ZAUFANA TRZECIA STRONA.PL

Zarządzanie cyklem życia bezpieczeństwa danych

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Marcin Fronczak

Prowadzi szkolenia z zakresu bezpieczeństwa chmur m.in. przygotowujące do egzaminu Certified Cloud Security Knowledge (CCSK). Certyfikowany audytor systemów informatycznych oraz ekspert w zarządzaniu ryzykiem i bezpieczeństwem informacji - CISA, CIA, CRISC.

ZAUFANA TRZECIA STRONA.PL

Agenda

aruba CLOUD

1. Podsumowanie zagadnień poruszanych w poprzednich artykułach
2. Przechowywanie danych w chmurze
3. Fazy cyklu życia danych w chmurze
3. Najlepsze praktyki ochrony danych w chmurze
4. Podsumowanie
5. Sesja pytań od uczestników

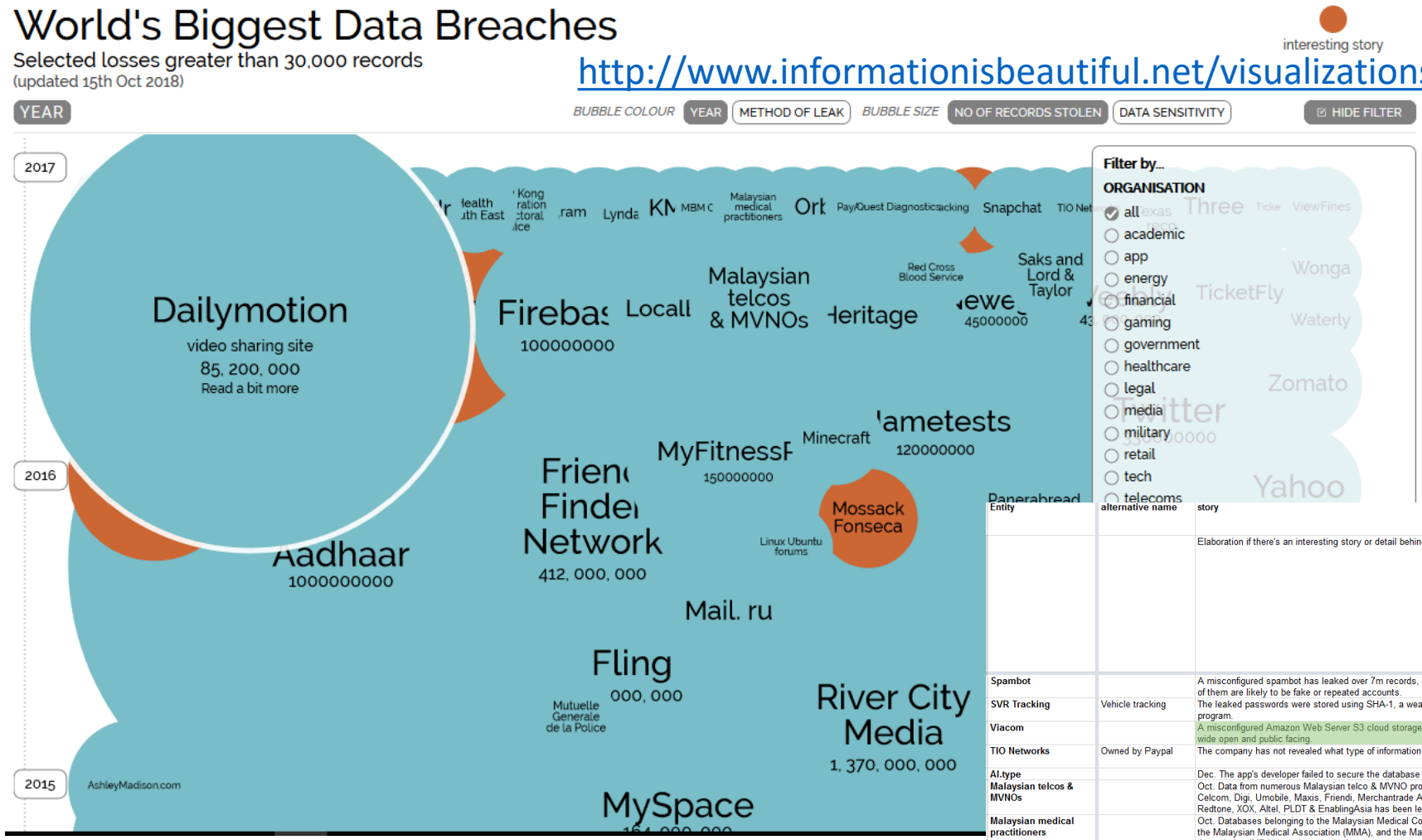
ZAUFANA TRZECIA STRONA.PL

Podsumowanie zagadnień

aruba CLOUD

- Architektura modelu cloud computingu wg NIST SP 800-145,
- Ryzyka natury organizacyjno-prawnej i zarządzania zgodnością na przykładzie pojęcia GRC – Governance, Risk management and Compliance,
- Standardy bezpieczeństwa, jakie powinna spełniać usługa chmurowa i jak możemy sprawdzić, czy te standardy faktycznie spełnia,
- RODO w chmurze
- Zarządzanie tożsamością w chmurze i standardy SAML, OpenID, OAuth,
- Wdrożenie i zarządzanie uprawnieniami w chmurze,
- Przygotowania do wielkiej awarii,
- Bezpieczeństwo centrum danych,
- Bezpieczeństwo środowiska wirtualnego,
- Szyfrowanie w chmurze
- Zarządzanie incydentami w chmurze
- Interoperacyjność i przenaszalność czyli jak uniezależnić się od dostawcy

