Forum Bezpieczeństwa Banków

IT Solution FACTOR | Hewlett Packard Enterprise

Jak wykorzystać bezpieczną, akcelerowaną platformę AI w ciągłej analizie anomalii, detekcji i przeciwdziałaniu praniu pieniędzy?

BEZPIECZEŃSTWO FILAREM ZGODNOŚCI

Marcin Krzemieniewski

Piotr Nogaś

AGENDA

- **System bezpieczeństwa End-to-end – zapotrzebowanie na moc obliczeniową.**
- Bezpieczna platforma HPE GL for Private Cloud Business Editon.
- Tsunami legislacyjne.
- Wymiana informacji - Cyber Threat Intelligence.
- HPE Swarm Learning – platforma AI dla bezpieczeństwa i zapobieganiu oszustwom i praniu pieniędzy.
- Podsumowanie proponowanego rozwiązania.

SYSTEM BEZPIECZEŃSTWA END-TO-END

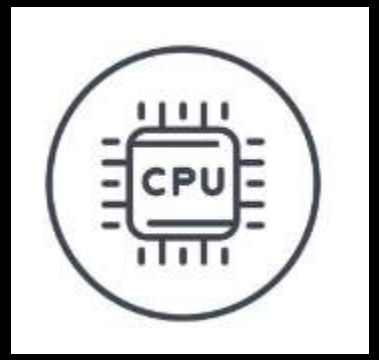
Gdzie mamy największe zapotrzebowanie na zasoby?

Dostępne **rozwiązania** zwirtualizowane:

- SIEM
- SOAR
- xDR
- Skanowanie AV
- NDR
- UEBA
- AntiFraud
- WAF
- Dekrypcja SSL
- IPS
- ....

Utrzymanie generycznej platformy

Optymalny dobór zasobów



IT Solution FACTOR | Hewlett Packard Enterprise

AGENDA

- System bezpieczeństwa End-to-end – zapotrzebowanie na moc obliczeniową.
- **Bezpieczna platforma HPE GL for Private Cloud Business Editon.**
- Tsunami legislacyjne.
- Wymiana informacji - Cyber Threat Intelligence.
- HPE Swarm Learning – platforma AI dla bezpieczeństwa i zapobieganiu oszustwom i praniu pieniędzy.
- Podsumowanie proponowanego rozwiązania.

PCBE: INTEGRACJA Z ISTNIEJĄCYM ŚRODOWISKIEM I SKALOWANIE

HPE INFOSIGHT

Zarządzanie pełnym stosem wspierane SI

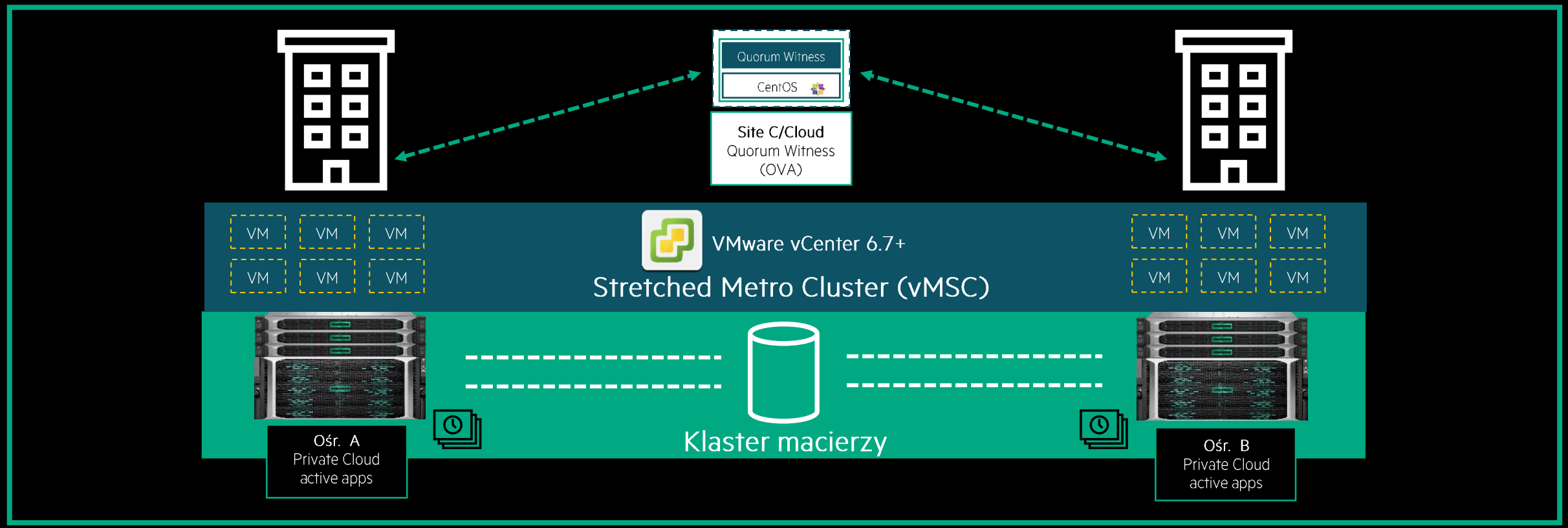
Sieć	Przełączniki z wbudowaną mikrosegmentacją (FW do L5), DDoS, Podłączenie do istniejącej infrastruktury: 2-8x 10/25/40/100GbE lub wykorzystanie przełączników klienta: 10/25/40/100 GbE	
Zarządzanie	VMware vCenter/power-shell/REST API (konsumpcja) Zintegrowane PCBE stack setup/manager/update: (Platforma)	
Wirtualizacja i konteneryzacja	VMware vSphere:	6.7-8.x
	Wbudowana opcja remediacji ransomware	
Przetwarzanie	HPE ProLiant:	DL3xx/5x0 CPU Intel/AMD
	GPU:	NVIDIA/AMD
	FPGA:	Intel/AMD
Pamięć masowa	HPE Alletra 5000/6000/MP Skalowanie: scale-up/scale-out	

Do 25% mniej rdzeni i RAM, do obsługi tego samego obciążenia - w porównaniu do vSAN

Dodatkowe środki bezpieczeństwa i automatyzacji akcelerowane sprzętowo.

TRYB VMWARE METRO STORAGE CLUSTER

RPO=0 przełączenie bieżącego bez utraty danych



Koherencja aplikacji
synchroniczne kopie VMek i aplikacji pomiędzy ośrodkami

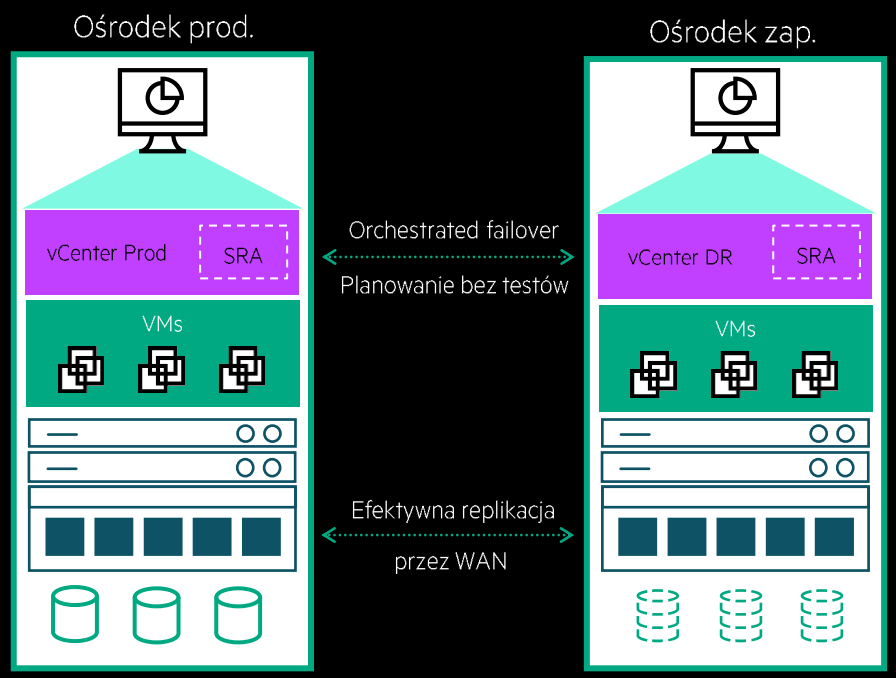
Odporność
na katastrofę ośrodka

Elastyczność
automatyczne przywrócenie aplikacji w działającym ośrodku

Certyfikacja
dla współpracy w trybie vMSC

REPLIAKCJA ASYNCHRONICZNA NA DOWOLNE ODLEGŁOŚCI

DR: Wsparcie dla łączy o niskiej jakości, przepustowości i wysokich opóźnieniach



Koherencja z aplikacjami
Repliki koherentne aplikacyjnie pomiędzy ośrodkami dla celów DR oraz DP

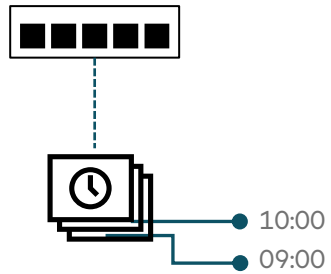
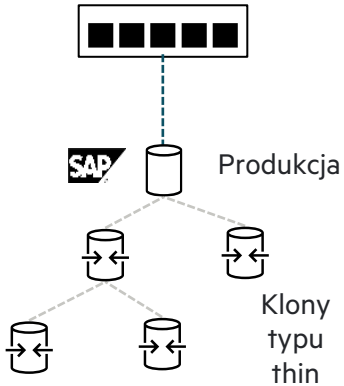
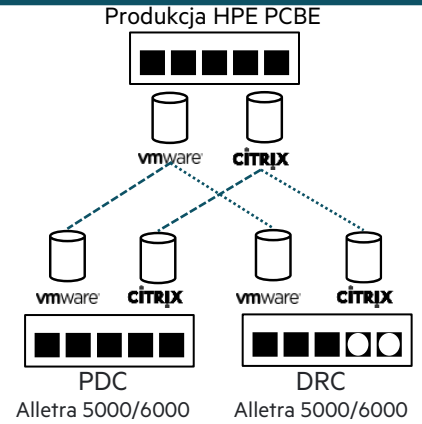
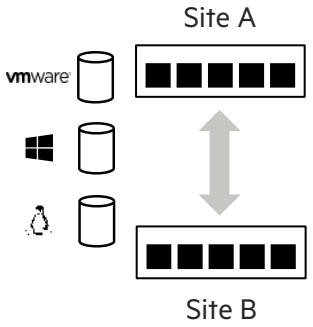
Efektywność
Uniklane skompresowane bloki przesyłane przez WAN

Elastyczne
Replikacja między róznymi generacjami i modelami pameci masowych

Zintegrowane
Zarządzane z klienta Webowego Vmware

WSPIERANY SPRZĘTOWO WSPÓŁISTNIEJĄCY BACKUP

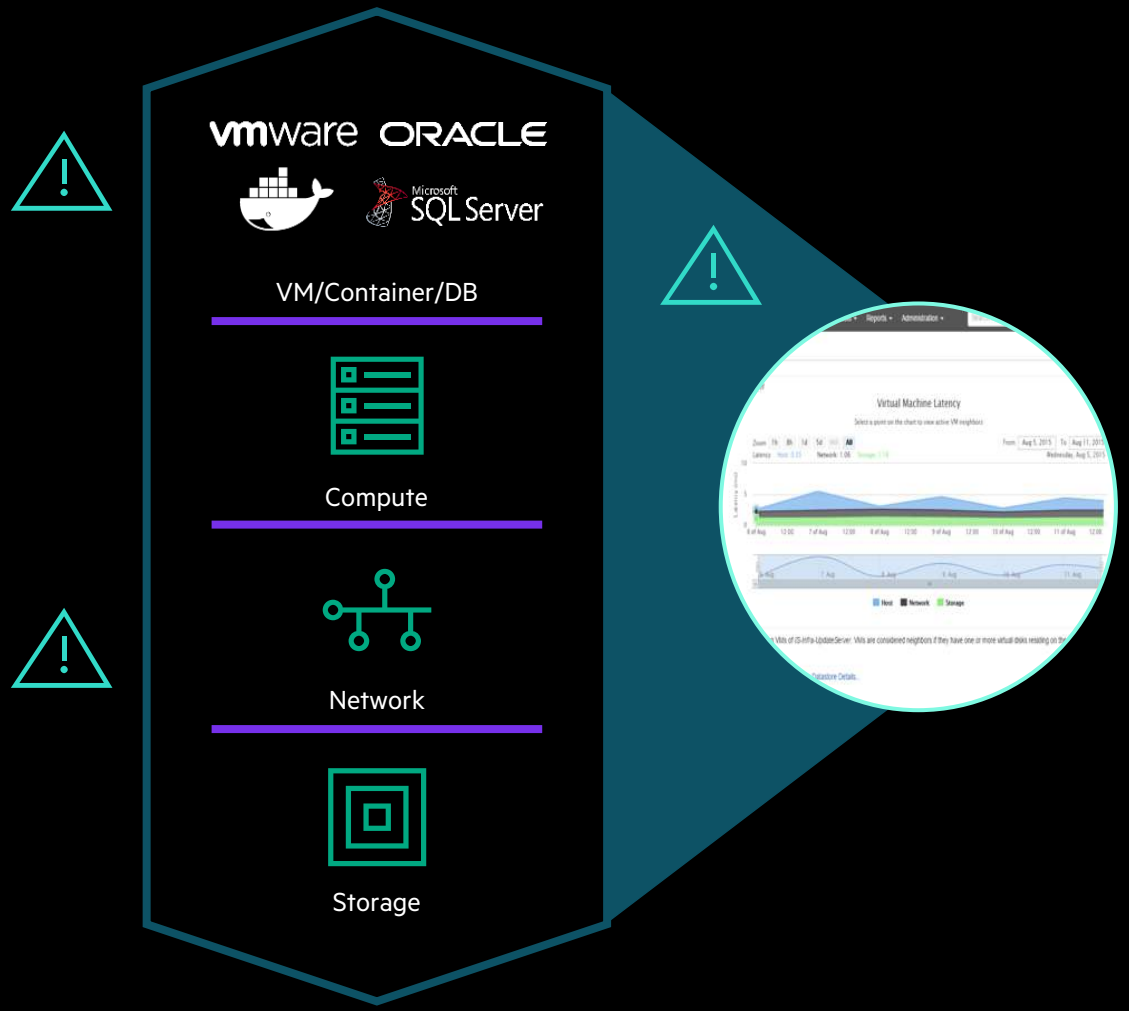
Aplikacyjnie spójne replikowane migawki akcelerowane sprzętowo z (chronione 2FA oraz immutability).

