Dostawca, dzięki wsparciu lokalnego zespołu, zapewnia indywidualną konfigurację usług – bardziej spersonalizowaną, niż w przypadku rozwiązań hyperscalerów.

Przeznaczenie i zastosowania Platformy OChK

Platforma OChK przeznaczona jest dla organizacji, które:

- potrzebują spersonalizowanego rozwiązania, zapewniającego im niezależność i umożliwiającego zmianę dostawcy komponentów infrastruktury,
- chcą optymalizować koszty środowiska IT przez łączenie różnych technologii chmurowych i zasobów on-premise w modelach wielochmurowych (multicloud) oraz hybrydowych,
- chcą zautomatyzować i usprawnić procesy zarządzania infrastrukturą chmurową, w tym z wykorzystaniem kodu (IaC),
- potrzebują kompleksowego wsparcia technicznego lokalnych ekspertów 24/7,
- ze względu na wymogi regulacyjne muszą przechowywać i przetwarzać dane (wszystkie lub ich część) wyłącznie na terenie Polski,
- oczekują najwyższego poziomu audytowalności i bezpieczeństwa, w tym zgodności z normami ISO w tym zakresie.

Jako chmura publiczna, Platforma OChK stanowi kompletną, wydajną i skalowalną platformę usług chmurowych, która zbudowana jest na niezależnych stosach technologicznych VMware i Openstack. Z kolei w modelu chmury prywatnej działa jako warstwa orkiestratora, która uzupełnia środowisko wirtualizacji on-premise o funkcje stosowane w chmurach publicznych. Umożliwia to zmianę wirtualizatora bez wpływu na procesy zarządzania środowiskiem.

Zastosowanie Platformy OChK jako chmury hybrydowej pozwala z kolei na podłączenie do niej środowiska lokalnego i wspólne zarządzanie zasobami zarówno w chmurze, jak i on-premise, za pośrednictwem portalu lub Terraform. Wreszcie, może również pełnić rolę zapasowego centrum danych (Disaster Recovery Center), chroniąc dane i procesy organizacji w przypadku awarii.

Dzięki tej wielozadaniowości, Platforma OChK spełnia oczekiwania wielu firm niezależnie od tego, jak definiują swoje potrzeby oraz na bazie jakiej technologii chcą budować swoją infrastrukturę.

Innowacyjność rozwiązania

Na tle konkurencyjnych rozwiązań Platforma OChK wyróżnia się kilkoma cechami. Dzięki temu, że wszystkie usługi Platformy OChK uruchamiane są na serwerach w centrach danych zlokalizowanych na terytorium RP, jej użytkownicy otrzymują gwarancję rezydencji swoich danych w kraju, a także ich właściwej redundantności. Jest to szczególnie istotne dla zachowania ciągłości działania organizacji, stałego dostępu do danych, a także możliwości łatwego i szybkiego odtworzenia ich w razie awarii lub ataku. Atutem Platformy OChK jest także lokalny zespół oraz know-how. Dostawca dzieli się wiedzą ekspercką zgromadzoną podczas realizacji licznych projektów

chmurowych i zapewnia pomoc zespołów: wsparcia, utrzymania i SOC, w trybie 24/7.

Kolejną zaletą Platformy OChK jest zapewnienie bezpieczeństwa i zgodności regulacyjnej. Odpowiada ona m.in na wymogi RODO i tzw. komunikatu chmurowego UKNF. Stosowane w architekturze Platformy OChK i dostępne w jej ramach mechanizmy oraz usługi bezpieczeństwa (m.in. pełna separacja danych, zarządzanie tożsamością, szyfrowanie danych kluczami klienta, złota kopia czy Security Operations Center), zapewniają kompleksową ochronę przechowywania i przetwarzania danych oraz zwiększają odporność organizacji na nieprzewidziane zdarzenia. Dostawca wdrożył, utrzymuje i doskonali Zintegrowany System Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania, regularnie recertyfikowany na zgodność z międzynarodowymi normami: ISO 27001, ISO 22301, ISO 27017, ISO 27018.

Platforma OChK umożliwia wykorzystanie Terraform i mechanizmów konfigurowania infrastruktury kodem (Infrastructure as Code). Pozwala to na bezpieczne zarządzanie zasobami, ich szybkie powoływanie i pomiar wykorzystania (metering) oraz szybkie automatyzowanie powtarzalnych procesów. Wdrożenie najlepszych praktyk FinOps, m.in. możliwości monitorowania kosztów w czasie rzeczywistym oraz właściwej konfiguracji uprawnień, alertów, buforów i środowisk testowych, przekłada się z kolei na optymalizację środowiska chmurowego i redukcję zbędnych kosztów.

W dbałości o niezależność technologiczną i komfort klientów, OChK umożliwia też zmianę wirtualizatora, dzięki czemu unikają oni niedogodności i ryzyk związanych, np. ze zmianami w modelu licencyjnym, a w konsekwencji koniecznością migracji do innej technologii. Dodatkowo, niezależnie od liczby wykorzystywanych rozwiązań, wszystkie zasoby IT, w tym uruchamiane lokalnie (on-premise), mogą być obsługiwane z poziomu jednej aplikacji. Podejście to zapewnia wyższy poziom bezpieczeństwa zasobów, a także znacznie ułatwia ich monitorowanie i zarządzanie nimi.

Przejrzysty i przyjazny interfejs panelu administratora, intuicyjne powoływanie zasobów IaaS czy precyzyjne zarządzanie uprawnieniami użytkowników sprawia, że praca na Platformie OChK jest prosta, maksymalnie zautomatyzowana i efektywna.

Chmura na własnych zasadach

Platforma OChK to kompleksowe, autorskie rozwiązanie zbudowane i rozwijane przez zespół inżynierek i inżynierów OChK. Jest wielozadaniowa i elastyczna, dzięki czemu można dostosować ją do specyficznych potrzeb i wymagań organizacji, nawet w zakresie zbudowania chmury prywatnej na infrastrukturze klienta. Wykorzystując technologię OChK organizacje mogą uniezależnić się od dostawców rozwiązań wirtualizacyjnych. Z perspektywy efektywności kosztowej, chroni to użytkowników także przed ponoszeniem nieprzewidzianych opłat. Wszystkie usługi Platformy OChK realizowane są z wykorzystaniem jednego intuicyjnego interfejsu użytkownika (GUI) oraz rozbudowanego API, które pozwala zautomatyzować zarządzanie infrastrukturą zgodnie z koncepcją Infrastructure as Code (IaC). Umożliwia to zachowanie takich samych standardów zarządzania zasobami, jak w chmurach publicznych globalnych dostawców. Przyjęte standardy bezpieczeństwa pozwoliły stworzyć produkt, który umożliwia klientom przyspieszenie realizacji celów biznesowych, a jednocześnie gwarantuje ciągłość działania.

Wdrożenia i klienci: PGZ Stocznia Wojenna, PKO Bank Polski, KIR.

Chmura obliczeniowa Oktawave

Produkt: usługi chmury infrastrukturalnej

Dostawca/Producent: Oktawave

Informacje: oktawave.com

Publiczna chmura obliczeniowa Oktawave pozwala na uruchamianie i przechowywanie zasobów w trzech certyfikowanych centrach w Polsce. Geograficzne rozproszenie miejsc przetwarzania danych, przy zastosowaniu odpowiednich narzędzi, gwarantuje wysoką dostępność, skalowalność i bezpieczeństwo dostarczanych usług IaaS/PaaS.

Oktawave to polska publiczna chmura obliczeniowa zapewniająca dostęp do rozwiązań o dużej skalowalności i wysokiej dostępności, do 99,99%. W ramach chmury Oktawave możliwe jest uruchamianie, przetwarzanie i przechowywanie dowolnych zasobów w postaci serwisów e-commerce, aplikacji biznesowych, rozwiązań korporacyjnych czy systemów IT. Usługi dostarczane są z trzech centrów danych w dwóch regionach dostępności zlokalizowanych na terenie Polski. Bezpieczeństwo rozwiązania potwierdzają certyfikaty CSA STAR, ISO 27001, ISO 22301, ISO 27017, ISO 27018 i PCI DSS. Chmura spełnia wymagania KNF, a także zapewnia zgodność z regulacjami RODO.

Filarem platformy chmurowej jest zaawansowana technologia, która współpracuje z większością systemów operacyjnych, w tym Linux, Microsoft Windows i FreeBSD. Zastosowana architektura umożliwia instalację dowolnych aplikacji open source oraz klasy korporacyjnej (SQL Server, SAP). W ramach infrastruktury dostępny jest szereg kompatybilnych ze standardami branżowymi narzędzi, które pozwalają na szybką automatyzację procesów CI/CD.

Usługi i zasoby

Oktawave Cloud Instance (OCI) to serwer wirtualny zapewniający skalowalną moc obliczeniową do budowy i rozwoju serwisów, aplikacji internetowych i dowolnych systemów użytkownika. Dzięki funkcji autoskalera, parametry OCI automatycznie dostosowują się do bieżącego zapotrzebowania na moc obliczeniową. Dane użytkowników przechowywane są w dyskowej pamięci masowej Oktawave Volume Storage (OVS), która zapewnia pięć poziomów wydajności od 1000 do 200 000 IOPS. Dzięki wykorzystaniu rozbudowanych, wielopoziomowych migawek możliwe są testy wielu wersji aplikacji jednocześnie, przy zachowaniu funkcji powrotu do stanu wyjściowego.

Oktawave Cloud Storage (OCS) to ekonomiczny system przechowywania i obsługi dużych ilości danych, w pełni zgodny z OpenStack SWIFT oraz Amazon S3. Rozwiązanie udostępnia przyjazny interfejs HTTP/API. Dzięki rozbudowanym mechanizmom kontroli dostępu do obiektów, możliwa jest pełna kontrola nad zasobami, czyli dokładne wskazanie kto, kiedy i na jakich prawach uzyska dostęp do odczytu lub zapisu określonych danych. Dostępna jest również funkcja wersjonowania danych. Automatyczne zarządzanie ruchem sieciowym, w zależności od stanu aplikacji i centrum danych umożliwia narzędzie Oktawave Traffic Manager.

Z kolei Oktawave Kubernetes to dedykowane wdrożenia środowisk Kubernetes w infrastrukturze chmurowej Oktawave. Każdy klaster Kubernetes budowany jest w architekturze wysokiej dostępności (HA), a pełna odpowiedzialność za jego działanie spoczywa na dostawcy chmury.

Wysoka dostępność

Platforma dostarcza narzędzia ułatwiające tworzenie lokalnych lub geograficznie rozproszonych środowisk wysokiej dostępności. Oprócz standardowych usług, takich jak wirtualna infrastruktura, chmura Oktawave oferuje zaawansowane rozwiązania z zakresu dystrybucji ruchu między wieloma serwerami OCI (load balancing) oraz zarządzania adresami IP, które mogą być dowolnie migrowane między OCI lub całymi subregionami (Floating IP). Skuteczne zarządzenie ruchem między geograficznie odległymi centrami danych obsługiwane jest przy pomocy narzędzia Oktawave Traffic Manager.

Chmura umożliwia zaawansowane zarządzanie Disaster Recovery Center (DRC) poprzez integrację z Disaster Recovery as a Service (DRaaS). Uruchomienie zapasowego ośrodka przetwarzania może być zautomatyzowane za pomocą w pełni zgodnego z Oktawave oprogramowania Terraform. Rozwiązania pozwalające na zarządzanie ruchem (Oktawave DNS) i monitorowanie dostępności aplikacji (Oktawave Watch) potrafią automatycznie i samodzielnie podjąć decyzję o uruchomieniu DRC i przekierować do niego ruch w sytuacji poważnej awarii. Z kolei rozproszenie geograficzne regionów obliczeniowych Oktawave (Warszawa i Kraków) zapewnia ochronę przed

incydentami lokalnymi, takimi jak katastrofy naturalne w obrębie jednego centrum danych.

Kierunek: rozwój

Chmura Oktawave wykorzystuje zaawansowane technologie podążając w kierunku rozwoju opartego na zasadach DevOps oraz praktykach CI/CD. Podejście to umożliwia szybkie dostarczanie aktualizacji, bez narażania na ryzyko utraty danych czy wystąpienia przestojów w działaniu usług.

W ramach IPCEI-CIS Oktawave otrzymało zgodę Komisji Europejskiej oraz Narodowego Centrum Badań i Rozwoju na dofinansowanie projektu chmury nowej generacji. Dotacja zostanie przeznaczona na rozwój platformy i opracowanie technologii kryptograficznego zabezpieczenia przetwarzania danych w chmurze, technologii przechowywania danych równolegle u wielu dostawców chmur oraz technologii do autentykacji danych między różnymi dostawcami. Uzyskane wsparcie potwierdza chęć dalszych inwestycji w nowoczesne technologie oraz środki zapewniające najwyższe standardy bezpieczeństwa, co pozwoli sprostać rosnącym wymaganiom klientów.

Korzyści: wdrożenie usług chmurowych

Implementacja chmury obliczeniowej Oktawave pozwala przedsiębiorstwom na znaczną poprawę efektywności operacyjnej oraz bezpieczeństwa infrastruktury IT. Gwarantowana dostępność na poziomie 99,99% oraz rozproszenie geograficzne centrów danych zapewniają nieprzerwane działanie aplikacji i usług. Oktawave spełnia wymagania KNF i RODO oraz posiada certyfikaty CSA STAR, ISO 27001, ISO 22301, ISO 27017, ISO 27018 i PCI DSS, co gwarantuje pełne bezpieczeństwo danych niezależnie od sektora działalności firmy. Organizacje mogą łatwo skalować zasoby obliczeniowe w zależności od bieżących potrzeb, co umożliwia optymalne zarządzanie kosztami i zasobami IT. Narzędzia zgodne ze standardami branżowymi pozwalają na szybką automatyzację procesów CI/CD, przyspieszając wdrażanie nowych aplikacji i usług oraz skracając czas ich wprowadzenia na rynek. Funkcje takie jak Oktawave Traffic Manager, Load Balancing oraz Floating IP umożliwiają efektywne zarządzanie ruchem między serwerami i centrami danych, zapewniając wysoką dostępność i bezpieczeństwo aplikacji.

Platforma wspiera większość systemów operacyjnych i umożliwia instalację dowolnych aplikacji open source oraz klasy korporacyjnej, co pozwala na dostosowanie infrastruktury do specyficznych potrzeb biznesowych i elastyczność technologiczną. Dodatkowo, funkcja autoskalera i ekonomiczny system przechowywania danych Oktawave Cloud Storage umożliwiają optymalizację kosztów związanych z infrastrukturą IT, dzięki płatności tylko za rzeczywiście wykorzystane zasoby. Integracja z Disaster Recovery as a Service (DRaaS) oraz zaawansowane narzędzia monitorowania i zarządzania ruchem zapewniają szybką i skuteczną reakcję na awarie, minimalizując czas przestoju i ryzyko utraty danych.

Kluczowe cechy:

- branżowe certyfikacje centrów danych,
- zgodność z wymaganiami KNF i RODO,
- ultraszybka infrastruktura chmury obliczeniowej, z wysoko wydajnymi oraz elastycznymi maszynami wirtualnymi i obiektową pamięcią masową,
- wysoka izolacja zasobów obliczeniowych między klientami,
- możliwość uruchomienia niemal dowolnego systemu operacyjnego,
- całodobowe wsparcie inżynieryjne, w aspektach technicznych i formalnych,
- intensywny rozwój platformy w zakresie innowacyjnych rozwiązań bezpieczeństwa.