Incydenty związane z danymi



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

https://www.databreaches.net/

https://www.idtheftcenter.org/

Entity	alternative name	story	YEAR	YEAR(2)	records lost	ORGANISATION	METHOD OF LEAK	NO OF RECORDS STOLEN	DATA SENSITIVITY	1st source
		Elaboration if there's an interesting story or detail behind it	years are encoded (0=2004, 8 = 2012, 9 = 2013, 10=2014, 11=2015, 12=2016, 13 = 2017, 14=latest		(use 3m, 4m, 5m or 10m to approximate unknown figures)			(use 3m, 4m, 5m or 10m to approximate unknown figures)	1. Just email address/Online information 20 SSN/Personal details 300 Credit card information 4000 Email password/Health records 50000 Full bank account details	
Spambot		A misconfigured spambot has leaked over 7m records, although many of them are likely to be fake or repeated accounts.	14	2017	711000000	web	poor security	711000000	4000	https://ww
SVR Tracking	Vehicle tracking	The leaked passwords were stored using SHA-1, a weak 20yr old hash program.	14	2017	540000	app	poor security	540000	4000	https://thel
Viacom		A misconfigured Amazon Web Server S3 cloud storage bucket was left wide open and public facing.	14	2017	3000000	web	hacked	3000000	4000	https://thel
TIO Networks	Owned by Paypal	The company has not revealed what type of information was stolen.	14	2017	1600000	financial	hacked	1600000	4000	https://ww
Al.type		Dec. The app's developer failed to secure the database server.	14	2017	31000000	app	poor security	31000000	4000	http://www
Malaysian telcos & MVNOs		Oct. Data from numerous Malaysian telco & MVNO providers, including Celcom, Digi, Umobile, Maxis, Friendi, Merchantrade Asia, Tunetalk, Redtone, XOX, Altel, PLDT & EnablingAsia has been leaked.	14	2017	46200000	telecoms	hacked	46200000	4000	https://ww
Malaysian medical practitioners		Oct. Databases belonging to the Malaysian Medical Council (MMC), the Malaysian Medical Association (MMA), and the Malaysian Dental Association (MDA) have been leaked.	14	2017	81309	healthcare	hacked	81309	4000	https://ww
MBM Company	Limogés Jewellery	Mar. Negligent storage of a customer database exposed full postal addresses, email addresses, IP addresses and plain-text passwords.	14	2018	1300000	retail	poor security	1300000	4000	https://ther
Orbitz		Mar. An old version of the Orbitz website was hacked, exposing personal details and payment card info. Orbitz is now owned by	14	2018	880000	web	hacked	880000	300	https://ww

2018 update | Jan 2015 update | July 2013 update (old) | Explore

https://docs.google.com/spreadsheets/d/1JeYUdnhjQJO_13r8iTeRxpU2pBKuV6RVRHoYCgiMfg/edit#gid=322165570