SmartSnap	SmartCopies	SmartReplicate	Peer Persistence
			
• Trwałe punkty przywrócenia • Efektywność (deduplikacja, kompresja oraz tzw. „thin”) • Natychmiastowe przywrócenie (w tym do wskazanego IRE) • Zapewnienie pełnej integralności • Konsystencja aplikacyjna i VADP	• Natychmiastowe klony typu „zero copy” • Efektywność (deduplikacja, kompresja oraz tzw. „thin”) • Szerokie zastosowanie: T&D, testy przywracania, CI/CD • Konsystencja aplikacyjna i VADP	• Przesyłane unikalne i skompresowane bloki • Szyfrowanie transmisji • Wsparcie dla wielu ośrodków zapasowych • Konsystencja aplikacyjna i VADP	• Granularne i efektywne • RPO=0 w przypadku utraty jednego ośrodka • Funkcjonalność wbudowana • Natychmiastowe przełączenie

Konsumpcja przez: GUI, Data Services Cloud Console, CLI, lub REST APIs (automatyzacja)

IT Solution FACTOR | Hewlett Packard Enterprise

WSPARCIE SI W ZARZĄDZANIU WYDAJNOŚCIĄ I ZASOBAMI



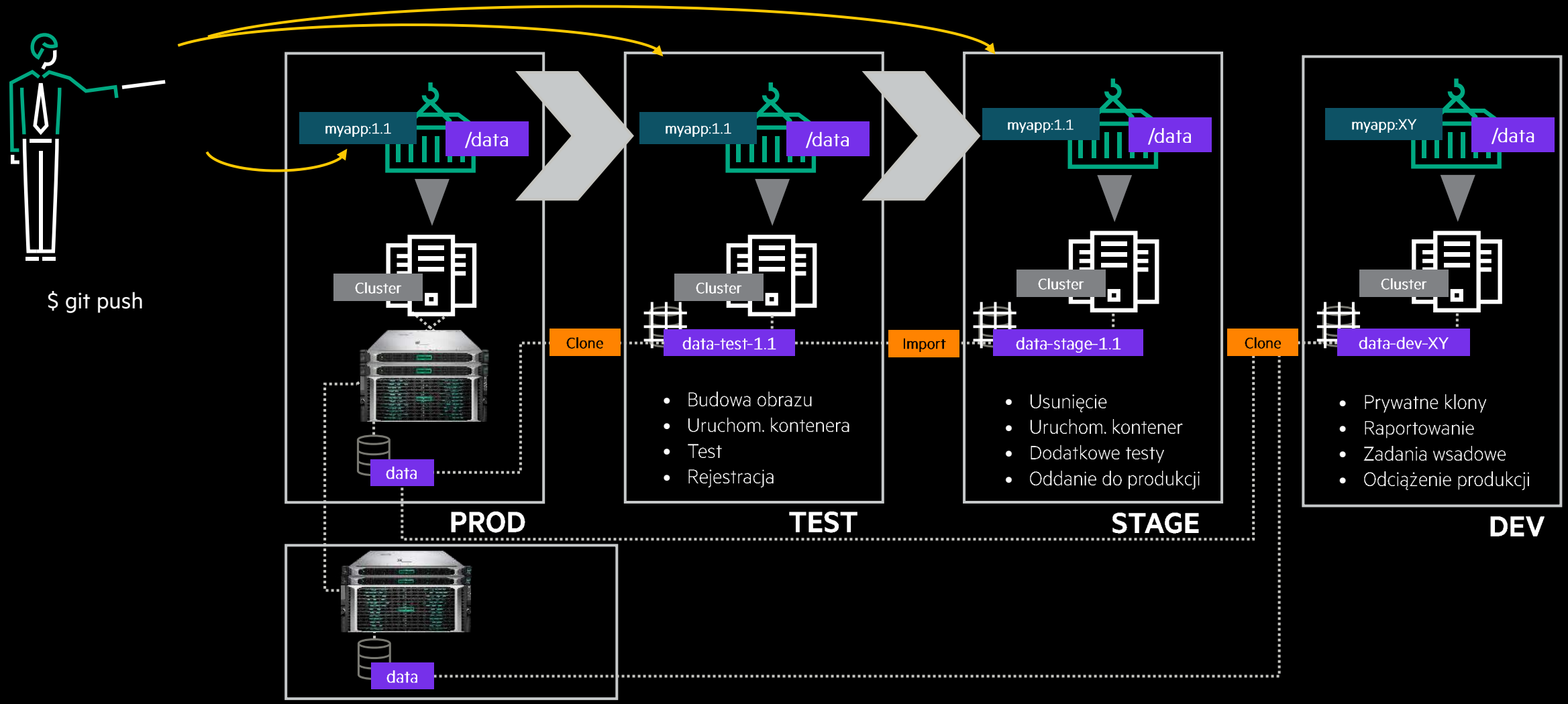
HPE InfoSight (zasilany SI)

- Zintegrowane procesy obsługi i planowania
- Analiza źródeł spadku wydajności
- Wskazanie uciążliwych VM'ek
- Zrównoważenie obciążenia węzłów
- Rekomedacje optymalizacji działania

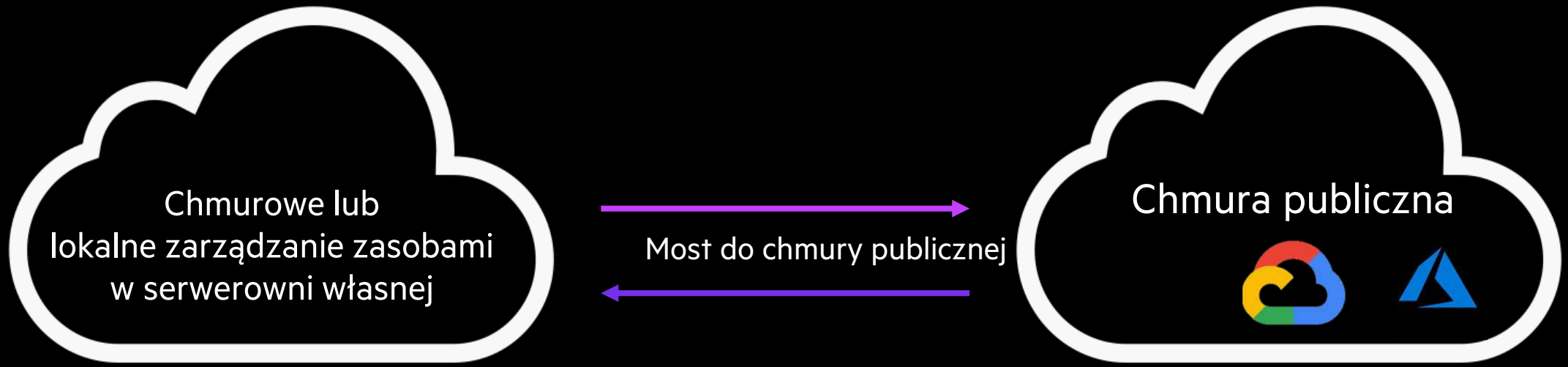
"na żądanie" dostępne w trybie 24x7. Nie wymaga alokacji zasobów.

WSPARCIE DLA DEVOPS ORAZ CI/CD

Continuous Integration/Continuous Delivery/Deployment



ZARZĄDZANIE MULTI-CHMURĄ



Chmura hybrydowa

DEV/TEST

PRODUKCJA

ANALITYKA

BC/HA/DR i
Ochrona danych

MATRYCA ODPOWIEDZIALNOŚCI

HPE GreenLake for Private Cloud Enterprise (Private Cloud Business Edition)

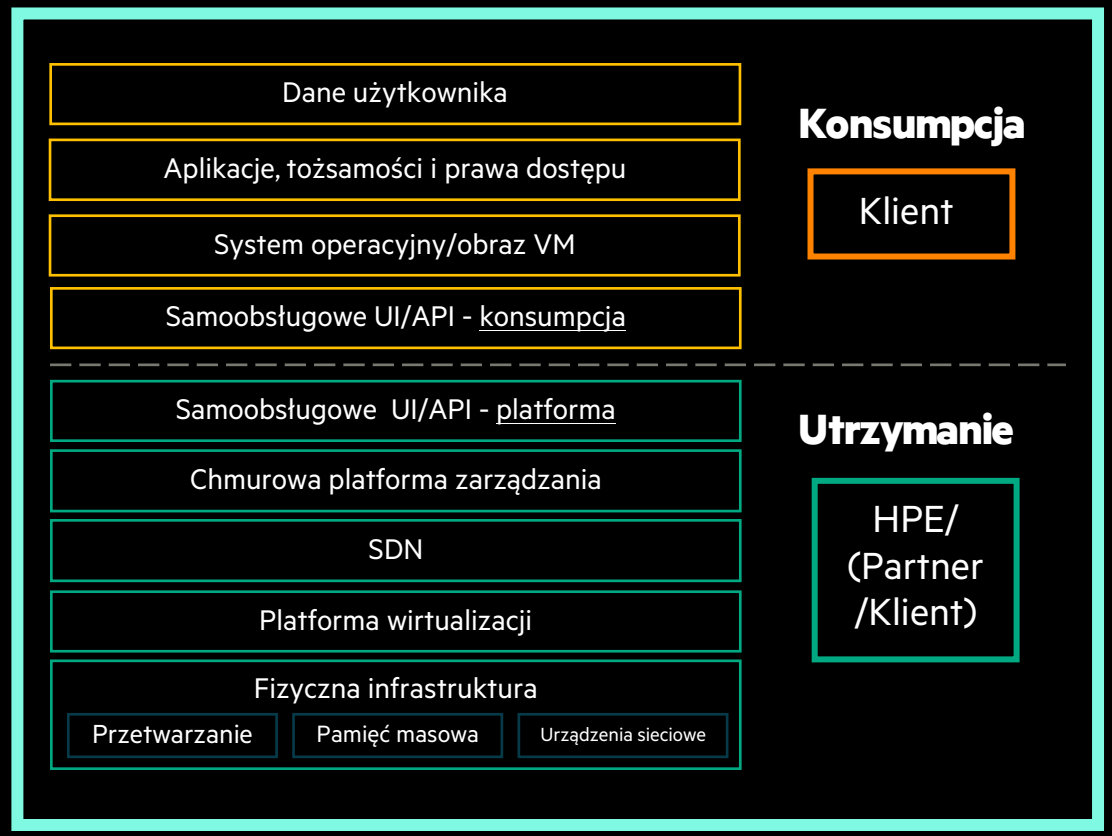
Klient zarządza na poziomie usług

- Systemy operacyjne i obrazy (VM)
- Aplikacje i narzędzia
- Dane aplikacyjne
- Konfiguracja i polityki sieciowe
- Bezpieczeństwo na brzegu sieci centrów przetwarzania

HPE (PARTNER/KLIENT) zarządza usługami infrastrukturalnymi

- Ochrony danych (backup)
- Tożsamością i prawami dostępu
- Bezpieczeństwem infrastruktury
- Odpornością i SLA