Wdrożenia i klienci:

Vision Express, Burda, Goldenline, Comp, Fru, Skycash, Mobiltek, Avis

SUPREMIS Cloud Platform

Produkt: usługi chmury infrastrukturalnej

Dostawca/Producent: SUPREMIS

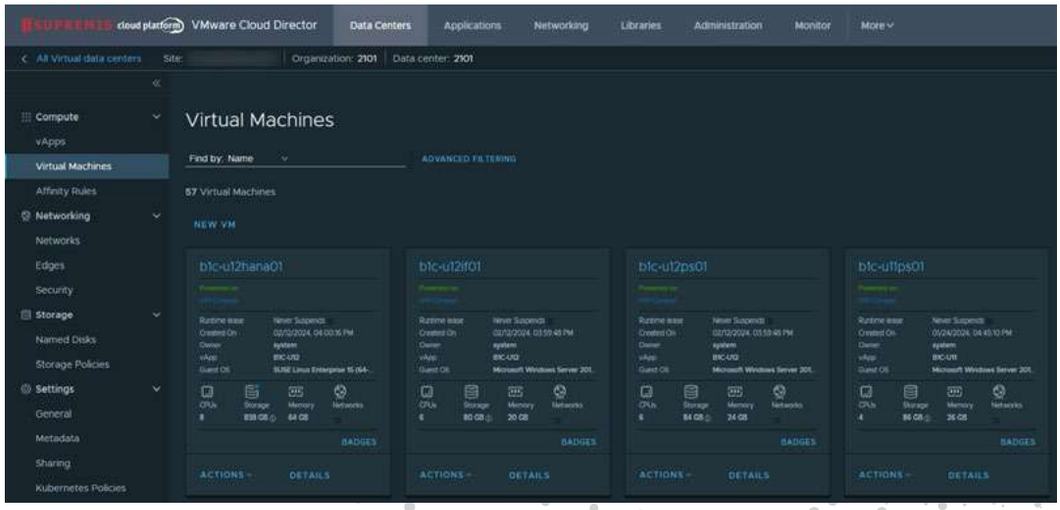
Informacje: supremis.pl

SAP Business One SAP S/4HANA Cloud

SUPREMIS Cloud Platform to prekursor usługi chmurowej dla SAP Business One oraz SAP HANA w Polsce. Skalowalne, certyfikowane przez SAP, środowisko pozwala firmom zrealizować dowolny scenariusz biznesowy – samodzielnie lub ze wsparciem wykwalifikowanych inżynierów.

SUPREMIS Cloud Platform to zaawansowane rozwiązanie chmurowe, zaprojektowane z myślą o zapewnieniu firmom najwyższego poziomu usług. Platforma wyróżnia się niezawodnością, wydajnością i bezpieczeństwem danych. Zbudowana z dbałością o każdy szczegół oferuje ciągłość pracy dzięki wielowarstwowej redundancji elementów środowiska fizycznego. Bezpieczeństwo i elastyczność usług sprawiają, że jest to idealne rozwiązanie zarówno dla małych środowisk IT jak i dla dużych przedsiębiorstw klasy korporacyjnej, poszukujących niezawodnej platformy chmurowej.

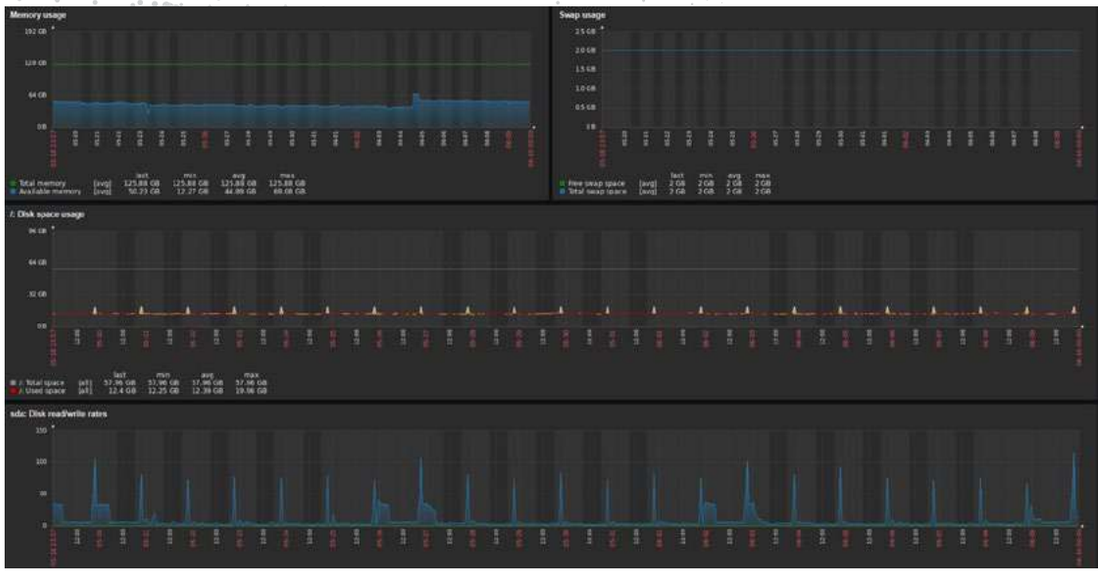
Platforma wyspecjalizowana jest w dostarczaniu infrastruktury dla systemów ERP, takich jak SAP oraz wysokowydajnych baz danych. SUPREMIS Cloud Platform zapewnia pełny stos usług chmurowych: SaaS, PaaS oraz IaaS. Oferując usługi chmurowe w modelach klasycznym i hybrydowym, SUPREMIS dostosowuje się do różnorodnych potrzeb biznesowych, umożliwiając wybór modelu chmury obliczeniowej jako aplikacji, platformy lub infrastruktury. Jednocześnie to model infrastrukturalny (IaaS, Infrastructure as a Service) zapewnia klientom największe możliwości zastosowań w obsłudze aplikacji biznesowych.



Chmura dla SAP

Wyróżnikiem SUPREMIS Cloud Platform na tle konkurencyjnych rozwiązań pozostaje wyspecjalizowana infrastruktura spełniająca certyfikację SAP dla bardzo wydajnych baz danych SAP HANA. Środowisko idealnie nadaje się do obsługi rozwiązań ERP takich jak SAP Business One, SAP S/4HANA oraz innych aplikacji spoza ekosystemu SAP. Partnerstwo na poziomie Gold z firmami SAP oraz Microsoft zapewniają dostęp do licencji w modelach subskrypcyjnych, a elastyczność serwisu pozwala klientom na samodzielną administrację środowiskiem chmurowym lub zlecanie obsługi inżynierom SUPREMIS. Niebagatelną zaletą oferty jest możliwość skorzystania z największej liczby certyfikowanych konsultantów SAP pokrywających pełne portfolio ERP: SAP Business One, SAP S/4HANA, SAP Business ByDesign.

SUPREMIS Cloud Platform zapewnia zasoby obliczeniowe bez konieczności inwestowania we własny sprzęt. Administratorzy mogą elastycznie



zarządzać zasobami, wdrażać maszyny wirtualne, skalować moc obliczeniową. To idealne rozwiązanie dla firm, które potrzebują niezawodnej i skalowalnej platformy do obsługi swoich aplikacji i zasobów IT.

W rezultacie SUPREMIS Cloud Platform daje możliwość i szansę mniejszym firmom konkurować z większymi dzięki dostępowi do technologii, która byłaby poza ich zasięgiem w modelu on-premise. Dużym firmom model IaaS daje zaś poczucie pełnego bezpieczeństwa oraz możliwość skupienia się na budowaniu przewagi rynkowej, bez spoglądania na sprawy techniczne.

Niezawodność i bezpieczeństwo

Klienci SUPREMIS korzystają z szerokiego wachlarza usług dostosowanych do indywidualnych potrzeb. Priorytetem dla dostawcy pozostaje bezpieczeństwo danych. Wszystkie dane chronione są politykami kopii zapasowych, co zapewnia ich ochronę przed utratą. Dodatkowo, środowisko monitorowane jest w czasie rzeczywistym, aby wykryć ewentualne zagrożenia i podjąć natychmiastową reakcję na nie. Dane pozostają bezpieczne, a firmy mogą skupić się na rozwijaniu biznesu.

Każdy element środowiska fizycznego jest zwielokrotniony, co gwarantuje ciągłość pracy. W przypadku awarii dowolnego z komponentów, system automatycznie przełącza się na zapasowy, minimalizując ewentualne przestoje. To kluczowe dla firm, które wymagają nieprzerwanej dostępności swoich aplikacji i danych.

SUPREMIS Cloud Platform oferuje szereg zalet, które mogą pomóc organizacjom w likwidacji długu technologicznego związanego z infrastrukturą on-premise. Zmniejsza to wydatki kapitałowe, zwiększa elastyczność i dostępność, poprawia bezpieczeństwo i ułatwia współpracę. Dodatkowo zapewnia organizacjom dostęp do najnowszych technologii i pomaga w spełnieniu wymagań w zakresie zgodności z przepisami, poprawie efektywności energetycznej i zmniejszeniu śladu węglowego.

Łatwe wdrożenia z chmurą

Elastyczność SUPREMIS Cloud Platform pozwoliła dostawcy wyspecjalizować się w dużych i trudnych wdrożeniach. W wielooddziałowej firmie, operującej w wielu krajach Europy, wykorzystanie platformy SUPREMIS umożliwiło centralizację zarządzania przedsiębiorstwem, a zastosowane narzędzia analityczne przyczyniły się do bardziej świadomego planowania.

Wdrożenie w oparciu o SUPREMIS Cloud Platform dla światowego potentata z branży spożywczej pozwoliło osiągnąć bezawaryjną pracę produkcyjną oraz zapewnić odpowiedni poziomu wydajności dla ogromnej ilości danych. Z kolei wdrożenie usług infrastrukturalnych SUPREMIS w branży nieruchomości umożliwiło klientowi zintegrowane zarządzanie nieruchomościami komercyjnym oraz przyśpieszało i zautomatyzowało raportowanie giełdowe oraz dla zarządu firmy.

Kluczowe cechy

- wyspecjalizowana infrastruktura chmurowa dla systemów ERP,
- dedykowana do obsługi aplikacji SAP (SAP Business One, SAP S/4HANA),
- wielowarstwowa redundancja elementów środowiska fizycznego,
- dostęp do licencji SAP i Microsoft w modelach subskrypcyjnych,
- bezkompromisowe bezpieczeństwo danych,
- certyfikowani konsultanci SAP.

Exea Data Center SIRP (Security Incident Response Platform)

Produkt: platforma zarządzania incydentami bezpieczeństwa

Dostawca/Producent: Exea Data Center

Informacje: exea.pl

Exea SIRP to zaawansowana platforma zapewnienia cyberbezpieczeństwa, która z jednego miejsca oferuje kompleksowy wgląd w stan zabezpieczeń sieci, systemów i danych organizacji. Rozwiązanie przeznaczone jest dla zespołów odpowiedzianych za ochronę, pomagając im w codziennej pracy związanej z reagowaniem na incydenty bezpieczeństwa.

Wiele organizacji zmaga się z brakiem odpowiedniego narzędzia do opisu i obsługi incydentów bezpieczeństwa. Najczęściej stosowaną praktyką jest korzystanie z systemów zgłoszeniowych, ale ich funkcjonalność często nie spełnia potrzeb w tym zakresie. Aby wypełnić lukę na rynku, Exea Data Center opracowała dedykowaną platformę, która zapewnia kompleksowe podejście do zarządzania incydentami bezpieczeństwa.

Centrum zarządzania incydentami

Platforma Exea SIRP składa się z dwóch głównych modułów: Panelu zespołu cyberbezpieczeństwa oraz Panelu klienta. Panel zespołu cyberbezpieczeństwa oferuje widoki inwentaryzacji organizacji, alertów bezpieczeństwa i obsłużonych incydentów. Zawiera dedykowane moduły do obsługi różnego typu komunikatów oraz bieżącej pracy związanej z ochroną organizacji przed cyberzagrożeniami.

Platforma SIRP zasilana jest automatycznie alertami z systemu SIEM, a więc narzędzia służącego do monitorowania, analizy i raportowania zdarzeń związanych z bezpieczeństwem informatycznym w organizacji. Alerty pobierane są za pomocą wbudowanego interfejsu API i zapisywane w bazie danych. Platforma sprawdza, czy dany komunikat wystąpił wcześniej jako incydent bezpieczeństwa. Jeśli nie, tworzony jest nowy przypadek (case) do obsłużenia przez administratorów.

Każdy komunikat weryfikowany jest przez zespół cyberbezpieczeństwa, który klasyfikuje go jako True Positive lub False Positive. Analityk bezpieczeństwa może przypisać osobę odpowiedzialną za obsługę danego incydentu oraz oznaczyć, czy wymaga ona podjęcia standardowej, czy szybkiej reakcji. Platforma umożliwia współpracę całego zespołu i dokumentowanie podejmowanych działań w jednym, dedykowanym miejscu. Pozwala na wspólne tworzenie notatek, wysyłanie powiadomień do klienta oraz tworzenie zgłoszeń w systemie ticketowym.

Każdy incydent bezpieczeństwa może zostać wzbogacany przez analityków bezpieczeństwa o nowe informacje z wykorzystaniem danych z zewnętrznych baz IoC (Indicators of Compromise). SIRP zintegrowana jest z kilkudziesięcioma zewnętrznymi bazami IoC, co pozwala na uzyskanie jak największej ilości informacji o potencjalnym atakującym. Podejście to ułatwia odkrycie źródła ataku, technik oraz metod jego przeprowadzenia, co jest niezbędne w procesie mitygacji nowych zagrożeń.

Platforma pozwala również na ręczne tworzenie incydentów bezpieczeństwa, jeśli nie zostały one wygenerowane automatycznie, a następnie postępowanie z nimi w podobny sposób, jak z alertami pochodzącymi z systemu SIEM. Jednocześnie, oprogramowanie gromadzi potwierdzone i zweryfikowane IoC na podstawie pracy analityków bezpieczeństwa.

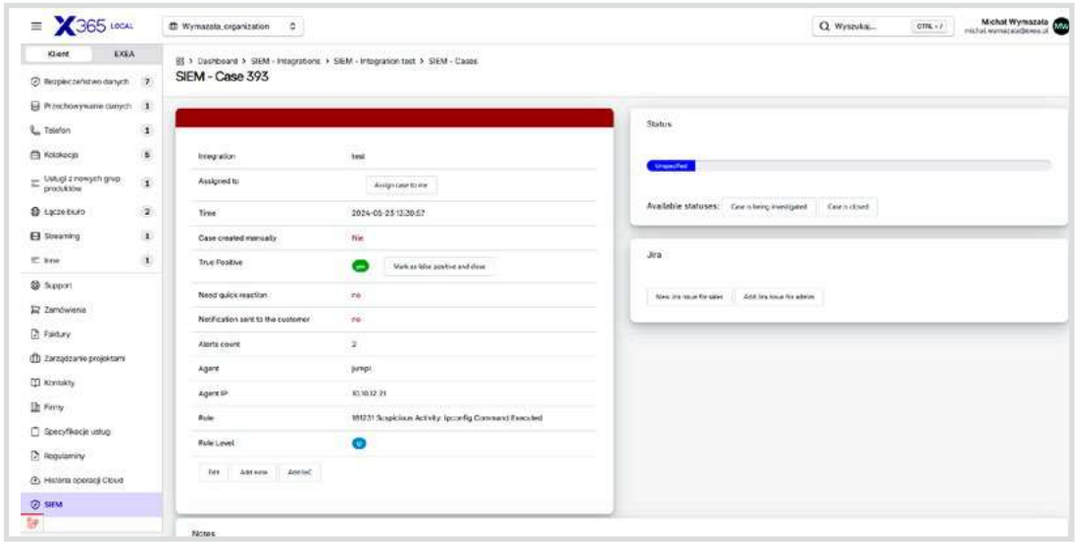
Panel klienta

Drugi z modułów, panel klienta, w sposób przekrojowy dostarcza wiedzy na temat bezpieczeństwa sieci. Aplikacja udostępnia informacje o urządzeniach, systemach, oprogramowaniu, danych kontaktowych i poziomie wsparcia. Klienci i menedżerowie znajdą tutaj zestawienia łącznej liczby zarejestrowanych i obsłużonych incydentów bezpieczeństwa.