ZAUFANA TRZECIA STRONA.PL

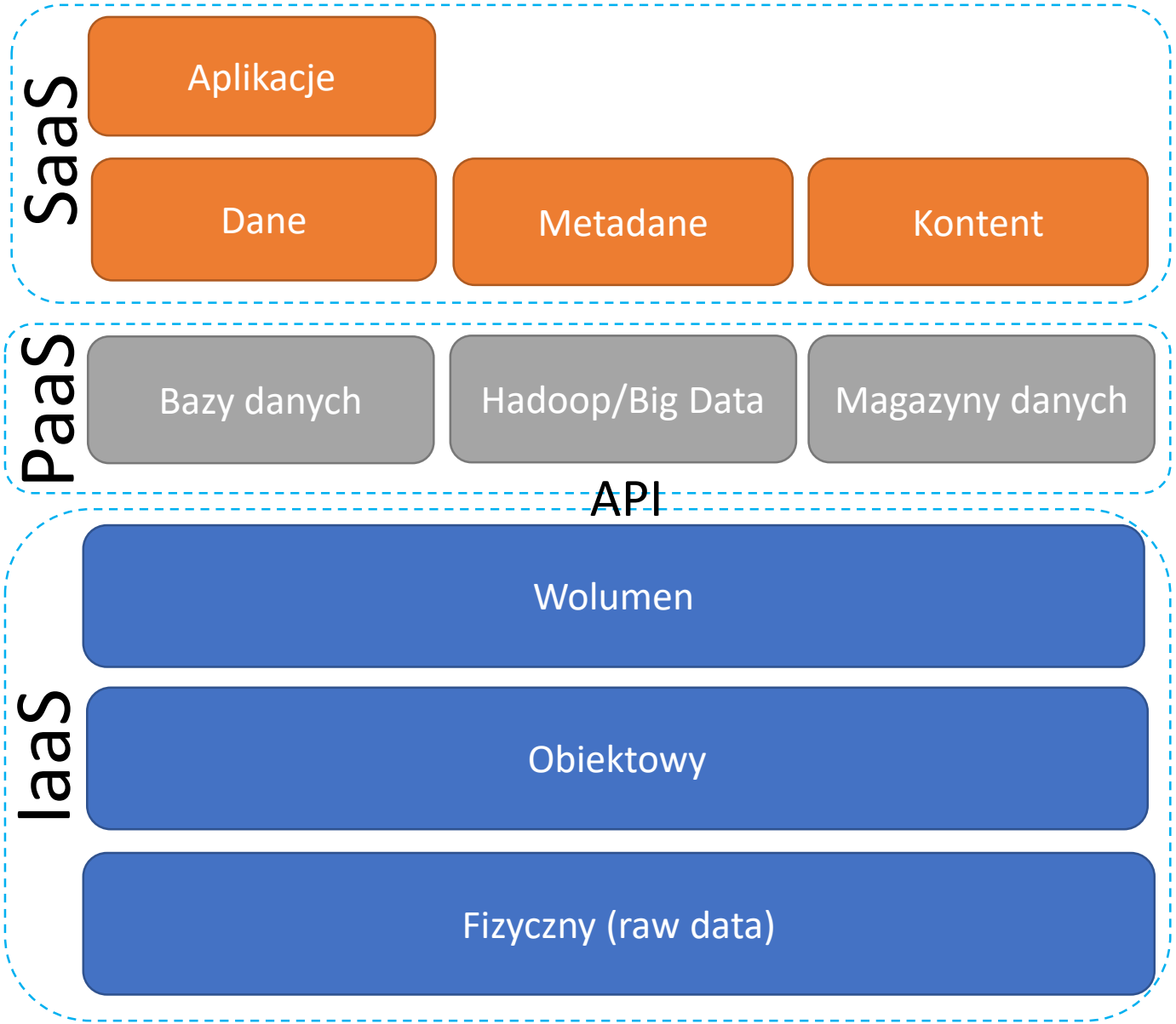
Dane w chmurze

aruba CLOUD

ZAUFANA TRZECIA STRONA.PL

Dane w chmurze

aruba CLOUD



Model SaaS umożliwia dostęp do informacji, raportów, plików, zdjęć poprzez stronę lub aplikację internetową i korzysta w tym celu z baz danych oraz magazynów obiektowych i wolumenowych.

PaaS dostarcza usługi w postaci baz danych, magazynów, platformy Big Data i korzysta przez API z baz danych oraz magazynów obiektowych i wolumenowych

Wydzielony obszar pamięci masowej w postaci wirtualnych dysków podłączanych do maszyn wirtualnych i wykorzystywanych jak fizyczne dyski lub macierze np. VMWare VMFS, Amazon EBS, RackSpace RAID i OpenStack Cinder.

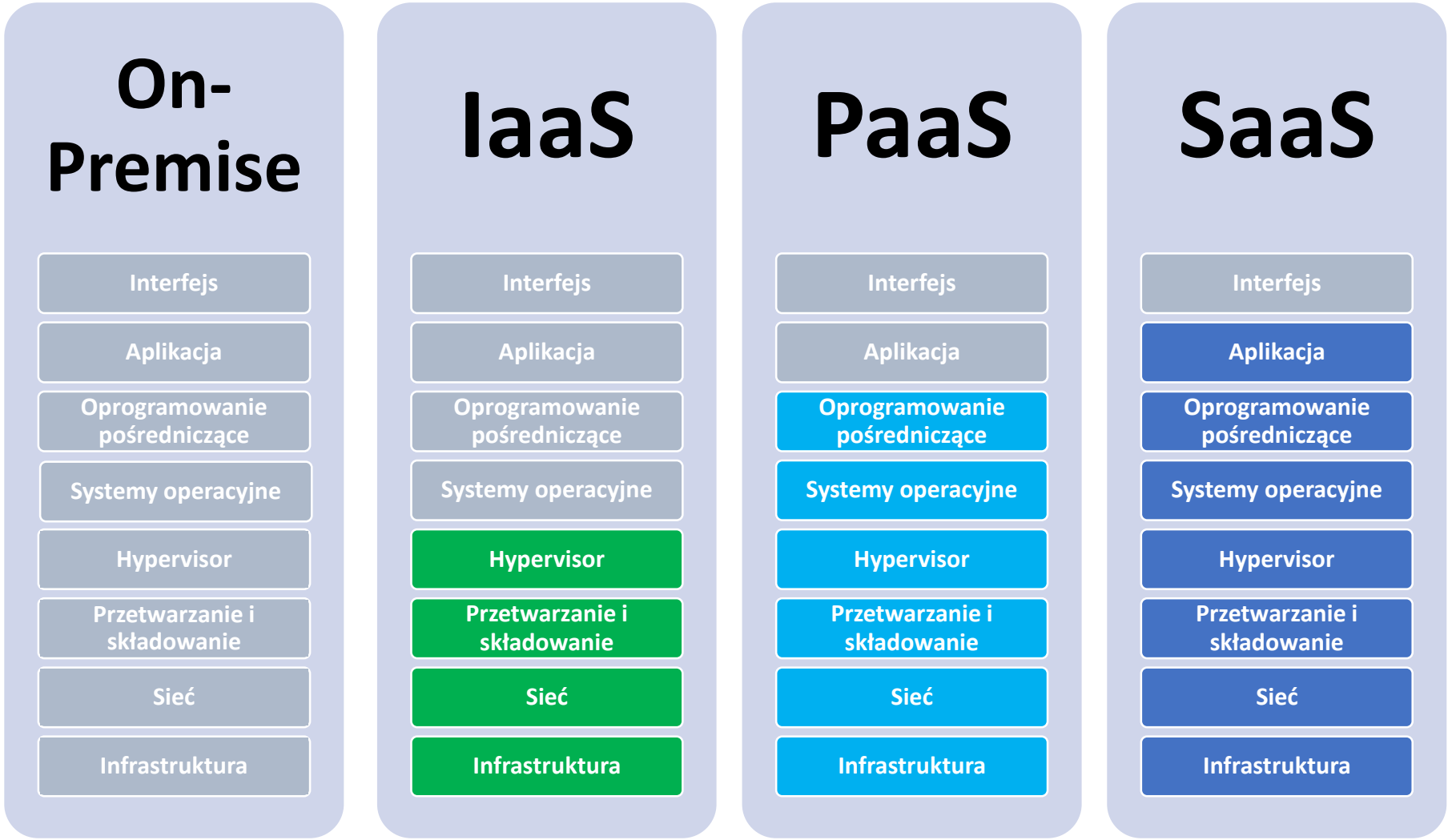
Repozytorium plików, które zawierają metadane i identyfikatory tworząc obiekty. Przykłady to Amazon S3, Aruba Cloud Object Storage, RackSpace Cloud Files, OpenStack Swift for private clouds