Podział odpowiedzialności pomiędzy HPE i klientem

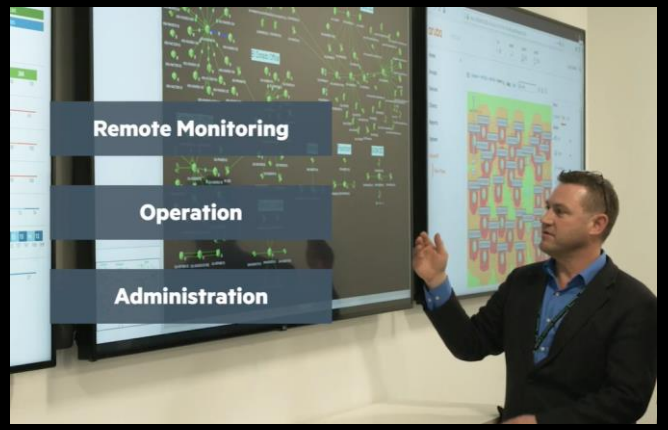


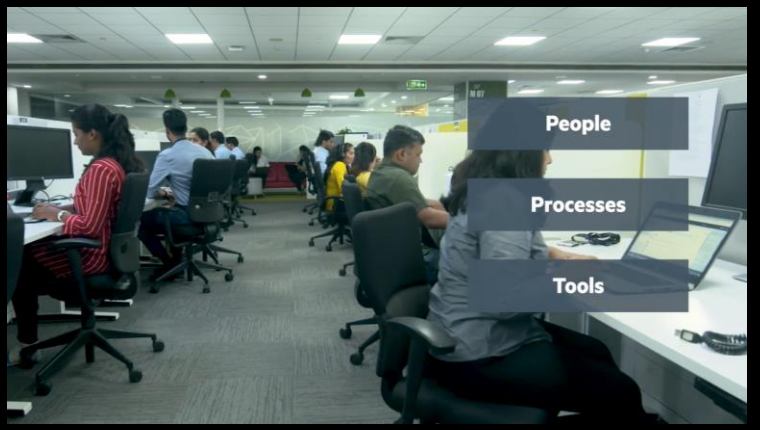
IT Solution FACTOR | Hewlett Packard Enterprise

HPE MANAGED SERVICES – BEZPIECZEŃSTWO I POLITYKI

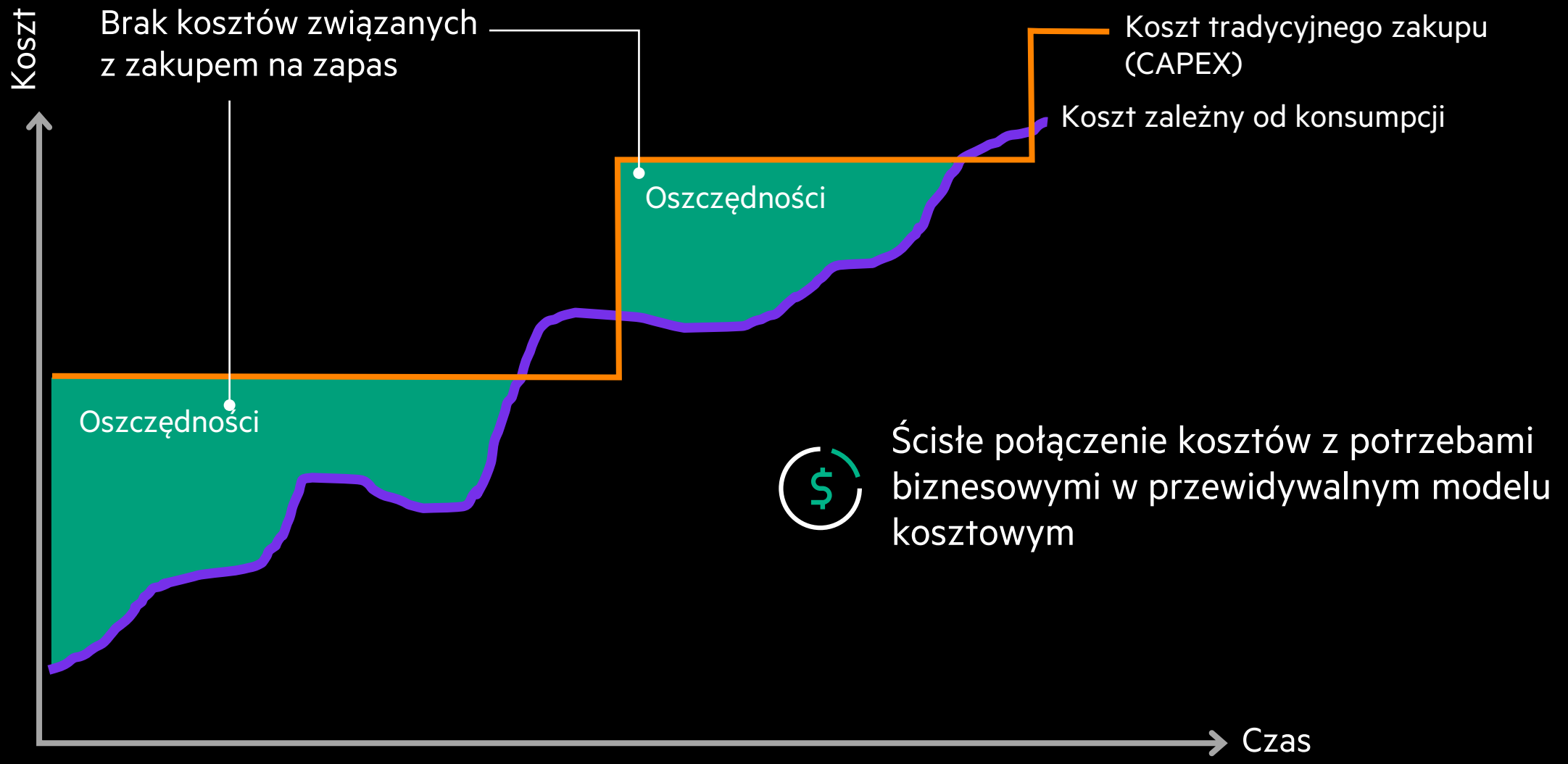
Zawarte w HPE GreenLake for Private Cloud Enterprise

- HPE Managed Services posiadają certyfikację ISO 27001, w oparciu o zasady/procedury i mechanizmy kontrolne.
- Miesięczne/kwartalne/półroczne/roczne audyty wewnętrzne i roczne audyty zewnętrzne
- Narzędzia używane przez HPE GMS posiadają certyfikaty ISO 27001, SOC 1 Typ I i SOC 2 Typ II
- Praktyka onboardingu/offboardingu zapewniająca włączenie/usunięcie poziomów dostępu, zgodnie z cyklem zaangażowania
- Kontrolne weryfikacje w tle
- 100% pracowników przeszkolonych w ITIL
- 100% obowiązkowych i regularnych szkoleń dla pracowników





DOSTĘPNE W TRYBIE TRADYCYJNYM I NA ŻĄDANIE (SUBSKRYPCJA)



Ścisłe połączenie kosztów z potrzebami biznesowymi w przewidywalnym modelu kosztowym

AGENDA

- System bezpieczeństwa End-to-end – zapotrzebowanie na moc obliczeniową.
- Bezpieczna platforma HPE GL for Private Cloud Business Editon.
- **Tsunami legislacyjne.**
- Wymiana informacji - Cyber Threat Intelligence.
- HPE Swarm Learning – platforma AI dla bezpieczeństwa i zapobiegania oszustwom i praniu pieniędzy.
- Podsumowanie proponowanego rozwiązania.

REGULACJE: KOSTKA I HIERARCHIA

EU Cybersecurity Regulatory Framework

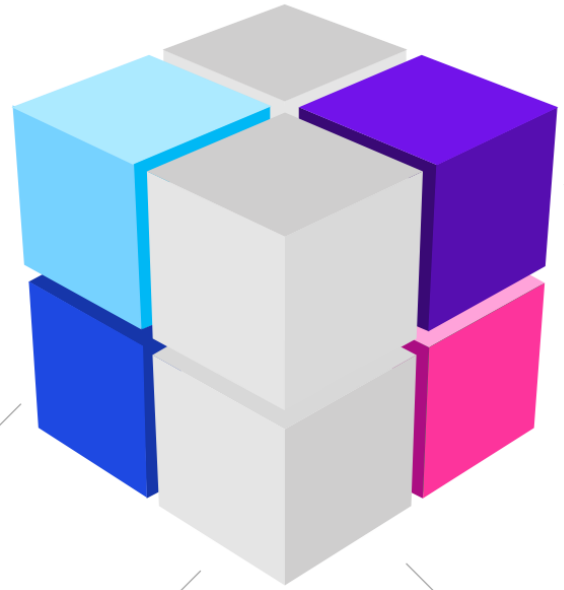
REGULATION (EU) 2019/881 on Cybersecurity Act (CSA)
Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.

Directive NIS2 (EU) 2022/2555
Sets cybersecurity measures on entities falling under critical infrastructure sectors.

DORA (Digital Operational Resilience Act) – Financial sector Regulation (EU) 2022/2554
Ensures that financial entities in EU remain resilient through a severe operational disruption.

Cyber Resilience Act (proposal)
Use of EU cybersecurity certifications and rules to ensure more secure hardware and software products.

RED - radio equipment directive 2014/53/EUEN
Establishes a framework for placing radio equipment on market and subjects certain categories of radio equipment to increased level of cybersecurity, personal data protection and privacy.



Regulation (EU) 2021/887 ECCC (Network of National Coordination Centres)
Boosts research excellence and the competitiveness of the Union in the filed of cybersecurity.

Directive (EU) 2019/1937 on Whistle-blower
Reports of violations of NIS requirements

Directive CER (EU) 2022/2557 (Resilience of critical entities)
strengthens the resilience of critical infrastructure to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage.

Network Code on sector-specific rules for cybersecurity aspects of cross border electricity flows (NCCS)
Sets a standard for cross border flows in EU.

(non exhaustive list)

IT Solution FACTOR | Hewlett Packard Enterprise

Source: https://assets.kpmg.com/content/dam/kpmg/be/pdf/2023/KPMG-Webinar-on-NIS2-2023-05-23.pdf

ZMIANY REGULACJI

Akt o Solidarności Cybernetycznej (CSA)

Wzmocnienie solidarności i zdolności Unii w zakresie wykrywania zagrożeń i incydentów cyberbezpieczeństwa, przygotowania się i reakcji na nie COM/2023/209

Stan:	propozycja
Data złożenia:	2023.04.18
Data wejścia w życie:	CY24H2 (oczekiwana)

Kluczowe postanowienia:

Europejski system ostrzegania o cyberbezpieczeństwie, ogólnoeuropejska sieć krajowych i transgranicznych centrów cybernetycznych.

Akt o Cyberbezpieczeństwie (CA)

w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013

Status: obowiązuje

Kluczowe postanowienia:

- Certyfikacja, **Nadzór rynku i zgodności,** współpraca między państwami członkowskimi, zainteresowanymi stronami z branży i ENISA

Akt o Odporności Cybernetycznej (CRA)

Status:	propozycja
Data złożenia:	2022.09.15
Data wejścia w życie:	CY24H1 (oczekiwana)

Kluczowe postanowienia:

Nakłada obowiązki w zakresie cyberbezpieczeństwa na wszystkie produkty zawierające elementy cyfrowe, których zamierzone i przewidywalne zastosowanie obejmuje bezpośrednie lub pośrednie połączenie danych z urządzeniem lub siecią. Nakłada obowiązek dbałości o bezpieczeństwo w cyklu życia produktu.

Dyrektywy CER/NIS 2

Status: weszły w życie 16 stycznia 2023 roku; wymagają transponowania do prawa krajowego

Kluczowe postanowienia:

Podlegają podmioty publiczne i prywatne. Tworzą komplementarne, zharmonizowane ramy prawne w zakresie zapewniania ciągłości usług kluczowych dla państwa oraz odporności (fizycznej i w cyberprzestrzeni) podmiotów je świadczących.

https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754614/EPRS_BRI(2023)754614_EN.pdf

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209

https://www.enisa.europa.eu/topics/incident-response/cyclone

ZMIANY REGULACJI

Akt w Sprawie Sztucznej Inteligencji (AIA)

Status: zatwierdzony przez PE 13.03.2024.

Stosuje się do:

dostawców wprowadzających do obrotu lub oddających do użytku systemy sztucznej inteligencji w UE, niezależnie od tego, czy dostawcy ci mają siedzibę w Unii czy w państwie trzecim

- **użytkowników systemów sztucznej inteligencji**, którzy znajdują się w Unii.

Dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję (ALD)

Projekt dyrektywy UE w sprawie odpowiedzialności za SI został opublikowany w dniu 28 września 2022 r., obecnie prowadzone są prace legislacyjne nad nim. Z uwagi na rozbieżności stanowisk ujawnione w trakcie tych prac, **uchwalenie w tej kadencji Parlamentu Europejskiego dyrektywy w sprawie odpowiedzialności za SI, należy uznać za wątpliwe.**

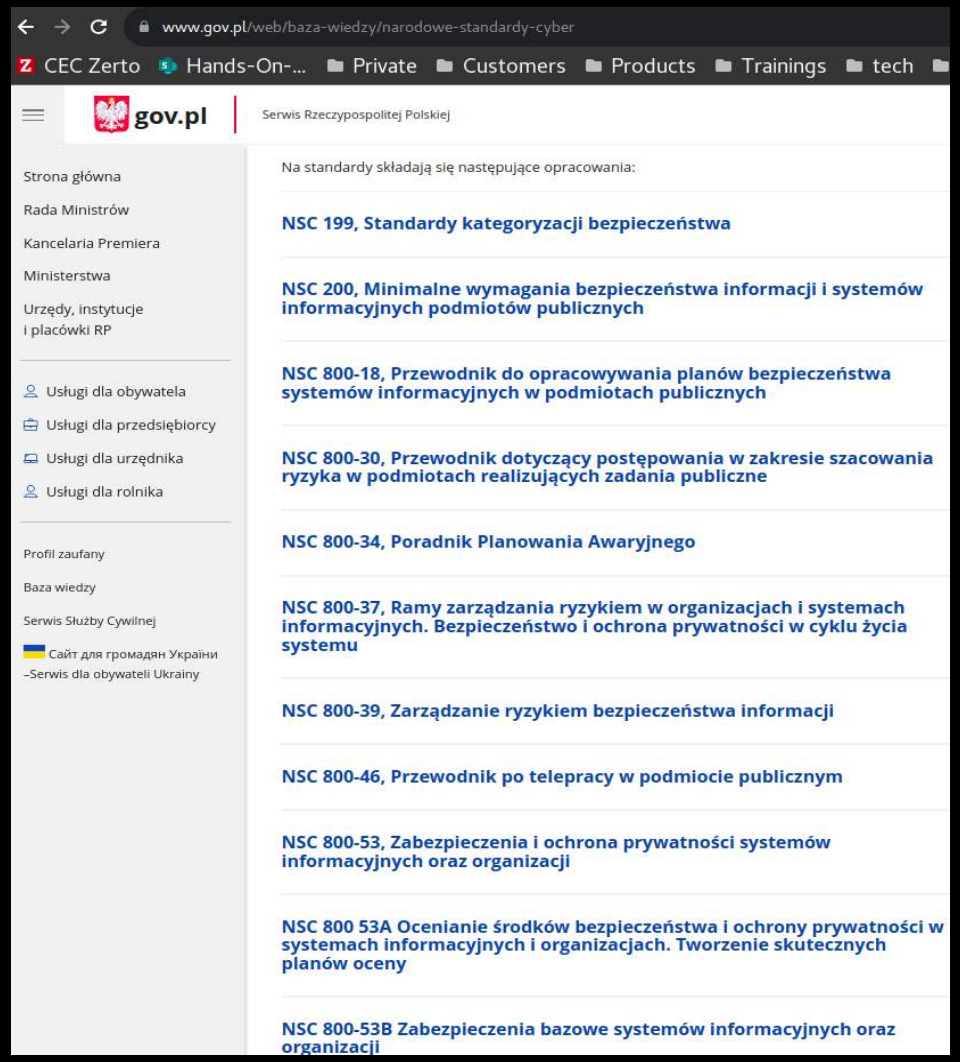
Ustawa - Prawo Komunikacji Elektronicznej (PKE).

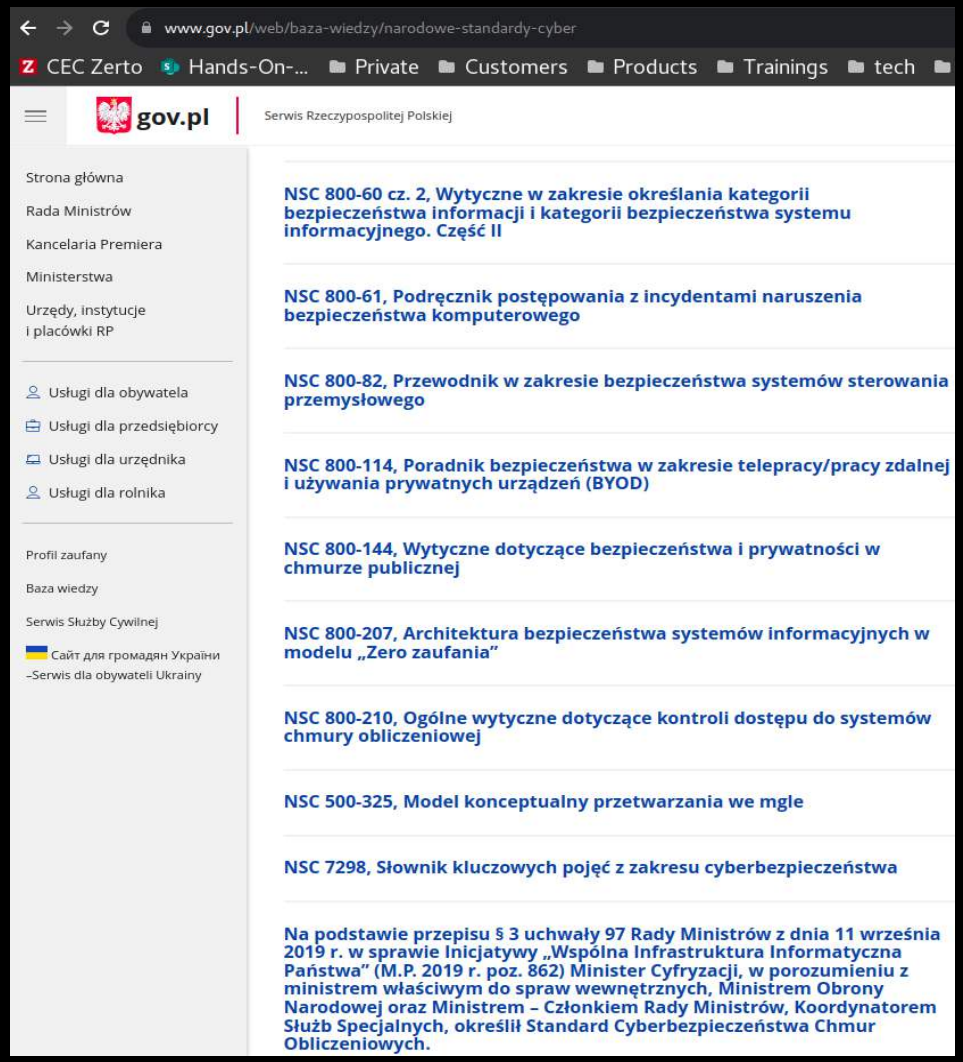
Status: projekt PKE został opublikowany. Z chwilą przyjęcia PKE dojdzie do uchylenia przepisów ustawy - Prawo telekomunikacyjne.

- rozszerza zakres podmiotowy na podmioty nie świadczące usług telekomunikacyjnych per se , ale świadczące usługi komunikacji interpersonalnej niewykorzystującej numerów, określane jako usługi OTT (Over-the-top) w tym **poczta elektroniczna, komunikatory internetowe, czy czaty internetowe.**

Źródła:
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52021PC0206
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52022PC0496
https://www.gov.pl/web/premier/projekt-ustawy-prawo-komunikacji-elektronicznej2

ZMIANY W REGULACJACH
Narodowe Standardy Cyberbezpieczeństwa





IT Solution FACTOR | Hewlett Packard Enterprise

Źródło: https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyberbezpieczenstwa2

ZMIANY REGULACJI

Ustawa o **cyfrowej odporności operacyjnej sektora finansowego** zmieniająca rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 i (UE) 2016/1011 (DORA)

Status: obowiązuje

Data wejścia w życie: 2023.01.16

harmonizuje przepisy dotyczące odporności operacyjnej sektora finansowego. Ma zastosowanie do 20 różnych typów podmiotów finansowych oraz zewnętrznych dostawców usług w zakresie technologii informacyjno-komunikacyjnych (ICT).

Kluczowe postanowienia:

- **Zarządzanie ryzykiem ICT** (w tym stron trzecich): zasady i wymagania dotyczące ram zarządzania ryzykiem ICT, w tym zewnętrznych dostawców ryzyka, kluczowe postanowienia umowne
- Cyfrowe **testy odporności operacyjnej**: testy podstawowe i zaawansowane
- **Incydenty ICT**: Wymagania ogólne; zgłaszanie właściwym organom poważnych incydentów związanych z ICT
- **Wymiana informacji**: Wymiana informacji i danych wywiadowczych na temat zagrożeń cybernetycznych
- **Nadzór kluczowych zewnętrznych dostawców**: Ramy nadzoru nad krytycznymi zewnętrznymi dostawcami ICT

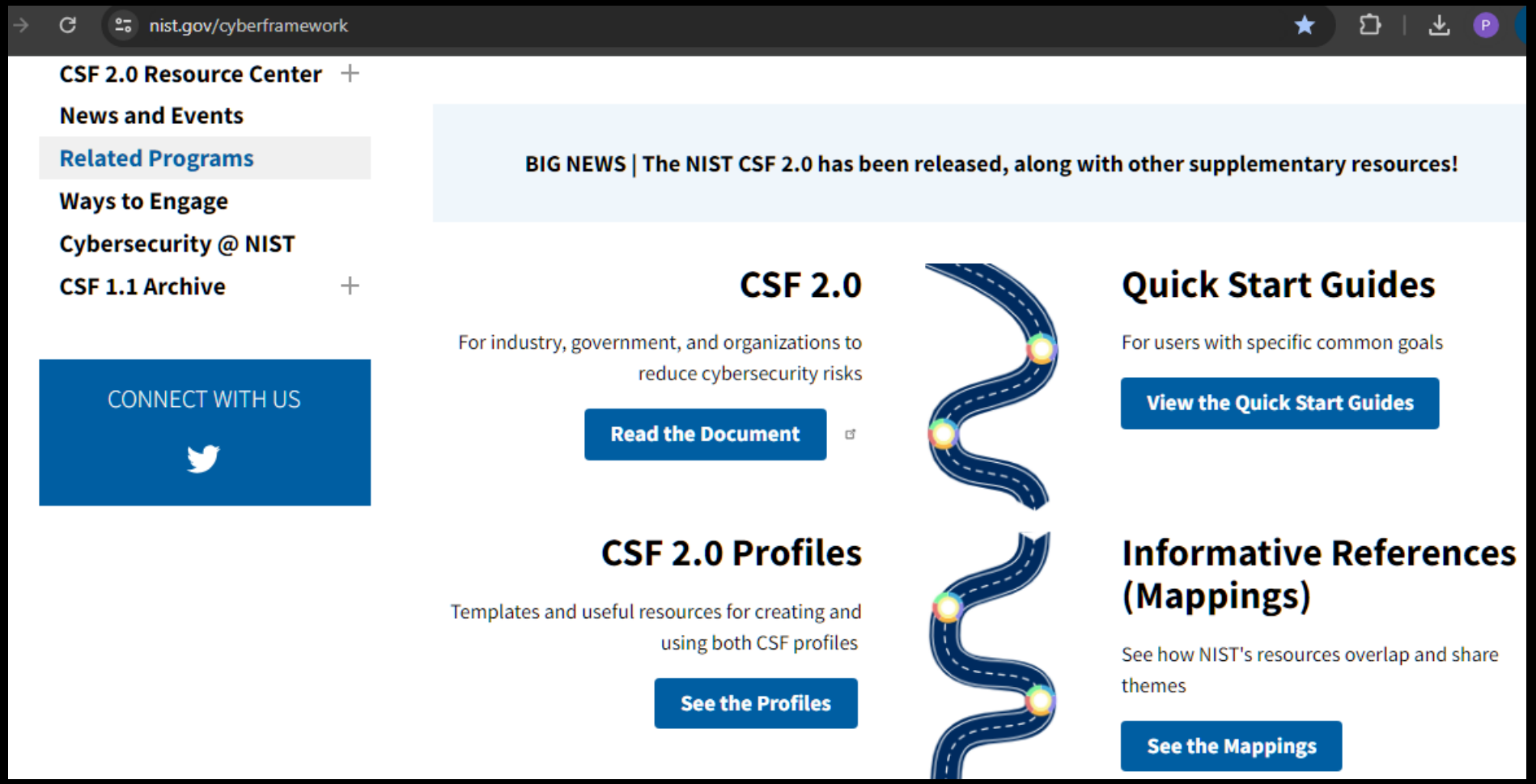
22,000

to szacowana liczba instytucji finansowych w Unii Europejskiej, dla których będzie miało zastosowanie Rozporządzenie DORA

Źródło: PWC

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554
https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

ZMIENNOŚĆ W ZAKRESIE ZGODNOŚCI



The agency has finalized the framework's first major update since its creation in 2014.