Dane w panelu klienta prezentowane są w formie podsumowań, wykresów oraz tabel. Panel umożliwia pobranie raportu zawierającego podsumowanie liczby i typów alertów oraz obsłużonych incydentów (case'ów) z ostatnich 7 dni lub całego miesiąca. Pozwala na kompleksowe rozliczanie zespołów cyberbezpieczeństwa pod kątem wykonanej pracy oraz czasu reakcji na pojawiające się incydenty.

Kluczowe funkcje systemu

Bezpośrednia integracja platformy SIRP z systemami klasy SIEM zapewnia łatwe wdrożenie oraz niezawodność działania. Podejście to gwarantuje spójność wymienianych danych oraz efektywność działań zespołów w zakresie monitorowania i analizy zdarzeń bezpieczeństwa.



Produkt wyposażono w kilka interesujących funkcji. Oś czasu incydentu bezpieczeństwa umożliwia śledzenie i analizę przebiegu incydentów w kontekście czasowym, co jest kluczowe dla szybkiego reagowania.

Zarządzanie IoC oraz wzbogacanie IoC za pomocą analizy pozwalają zaś na efektywne zarządzanie wskaźnikami kompromitacji oraz wzbogacanie ich o dodatkowe informacje dzięki analizie. Baza IoC zawiera zbiór wskaźników kompromitacji, co ułatwia identyfikację i reakcję na potencjalne zagrożenia.

Inną unikalną cechą produktu, wyróżniającą go na tle konkurencyjnych rozwiązań są notatki do incydentów bezpieczeństwa. Notatki umożliwiają dokumentowanie działań podejmowanych w ramach reakcji na incydent oraz wymianę informacji między członkami zespołu. Dodatkowo, platformę wyposażono w funkcję zarządzania zadaniami. Wspomaga ona organizację pracy zespołu przez przypisywanie zadań oraz monitorowanie ich realizacji.

Z kolei moduł Zarządzanie dowodami umożliwia gromadzenie i analizę danych oraz dowodów związanych z incydentami, co wspiera proces dochodzeniowy. Platforma zapewnia szybki i efektywny sposób generowania raportów dotyczących incydentów oraz działań podejmowanych w związku z nimi.

Dzięki tym funkcjom platforma Exea SIRP stanowi kompleksowe narzędzie wspierające działania zespołów odpowiedzialnych za cyberbezpieczeństwo, zapewniając skuteczną reakcję na pojawiające się zagrożenia. Rozwiązanie dostępne jest w języku polskim i angielskim, choć preferowaną opcją jest ta druga ze względu na terminologię wykorzystywaną w obszarze cyberbezpieczeństwa.

Platforma Exea SIRP reprezentuje innowacyjne podejście do zarządzania incydentami bezpieczeństwa, wykorzystując najnowsze technologie i metody, aby skutecznie reagować na rosnące zagrożenia cybernetyczne. Rozwiązanie nie tylko automatyzuje i usprawnia procesy związane z reakcją na incydenty bezpieczeństwa, ale zapewnia także intuicyjny interfejs użytkownika oraz narzędzia do efektywnej współpracy zespołowej. Całość zastosowanych rozwiązań zwiększa efektywność działań i redukuje ryzyko bezpieczeństwa. Dostawca regularnie angażuje klientów w proces zbierania opinii i sugestii, co pozwala doskonalić rozwiązanie zgodnie z ich rzeczywistymi potrzebami i oczekiwaniami.

Exea Data Center

Centrum przetwarzania danych Exea Data Center dostarcza nowoczesne i zaawansowane usługi z obszaru cloud, data center, disaster recovery oraz cybersecurity. Każdego roku w ramach prac B+R Exea tworzy rozwija i nowe usługi wspierające transformację cyfrową przedsiębiorstw. Centrum w swoich działaniach stosuje zrównoważone podejście do środowiska i otoczenia zgodnie ze strategią ESG.

Kluczowe cechy

- bezpośrednia integracja z systemami klasy SIEM,
- oś czasu incydentu bezpieczeństwa,
- zarządzanie bazą IoC oraz wzbogacanie IoC za pomocą zewnętrznych źródeł,
- notatki do incydentów bezpieczeństwa,
- moduły Zarządzanie zadaniami i Zarządzanie dowodami,
- dostępność w języku polskim i angielskim (preferowany).

Play Rozwiązania dla Biznesu

Produkt: usługi chmury infrastrukturalnej

Dostawca/Producent: Play Rozwiązania dla Biznesu / 3S Data Center

Informacje: play.pl/duze-firmy

Play Rozwiązania dla Biznesu w obszarze chmury obliczeniowej oraz centrów przetwarzania danych (tzw. CPD) to kompleksowy Ekosystem IT, który oferuje niezawodne i skalowalne rozwiązania dla przedsiębiorstw. Bazuje na modułowej budowie, zapewniając klientom bezpieczeństwo, wysoką dostępność, elastyczność, skalowalność i możliwość dostosowania różnych technologii do ich indywidualnych potrzeb. Usługa Play Rozwiązania dla Biznesu świadczona jest przez spółkę 3S Data Center, będącą częścią Grupy Play.

Play Rozwiązania dla Biznesu – Chmura i Centra Danych oparte są o sześć ośrodków centrów danych, rozmieszczonych strategicznie w całej Polsce. Każdy z nich działa jako niezależna jednostka, zapewniając redundancję i wysoką dostępność, a także zgodność lokalizacji danych z przepisami prawnymi i normami ISO 27001, 27017 oraz 27018, które odpowiadają za bezpieczeństwo i przetwarzanie danych w usługach chmurowych.

18 modularnych produktów chmurowych

W ramach Play Rozwiązania dla Biznesu – Chmura i Centra Danych dostępny jest szeroki zakres usług, takich jak wirtualne centrum danych, backup i replikacja, storage oraz rozwiązania z zakresu obsługi baz danych i konteneryzacji. W ramach chmury dostarczane są zasoby sieci, usługi bezpieczeństwa, monitorowania i licencje. Obecnie liczba komponentów systemu, z których partnerzy biznesowi mogą tworzyć kompletne środowiska chmurowe wynosi 18 i jest sukcesywnie rozszerzana o kolejne usługi i produkty. Za właściwe połączenie wybranych komponentów odpowiada zespół inżynierów o wysokich kompetencjach, współpracujący z czołowymi dostawcami sprzętu i oprogramowania takimi, jak Microsoft, VMware oraz Veeam.

Usługa objęta jest wsparciem certyfikowanych inżynierów, odpowiedzialnych za utrzymanie, monitorowanie i zarządzanie infrastrukturą dedykowaną i chmurową. Wykwalifikowani specjaliści gotowi są sprostać wszelkim wymaganiom klientów zapewniając profesjonalne doradztwo techniczne.

Istotnym elementem infrastruktury Play Rozwiązania dla Biznesu – Chmura i Centra Danych jest rozległa sieć szkieletowa, która zapewnia szybkie i niezawodne połączenia między różnymi ośrodkami danych oraz zewnętrznymi systemami klientów. Ta wydajna, bezpieczna sieć umożliwia szybkie przesyłanie danych, zapewniając optymalne środowisko pracy dla aplikacji i usług w chmurze.

Jednym z kluczowych aspektów Play Rozwiązania dla Biznesu – Chmura i Centra Danych jest połączenie z chmurą publiczną. Dzięki tej integracji klienci mogą korzystać z usług i zasobów zewnętrznych dostawców chmury publicznej, takich jak usługi obliczeniowe, bazy danych czy narzędzia analityczne. Połączenie to zapewnia elastyczność i skalowalność, umożliwiając wykorzystanie najnowocześniejszych technologii i narzędzi dostępnych na rynku, przy zachowaniu efektywności finansowej.

3S Data Center jest częścią Grupy Play, która należy do francuskiej Grupy iliad - jednego z największych operatorów telekomunikacyjnych w Europie. Dzięki strategicznej współpracy usługi firmy stają się jeszcze bardziej dostępne i kompleksowe. Przynależność do silnej grupy spółek pozwala 3S Data Center na korzystanie z najnowszych technologii i najlepszych praktyk w branży, co sprawia, że razem stają się siłą telekomunikacyjną w Europie.

Usługi Play Rozwiązania dla Biznesu, świadczone przez 3S Data Center, to zespół komponentów, który obejmuje przechowywanie danych, zarządzanie nimi, rozwiązania chmurowe, ochronę przed cyberatakami oraz backup i odzyskiwanie danych. Oferowane rozwiązania oparte są na modułowej architekturze, co pozwala łatwo dostosować je do indywidualnych potrzeb naszych klientów, którzy stają się naszymi partnerami biznesowymi.

Oracle Private Cloud

Jednym z 18 elementów komplementarnego ekosystemu chmurowego dostarczanego przez Play Rozwiązania dla Biznesu jest kompletna platforma Oracle Private Cloud, oparta o OLVM (Oracle Linux Virtualization Manager). Oracle Private Cloud to spójna platforma chmurowa dedykowana pod rozwiązania aplikacyjne i bazodanowe Oracle z możliwością szybkiego skalowania środowiska

IT, jednego spójnego systemu backupowego oraz replikacji baz danych pomiędzy środowiskami.

Środowisko cechuje wysoki procent dostępności SLA, odpowiednią technologię dla środowisk aplikacyjnych i bazodanowych oraz utrzymywane jest przez certyfikowanych inżynierów, umożliwiających wsparcie merytoryczne w obszarach Oracle. Środowisko w modelu hybrydowym połączone jest z chmurową platformą prywatną, opartą o technologię VMware vCloud Director.

Podstawowym i kluczowym elementem Oracle Private Cloud jest skalowalność zasobów obliczeniowych dla środowiska aplikacyjnego i bazodanowego, zgodność licencyjna dla baz danych Oracle (Hard Partitioning), bezpieczeństwo sieciowe przed atakami wolumetrycznymi oraz ransomware.

Zaimplementowane rozwiązanie SyncGuard firmy SIMORA pozwala w bardzo szybki i prosty sposób replikować bazy pomiędzy maszynami fizycznymi i wirtualnymi oraz w krótkim i zdefiniowanym czasie przełączać je w jedną i drugą stronę. Rozwiązanie to dotychczas było zarezerwowane tylko dla klientów „premium" ze względu na bardzo drogie licencje Enterprise Edition, dedykowanych dla wielkich korporacji. Obecnie, dzięki platformie hybrydowej, każdy klient z dowolną wersją licencji bazy danych Oracle, może skorzystać z tego narzędzia.

Zaletą platformy Oracle Private Cloud jest wykorzystanie technologii VMware dla środowiska aplikacyjnego oraz Oracle Linux Virtualization Manager dla środowiska bazodanowego. Dodatkowym atutem jest zaimplementowanie jednego spójnego systemu kopii zapasowych, opartego o rozwiązania Veeam. Dzięki temu, wszystkie backupy klienta przetrzymywane są na jednej platformie, zlokalizowanej w wielu miejscach fizycznych. Klient ma możliwość wyboru technologii przechowywania danych. W zaimplementowanym rozwiązaniu na platformie przewidziana jest pamięć blokowa, gdzie dane odkładane są do chmury Veeam Cloud Connect oraz pamięć obiektowa oparta o technologię Cloudian. Dzięki temu przechowywanie danych jest znacząco tańsze, a mechanizmy szyfrowania i zabezpieczania danych sprawiają, że kopie bezpieczeństwa są zabezpieczone na poziomie producenta rozwiązania, a nie dostawcy. Oznacza to, że w przypadku zablokowania kopii danych przed skasowaniem, tylko i wyłącznie producent oprogramowania po rygorystycznej weryfikacji zgłoszenia, jest w stanie usunąć lub zmodyfikować te dane. Całość rozwiązania jest monitorowana w systemie 24/7/365.

Dzięki zastosowaniu Oracle Private Cloud od Play Rozwiązania dla Biznesu firmy otrzymują możliwość w bezpieczny, szybki i efektywny czasowo i finansowo sposób zaimplementowania lub zmigrowania rozwiązania Oracle oraz VMware do modelu chmurowego.

Rozwiązanie gwarantuje nieograniczoną i bezprzerwową pracę oraz pomaga w praktycznym urzeczywistnianiu inteligentnego i autonomicznego biznesu. Jest to jeden z najbardziej elastycznych i łatwo konfigurowalnych samodzielnie przez klienta systemów, którego otwartość na integracje i łatwość ich wykonania ułatwia rozszerzanie i łączenie środowiska bazodanowego ze środowiskiem aplikacyjnym.

Chmura i Centra Danych

Do głównych korzyści biznesowych, które organizacje mogą osiągnąć w wyniku wykorzystania usług Play Rozwiązania dla Biznesu – Chmura i Centra Danych należy przyspieszenie procesu cyfryzacji, dzięki jednej platformie, która zapewnia funkcje dostosowane do potrzeb branży i pozwala na wymierne obniżenie kosztów, zwiększenie poziomu obsługi klienta, czy poprawę efektywności biznesowej i maksymalizowanie rentownych strumieni przychodów.

Wdrożenie usług chmurowych Play Rozwiązania dla Biznesu pomaga firmom w ograniczaniu kosztów utrzymania IT, dzięki możliwości samodzielnej parametryzacji rozwiązania, podniesienia bezpieczeństwa systemów informatycznych czy w końcu minimalizację ryzyka działalności przez przeniesienie części ryzyk związanych z zapewnieniem zasobów obliczeniowych na zewnętrznego dostawcę.

Kluczowe cechy:

- 18 modularnych produktów chmurowych, które razem pozwalają stworzyć kompletny Ekosystem IT, oparty na środowiskach chmury obliczeniowej,
- 6 centrów danych zlokalizowanych w Katowicach, Warszawie, Gdańsku i Bytomiu,
- dedykowana usługa Oracle Private Cloud do obsługi środowiska bazodanowego Oracle,
- monitorowanie usługi w systemie 24/7/365,
- przynależność do silnej grupy telekomunikacyjnej (Play/iliad).

Usługi chmury infrastrukturalnej Polcom

Produkt: usługi chmury infrastrukturalnej

Dostawca/Producent: Polcom

Informacje: polcom.com.pl

Spółka Polcom specjalizuje się w świadczeniu outsourcingu IT oraz udostępnianiu elastycznej i bezpiecznej infrastruktury w modelu usługowym. Bogate portfolio firmy obejmuje zaawansowane rozwiązania z zakresu zapasowego centrum danych Polcom Disaster Recovery, monitoringu bezpieczeństwa infrastruktury - Polcom Security Operations Center oraz infrastruktury dla obsługi aplikacji biznesowych Polcom SAP Cloud Platform.

Polcom jest właścicielem dwóch, spełniających międzynarodowe standardy bezpieczeństwa i jakości, ośrodków przetwarzania danych, które pozwalają spółce świadczyć klientom szeroki zakres usług outsourcingu IT - od prostych usług kolokacji po usługi chmury obliczeniowej, backupu danych, zapewnienia ciągłości działania i zapasowego centrum danych. Usługi Polcom Disaster Recovery, Polcom Security Operation Center czy Polcom SAP Cloud Platform pozwalają na realizację nawet najbardziej złożonych, globalnych projektów biznesowych.

Polcom Disaster Recovery

Usługa Polcom Disaster Recovery (Polcom DR) gwarantuje ciągłość działania firmy poprzez zapewnienie zapasowego centrum przetwarzania danych, które stanowi kompleksowe wsparcia dla kluczowych procesów biznesowych organizacji w zakresie ich dostępności. Rozwiązanie jest dostosowane do indywidualnych potrzeb klienta. W przypadku wystąpienia nieprzewidzianych zdarzeń, takich jak awaria sprzętu czy katastrofa, usługa Polcom Disaster Recovery uruchamia scenariusz przełączenia funkcji głównego centrum przetwarzania danych do miejsca zapasowego oraz daje możliwość udostępnienia stanowisk biurowych w celu kontynuowania podstawowej działalności operacyjnej firmy.