Fizyczne media, surowe dane, możliwe mapowanie

ZAUFANA TRZECIA STRONA.PL

Dane w chmurze

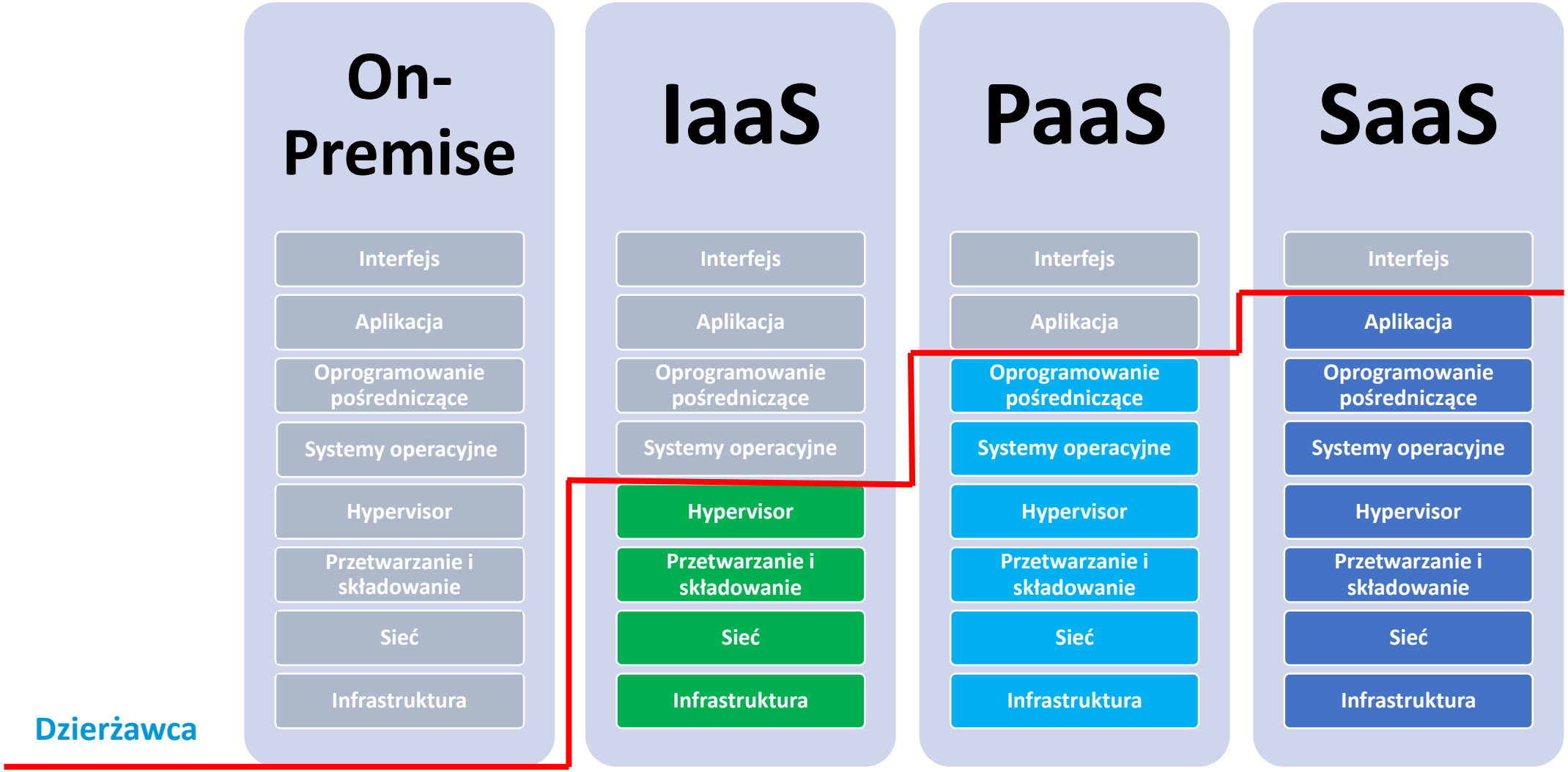
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Dane w chmurze