February 26, 2024

IT Solution FACTOR | Hewlett Packard Enterprise

AGENDA

- System bezpieczeństwa End-to-end – zapotrzebowanie na moc obliczeniową.
- Bezpieczna platforma HPE GL for Private Cloud Business Editon.
- Tsunami legislacyjne.
- **Wymiana informacji - Cyber Threat Intelligence.**
- HPE Swarm Learning – platforma AI dla bezpieczeństwa i zapobieganiu oszustwom i praniu pieniędzy.
- Podsumowanie proponowanego rozwiązania.

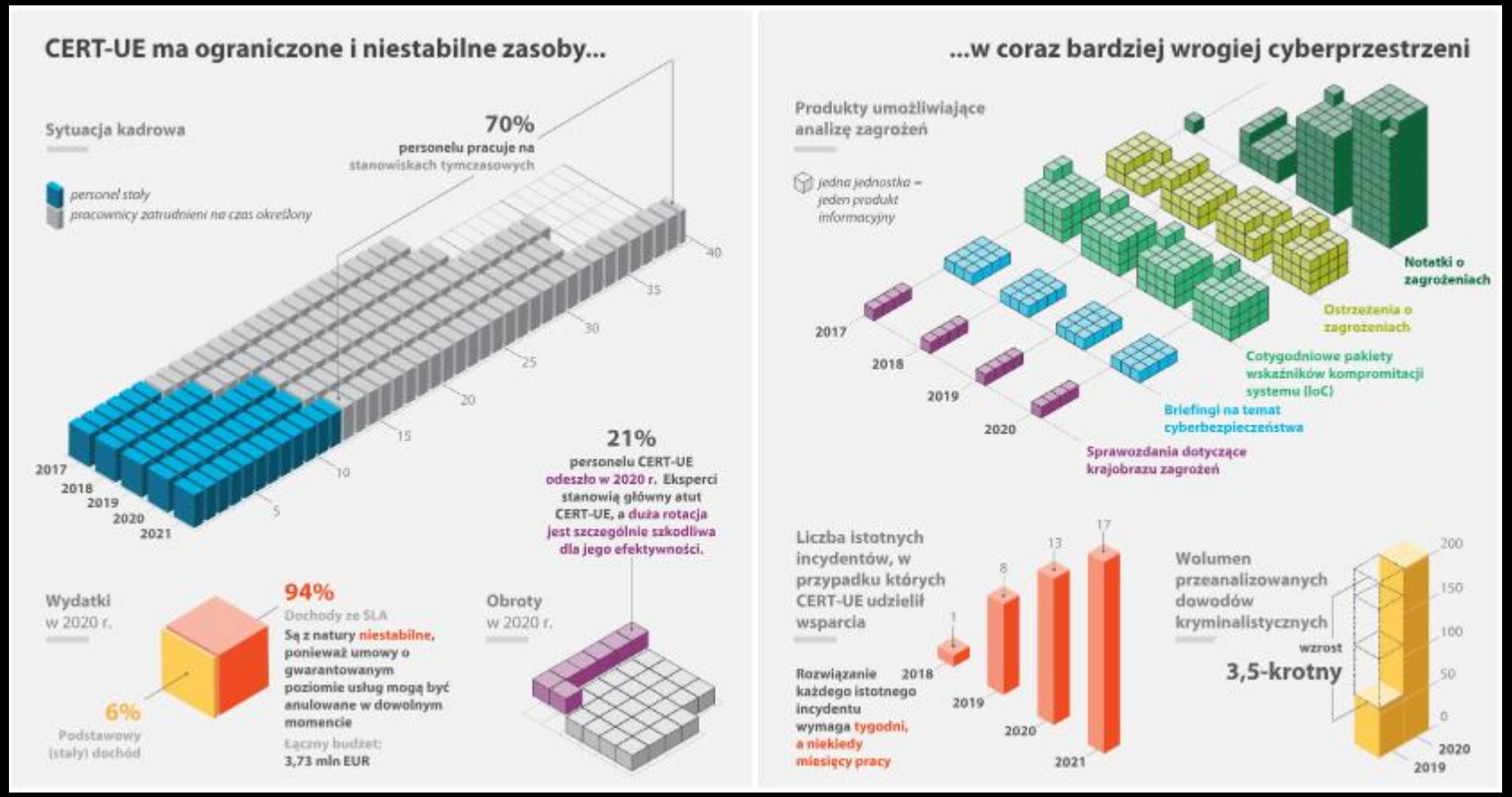
CTI NA POZIOMIE UE

- **7 stycznia 2024r**., weszło w życie nowe rozporządzenie w sprawie cyberbezpieczeństwa ustanawiające środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i jednostkach organizacyjnych Unii. W rozporządzeniu ustanawia się środki służące ustanowieniu wewnętrznych ram zarządzania ryzykiem w cyberprzestrzeni, zarządzania nim i jego kontroli dla każdego podmiotu Unii oraz ustanawia się nową międzyinstytucjonalną **Radę ds. Cyberbezpieczeństwa (IICB)** w celu monitorowania i wspierania ich wdrażania przez podmioty Unii.
- Zapewnia to rozszerzony mandat zespołu reagowania na incydenty komputerowe w instytucjach, organach, urzędach i agencjach **UE (CERT-UE)** jako **centrum wywiadu o zagrożeniach**, wymiany informacji i koordynacji reagowania na incydenty, centralnego organu doradczego i dostawcy usług. Zgodnie ze swoim mandatem CERT-UE zostaje przemianowany na **Służbę ds. Cyberbezpieczeństwa** dla instytucji, organów, urzędów i agencji Unii, ale zachowuje nazwę skróconą „CERT-UE”.
- Zgodnie z harmonogramem określonym w rozporządzeniu, **podmioty Unii ustanowią wewnętrzne procesy** zarządzania cyberbezpieczeństwem i będą stopniowo wprowadzać konkretne środki zarządzania ryzykiem w cyberprzestrzeni przewidziane w rozporządzeniu. IICB zostanie utworzona i rozpocznie działalność tak szybko, jak to możliwe, w celu zapewnienia strategicznego kierowania CERT-UE w ramach jego rozszerzonego mandatu, zapewnienia wskazówek i wsparcia podmiotom Unii oraz monitorowania wdrażania rozporządzenia.

Źródło: https://www.riskcompliance.pl/news/nowe-przepisy-zwiekszajace-cyberbezpieczenstwo-instytucji-ue/

WYMIANA INFORMACJI

- Agregacja danych
- Normalizacja danych
- Standaryzacja informacji
- Przetwarzanie w czasie zbliżonym do rzeczywistego



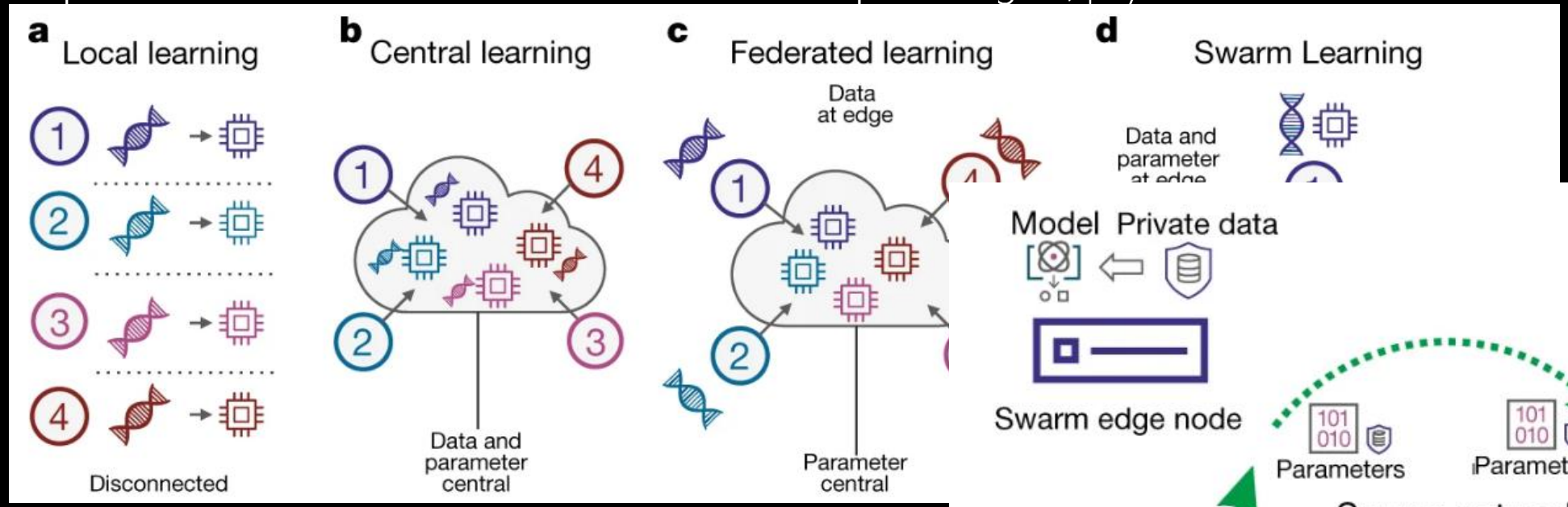
IT Solution FACTOR | Hewlett Packard Enterprise

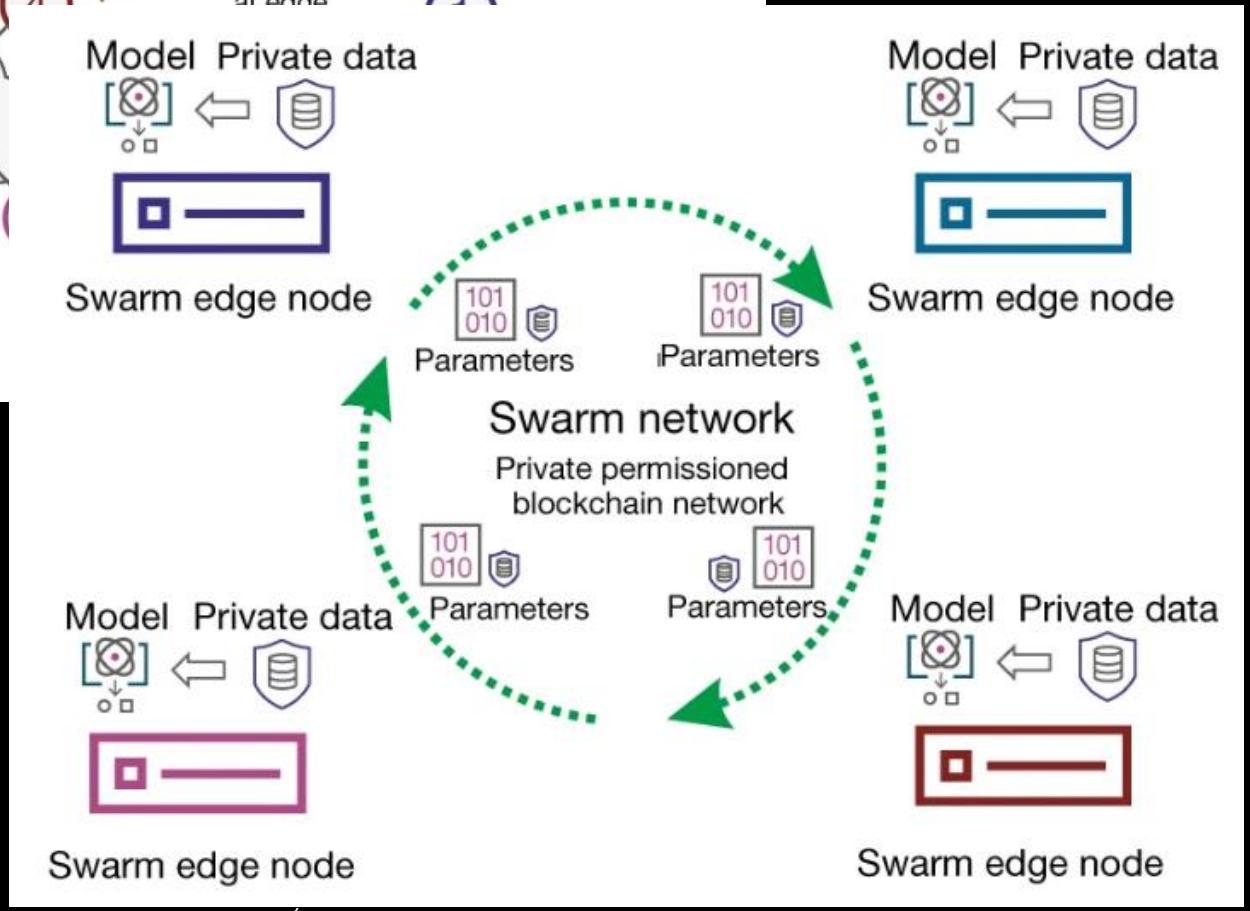
AGENDA

- System bezpieczeństwa End-to-end – zapotrzebowanie na moc obliczeniową.
- Bezpieczna platforma HPE GL for Private Cloud Business Editon.
- Tsunami legislacyjne.
- Wymiana informacji - Cyber Threat Intelligence.
- **HPE Swarm Learning – platforma AI dla bezpieczeństwa i zapobieganiu oszustwom i praniu pieniędzy.**
- Podsumowanie proponowanego rozwiązania.