Rozwiązanie Polcom Disaster Recovery zapewnia ciągłość działania przedsiębiorstwa przez udostępnienie zapasowego centrum przetwarzania danych oraz zdefiniowanie scenariusza postępowania na wypadek wystąpienia nieoczekiwanych zdarzeń bądź katastrofy. Z uwagi na indywidualne podejście do każdego projektu biznesowego, usługa jest dostosowywana do potrzeb konkretnego klienta, jednocześnie spełniając wyśrubowane normy i wymagania dotyczące jakości oraz bezpieczeństwa.

W ramach Polcom Disaster Recovery klient otrzymuje całodobowe wsparcie ze strony wykwalifikowanych specjalistów Polcom, którzy realizują zadania na podstawie ustalonych scenariuszy oraz wypracowanych na przestrzeni lat najlepszych praktyk postępowania. Polcom Data Center, jako lokalizacja zapasowa, gwarantuje dostęp do kompleksowej infrastruktury informatycznej pozwalającej na płynne i bezproblemowe przełączenie działalności operacyjnej firmy klienta z siedziby głównej do zapasowej. Rozwiązanie pozwala zminimalizować ryzyko utraty kontroli nad kluczowymi procesami związanymi z zarządzaniem przedsiębiorstwem w razie jakiejkolwiek sytuacji kryzysowej lub siły wyższej.

Usługa realizowana jest z zachowaniem wysokiego stopnia bezpieczeństwa oraz zgodnie z certyfikacją ISO 9001, ISO27001 oraz ISO 27017. Klient otrzymuje gwarantowany poziom SLA oraz zapewnienie wymaganego czasu reakcji na wypadek katastrofy.

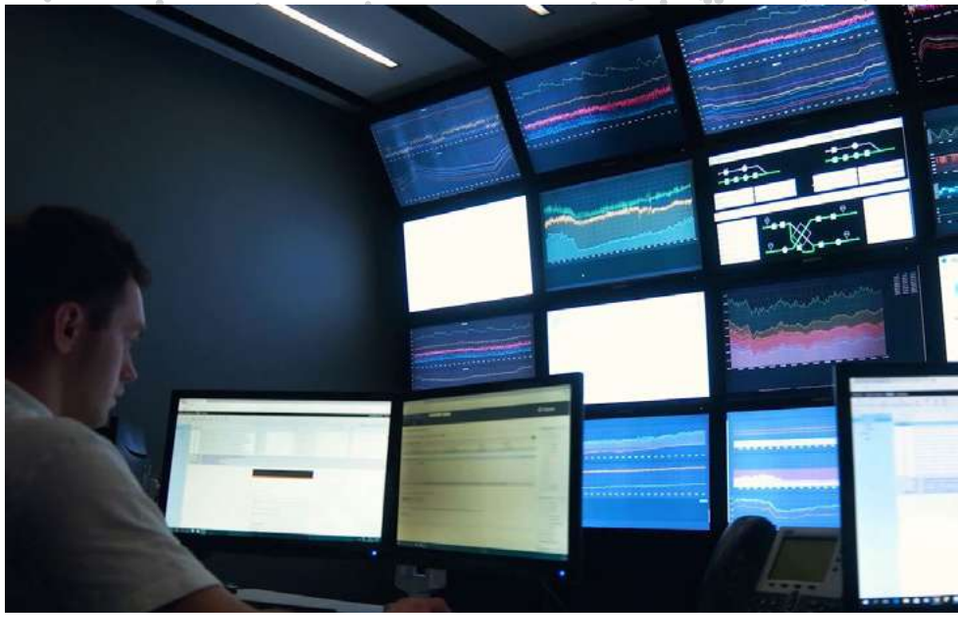
Polcom Security Operation Center as a Service (SOC)

Decyzja o wdrożeniu dyrektywy NIS2 otwiera kolejny etap w zakresie rozwoju cyberbezpieczeństwa. Nie jest to jedyny akt prawny, który nakłada na przedsiębiorstwa i instytucje publiczne obowiązki dotyczące zabezpieczenia danych. Należą do nich także RODO, DORA czy przepisy KNF. Kluczem do szybkiego zaadaptowania się do nowych przepisów oraz rosnącego zagrożenia cyberatakiem może być wsparcie ze strony zewnętrznego dostawcy, który oferuje rozwiązanie Security Operation Center.

Polcom Security Operation Center as a Service (SOC) to usługa polegająca na zapewnieniu zewnętrznego zespołu specjalistów ds. bezpieczeństwa, który monitoruje zasoby i infrastrukturę w trybie ciągłem – 24 godziny na dobę, 7 dni w tygodniu. Zespół SOC wykrywa, analizuje i reaguje na incydenty w czasie rzeczywistym i pozwala na ich raportowanie do odpowiednich, wskazanych przez dyrektywę organów. SOC proaktywnie przeciwdziała atakom, a dedykowany zespół specjalistów pełni także rolę doradczą. Pomaga wybrać najlepsze technologie z zakresu cybersecurity, analizuje globalne dane o zagrożeniach i najnowszych metodach przeprowadzania ataków.

Usługa Polcom SOC opiera się na czterech filarach bezpieczeństwa: wykrywaniu zagrożeń, odpowiedzi

na nie, działaniach prewencyjnych oraz raportowaniu. Polcom SOC zapewnia natychmiastową widoczność podejrzanych zachowań w sieci: nowych i takich, które dotąd nie były znane. Wykorzystując wiedzę na ten temat pozwala szybko zareagować na cyberataki, bez zakłócania działalności biznesowej. Skrócenie czasu reakcji na incydenty wynosi nawet 92%. Jednocześnie, przez nadanie priorytetów lukom w zabezpieczeniach, specjaliści Polcom z zakresu cybersecurity mogą szybciej dostrzec korelacje pomiędzy incydentami, co pozwala skutecznie zapobiegać potencjalnym zagrożeniom. Co więcej, oprócz bieżących raportów, usługa zapewnia także raporty biznesowe, pozwalające na analizę i budowę długofalowej strategii cyberbezpieczeństwa firmy.



Polcom SOC przygotowuje przedsiębiorstwa na incydenty bezpieczeństwa nie tylko w kontekście NIS2, ale pozwala na sprawne reagowanie na potencjalne zagrożenia, a co za tym idzie, zapewnia ciągłość działania w przypadku nieprzewidzianych zdarzeń i katastrof, co warto uwzględnić w budowaniu strategii biznesowej firm i instytucji.

Polcom SAP Cloud Platform

Złożony charakter systemu SAP sprawia, że wymaga on specjalnej oraz wysokowydajnej infrastruktury informatycznej. W ramach usługi Polcom SAP Cloud Platform firma udostępnia kompleksowe środowisko niezbędne do uruchamiania i prawidłowego funkcjonowania systemu SAP. Dostawca zapewnia klientom w pełni funkcjonalną oraz elastyczną platformę informatyczną, zoptymalizowaną pod kątem obsługi oprogramowania ERP, które wspomaga zarządzanie przedsiębiorstwem.

W ramach usługi Polcom SAP Cloud Platform dostawca udostępnia wydajne i bezpieczne środowisko informatyczne, niezbędne do uruchomienia systemów typu SAP i SAP HANA. W trosce o bezpieczeństwo Polcom dba o należytą ochronę danych klientów przed jakąkolwiek ingerencją z zewnątrz m.in. przez szyfrowanie transmisji danych przy użyciu klucza SSL oraz stosowanie nowoczesnym systemów zabezpieczeń Klienci otrzymują kompleksową pomoc na każdym etapie projektu oraz pełne wsparcie w procesie migracji systemu do chmury obliczeniowej.

W ramach usługi Polcom zapewnia gotową platformę informatyczną, zoptymalizowaną pod kątem oprogramowania SAP i wymagań biznesowych, elastyczne środowisko dla tworzenia, hostowania i wdrażania aplikacji oraz usługi zarządzania środowiskiem IT, oprogramowaniem, systemami operacyjnymi, pamięcią masową oraz siecią.

Polcom SAP Cloud Platform gwarantuje wysokie bezpieczeństwo przechowywanych i przetwarzanych danych dzięki zastosowanym mechanizmom oraz możliwości wykonywania kopii zapasowych według ustalonego z klientem scenariusza. Czas wdrożenia systemu jest istotnie krótszy, ponieważ implementacja rozwiązania ERP nie jest zależna od opóźnień w zakresie łańcuchów dostaw. Platforma zapewnia także wysoką skalowalność w stosunku do zmieniających się dynamicznie wymagań projektowych. Dzięki udostępnianiu infrastruktury w modelu chmurowym, klient końcowy zyskuje elastyczność oraz wyższy stopień dostępność wykorzystywanych systemów.

Polcom zapewnia pełną opiekę administracyjną, dzięki czemu klienci mogą skupić się na korzystaniu z warstwy biznesowej, bez konieczności sprawowania opieki technicznej nad platformą IT. Co więcej, dostawca nie tylko utrzymuje platformę, ale także monitoruje jej poprawne funkcjonowanie i proaktywnie doradza klientowi, w jaki sposób optymalizować jej działanie.

Kluczowe cechy:

- projektowy charakter usługi, która gwarantuje pełne wsparcie klienta biznesowego w zakresie stworzenia koncepcji projektowej, migracji do chmury i zarządzaniu środowiskiem,
- zestaw komplementarnych usług chmurowych z zakresu monitoringu czy zapasowego centrum danych,
- dwa własne centrach danych Polcom o wysokiej dostępności dzięki zastosowanym mechanizmom replikacji synchronicznej,
- ciągłe monitorowanie funkcjonowania platformy i proaktywne doradztwo klientom w zakresie jej optymalizacji,
- certyfikacje ISO 27017, ISO 27001, ISO 9001, PCI DSS,
- zgodność z RODO, wytycznymi KNF oraz prawem bankowym.

Tenable Cloud Security

Produkt: zaawansowana platforma do ochrony środowisk chmurowych

Dostawca/Producent: Tenable

Informacje: tenable.com

Tenable Cloud Security to kompleksowe rozwiązanie CNAPP, które redukuje ryzyko cybernetyczne, integrując dane z różnych narzędzi w jednolity system. Zapewnia analizę ryzyka i automatyzację zarządzania zgodnością, co pozwala na szybką identyfikację i naprawę luk w zabezpieczeniach.

Tenable Cloud Security to zaawansowana platforma do ochrony środowisk chmurowych (CNAPP), która zapewnia kompleksowe zabezpieczenie infrastruktury, tożsamości i danych użytkowników oraz korzystania z zasobów w środowiskach chmurowych. Rozwiązanie to upraszcza identyfikację i korygowanie ryzyka w środowiskach wielochmurowych, zmniejszając ryzyko ataku lub wycieku danych przy jednoczesnej poprawie produktywności.

Rozwiązanie adresuje wyzwania związane z rosnącą złożonością i rozproszonym charakterem nowoczesnych środowisk chmurowych, oferując zintegrowane podejście do zabezpieczeń. Dzięki pełnej inwentaryzacji zasobów i podatności w różnych chmurach, Tenable Cloud Security umożliwia lepsze zarządzanie i zabezpieczanie środowisk chmurowych. Platforma szybko identyfikuje i priorytetyzuje luki w zabezpieczeniach, umożliwiając natychmiastowe działania naprawcze. Automatyczne skanowanie konfiguracji i zasobów w różnych chmurach jak również identyfikacja naruszeń i automatyzacja procesów naprawczych, ułatwiają spełnianie wymagań regulacyjnych.

Wiele funkcjonalności w jednej konsoli i licencji

Lista funkcji zabezpieczeń wchodzących w skład produktu obejmuje moduły Cloud Workload Protection (CWP), Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), Kubernetes Security Posture Management (KSPM), Infrastructure as Code (IaC) Security oraz Cloud Detection and Response (CDR).

Oprogramowanie łączy wiele zaawansowanych technologii w jednym zintegrowanym produkcie. Zapewnia pełne spektrum ochrony chmurowej, obejmując zarówno zarządzanie uprawnieniami, zabezpieczenia infrastruktury, jej monitorowanie oraz reakcję na zagrożenia. Ta wszechstronność eliminuje potrzebę stosowania wielu odrębnych narzędzi, co upraszcza zarządzanie i zmniejsza ryzyko luk w zabezpieczeniach. Produkt Tenable Cloud Security pomaga łatwo zwiększyć bezpieczeństwo w różnych chmurach, takich jak: AWS, Azure i GCP. Produkt pozwala na korzystanie w wielu rozwiązań:

- Kompleksowy CNAPP: jako pełne rozwiązanie CNAPP, Tenable Cloud Security umożliwia zabezpieczenie infrastruktury chmurowej od procesu programowania do środowiska produkcyjnego. Stale analizuje wszystkie zasoby chmury — w całej infrastrukturze, danych do uwierzytelnienia i aplikacjach — aby wyodrębnić najważniejsze zagrożenia, wykryć nieznane zagrożenia i w ciągu kilku godzin dostarczyć przydatne informacje. Produkt identyfikuje również kluczowe ryzyko dla infrastruktury chmury — identity — wykrywając,

ustalając priorytety i korygując nadmierne uprawnienia i błędne konfiguracje na dużą skalę.
- Zarządzanie stanem zabezpieczeń w chmurze (CSPM) umożliwia monitorowanie ryzyka poprzez stałe przeglądanie i ocenę ustawień oraz konfiguracje środowiska chmury. Mapowanie wykrytych zagrożeń pod kątem standardów i zasad zabezpieczeń, pozwala na utrzymanie standardów i zgodności z przepisami w środowiskach wielochmurowych.
- Zarządzanie uprawnieniami do infrastruktury chmurowej (CIEM): analizuje wszystkie dane dotyczące kont i ich uprawnień oraz pełny kontekst ryzyka, który ujawnia i nadaje priorytety niewidocznym na pierwszy rzut oka zagrożeniom, takim jak toksyczne kombinacje czy eskalacja uprawnień. Zbyt duże uprawnienia lub nieużywane uprawnienia mogę być automatycznie korygowane.
- Cloud Workload Protection (CWPP): stale skanuje, wykrywa i wizualizuje najbardziej krytyczne zagrożenia związane z obciążeniami, w tym luki w zabezpieczeniach, poufne dane, złośliwe oprogramowanie i błędne konfiguracje, na maszynach wirtualnych, w kontenerach i funkcjach bezserwerowych.
- Kubernetes Security Posture Management (KSPM): pozwala wykryć, ustalić priorytety i skorygować luki w zabezpieczeniach oraz automatyzować zgodność klastrów Kubernetes w całej infrastrukturze chmury. Korzystając z Tenable Cloud Security, można ujednolicić raporty z konfiguracji różnych kontenerów Kubernetes i umożliwić uczestnikom projektu podjęcie kroków w celu ograniczenia błędów w konfiguracjach.
- Infrastruktura jako kod (IaC): umożliwia programistom skanowanie, wykrywanie i naprawianie błędów konfiguracji i innych zagrożeń zanim kod trafi w całości do chmury. Rozwiązanie CNAPP firmy Tenable umożliwia zespołom stosowanie zabezpieczeń w narzędziach DevOps do workflow, w tym Hashi Terraform i AWS CloudFormation, oraz automatyczne korygowanie priorytetowych ustaleń w ich natywnych środowiskach IaC.
- Dostęp just in time (JIT): umożliwia nadawanie uprawnień ograniczonych w czasie i wtedy gdy jest to potrzebne dla programistów. Takie podejście umożliwia unikanie stosowania długotrwałych i często wysokich uprawnień, jednocześnie zmniejszając powierzchnię ataku w chmurze.