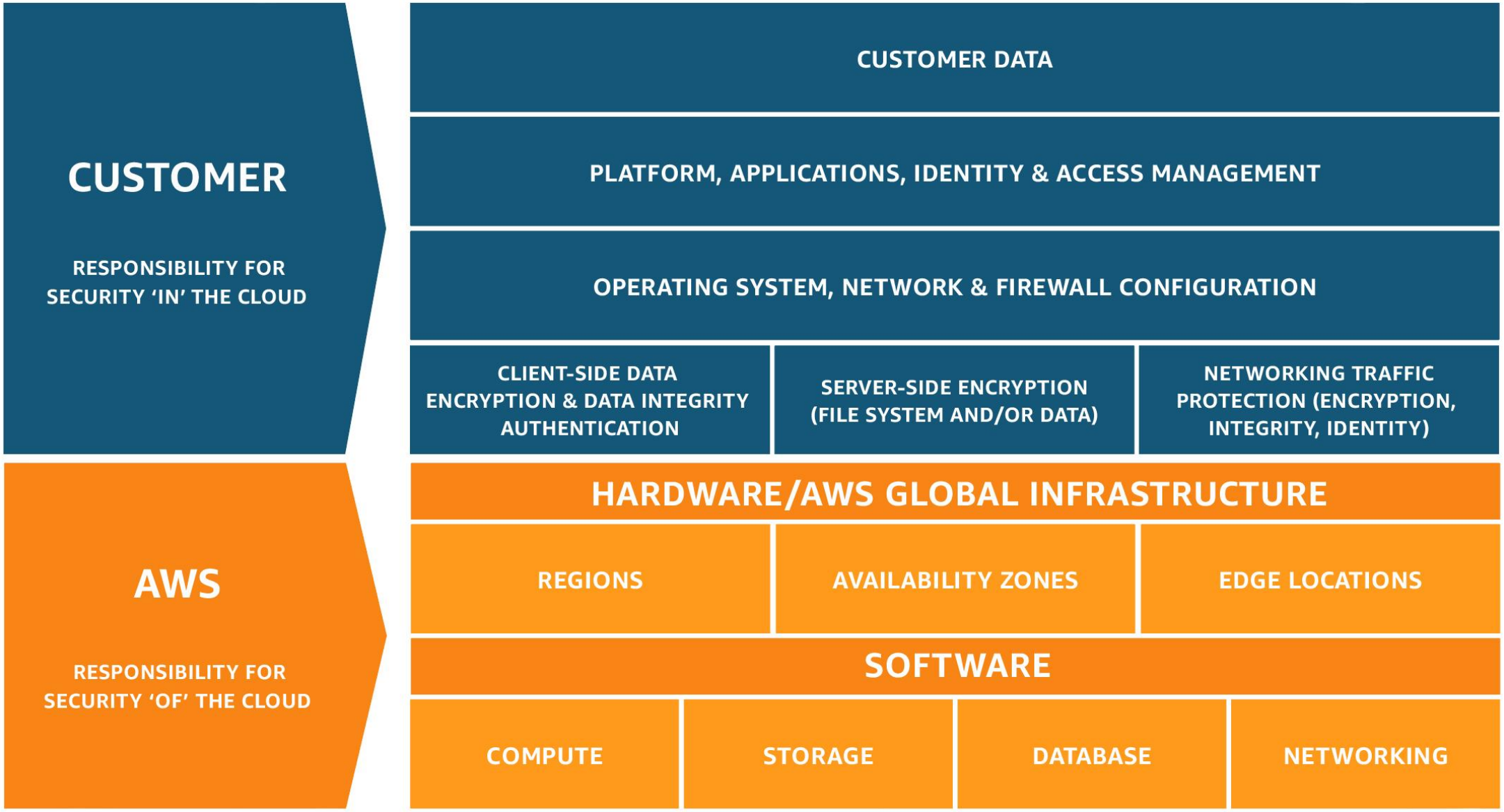
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Odpowiedzialność