SWARM LEARNING

Odpowiedź na oszustwa i ataki kierowane AI: wspólna logika, prywatne dane.



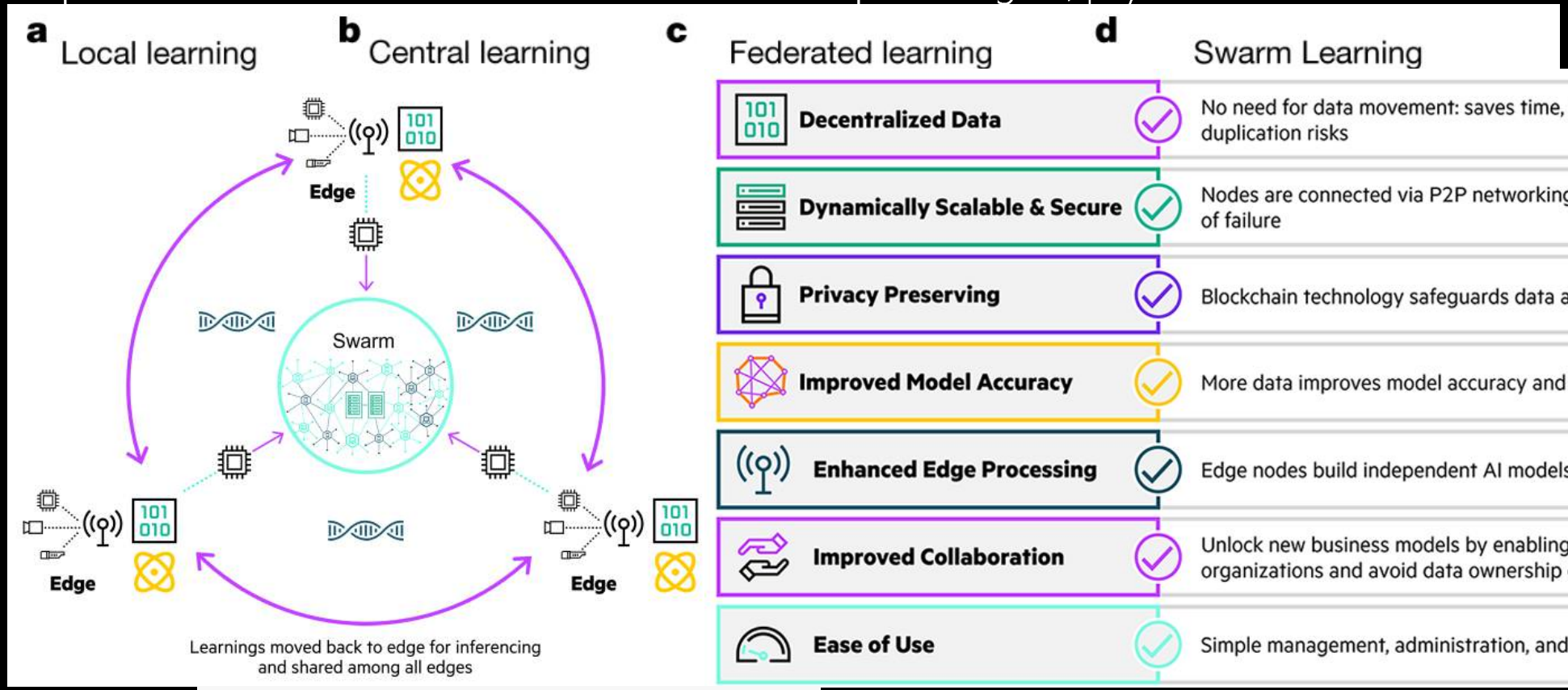


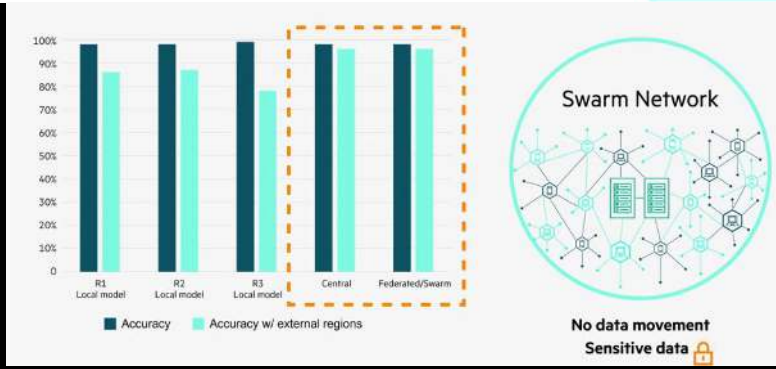
Źródło: https://github.com/HewlettPackard/swarm-learning

IT Solution FACTOR | Hewlett Packard Enterprise

SWARM LEARNING

Odpowiedź na oszustwa i ataki kierowane AI: wspólna logika, prywatne dane.





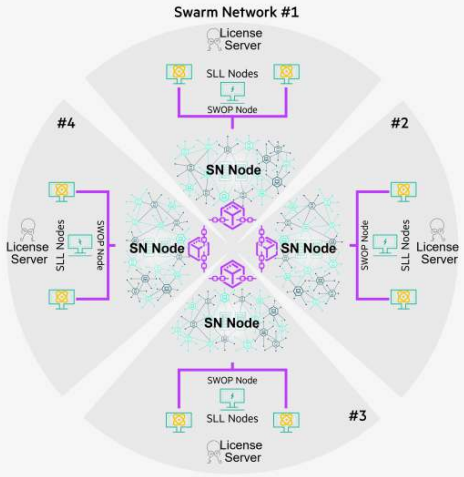
Źródło: https://github.com/HewlettPackard/swarm-learning

SWARM LEARNING

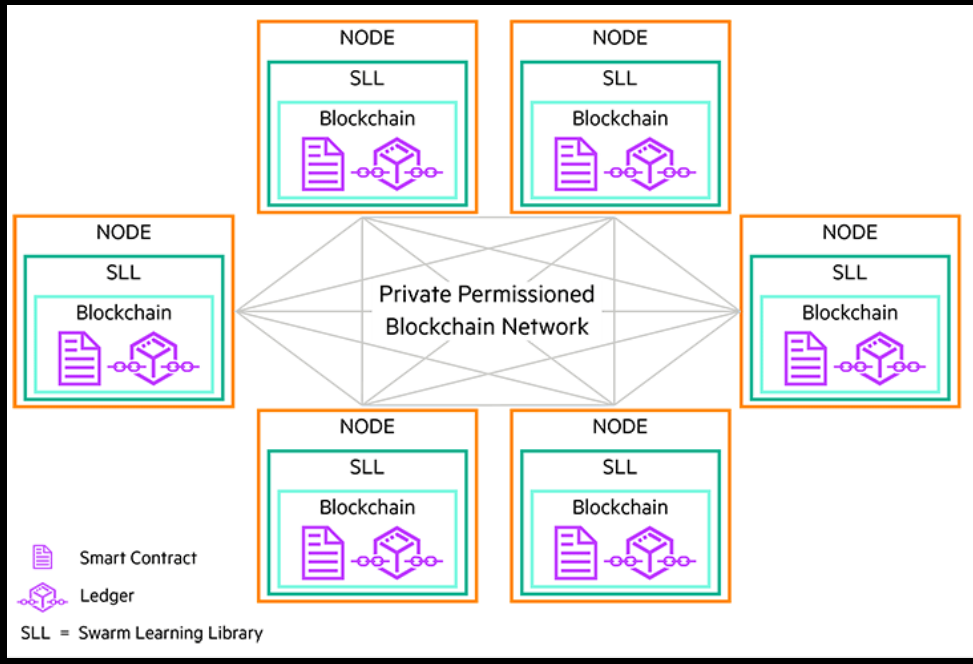
Architektura

Swarm Architecture:

1. Swarm Network (SN)
2. Swarm Learning Library (SLL)
3. Swarm Command Interface (SWCI)
4. Swarm Operator (SWOP)
5. License Server
6. WebUI

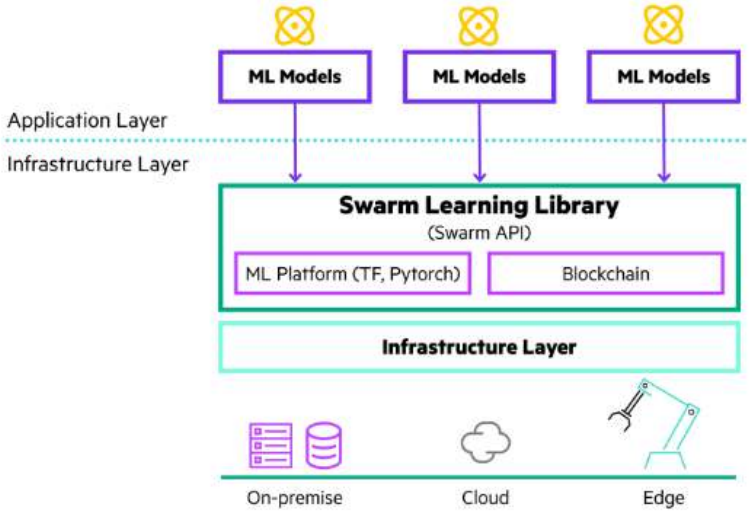


Start with a small Swarm Network and then grow it into a larger network by combining them.



- Leveraged by Swam Learning as a control plane
- Allow Swarm nodes to see each other's states to coordinate models synchronously
- Dynamic on boarding of new nodes
- Eliminates central custodian
- Enhances security: Prevents unauthorized access, insider/ reconstruction attacks

Swarm Learning Library Stack

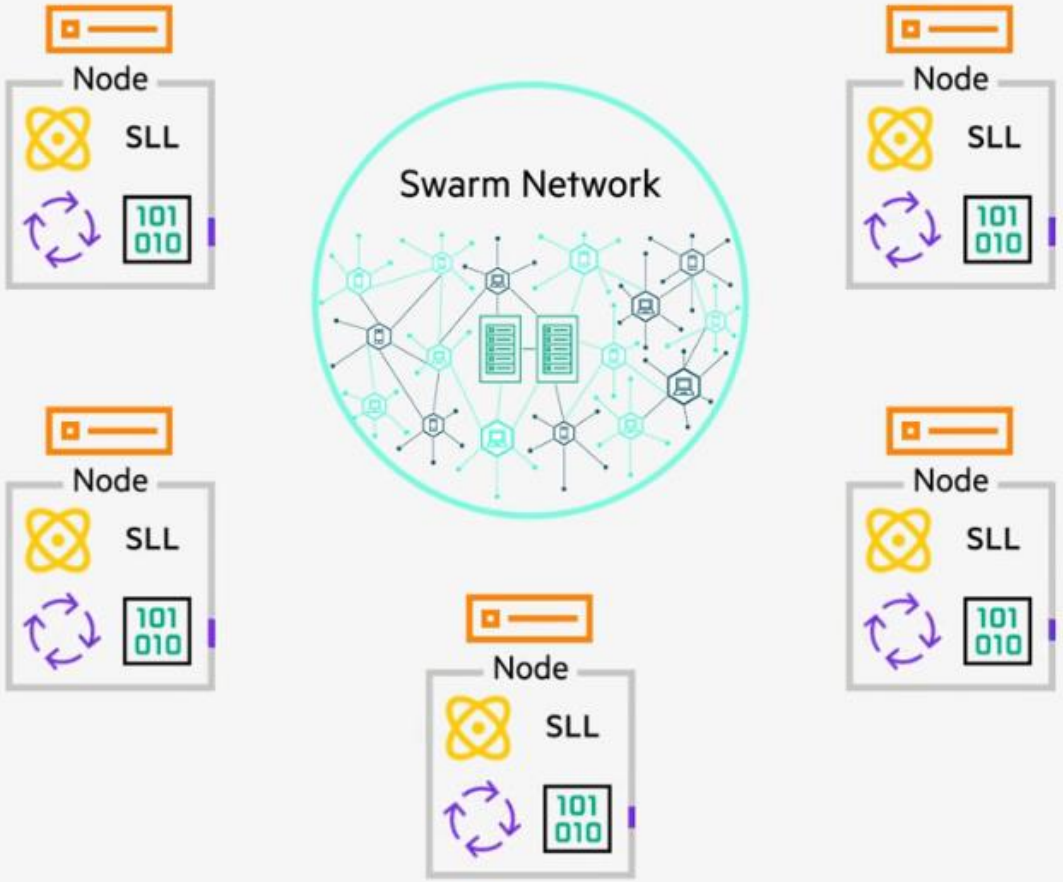


- Swarm Learning Library (SLL) provided as containers
- Simple callback API for integration with ML models
- Tunable hyper parameters
- Management commands to control the network
- Supports standard ML frameworks and platforms
- Runs on any supported Docker container infrastructure