Automatyzacja zadań i compliance

Tenable Cloud Security to bezagentowe rozwiązanie, które można wdrożyć w kilka minut. Dzięki niemu organizacje mogą skutecznie priorytetyzować ryzyka i realizować działania naprawcze od kodu, aż po samą implementację w chmurze. Platforma wspiera pełne spektrum ochrony chmurowej, eliminując potrzebę stosowania wielu odrębnych narzędzi. Dzięki integracji z rozwiązaniami IaC oraz JIT, Tenable Cloud Security umożliwia dynamiczne i elastyczne skalowanie zabezpieczeń w czasie rzeczywistym, dostosowując się do zmieniających się potrzeb i obciążenia systemów chmurowych. Jest to szczególnie ważne dla firm, które szybko się rozwijają i muszą na bieżąco dostosowywać swoje zasoby.

Co więcej, rozwiązanie Cloud Security wspiera zarządzanie zgodnością z różnorodnymi regulacjami i standardami branżowymi dzięki funkcjonalności CSPM i KSPM. Tenable Cloud Security umożliwia przeprowadzanie inspekcji środowisk wielochmurowych pod kątem standardów branżowych, takich jak CIS, AWS Well Architected, RODO, HIPAA, ISO, NIST, PCI-DSS, SOC2, CIS for Kubernetes i innych, a także tworzyć własne niestandardowe kontrole. Ponadto produkt pomaga szybko generować szczegółowe raporty dotyczące zgodności wewnętrznej, audytów zewnętrznych i codziennych operacji bezpieczeństwa (inwentaryzacja zasobów, błędne konfiguracje, konfiguracje sieci itp.). Ułatwia to firmom spełnianie wymogów prawnych oraz utrzymanie wysokich standardów bezpieczeństwa i zgodności.

Tenable Cloud Security to usługa hostowana na platformie AWS. Usługa integruje się z:
- dostawcami tożsamości i środowiskami infrastruktury chmurowej za pośrednictwem interfejsu API,
- Infrastucture as a Code. Tenable integruje się z pipeline/repozytoriami kodu oraz skanuje IaC, umożliwiając wykrycie błędów konfiguracji w kodzie a także synchronizuje kod skojarzony z zasobami w chmurze, aby śledzić zasoby z powrotem do ich źródeł (Cloud to Code),
- narzędziami do obsługi zgłoszeń, powiadomień i SIEM, takimi jak Jira, Slack i Splunk.

Tenable Cloud Security można wdrożyć jako samodzielne rozwiązanie lub można go kupić w ramach większego rozwiązania jako jeden z modułów w rozwiązaniu Tenable ONE.

Kluczowe cechy:

- łatwość wdrożenia, nie wymaga agenta,
- nadzór na różnymi chmurami w jednej konsoli, z możliwością analiz środowisk hybrydowych, on premise oraz kontenerów,
- szczegółowa inwentaryzacja zasobów w chmurze, w tym komputerów, sieci, tożsamości i danych,
- wizualizator konfiguracji, ekspozycja sieci, ryzyka ataku i uprawnień dostępu,
- analiza błędów konfiguracyjnych systemów,
- dynamiczna i kontekstowa analiza ryzyka oraz jego priorytetyzacja,
- przejrzysty, intuicyjny interfejs.

Perceptus perc.pass

Produkt: menedżer haseł dla firm i instytucji publicznych

Dostawca/Producent: Perceptus

Informacje: percpass.com

Perc.pass to pierwszy polski menedżer haseł zaprojektowany dla zespołów, które dzięki niemu mogą szybko dzielić się dostępem do różnych narzędzi. Aplikacja oferuje innowacyjną metodę szyfrowania zero-knowledge, która w połączeniu z dwuskładnikowym uwierzytelnianiem zapewnia użytkownikom maksymalne bezpieczeństwo. Wrażliwe dane przechowywane i przetwarzane są na terytorium Polski, co czyni ją unikalnym rozwiązaniem na rynku.

Perc.pass to pierwszy polski menedżer haseł. Jest unikalny, ponieważ jako jedyny zapewnia bezpieczne gromadzenie danych dostępowych przy zachowaniu pełnej świadomości miejsca ich przechowywania. Aplikacja zaprojektowana została dla firm oraz instytucji publicznych w celu ułatwienia zarządzania hasłami grupie osób. Zapewnia mechanizmy umożliwiające współdzielenie i kontrolowanie dostępu do haseł, którymi zabezpieczane są wrażliwe informacje, czy narzędzia na których pracują poszczególne grupy. Wersja dla kont indywidualnych dostępna jest bezpłatnie, pakiety firmowe są dopasowane do wielkości organizacji.

Cyfrowy bunkier dla haseł

Perc.pass zapewnia pełne bezpieczeństwo danych przez implementację kilku innowacyjnych rozwiązań zapewniających maksymalny poziom bezpieczeństwa danych: szyfrowania metodą zero-knowledge, dwuskładnikowego uwierzytelniania oraz szyfrowania danych w spoczynku z wykorzystaniem HSM.

Szyfrowanie odbywa się zawsze po stronie użytkownika, a przesyłane i gromadzone w bazie danych loginy oraz hasła pozostają stale zaszyfrowane. Zabezpieczanie materiału kryptograficznego odbywa się za pomocą klucza symetrycznego opartego na haśle głównym, które zna jedynie użytkownik konta. To praktyczna realizacja zasady zero-knowledge, która zabezpiecza hasła nawet w przypadku wycieku bazy danych. Dodatkowo, dane w spoczynku szyfrowane są przy wykorzystaniu sprzętowego modułu bezpieczeństwa (HSM).

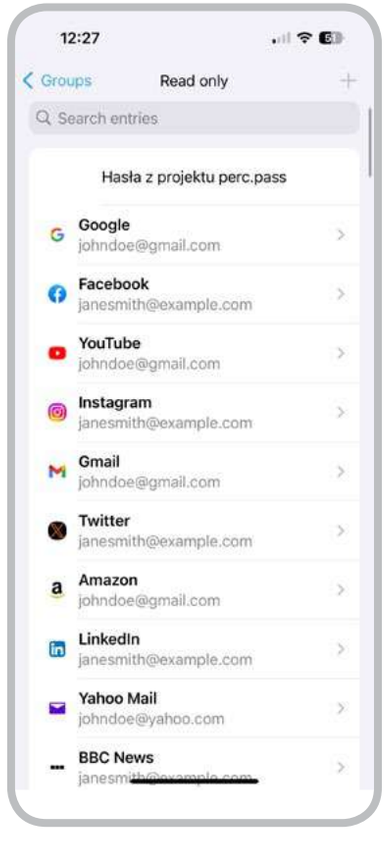
Perc.pass dba o wiarygodność danych uwierzytelniających przechowywanych w sejfie. Aplikacja sprawdza, czy poziom trudności haseł jest wystarczająco wysoki, sugerując zmiany, jeśli jest inaczej. Funkcja ta zwalnia użytkownika z myślenia o tym, jak skomplikowane powinno być hasło. Jednocześnie perc.pass umożliwia automatyczne generowanie trudnych do złamania, a więc w pełni bezpiecznych haseł.

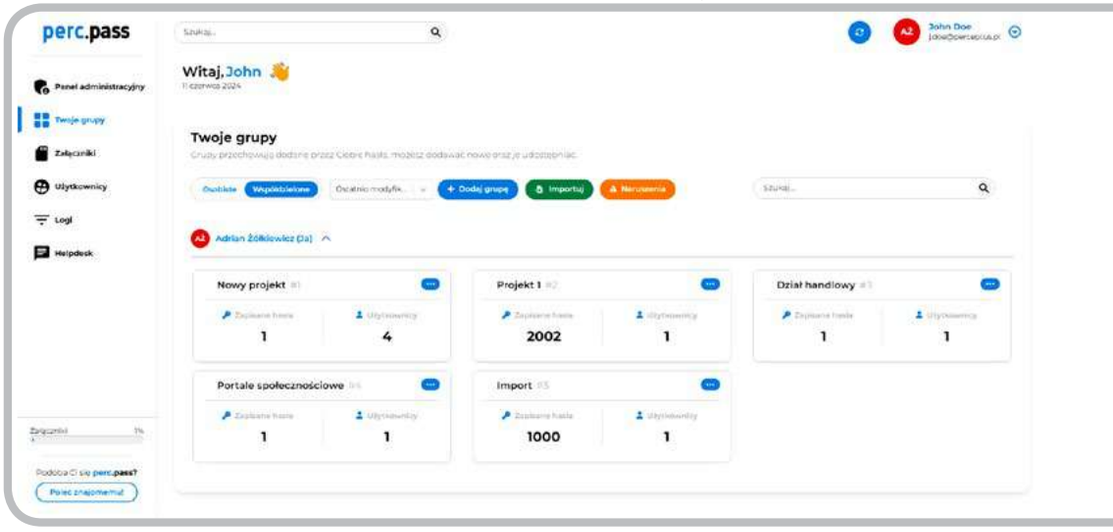
Dodatkowo, program sprawdza zasoby ciemnego internetu (dark web monitoring) porównując dane w sejfie użytkownika lub w grupach współdzielonych z listą haseł ujawnionych (skompromitowanych) w wyciekach. W przypadku zauważonego naruszenia bezpieczeństwa program sugeruje zmianę hasła.

Współpraca w grupie

Poza wygodnym przechowywaniem haseł w bezpiecznym środowisku perc.pass zapewnia efektywne mechanizmy ich współdzielenia w grupie osób. Członkowie grupy mają dostęp do współdzielonych haseł. Wszelkie operacje na danych są monitorowane i zapisywane w logach, co daje administratorom możliwość kontrolowania kto i kiedy uzyskał dostęp do hasła, a także kto zmieniał dane dostępowe w systemie.

Właściciel grupy może odebrać uprawnienia do danych wybranej osobie, blokując w ten sposób dostęp do przeglądania i używania współdzielonych haseł. Dostępy mogą być też zawieszone czasowo, np. kiedy dana osoba wybiera się na dłuższy urlop. Mechanizm ten usprawnia zarządzanie dostępem do haseł osobom, które zmieniają stanowisko lub odchodzą z firmy. To sposób na kontrolowany





offboarding, dzięki któremu pracownik, który kończy pracę ma natychmiast odebrany dostęp do wrażliwych systemów i danych firmowych. Jednocześnie współdzielenie haseł ułatwia skuteczne wdrażanie nowych osób w organizacji (onboarding). Nowy członek zespołu nie musi szukać haseł, których pozostali pracownicy nie mogą sobie przypomnieć.

Autouzupełnianie haseł

Wtyczka perc.pass dla najpopularniejszych przeglądarek internetowych usprawnia logowanie do stron i aplikacji webowych. Funkcja autouzupełniania danych uwierzytelniających, bez konieczności ich wyszukiwania, eliminuje konieczność samodzielnego sięgania do bazy menedżera haseł. Wystarczy, aby użytkownik kliknął ikonkę perc.pass pojawiającą się w formularzu logowania, a system sam wyszuka i podpowie odpowiednie rekordy z bazy haseł. Działanie to jest tak intuicyjne, że nie wymaga żadnej instrukcji. Funkcja autouzupełniania, działająca na tej samej zasadzie, obsługiwana jest również w aplikacjach mobilnych iOS oraz Android.

System weryfikuje dane dostępowe w oparciu o domenę strony logowania. Hasło nie zostanie zaproponowane, jeśli domena nie została zapisana w systemie. Dzięki tej funkcji zyskujemy dodatkowo cenne sekundy na zastanowienie się czy na pewno jesteśmy na stronie, na której powinniśmy być. W rezultacie perc.pass na swój sposób chroni nas także przed atakiem phishingowym.

Perc.pass to pierwszy i jedyny polski menedżer haseł, przydatny każdemu kto korzysta z cyfrowych udogodnień, prywatnie i w ramach służbowych obowiązków. Produkt wykorzystywany jest w firmach działających w sektorze IT i e-commerce, w jednostkach samorządu terytorialnego oraz państwowych uczelniach wyższych. Znacząco wpływa na poziom zabezpieczeń osób prywatnych, firm i urzędów.

Zaprojektowane rozwiązanie jest w pełni transparentne, a jego bezpieczeństwo było testowane podczas zewnętrznego audytu firmy Securitum. Perc.pass wykorzystuje kryptografię i uwierzytelnianie wieloskładnikowe, aby zabezpieczać dane, pozostając przy tym prostym w obsłudze. Dodatkowe udogodnienia, w postaci aplikacji mobilnej czy wtyczki dla przeglądarek internetowych, pozwalają sprawniej i efektywniej realizować procesy biznesowe.

Kluczowe cechy:

- pełna świadomość miejsca przechowania danych na terenie Polski,
- szyfrowanie haseł po stronie użytkownika (zasada zero-knowledge),
- szyfrowanie danych w spoczynku przez HSM,
- wygodne autouzupełnianie haseł w przeglądarkach i aplikacji mobilnej,
- łatwe współdzielenie haseł i pełna kontrola nad ich wykorzystaniem,
- przeprowadzony audyt bezpieczeństwa firmy Securitum.

Symfonia Obieg Dokumentów

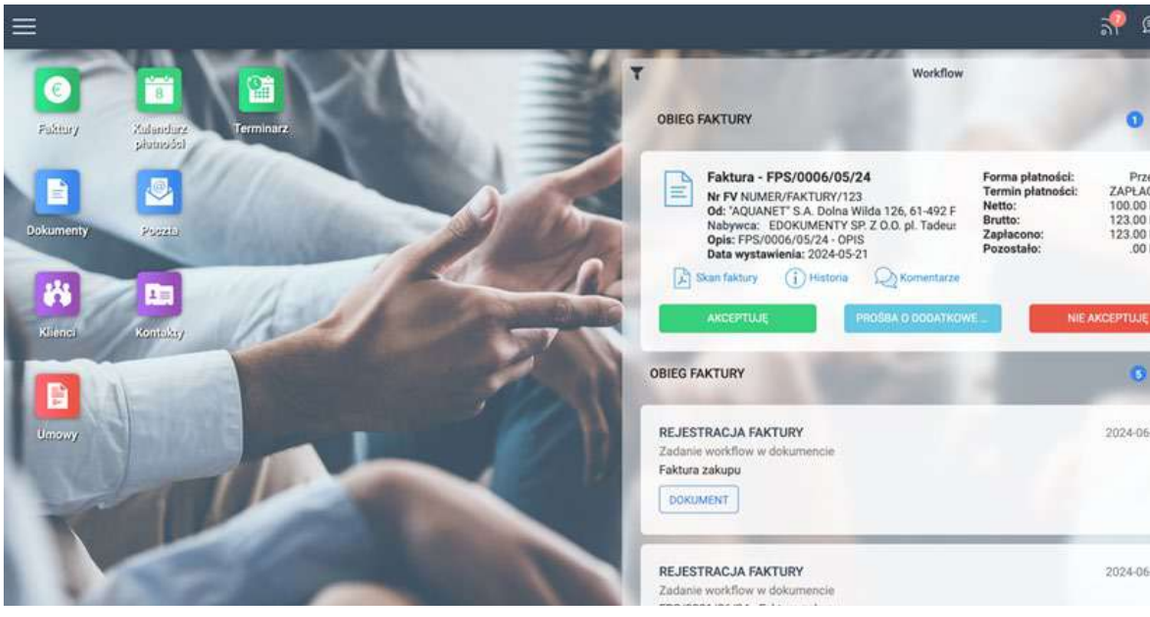
Produkt: platforma obiegu dokumentów i pracy grupowej

Dostawca/Producent: Symfonia

Informacje: symfonia.pl

Symfonia Obieg Dokumentów to chmurowa platforma łącząca rozwiązanie ECM z elementami pracy grupowej oraz systemu ERP. Aplikacja dostępna jest przez przeglądarkę, a jej intuicyjny interfejs pozwala na efektywną pracę z wieloma danymi jednocześnie. Nowoczesna technologia zapewnia zaś niezwykłą szybkość działania i niezawodność.