aruba CLOUD



Cykl życia danych

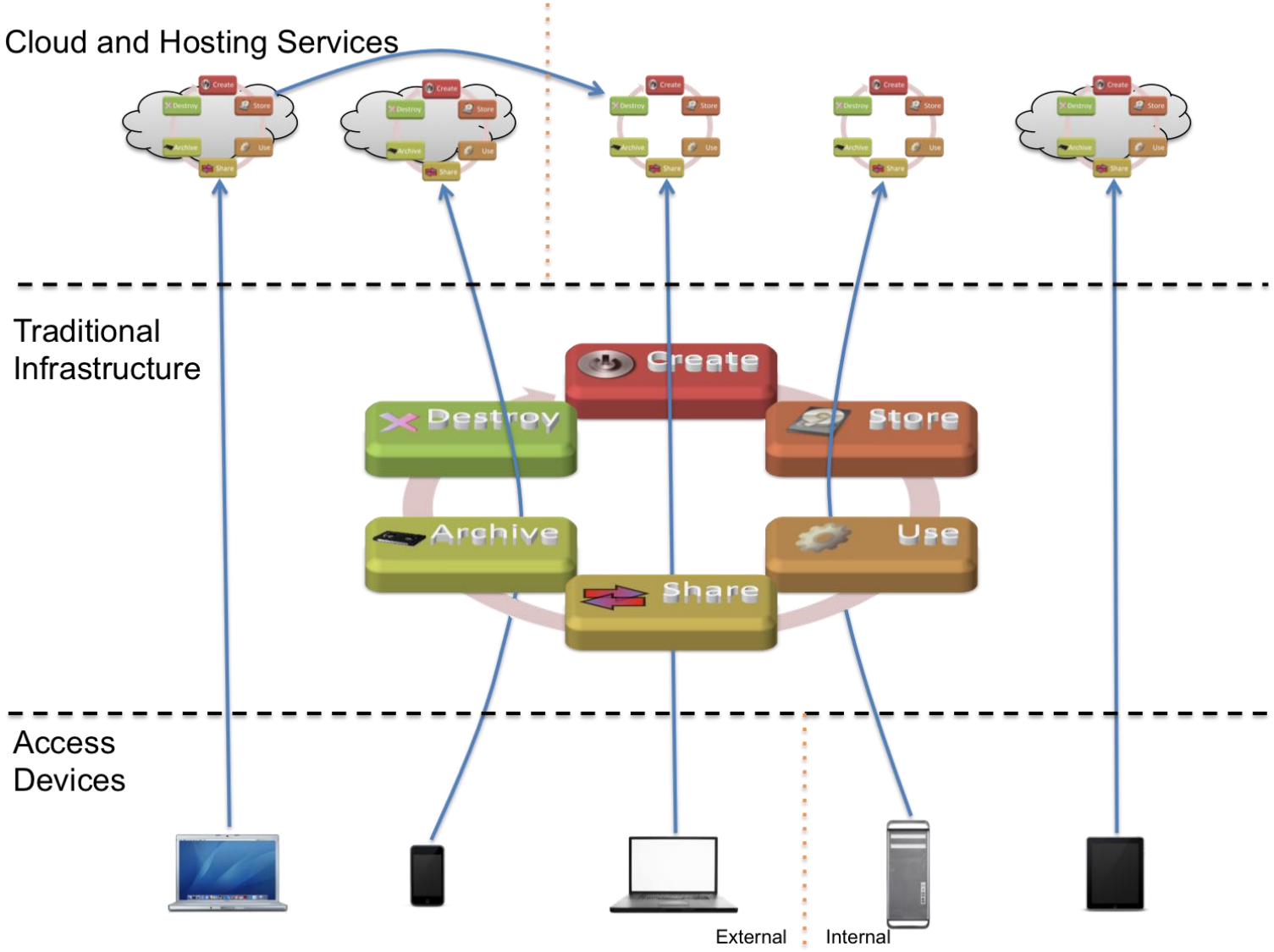
1. Wytworzenie lub zmiana/aktualizacja, modyfikacja danych w postaci cyfrowej
2. Przechowywanie jest działaniem mającym na celu składowanie danych w repozytorium i występuje zazwyczaj równolegle z procesem tworzenia
3. Korzystanie obejmuje przeglądanie, przetwarzanie i wszelkie działania wyłączając modyfikację
4. Dzielenie polega na udostępnieniu informacji innym użytkownikom , klientom, partnerom
5. Archiwizacja umożliwia dostęp i korzystanie z danych w zdefiniowanym okresie czasu
6. Niszczenie polega na całkowitym usunięciu danych przy wykorzystaniu fizycznych lub logicznych środów.