IT Solution FACTOR | Hewlett Packard Enterprise

SWARM LEARNING

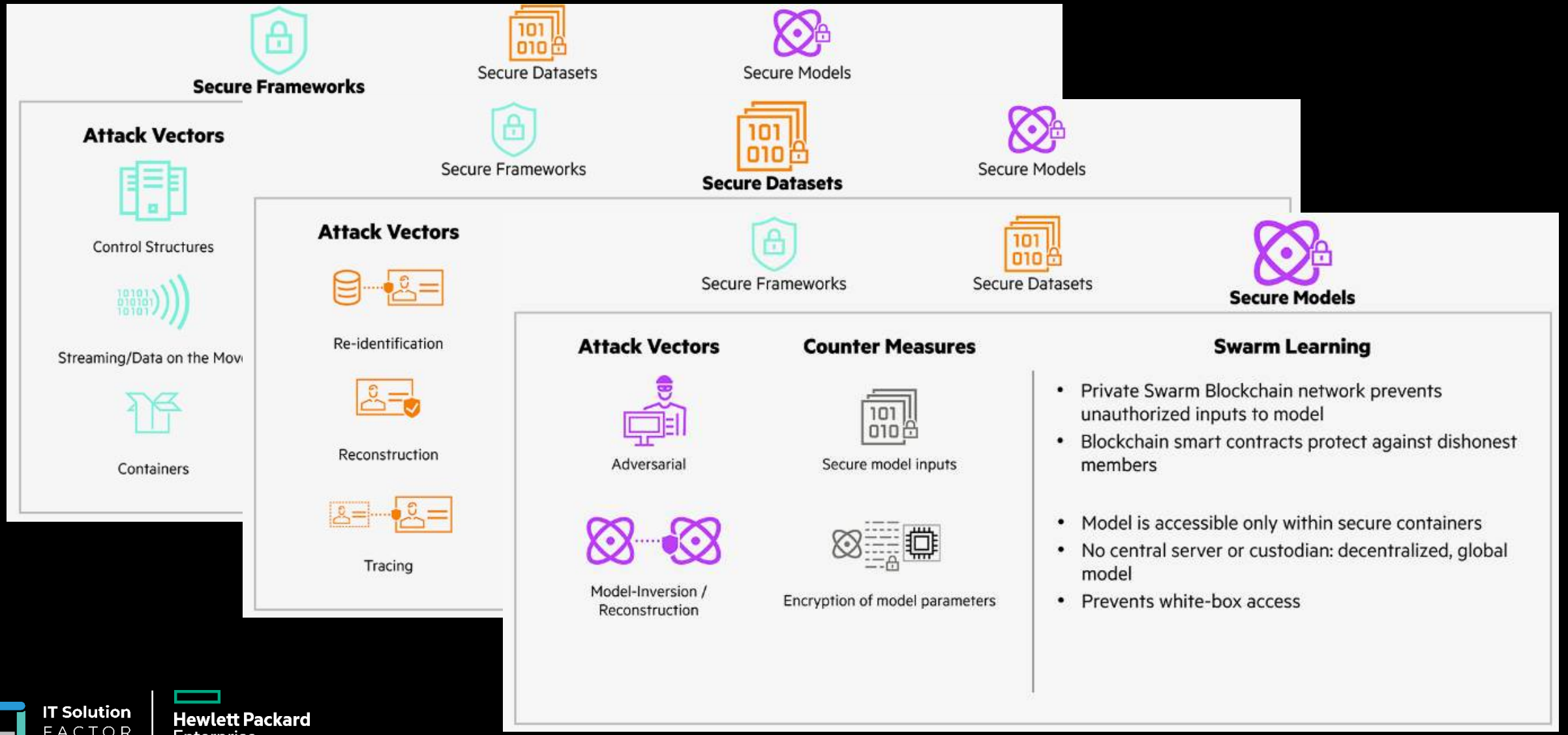
Proces nauczania



1. **Register**
   Nodes register to Swarm Network and receive ML model
2. **Train**
   Nodes train the model on local data for a time-window epoch and shares insights
3. **Merge**
   An Elected Leader merges parameters and shares updated learnings back to models
4. **Repeat Cycle**
   Repeat 1 & 2 until desired accuracy is achieved

SWARM LEARNING

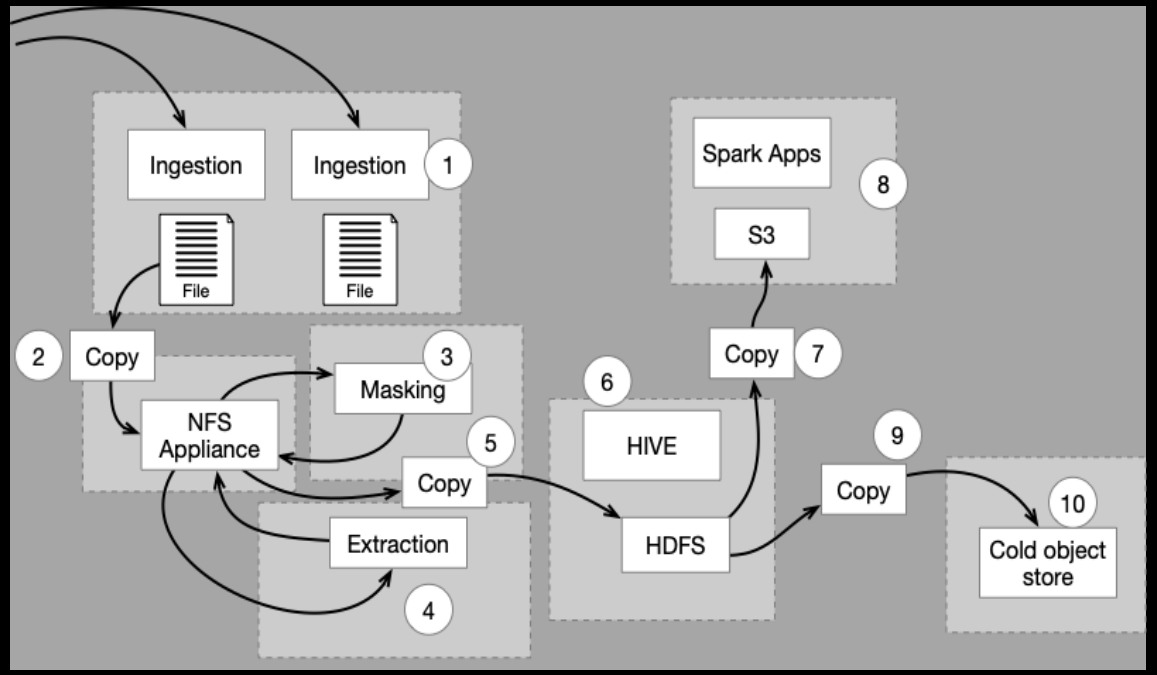
Bezpieczeństwo w każdym zakresie



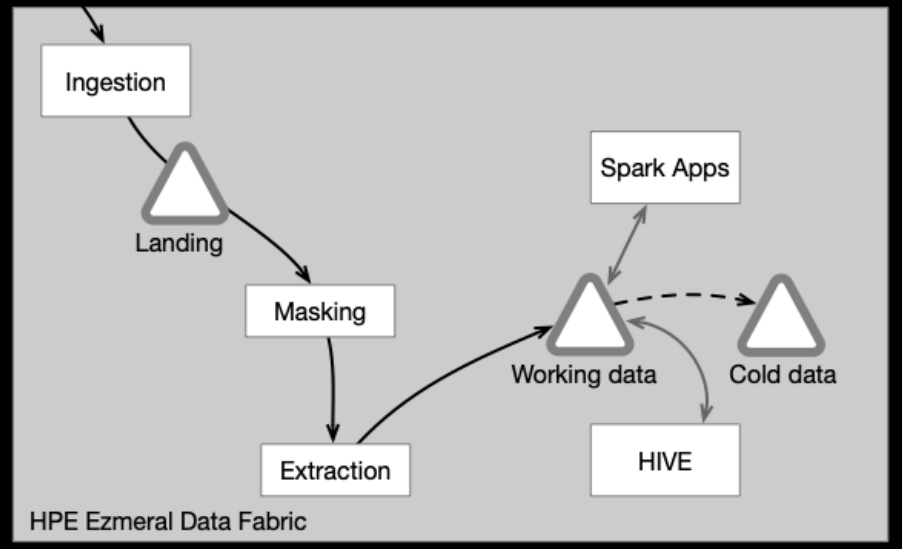
IT Solution FACTOR | Hewlett Packard Enterprise

KLUCZOWE TECHNOLOGIE

Lokalne dane: architektura optymalizująca procesy



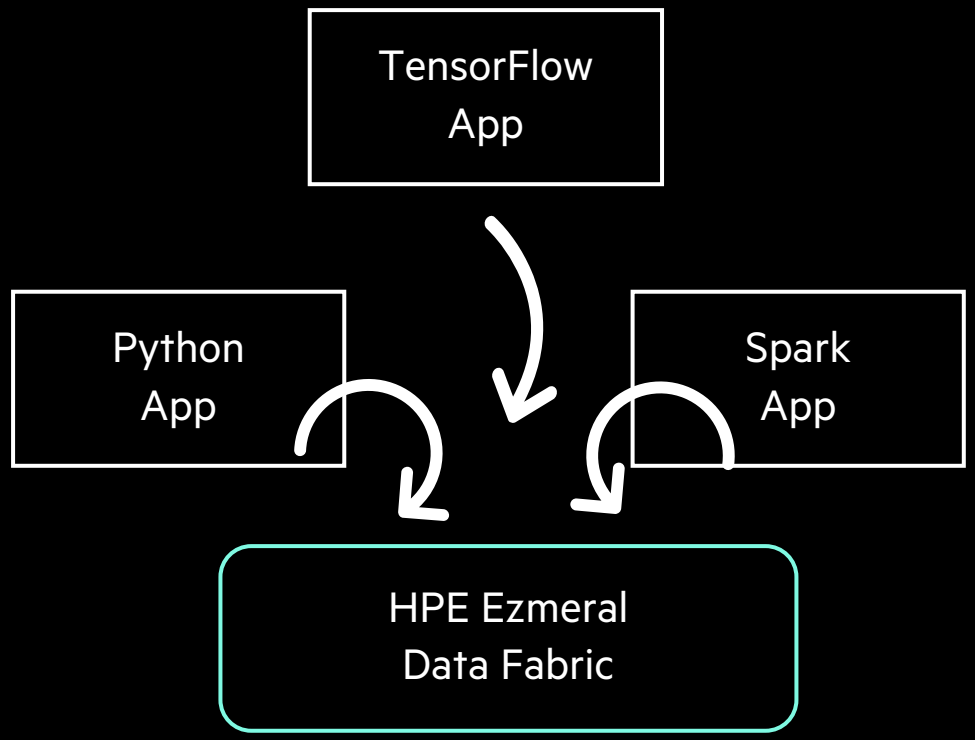
Typowy przepływ rozwiązań silosowych



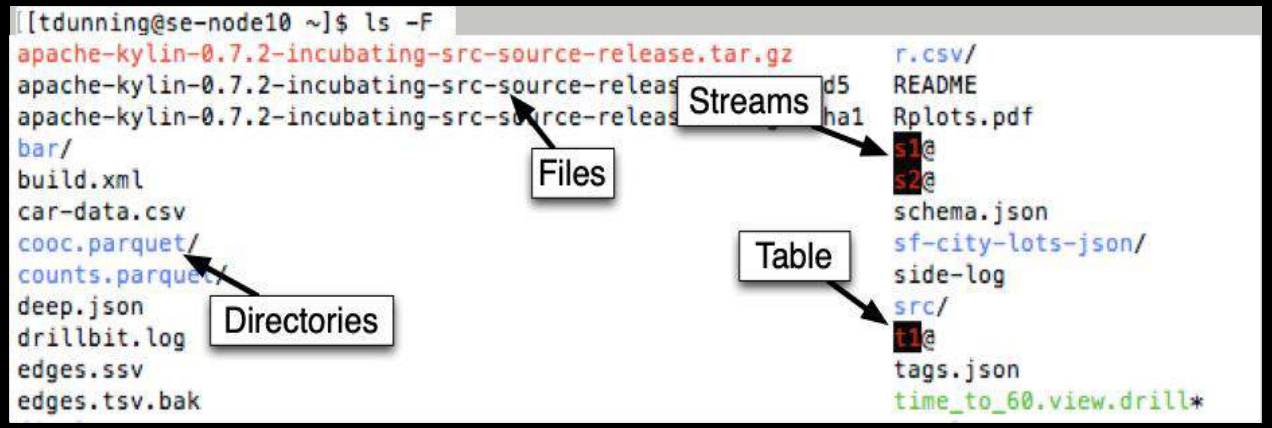
Wspólna infrastruktura HPE Ezmeral Data Fabric

KLUCZOWE TECHNOLOGIE

Data Lake – Demokratyzacja danych



- Uniwersalny dostęp preferowanym narzędziem.
- Komendy Linux, Apache Spark/Kafka i hadoop w miejscu składowania danych.
- Rozwiązania własne i nowoczesne metody analityczne bez konieczności kopiowania transformacji danych.