Symfonia Obieg Dokumentów odpowiada na potrzebę tworzenia cyfrowych miejsc pracy tzw. digital workplace. Łączą one ludzi z informacjami i procesami, aby zapewniać efektywną komunikację i nowoczesne metody zarządzania firmą. Główne założenie systemu opiera się na idei, aby w jednym miejscu zebrać elementy aplikacji z obszarów ECM, ERP i CRM, a następnie udostępnić je w jednym, spójnym interfejsie okienkowym, niczym w systemie operacyjnym.



Platforma oferuje kilkadziesiąt obszarów zastosowań, z których najczęściej wykorzystywane są funkcje obiegu dokumentów, w tym w szczególności związane z fakturami zakupu i procesami zakupowymi. System cechuje się łatwością konfiguracji, w tym z użyciem predefiniowanych szablonów. Ma wbudowane narzędzia pracy grupowej oraz mechanizmy wersjonowania dokumentów i plików.

Obieg dokumentów

Wszystkie dokumenty i pliki podlegają uniwersalnym zasadom porządkowania, a praca z nimi może odbywać się według ustalonych zasad obiegu i przetwarzania informacji w firmie. W ciągu chwili system OCR odczytuje pola z plików PDF lub zeskanowanych faktur papierowych przenosząc je na metrykę. Funkcjonalność OCR dostępna jest także w aplikacji mobilnej na telefonie. Co więcej, dokumenty można w łatwy sposób dodawać bezpośrednio z poczty email, bez pobierania załączników na dysk.

System oferuje gotowe szablony procesów, które konfigurowane według własnych potrzeb, pozwalają odzwierciedlić proces obiegu dokumentów w niemal każdej wielkości firmie. Zaawansowany podsystem uprawnień zapewnia zaś zabezpieczenie dostępu do wybranych informacji tylko dla uprawnionych pracowników. Mechanizm ten minimalizuje ryzyko wystąpienia błędów i ujawnienia poufnych informacji. Funkcje Poczta, Kalendarz, Czat i Komentarze wraz z Powiadomieniami przyspieszają obsługę spraw związanych z przetwarzaniem danych. Korzystając z kontekstu dokumentu, użytkownik może zlecać zadania, komentować a nawet prowadzić czat ze swoimi współpracownikami. Z kolei funkcja wersjonowania dokumentów tekstowych, arkuszy i prezentacji znacznie upraszcza procesy tworzenia i wielokrotnego edytowania tego samego pliku. W systemie panuje porządek, a pracownicy nie tracą czasu na poszukiwanie ostatniej wersji danego dokumentu.

Kluczowe funkcje

Do najbardziej innowacyjnych cech wyróżniających produkt na tle konkurencyjnych rozwiązań należą unikalny interfejs użytkownika, mechanizmy pracy grupowej, zestaw wbudowanych, gotowych aplikacji oraz integracje z oprogramowaniem Symfonia Finanse i Księgowość. Symfonia Obieg Dokumentów jest również gotów do współpracy z innymi popularnymi platformami ERP działającymi na rynku poprzez właściwe dla tych

systemów formaty wymiany plików. System posiada również własny format XML, możliwy do wykorzystania w eksporcie dedykowanym do innego systemu finansowo-księgowego, przez co można założyć, że Symfonia Obieg Dokumentów jest zgodny z każdym systemem finansowo-księgowym dostępnym na rynku. Wystarczy, że ten system będzie potrafił obsłużyć wspomniany plik XML.

Program wyposażono w uniwersalne repozytorium dokumentów w firmie, bazę danych kontrahentów i produktów oraz w pełni funkcjonalnego klienta poczty IMAP.

Praca w Symfonii Obieg Dokumentów, mimo że wykonywana w przeglądarce, bardziej przypomina korzystanie z komputera z systemem Windows lub OS X. Użytkownik może otwierać wiele okien jednocześnie, minimalizować je do paska zadań, a także przeciągać zawartość między nimi. Tak zaprojektowany interfejs pozwala dużo szerzej i efektywniej wykorzystać funkcje systemu, niż tylko w sposób zaplanowany dla danego procesu, jak ma to miejsce w konkurencyjnych rozwiązaniach.

Zamiast tworzenia procedur i formularzy do obsługi powtarzalnych procesów, lub korzystania z ich szablonów, system oferuje gotowe aplikacje takie jak Faktury zakupu, Archiwum umów, Obieg wniosków zakupowych, Delegacje, Zakupy, Pipeline, Intranet i wiele innych. Każda aplikacja ma rozbudowaną konfigurację, dzięki której administrator biznesowy może dopasować system do indywidualnych potrzeb firmy. Podejście to znacząco upraszcza się i przyspiesza wdrożenie aplikacji w organizacji.

Dzięki zaawansowanej integracji z Symfonii Finanse i Księgowość możliwe jest definiowanie i korzystanie ze schematów księgowań i podgląd wszystkich zapisów księgowych przed ich eksportem.

Symfonia Obieg Dokumentów pozwala podpiąć skrzynkę poczty elektronicznej, aby przechwytywać z niej wybrane wiadomości e-mail oraz pliki. Informacje zebrane z poczty służą do tworzenia zadań przydzielanych pracownikom. Zamiast odpisywać na e-mail, użytkownicy mogą odpowiadać współpracownikom korzystając z komentarzy w zadaniu. Jednocześnie, skrzynki mogą być współdzielone przez wielu użytkowników dla jeszcze sprawniejszej obsługi w biurach obsługi klienta, kancelariach i działach helpdesk.

Aby dokumenty można było szybko przeglądać i odszukiwać, Symfonia Obieg Dokumentów oferuje unikalny, ale zarazem niezwykle uniwersalny sposób organizacji dokumentów w oparciu o stanowiska i działy

w firmie. Dodatkowe foldery, w których można umieszczać dokumenty, tworzy się w działach jako Teczki, a powiązane ze sobą tematycznie dokumenty, można dodatkowo trzymać w Sprawach, aby odzwierciedlały przebieg załatwienia każdej sprawy.

Wbudowane w system narzędzia współpracy: kalendarz i lista zadań, czat i powiadomienia pozwalają znacznie szybciej załatwić sprawy związane z dokumentami. Korzystając z kontekstu umieszczonych w systemie dokumentów można zlecać zadania, komentować je, a nawet prowadzić czat ze swoimi współpracownikami.

System wyposażony jest we wbudowaną bazę kontrahentów, która pozwala na tworzenie i przeglądanie danych w kontekście każdego klienta i dostawcy, podobnie jak w systemach CRM i ERP. Dodatkowo, w celu wsparcia procesów zakupowych i sprzedażowych, użytkownicy mogą korzystać z rozbudowanej i funkcjonalnej bazy danych towarów i produktów.

Kluczowe cechy:

- unikalny interfejs użytkownika,
- mechanizmy pracy grupowej,
- gotowe, zaawansowane aplikacje,
- integracja z Symfonia Finanse i Księgowość,
- wbudowany klient poczty IMAP.

Wdrożenia i klienci: Zdrojowa Hotels, Huta Pokój, Fundacja Św. Mikołaja

Soneta TRIVA ERP

Produkt: zintegrowany system zarządzania przedsiębiorstwem

Dostawca/Producent: Soneta

Informacje: triva.pl

TRIVA ERP to eksperckie narzędzie do zarządzania procesami w przedsiębiorstwie. Produkt może zostać dopasowany do dowolnej branży i niemal każdej specyfiki działania firmy.

TRIVA jest nowoczesnym systemem ERP stworzonym dla średnich i dużych firm, umożliwiającym organizację przepływu pracy i informacji oraz pomagającym użytkownikom efektywnie pracować, zarządzać zmianami i konkurować na rynku. TRIVA automatyzuje i ujednolica analizę biznesową oraz finansową, a także pomaga nadzorować procesy w firmie. Każdy z tych obszarów jest wspierany natywnie przez Business Intelligence (BI), Automatyzację procesów biznesowych (Workflow) oraz umożliwia organizację pracy zdalnej.

Oprogramowanie usprawnia zarządzanie firmą dzięki stosowaniu technologii informatycznych, przyczynia się do zwiększenia sprzedaży przez automatyzację procesów handlowych, podnosi również produktywność dzięki dostarczeniu mechanizmów pozwalających zautomatyzować szereg innych procesów w organizacji, co przyczynia się do podniesienia wspomnianej produktywności np. w zakresie procesów finansowych. W rezultacie TRIVA pozwala na szybsze podejmowanie decyzji dzięki udostępnieniu menedżerom przejrzystej i wiarygodnej informacji zarządczej.

Wsparcie procesów biznesowych

System TRIVA ERP przynosi przedsiębiorstwu korzyści w postaci niższych kosztów ogólnych. Jest to możliwe dzięki lepszemu dostosowaniu technologii do konkretnych potrzeb organizacji, a także skalowalności, łatwości wdrażania i zarządzania oraz wysokiej niezawodności. Dodatkowo, TRIVA kompleksowo obsługuje wszystkie biznesowe i operacyjne procesy organizacji. Wspiera i automatyzuje przetwarzanie danych oraz wymianę informacji pomiędzy użytkownikami systemu.

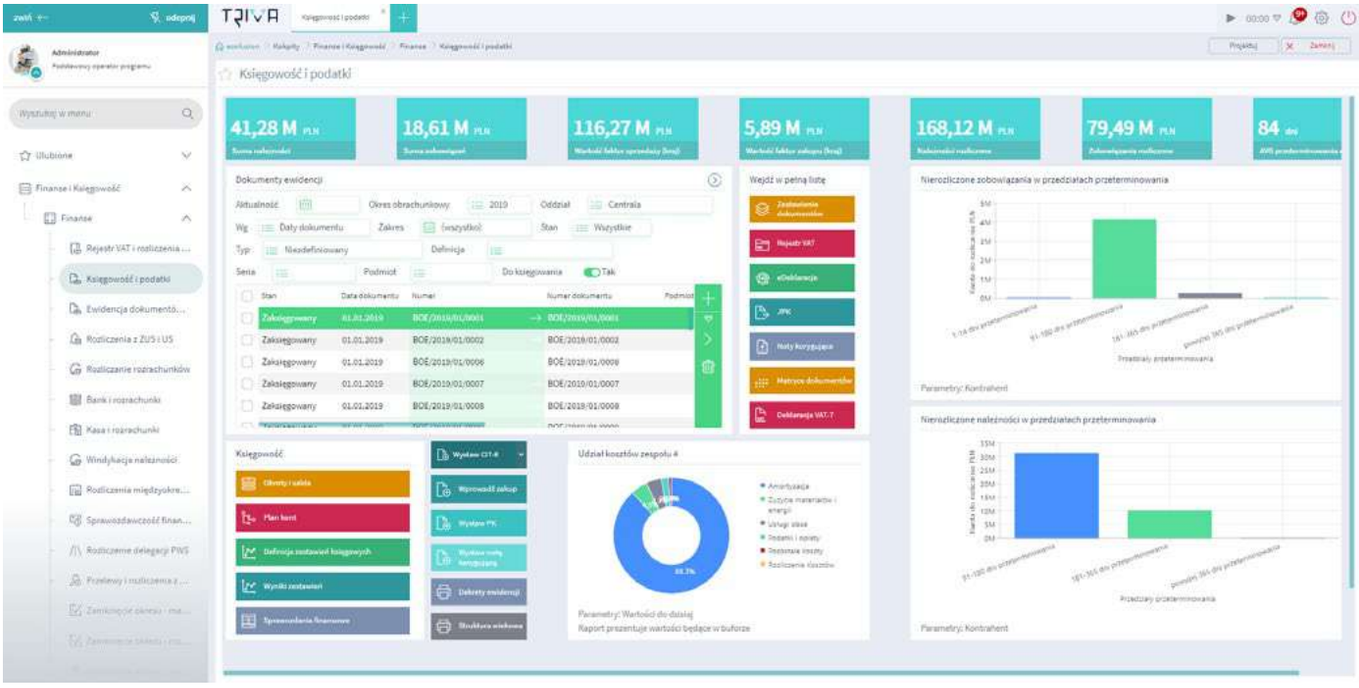
Jako w pełni zintegrowany system, TRIVA umożliwia zarządzanie głównymi procesami biznesowymi, zapewniając oszczędność kosztów, większą produktywność i dostosowanie do zmieniającego się otoczenia. TRIVA oferuje niespotykaną wydajność oraz dokładność w zakresie raportowania. Dane finansowe przedstawiane są w formule przejrzystych kokpitów zawierających niezbędne informacje oraz funkcje, które w łatwy sposób można dopasować do indywidualnych potrzeb użytkownika. Istnieje możliwość generowania raportów i analiz w czasie rzeczywistym, co pozwala podejmować lepsze i szybsze decyzje zarządcze.

System TRIVA ERP pozwala monitorować rezultaty działań marketingowych na każdym etapie – od pozyskania lead aż po finalną transakcję. W ten sposób pracownicy mogą na bieżąco sprawdzać efektywność projektów marketingowych w kontekście konwersji na konkretną sprzedaż. Dzięki integracji poszczególnych obszarów i funkcjonalności, np. CRM, Sprzedaż i zakupy oraz BI, firma ma dostęp do zawsze aktualnej i pełnej informacji na temat efektywności działań sprzedażowych. Łatwiej też wspierać działania handlowe skupiając się na potrzebach klientów, a nie koncentrując się na obsłudze systemu.

TRIVA ma wbudowany zintegrowany system Business Intelligence, który dzięki warstwie modelowania i łączenia danych z różnych źródeł tworzy cross-obszarowe modele biznesowe. Warstwa prezentacji odpowiada za wizualizację tych modeli na wskaźnikach, w tabelach (również przestawnych) oraz wykresach, co sprawia, że przekaz jest czytelny, a podejmowanie na jego podstawie decyzji szybkie i efektywne. Omawiany tutaj mechanizm Business Intelligence, często nazywany po prostu BI, w systemie TRIVA jest zawsze dostępny, niezależnie od rodzaju i ilości zakupionych licencji.

Poza funkcjami analizy dużych zbiorów danych TRIVA umożliwia automatyzację procesów biznesowych za pomocą wbudowanych mechanizmów Workflow. Te narzędzia skracają czas trwania procesów, zwiększają ich efektywność i redukują koszty. Eliminowane są czasochłonne, ręczne procesy, które są podatne na błędy, oraz fragmentaryczne rozwiązania, które działają tylko w odosobnionych obszarach, zamiast integrować się z całością systemu.

TRIVA to także rozwiązanie, które usprawnia zarządzanie zasobami ludzkimi, korzystając z aktualnych trendów i najlepszych praktyk wspieranych przez system informatyczny. Przykładowo, pomaga efektywnie zarządzać planem i kosztami szkoleń pracowników, monitorować ich postępy i oceniać efektywność, kontrolować okresowe badania i szkolenia zatrudnionych osób, spełniając tym samym wymogi prawne i normy jakościowe.



Chmurowy ERP

System ERP TRIVA wspiera rozwiązania chmurowe, co umożliwia korzystanie z najnowszych, wydajnych technologii i innowacji. Dzięki wsparciu dla rozwiązań chmurowych, takich jak np. Azure, klienci mogą korzystać z TRIVA w chmurze a firma Soneta stale wspiera i rozwija to podejście.

TRIVA może być dostosowywana do indywidualnych potrzeb i wymagań klientów dzięki wykorzystaniu technologii low-code. Użytkownicy mogą samodzielnie konfigurować Kokpity (interfejs systemu) wzbogacając ich funkcjonalność obsługą procesów workflow oraz informacjami z BI. W efekcie system staje się elastyczny, skalowalny i łatwy w obsłudze.

Na tle konkurencyjnych rozwiązań TRIVA ERP wyróżnia się wysoką kompleksowością i konfigurowalnością, zgodnością z polskim prawem oraz wysoką mobilnością i bezpieczeństwem.