ZAUFANA TRZECIA STRONA.PL

Lokalizacja i dostęp

aruba CLOUD

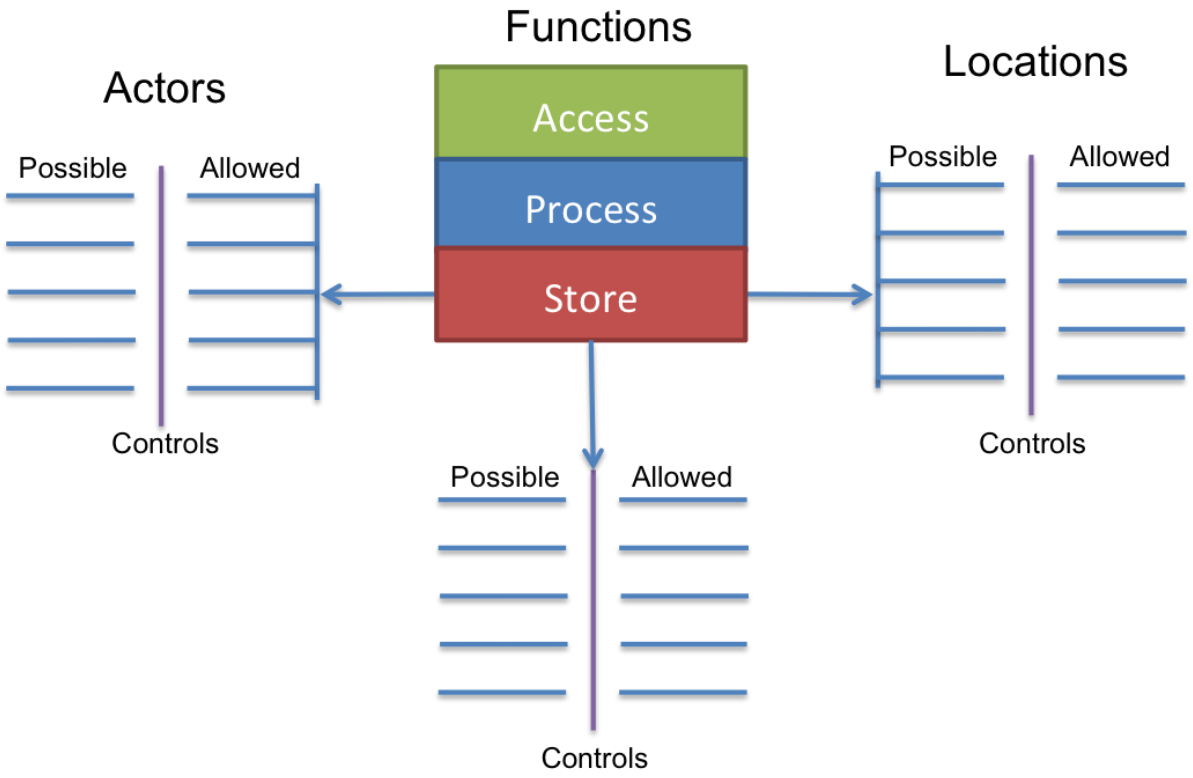
- Gdzie są moje dane?
- Kto ma do nich dostęp?
- Z jakich urządzeń?
- Jakie działania może na nich wykonać?
- Czy można przenosić dane pomiędzy lokalizacjami?
- Jaki jest cykl życia danych w tych lokalizacjach?



ZAUFANA TRZECIA STRONA.PL

Funkcje, aktorzy dostęp

aruba CLOUD



	Create	Store	Use	Share	Archive	Destroy
Access	X	X	X	X	X	X
Process	X		X			
Store		X			X	

Funkcje

Access: Przegląd/dostęp do danych, kopiowanie, przesyłanie, wymiana informacji

Process: Operacje na danych jak aktualizacja, transakcje biznesowe itd.

Store: Przechowywanie danych (w plikach, bazach danych, hurtowniach itd.)

Aktorzy

Użytkownicy, konta systemowe, aplikacje, urządzenia

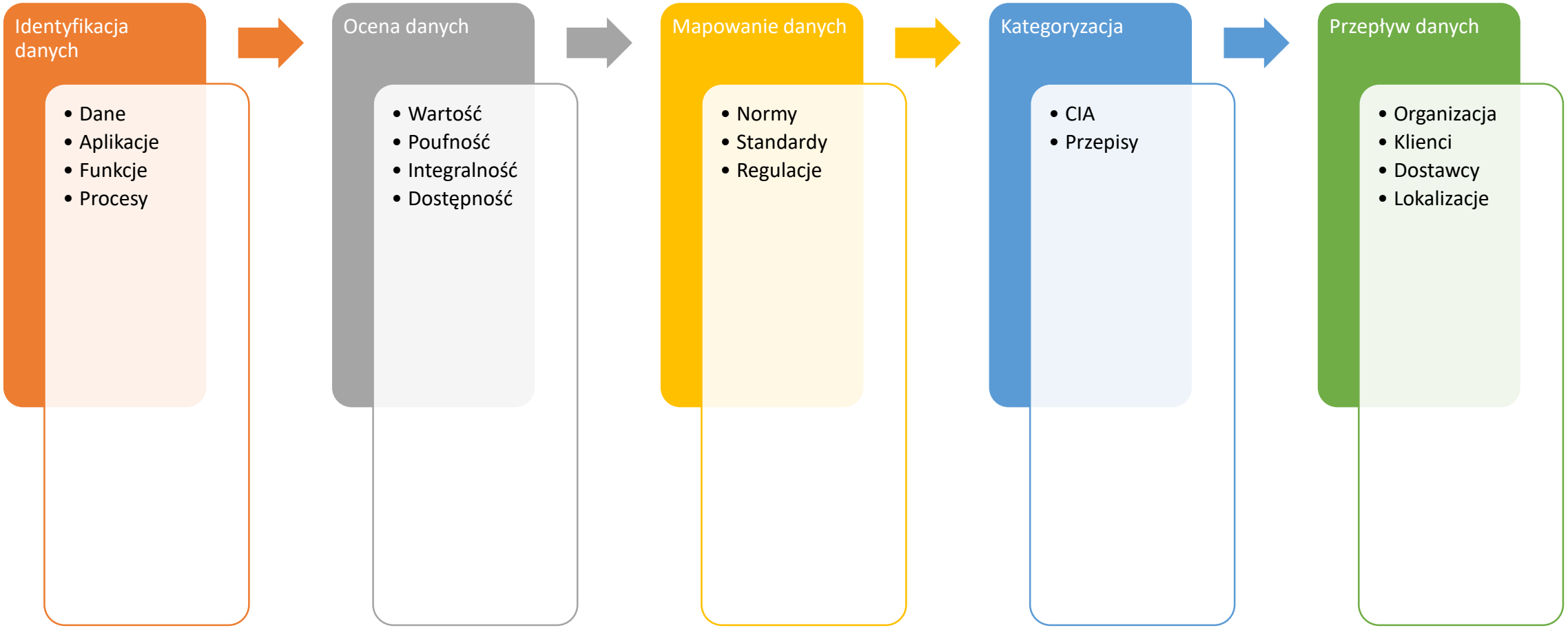
Lokalizacje

model (on-premise, chmura, zewnętrzne), geograficzne, warstwa chmury, środowisko.