AGENDA

- System bezpieczeństwa End-to-end – zapotrzebowanie na moc obliczeniową.
- Bezpieczna platforma HPE GL for Private Cloud Business Editon.
- Tsunami legislacyjne.
- Wymiana informacji - Cyber Threat Intelligence.
- HPE Swarm Learning – platforma AI dla bezpieczeństwa i zapobieganiu oszustwom i praniu pieniędzy.
- **Podsumowanie proponowanego rozwiązania.**

STRATEGIA IT: WGLĄD W TRENDY TRANSFORMACJI W EU (IDC)

Strategiczne obszary zmian/inwestycji w najbliższych latach:

- Data Management: Data protection, data security, data services, data mobility, analytics, data monetization, and full data life cycle topics
- Cloud data services: DPaaS, DRaaS, cloud storage, object storage, cloud tiering, cloud backup, cloud gateways
- Data-Driven Strategies: Data-related investment plans, and strategies to turn data into insights; cloud storage trends
- DataOps: Modern processes to bring together data users and data sources
- Driving modernization and digital transformation with data-driven strategy
- Information Architecture for Future of Intelligence: Data enabling platforms, data access, orchestration and integrity for platform technologies such as containers and PaaS

2022 IDC European Cloud Data Management Strategies

STRATEGIA: GŁÓWNE TECHNOLOGIE

- ## Generative Artificial Intelligence (AI)

  Generative AI can be used for a range of activities such as creating software code, facilitating drug development and targeted marketing, but also misused for scams, fraud, political disinformation, forged identities and more. By 2025, Gartner expects generative AI to account for 10% of all data produced, up from less than 1% today.

- ## Data Fabric

  A data fabric's real value is its ability to dynamically improve data usage with its inbuilt analytics, cutting data management efforts by up to 70% and accelerating time to value.

- ## Distributed Enterprise

  With the rise in remote and hybrid working patterns, traditional office-centric organizations are evolving into distributed enterprises comprised of geographically dispersed workers.

- ## Cloud-Native Platforms (CNPs)

  To truly deliver digital capabilities anywhere and everywhere, enterprises must turn away from the familiar "lift and shift" migrations and toward CNPs. CNPs use the core capabilities of cloud computing to provide scalable and elastic IT-related capabilities "as a service" to technology creators using internet technologies, delivering faster time to value and reduced costs.

- ## Autonomic Systems

  Autonomic systems are self-managing physical or software systems that learn from their environments. - dynamically modify their own algorithms without an external software update, - in the longer term, will become common in physical systems such as robots, drones, manufacturing machines and smart spaces.

- ## Decision Intelligence (DI)

  Decision intelligence is a practical discipline used to improve decision making by explicitly understanding and engineering how decisions are made, and outcomes evaluated, managed and improved by feedback.

- ## Composable Applications

  In the continuously changing business context, demand for business adaptability directs organizations toward technology architecture that supports fast, safe and efficient application change.

- ## Hyperautomation

  Hyperautomation enables accelerated growth and business resilience by rapidly identifying, vetting and automating as many processes as possible focusing on three key priorities: improving the quality of work, speeding up business processes, and enhancing the agility of decision-making.

- ## Privacy-Enhancing Computation (PEC)

  - As well as dealing with maturing international privacy and data protection legislation, CIOs must avoid any loss of customer trust resulting from privacy incidents.
  - PEC techniques protect personal and sensitive information at a data, software or hardware level for sharing, pooling and analyzing data without compromising privacy.

- ## Cybersecurity Mesh

  - Assets and users can be anywhere, meaning the traditional security perimeter is gone. CSMA provide an integrated security structure and posture to secure all assets, regardless of location, to reduce the financial impact of individual security incidents.

- ## AI Engineering

  - AI engineering is an integrated approach for operationalizing AI models. In order to continually enhance value through rapid AI change.

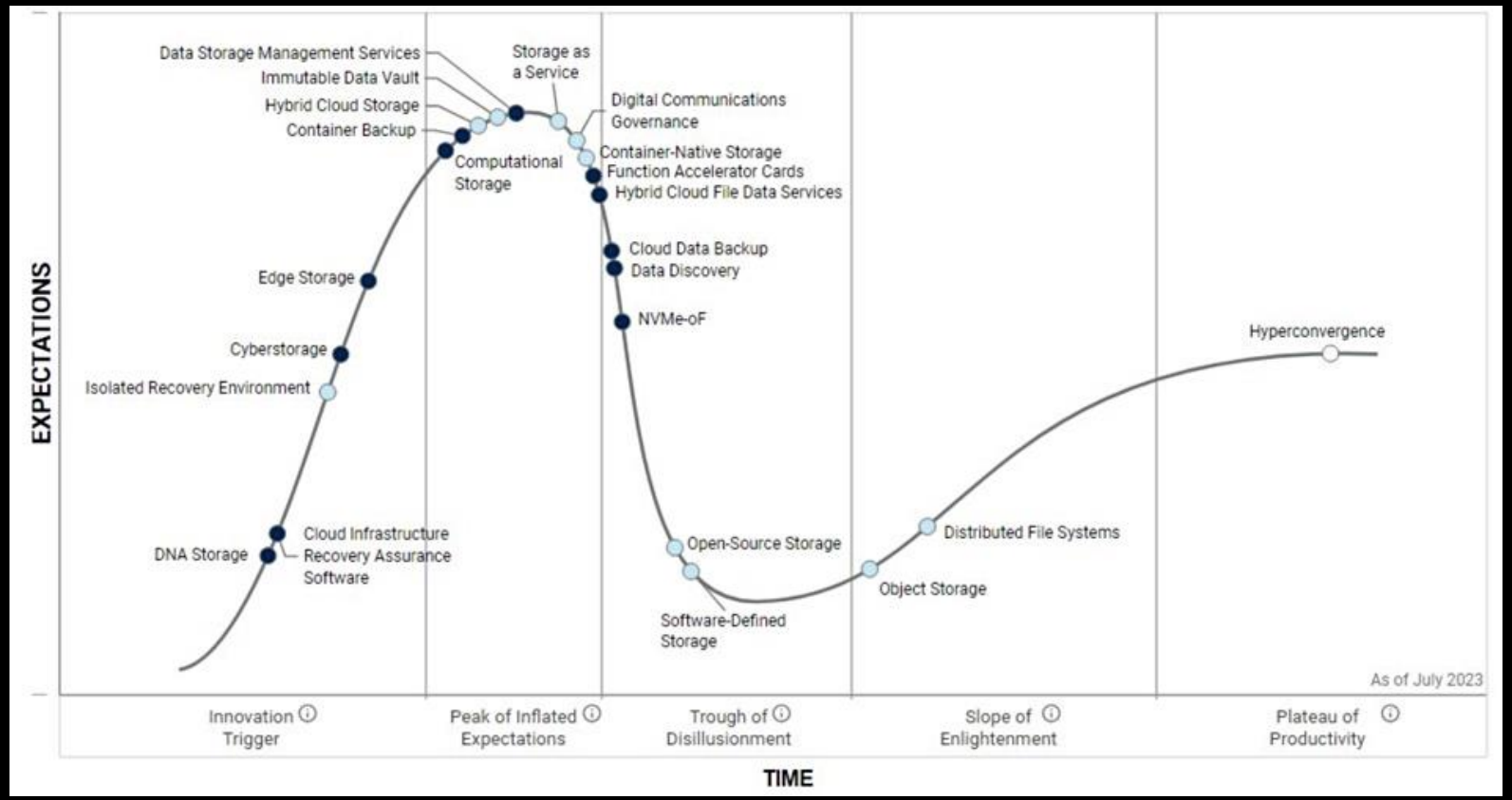
- ## Total Experience (TX)

  - TX is a business strategy that combines the disciplines of customer experience (CX), employee experience (EX), user experience (UX) and multiexperience (MX).

Gartner's top strategic technology trends for 2022

DOJRZAŁOŚĆ TECHNOLOGIE PRZETWARZANIA I OCHRONY DANYCH

HPE z pomocą 3-5 zintegrowanych produktów dostarcza wszystkie niezbędne technologie



CloudData Backup (Veeam)
Computional Storage (EDF)
Container Backup (Veeam)
Container Native storage (EDF, PCBE)
Cyberstorage (Veeam, StoreOnce, PCBE)
Data Storage Mgmnt. Svcs (PCBE)
Data Discovery (EDF+3rd party)
Digital Communication Governance (EDF+3rd party)
Distributed File System (EDF)
DNA Storage
Edge Storage (EDF)
Hybrid cloud storage (EDF)
HyperConvergence (PCBE)
Immutable Data Vault (EDF, StoreOnce, PCBE)
IRE/Cloud Infrastr. Recovery Assur. SW (PCBE/StoreOnce/Veeam)
NVMe-oF (PCBE)
Object Storage (EDF)
Open-Source Storage
Software Defined Storage (EDF)
Storage as a service (PCBE, EDF)

Źródło: Gartner Hype Cycle for Storage and Data Protection Technologies, 2023

CYBERSECURITY – MAPOWANIE NIEZBĘDNYCH FUNKCJONALNOŚCI

Lp	Technologia	PCBE	EDF	StoreOnce	Veeam*	Network	Wyjaśnienia
1.	Immutability	X	X	X	X		Zintegrowana retencja repozytoriów (Veeam ISV-DI) – eliminacja ryzyka błędu ludzkiego; akcelerowane sprzętowo. Repozytoria zabezpieczone przed skasowaniem (immutable)
2.	RTO (100TB)	<15 min	<4h*	<4h*	<4h*		RTO<15min niezbędne dla usług wymagających wysokiej dostępności. oraz dla mitygacji ransomware.
3.	2 składnikowa autentykacja	X	X	X	X	X	Specyfikowane w DORA, CER, NIS 2, NSC, zalecenia CeZ
4.	2 składnikowa autoryzacja	x		X			Dodatkowe zabezpieczenie przed błędem ludzkim i ransomware
5.	(mikro/dynamiczna) segmentacja	X	X	X		X	EDF z SPIFFE/SPIRE – mikrosegmentacja CX-10000 (mikro)segmentacja + dynamiczna segmentacja; EDR/XDR itp.
6.	Detekcja i mitygacja ransomware	X		X	X		Dzięki wbudowanym algorytmom detekcji, zdublowanym narzędziom przywrócenia w tym natychmiastowego równoległego przywracania danych.
7.	szyfrowanie	X	X	X	X	X	Transmisji i składowanie danych; CX 10000 – 800Gbps sprzętowo szyfrowanych tuneli.
8.	Śluza dla backupu	X		X	X		Wszystkie repozytoria i systemy kopii zapasowych w każdym ośrodku są w stale odseparowane (okna synchronizacji są zbędne) i zapewniają Immutability.
9.	Ochrona danych (backup)	X			X		Zwielokrotnione narzędzia odzyskiwania danych (koegzystencja). Paradygmat 3-2-1 akcelerowany sprzętowo.
10.	Dystrybuowany FW L4-L5	X				X	(Dynamiczna) segmentacja oraz mikrosegmentacja akcelerowana sprzętowo w przełączniku ToR zintegrowanym z platformą wirtualizacyjną.
11.	Izolowane środowiska przywracania (IRE)	X	X	X	X	X	Pełna automatyka, wsparcie dla Infrastructure as Code (IaC), ponad 10-krotne skrócenie testów przywracania/mitygacji skutków ransomware bez wpływu na produkcję.
12.	Akceleracja sprzętowa	X	X	X		X	Sprzętowa akceleracja przetwarzania (CPU, GPU, FPGA, APU) i bezpieczeństwa DPU, Immutability, remediacja ransomware, mikrosegmentacja, DDOS, VPN.

*- Opcja

Forum Bezpieczeństwa Banków

IT Solution FACTOR | Hewlett Packard Enterprise

Dziękujemy

BEZPIECZEŃSTWO FILAREM ZGODNOŚCI

E: piotr.nogas@hpe.com
M: +48 601 890 046

E: marcin.krzemieniewski@itsf.com.pl
M: +48 695 883 956