Wdrożenie systemu TRIVA ERP działa jak katalizator wzrostu, innowacji i transformacji cyfrowej. Rozwiązanie zapewnia kompleksowe podejście do przepływu pracy i dokumentów w firmie oraz z jej otoczeniem biznesowym. Uzyskano to dzięki zastosowaniu elastycznego i ergonomicznego Interfejsu Kokpitów dla pracowników oraz dostępowi do Pulpitów samoobsługi pracowniczej dla użytkowników. Kontrahenci firm które używają systemu TRIVA również mogą korzystać z tej technologii, co wspiera pracę handlowców.

Oprogramowanie dostępne jest przez przeglądarkę lub dedykowaną aplikację mobilną. Każda osoba w firmie może realizować swoje zadania z dowolnego miejsca i z dowolnego urządzenia, zaczynając od prezesa firmy, przez menedżerów a na szeregowych pracownikach kończąc.

Kluczowe cechy

- kompleksowość i konfigurowalność,
- zgodność z polskim prawem,
- aplikacja mobilna i wersja przeglądarkowa,
- kokpity projektowane w technologii no-code,
- ujednolicony widok firmy w czasie rzeczywistym.

Wdrożenia i klienci: Międzynarodowe Targi Poznańskie, Muzeum Narodowe w Krakowie

Symfonia eBiuro

Produkt: aplikacja dla biur rachunkowych i jednoosobowych działalności gospodarczych

Dostawca/Producent: Symfonia

Informacje: symfonia.pl

Symfonia eBiuro to chmurowa aplikacja dla biur rachunkowych i jednoosobowych działalności gospodarczych, która pozwala sprawnie zarządzać uproszczoną księgowością, magazynem oraz sprawami kadrowo-płacowymi. System umożliwia szybkie przetwarzanie dokumentów z wykorzystaniem mechanizmów OCR, płynnie integruje się z oprogramowaniem finansowo-księgowym oraz usprawnia kontakty z klientami.

Symfonia eBiuro to chmurowa platforma z aplikacją mobilną do zarządzania biznesem, dostępna przez całą dobę z dowolnego miejsca i urządzenia. Rozwiązanie przeznaczone jest dla mikro i małych przedsiębiorstw oraz biur rachunkowych, umożliwiając zarządzanie procesami księgowymi, kadrowo-płacowymi oraz magazynowymi. Platforma umożliwia wygodne wprowadzanie dokumentów sprzedażowych i kosztowych. Elektroniczny obieg dokumentów, wspierany przez zaawansowane rozwiązanie OCR, zintegrowany został z ok. 20 systemami finansowo-księgowymi.

Moduły nowoczesnego biura

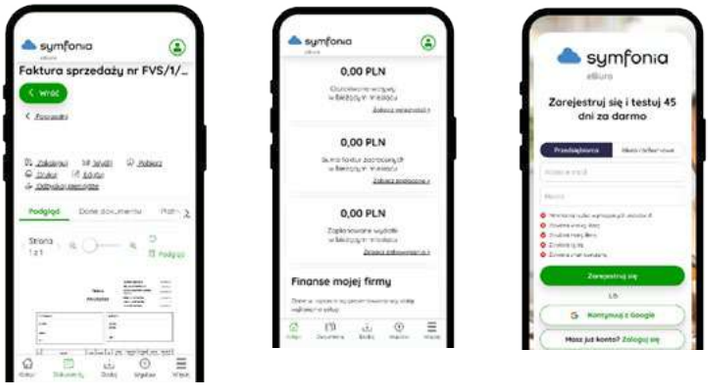
Wszystkie moduły, w tym KPiR, integracja z FK, OCR, fakturowanie, kadry i płace, konsultacje z klientem online oraz rozliczenia firm obsługiwane są z jednego miejsca. Sama aplikacja dostępna jest zaś w trzech wersjach językowych: polskiej, ukraińskiej i angielskiej.

Moduł Księgowość umożliwia samodzielne prowadzenie księgowości w zakresie księgowania dokumentów, zarządzania środkami trwałymi, rozliczania się z ZUS i US. Z kolei moduł Kadry i Płace pozwala dodawać umowy, rozliczać wynagrodzenia i delegacje, prowadzić ewidencję czasu pracy, a także generować wypłaty oraz wymagane deklaracje ZUS i US. Trzeci z dostępnych modułów Magazyn pozwala na bieżąco kontrolować stany magazynowe towarów oraz generować niezbędne dokumenty. Integracja z systemem Symfonia Finanse i Księgowość umożliwia przesyłanie danych między Symfonią eBiuro, a wspomnianym programem.

Moduł Konsultacje z klientem online pozwala na komunikację z klientem bezpośrednio w aplikacji oferując przy tym możliwość dodawania załączników. Ostatni z modułów, Rozliczanie firm tworzy zestawienia finansowe, w tym podatkowe i ubezpieczeniowe, z opcją ich wysyłki do rozliczanych firm.

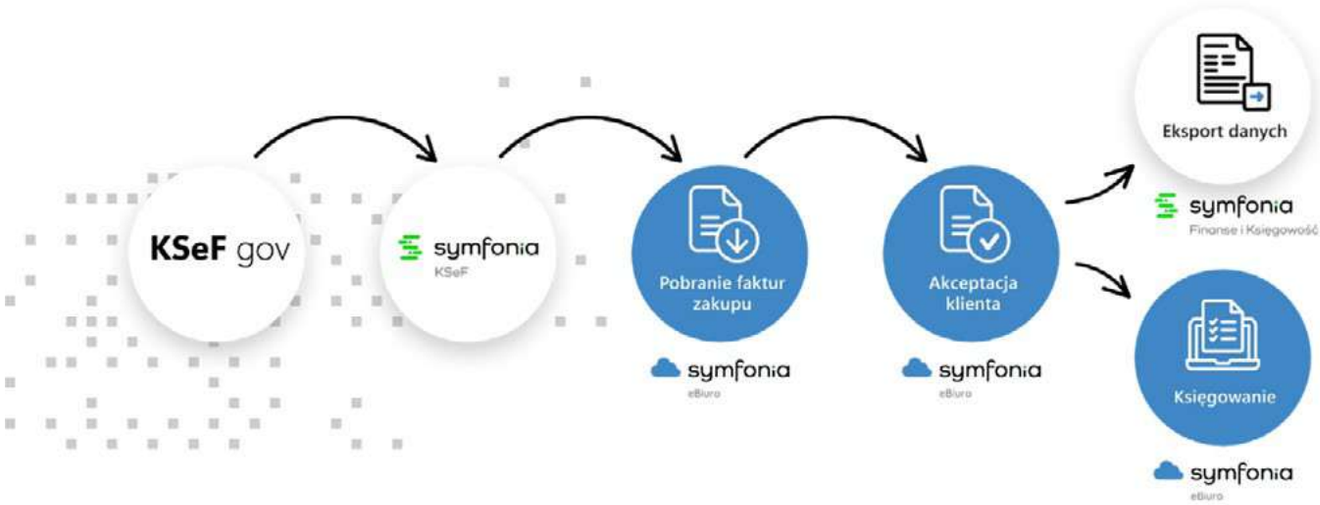
Unikalne cechy produktu

Na tle konkurencyjnych rozwiązań Symfonia eBiuro wyróżnia się pracą w chmurze, aplikacją mobilną oraz dedykowaną platformą komunikacji z klientem. Aplikacja bezpośrednio integruje się z ok. 20 systemami finansowo-księgowymi oraz ZUS, eliminując ryzyko błędów i zapewniając zgodność z przepisami.



Dzięki pracy w chmurze użytkownicy mają dostęp do danych o każdej porze z dowolnego miejsca na świecie. Aplikacja mobilna umożliwia zarządzanie biznesem, wykonywanie czynności księgowych oraz komunikację z klientami z poziomu smartfona. Podejście to zapewnia elastyczność, wygodę i mobilność użytkownikom, a biurom rachunkowym oszczędza czas i podnosi efektywność pracy.

W aplikacji dostępna jest dedykowana platforma do komunikacji z klientami, umożliwiająca szybką wymianę informacji i dokumentów. Biura rachunkowe mogą automatyzować procesy związane z obsługą klientów. Wbudowany system OCR ułatwia księgowanie dokumentów przez automatyczne rozpoznawanie ich



treści. Integracja zaawansowanego OCR i dedykowanej platformy komunikacyjnej pozwala na szybsze i bardziej efektywne zarządzanie klientami oraz procesami biznesowymi.

Wewnętrzna sekcja rozliczeń firm pozwala klientom na szybkie i łatwe sprawdzenie kwot do zapłacenia podatków oraz otrzymywanie przypomnień o płatnościach, co eliminuje zaległości i poprawia relacje z biurem rachunkowym.

Symfonia eBiuro to nie tylko kompleksowe rozwiązanie dla biznesu, które gwarantuje oszczędność czasu, automatyzację procesów i transparentność działania. Wsparcie techniczne w języku polskim, instrukcje, szkolenia i webinary zapewniają kompleksową obsługę użytkowników, przyczyniając się do sukcesu produktu na rynku. Regularne aktualizacje, co 4-5 tygodni, dostarczają nowych funkcjonalności i poprawek, odzwierciedlając zaangażowanie w ciągłe doskonalenie produktu.

Symfonia eBiuro to aplikacja dla biur rachunkowych i jednoosobowych działalności gospodarczych, która pozwala sprawnie zarządzać uproszczoną księgowością, magazynem oraz sprawami kadrowo-płacowymi. Organizacje, które potrzebują szerszego zakresu funkcjonalności, mogą zintegrować narzędzie z Symfonią Finanse i Księgowość. W ten sposób pracownicy uzyskują dostęp do zaawansowanych modułów księgowości, a więc możliwość obsługi większych firm.

Przykładowy scenariusz obiegu i akceptacji faktury w Symfonii eBiuro zakłada, że klient za pomocą kilku kliknięć ewidencjonuje i akceptuje faktury, podczas gdy księgowy może wygodnie zaksięgować je bezpośrednio w platformie Symfonia eBiuro (o ile firma rozlicza się w oparciu o uproszczoną księgowość) lub pobrać je do Symfonii Finanse i Księgowość.

Kluczowe cechy Symfonii eBiuro:

- praca w chmurze,
- aplikacja mobilna,
- bezpośrednie integracje z ok. 20 systemami finansowo-księgowymi oraz ZUS,
- dedykowana platforma komunikacji z klientem,
- wbudowany, zaawansowany OCR,
- sekcja rozliczeń, która poprawia relacje z biurem rachunkowym.

Wdrożenia i klienci: Biuro Rachunkowe Meritum, Biuro Rachunkowe Agnieszka Bujnicka, Biuro Rachunkowe Dara Svitlana Tochii, Firma Multi Technology

NVIDIA AI Computing by HPE

Produkt: portfolio rozwiązań dla wdrażania generatywnej sztucznej inteligencji

Dostawca/Producent: Hewlett Packard Enterprise / NVIDIA

Informacje: hpe.com

NVIDIA AI Computing by HPE to portfolio opracowanych przez Hewlett Packard Enterprise (HPE) i NVIDIA rozwiązań AI pozwalających przedsiębiorstwom na szybsze wdrażanie generatywnej sztucznej inteligencji. Informacja o współpracy ogłoszona została w czerwcu 2024 roku podczas konferencji HPE Discover w Las Vegas. Produkty z oferty, będące wynikiem kompleksowego, wieloletniego partnerstwa i zaangażowania obu firm, dostępne będą w sprzedaży od jesieni tego roku.

Generatywna AI ma ogromny potencjał, by przyspieszyć transformację biznesu. Jednak poziom skomplikowania obecnych technologii AI wiąże się ze zbyt wieloma ryzykami i barierami, które spowalniają ich powszechną adopcję w przedsiębiorstwach i mogą zagrozić najcenniejszemu majątkowi firmy, jakim są jej dane. Aby uwolnić ogromny potencjał generatywnej AI, HPE i NVIDIA wspólnie opracowały chmurę prywatną pod kątem sztucznej inteligencji, umożliwiając firmom skoncentrowanie się na opracowywaniu nowych przypadków użycia AI na rzecz zwiększenia produktywności i wykorzystania nowych strumieni przychodów.

Sojusz dostawców

Kluczowym komponentem NVIDIA AI Computing by HPE jest HPE Private Cloud AI - pierwsze tego rodzaju rozwiązanie, zapewniające integrację sieciowych i programowych produktów AI od NVIDIA z pamięcią masową, rozwiązaniami obliczeniowymi i chmurowymi HPE GreenLake. Wykorzystując tę technologie, firmy dowolnej wielkości mogą wejść na energooszczędną, szybką i elastyczną ścieżkę zrównoważonego opracowywania i wdrażania zastosowań generatywnej AI.

HPE Private Cloud AI to unikalne, oparte na chmurze rozwiązanie pozwalające szybciej uzyskać zwrot z inwestycji przy jednoczesnym zarządzaniu ryzykiem wynikającym ze stosowania sztucznej inteligencji. Podstawą dostępnego w jego ramach stosu oprogramowania do AI i danych jest platforma programowa NVIDIA AI Enterprise, która zawiera również mikrousługi wnioskowania NVIDIA NIM.

HPE Private Cloud AI wykorzystuje kopilota AI OpsRamp pomagającego zwiększyć efektywność działań IT. Zawiera samoobsługowe rozwiązanie chmurowe z zarządzaniem pełnym cyklem życia. Produkt dostępny jest w czterech konfiguracjach o różnej skali, dzięki czemu jest odpowiednie dla szerokiego zakresu zadań i przypadków użycia z wykorzystaniem AI.

Nowy kopilot OpsRamp wykorzystuje platformę obliczeniową NVIDIA do interpretacji dużych zestawów danych, której wyniki są prezentowane przez asystenta konwersacyjnego pozwalającego na zwiększenie efektywności zarządzania. OpsRamp będzie również zintegrowany z interfejsami API CrowdStrike, udostępniając jednolity widok mapy usług bezpieczeństwa punktów końcowych w całej swojej infrastrukturze i aplikacjach.

Wyselekcjonowane narzędzia AI

Platforma programowa NVIDIA AI Enterprise przyspiesza analizę danych i usprawnia opracowywanie i wdrażanie do produkcji kopilotów oraz innych zastosowań GenAI. NVIDIA NIM dostarcza łatwe w użyciu mikrousługi optymalizujące wydajność wnioskowania i zapewniające płynne przejście od prototypu do wdrożenia produkcyjnego modeli AI do różnych zastosowań.

Oprogramowanie HPE AI Essential stanowi uzupełnienie dla NVIDIA AI Enterprise i NVIDIA NIM. Jest to gotowy do użycia zestaw wyselekcjonowanych narzędzi do AI i danych, które zapewniają elastyczne rozwiązania, ciągłe wsparcie i usługi takie jak np. compliance dla danych i modeli czy funkcje zapewniające zgodność, przejrzystość i powtarzalność w całym cyklu życia AI.

Aby zapewnić optymalną wydajność oprogramowania do AI i danych, HPE Private Cloud AI zapewnia w pełni zintegrowany stos infrastruktury dla AI, w tym

rozwiązanie sieciowe NVIDIA Spectrum-X Ethernet, HPE GreenLake for File Storage i serwery HPE ProLiant z wsparciem dla platform NVIDIA L40S, NVIDIA H100 NVL Tensor Core i GH200 NVL2.

HPE Private Cloud AI bazuje na chmurze HPE GreenLake, co ułatwia zarządzanie, pozwala na automatyzację, orkiestrację i zarządzanie punktami końcowymi, obciążeniami roboczymi i danymi w środowiskach hybrydowych. Usługi w chmurze obejmują m.in. wskaźniki zrównoważonego rozwoju dla obciążeń roboczych i punktów końcowych. Z chmurą HPE GreenLake zintegrowane jest działanie OpsRamp AI, aby zapewnić obserwowalność i AIOps dla wszystkich produktów i usług HPE. OpsRamp zapewnia teraz obserwowalność dla całego stosu obliczeniowego NVIDIA, w tym dla oprogramowania NVIDIA NIM i AI, procesorów graficznych NVIDIA Tensor Core i klastrów AI, a także dla przełączników NVIDIA Quantum InfiniBand i NVIDIA Spectrum Ethernet. Administratorzy IT uzyskują wyniki analiz pozwalające na identyfikację anomalii i monitorowanie infrastruktury i obciążeń opartych na AI w hybrydowych środowiskach wielochmurowych.

Konfiguracje rozwiązań

Dostępne konfiguracje z najnowszymi GPU, CPU i superchipami NVIDIA obejmują:

- HPE Cray XD670 z obsługą ośmiu procesorów graficznych NVIDIA H200 NVL Tensor Core do tworzenia dużych modeli językowych (LLM),
- serwer HPE ProLiant DL384 Gen12 z NVIDIA GH200 NVL2 dla użytkowników LLM korzystających z dużych modeli i RAG,
- serwer HPE ProLiant DL380a Gen12 z obsługą do ośmiu procesorów graficznych NVIDIA H200 NVL Tensor Core dla użytkowników LLM potrzebujących elastycznej skalowalności swoich obciążeń roboczych GenAI.

HPE będzie wspierać NVIDIA GB200 NVL72 / NVL2, a także nowe architektury NVIDIA Blackwell, NVIDIA Rubin i NVIDIA Vera.

Dodatkowo, rozwiązanie HPE GreenLake for File Storage uzyskało certyfikację NVIDIA DGX BasePOD i walidację pamięci masowej NVIDIA OVX. Dzięki temu stanowi sprawdzone rozwiązanie do przechowywania plików, które pozwala szybciej przetwarzać duże zadania związane z AI, GenAI i obciążeniami wykorzystującymi procesory graficzne. HPE wprowadza to rozwiązanie równocześnie z zapowiedzianymi programami certyfikacji pamięci masowej dla architektury referencyjnej.

AI w drodze ku transformacji

Generatywna sztuczna inteligencja i szybsze obliczenia umożliwiają kompleksową transformację, ponieważ do rewolucji dołączają wszystkie branże. NVIDIA i HPE jeszcze nigdy tak głęboko nie zintegrowały swoich technologii. Dziś, łącząc cały stos obliczeniowy NVIDIA AI z technologią chmury prywatnej HPE, obie firmy są w stanie wyposażyć klientów korporacyjnych i specjalistów zajmujących się AI w najbardziej zaawansowaną infrastrukturę obliczeniową i usługi pozwalające poszerzyć granice zastosowań sztucznej inteligencji.

Wszystkie produkty i usługi wchodzące w skład NVIDIA AI Computing by HPE zostaną wprowadzone na rynek w ramach wspólnej strategii, która obejmuje zespoły sprzedażowe i partnerów handlowych, szkolenia oraz globalną sieć integratorów systemów — w tym Deloitte, HCLTech, Infosys, TCS i Wipro. Podejście to ma pomóc przedsiębiorstwom z różnych branż w realizacji złożonych zadań z wykorzystaniem sztucznej inteligencji.

Kluczowe cechy:

- cztery gotowe konfiguracje o różnej wydajności,
- obsługa wnioskowania, dostrajania i obciążeń RAG AI, które wykorzystują poufne dane,
- kontrola w zakresie prywatności danych, bezpieczeństwa, przejrzystości i governance,
- chmura z funkcjami ITOps i AIOps w celu zwiększenia produktywności,
- szybka ścieżka do elastycznego użytkowania, pozwalająca przygotować się na przyszły rozwój sztucznej inteligencji i związanych z nią możliwości.

Chmura w 2024 roku

Analitycy twierdzą, że rynek usług chmurowych dynamicznie rośnie i będzie rósł w najbliższych latach. Przyczyni się do tego głównie popularyzacja aplikacji sztucznej inteligencji.

WIESŁAW PAWŁOWICZ

Model chmurowy jest dobrze przygotowany do zaspokajania potrzeb użytkowników w zakresie wprowadzania innowacyjnych rozwiązań, opracowywania i wdrażania nowych aplikacji, a w szczególności sztucznej inteligencji i uczenia maszynowego. Dlatego, wg analityków rynku, popyt na usługi oferowane w chmurach publicznych będzie rósł w najbliższych latach. Można mieć nadzieję, że nowe regulacje prawne dotyczące przetwarzania w chmurze modeli AI planowane przez amerykański rząd nie zahamują tego rozwoju i polityka nie wpłynie negatywnie na rynek.

Jak rośnie chmura

Według IDC globalne przychody generowane przez usługi w chmurze publicznej osiągnęły w 2022 r. wartość 545,8 mld dol. i wzrosły o 22,9% w porównaniu z rokiem poprzednim. Jeszcze szybciej, bo o 28,8%, rósł popyt na podstawowe usługi chmurowe IaaS (infrastruktura jako usługa), PaaS (platforma jako usługa) oraz SaaS (oprogramowanie jako usługa). Zdaniem analityków z IDC, wydatki na IaaS i PaaS będą nadal rosnąć szybciej niż cały rynek usług świadczonych w chmurach publicznych.

Z kolei Gartner prognozuje, że globalne wydatki na usługi w chmurze publicznej w 2024 r. wyniosą 679 mld dol., a w roku 2027 przekroczą poziom 1 bln dol. Do 2028 r. chmury obliczeniowe staną się dla firm niezbędnym czynnikiem pozwalającym na utrzymanie konkurencyjności biznesu.

Podobne są najnowsze przewidywania IDC. Firma szacuje, że światowe wydatki na usługi w chmurze publicznej osiągną wartość 1,35 bln dol. już w roku 2027. Stany Zjednoczone będą wówczas największym rynkiem chmury publicznej, z prognozowanymi wydatkami na poziomie 697 mld dol. Na drugim miejscu uplasuje się Europa z inwestycjami o łącznej wartości 273 mld dol., a na trzecim Chiny (117 mld dol.).

Centra danych będą się kurczyć i migrować do dostawców usług kolokacyjnych opartych na platformach PaaS. W połączeniu z nowymi modelami as-a-service dla infrastruktury fizycznej przyniesie to chmurocentryczność usług i infrastrukturę lokalną opartą na modelach ekonomicznych

Dane IDC wskazują również na postępującą konsolidację. Chociaż pięciu największych dostawców usług w chmurze publicznej ma w rynku udział mniejszy niż 50%, to ich przychody rosły w 2022 r. szybciej niż średnia rynkowa, bo o 27,3%.

Największym dostawcą chmury publicznej na świecie jest Microsoft, którego udział w całym rynku wynosi 16,8%. Za nim plasuje się AWS (13,5%), a pierwszą piątkę największych dostawców uzupełniają: Salesforce, Google i Oracle.

Co będzie wpływać na wzrost popytu na usługi

„Wiele firm aktywnie inwestuje obecnie w technologie chmurowe przede wszystkim ze względu na ich potencjał we wspieraniu innowacji i zwiększania przewagi konkurencyjnej" – mówi Milind Govekar, analityk z firmy Gartner. Trend ten zauważają dostawcy i zwiększają inwestycje w rozbudowę infrastruktury.

Według Gartnera do 2027 roku 35% infrastruktury centrów danych będzie zarządzane z poziomu płaszczyzny sterowania opartej na chmurze. Firmy powinny się skupić na budowaniu w centrach danych infrastruktury natywnej dla chmury, migracji obciążeń z firmowych centrów danych do obiektów kolokacyjnych lub przyjęciu modeli as-a-service dla infrastruktury fizycznej.

„Ma to z jednaj strony stworzyć możliwości obsługi nowej, przewidywanej fali migracji aplikacji korporacyjnych do chmury, a z drugiej strony zapewnić podstawę do uruchamiania, wymagającego dużej mocy przetwarzania, zaawansowanego oprogramowania sztucznej inteligencji AI, które można będzie szybko wdrożyć na dużą skalę" – uważa Dave McCarthy, wiceprezes IDC ds. badań.

Zdaniem analityków IDC głównym czynnikiem powodującym w najbliższych latach zwiększanie wydatków na usługi w chmurach publicznych będzie wzrost wykorzystania generatywnej sztucznej inteligencji. „Jednocześnie nasze badania pokazują, że większość firm uważa dostawcę chmury publicznej za najbardziej strategicznego partnera technologicznego w ich biznesie" – mówi Lara Greden, dyrektor ds. badań w IDC.

Z kolei Gartner przewiduje, że do 2028 r. ponad 50% przedsiębiorstw będzie korzystać z branżowych platform chmurowych umożliwiających przyspieszenie realizacji inicjatyw biznesowych. W efekcie korzystanie z usług chmurowych stanie się standardem i koniecznością dla utrzymania się na konkurencyjnym rynku.

Najważniejsze trendy w rozwoju usług chmurowych

Gartner zaprezentował w 2023 r. najważniejsze, zdaniem analityków tej firmy, trendy dotyczące rozwoju usług chmurowych, centrów danych i infrastruktury brzegowej. Wykorzystanie chmury publicznej jest niemal powszechne, ale wiele wdrożeń jest doraźnych i źle zaimplementowanych. Dlatego jednym z największych wyzwań w najbliższych latach będzie konieczność ponownego przeanalizowania infrastruktury chmurowej, aby uczynić ją bardziej wydajną, odporną i opłacalną.

Zdaniem analityków Gartnera, analizy takie powinny koncentrować się na optymalizacji kosztów poprzez eliminację nadmiarowej, zbyt rozbudowanej lub nieużywanej infrastruktury chmurowej. Warto też budować odporność biznesową, która nie wymaga nadmiarowości na poziomie usług.

Trzeba pamiętać, że odpowiednio wdrożona infrastruktura chmurowa może być dobrym sposobem

Fot.: Freepik

np. na złagodzenie zakłóceń w łańcuchach dostaw lub ułatwić modernizację istniejącej infrastruktury. Według Gartnera 65% obciążeń i aplikacji do 2027 r. będzie zoptymalizowana i gotowa do pracy w chmurach. Dla porównania, w 2022 r. było to tylko 45%.

Nowe architektury i aplikacje będą jednak wymagać nowych rodzajów infrastruktury. Firmowe zespoły IT staną przed wyzwaniem sprostania rosnącym wymaganiom nowych typów infrastruktury, takich jak: infrastruktura brzegowa, aplikacje intensywnie wykorzystujące dane (analityka Big Data i sztuczna inteligencja), stosowanie architektur innych niż x86 dla wyspecjalizowanych obciążeń, bezserwerowe systemy brzegowe lub usługi mobilne 5G. Dlatego też Gartner przewiduje, że do 2026 r. 15% lokalnych obciążeń produkcyjnych będzie działać w kontenerach, w porównaniu z mniej niż 5% w roku 2022.

Centra danych będą się kurczyć i migrować do dostawców usług kolokacyjnych opartych na platformach PaaS. W połączeniu z nowymi modelami as-a-service dla infrastruktury fizycznej przyniesie to chmurocentryczność usług i infrastrukturę lokalną silnie opartą na modelach ekonomicznych. Według Gartnera do 2027 r. 35% infrastruktury centrów danych będzie zarządzane z poziomu płaszczyzny sterowania opartej na chmurze, w porównaniu z mniej niż 10% w roku 2022. Dlatego firmy powinny się skupić na budowaniu w centrach danych infrastruktury natywnej dla chmury, migracji obciążeń z firmowych centrów danych do obiektów kolokacyjnych lub przyjęciu modeli as-a-service dla infrastruktury fizycznej.

Warto zauważyć, że to brak umiejętności w lokalnych zespołach IT jest największą barierą hamującą inicjatywy modernizacji infrastruktury i wiele firm twierdzi, że nie jest w stanie zatrudnić specjalistów, aby wypełnić te luki. Takie firmy nie odniosą sukcesu, jeśli nie nadadzą priorytetu organicznemu wzrostowi umiejętności, zachęcając specjalistów do przyjmowania nowych ról jako inżynierów niezawodności lub konsultantów merytorycznych dla zespołów programistów i jednostek biznesowych. Gartner przewiduje, że do 2027 r. 60% zespołów ds. infrastruktury centrów danych będzie posiadać odpowiednie umiejętności w zakresie automatyzacji i chmury, w porównaniu z 30% w 2022 r.

Brak umiejętności w lokalnych zespołach IT to największa bariera hamująca inicjatywy modernizacji infrastruktury. Gartner przewiduje, że do 2027 roku 60% zespołów ds. infrastruktury centrów danych będzie posiadać odpowiednie umiejętności w zakresie automatyzacji i chmury, w porównaniu z 30% w roku 2022.

Jak polityka może wpłynąć na rozwój chmurowych usług AI

Obecnie trwa wojna o globalną dominację w erze AI. Chcąc ograniczyć chińskie postępy w dziedzinie sztucznej inteligencji, rząd Stanów Zjednoczonych rozważa możliwość wprowadzenia prawnych regulacji nakładających na amerykańskich dostawców usług chmurowych, takich, jak: Amazon, Google i Microsoft, obowiązek ujawniania informacji o klientach korzystających z platform do opracowywania aplikacji AI.

O tym, że przepisy takie mają być wymierzone głównie w chińskie firmy, otwarcie mówią przedstawiciele amerykańskiej administracji. „Chcemy mieć pewność, że zamkniemy każdą drogę, którą Chińczycy mogliby uzyskać dostęp do naszych modeli AI lub trenować własne przy wykorzystaniu usług świadczonych przez amerykańskie

firmy" – powiedziała Gina Raimondo, sekretarz handlu USA, w wywiadzie dla Bloomberga.
Jest to kolejny etap wojny gospodarczej między Stanami Zjednoczonymi i Chinami po wprowadzeniu zakazu eksportu procesorów AI w październiku 2022 r. oraz, rok później, zakazu sprzedaży chińskim firmom urządzeń do produkcji zaawansowanych układów scalonych. Sankcje takie można jednak omijać, wykorzystując do trenowania modeli sztucznej inteligencji usługi AI w chmurze oferowane przez dostawców, głównie amerykańskich, którzy dysponują najnowszymi procesorami do obsługi aplikacji AI oraz dostępem do większości istniejącej na całym świecie infrastruktury niezbędnej do tworzenia i trenowania modeli sztucznej inteligencji. Stąd też pomysł na uszczelnienie systemu sankcji.

„Ale regulacje takie mogą rzucić cień na globalny ekosystem AI. Po pierwsze, zagraniczne firmy stanęłyby w obliczu większej kontroli i nadzoru ze strony rządu USA. Może to prowadzić do opóźnień, dodatkowych kosztów i potencjalnych ograniczeń w rozwoju i wdrażaniu aplikacji AI" –mówi Charlie Dai, wiceprezes i główny analityk w firmie Forrester.
Wymóg ujawniania poufnych informacji na temat technologii, wykorzystania danych i operacji biznesowych może budzić poważne obawy o ochronę własności intelektualnej. Firmy będą się wahać, czy udostępniać zastrzeżone informacje, które mogą zostać przywłaszczone lub wykorzystane przez konkurencję.

„Większa przejrzystość może ujawnić wrażliwe dane i zwiększyć ryzyko naruszenia danych lub innych incydentów związanych z bezpieczeństwem. Jest to szczególnie niepokojące dla przedsiębiorstw przetwarzających wrażliwe dane. Oprócz tego niepewność dotycząca prawa może osłabić inwestycje w badania i rozwój sztucznej inteligencji, bo firmy obawiają się, że dzisiejsze dopuszczalne praktyki mogą jutro podlegać nowym ograniczeniom" – zwraca uwagę Charlie Dai.

W efekcie, planując wykorzystanie usług chmurowych, trzeba wziąć pod uwagę nie tylko efekty biznesowe i ekonomiczne, ale też dodatkowy czynnik polityczny.

Fot.: Freepik


FOUNDRY
Formerly IDG Communications