ZAUFANA TRZECIA STRONA.PL

Klasyfikacja

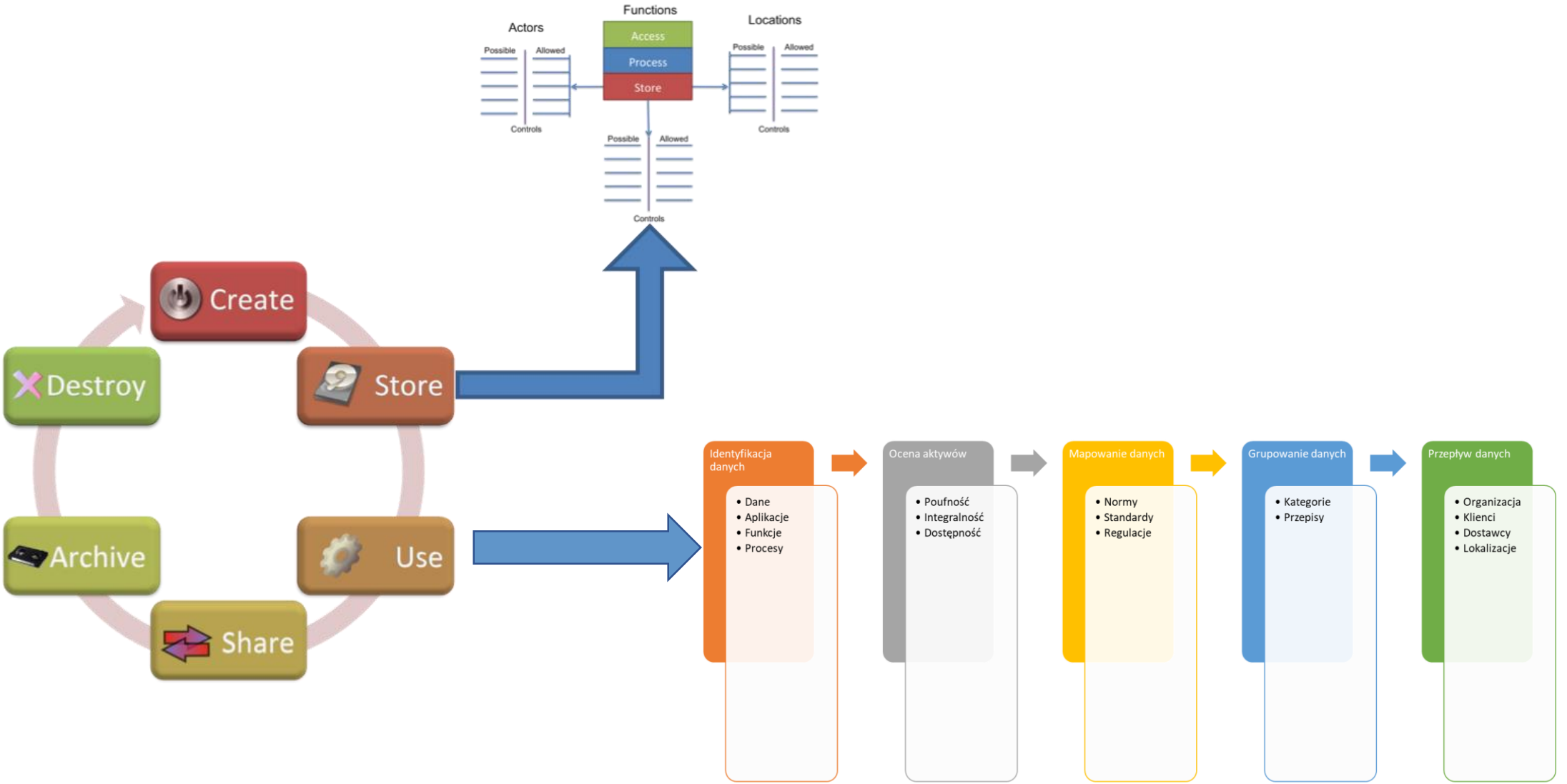
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Mapowanie

aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Mapowanie

aruba CLOUD

Kategoria	Funkcje	Aktorzy								Lokalizacja									
		Admin		Internal		Aplikacja		External		SaaS		PaaS		Iaas		EU		Non EU	
	Możliwe(M)/ Dopuszczalne (D)	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
Dane osobowe	Access	✓	✓	✓	✓	×	×	✓	×	×	✓*	×	✓*	×	✓*	✓	✓	✓	×
	Process	✓	✓	✓	✓	×	×	✓	✓	×	✓*	×	✓*	×	✓*	✓	✓	✓	×
	Store	✓	✓	✓	✓	✓	✓	×	×	×	✓*	×	✓*	×	✓*	✓	✓	✓	×

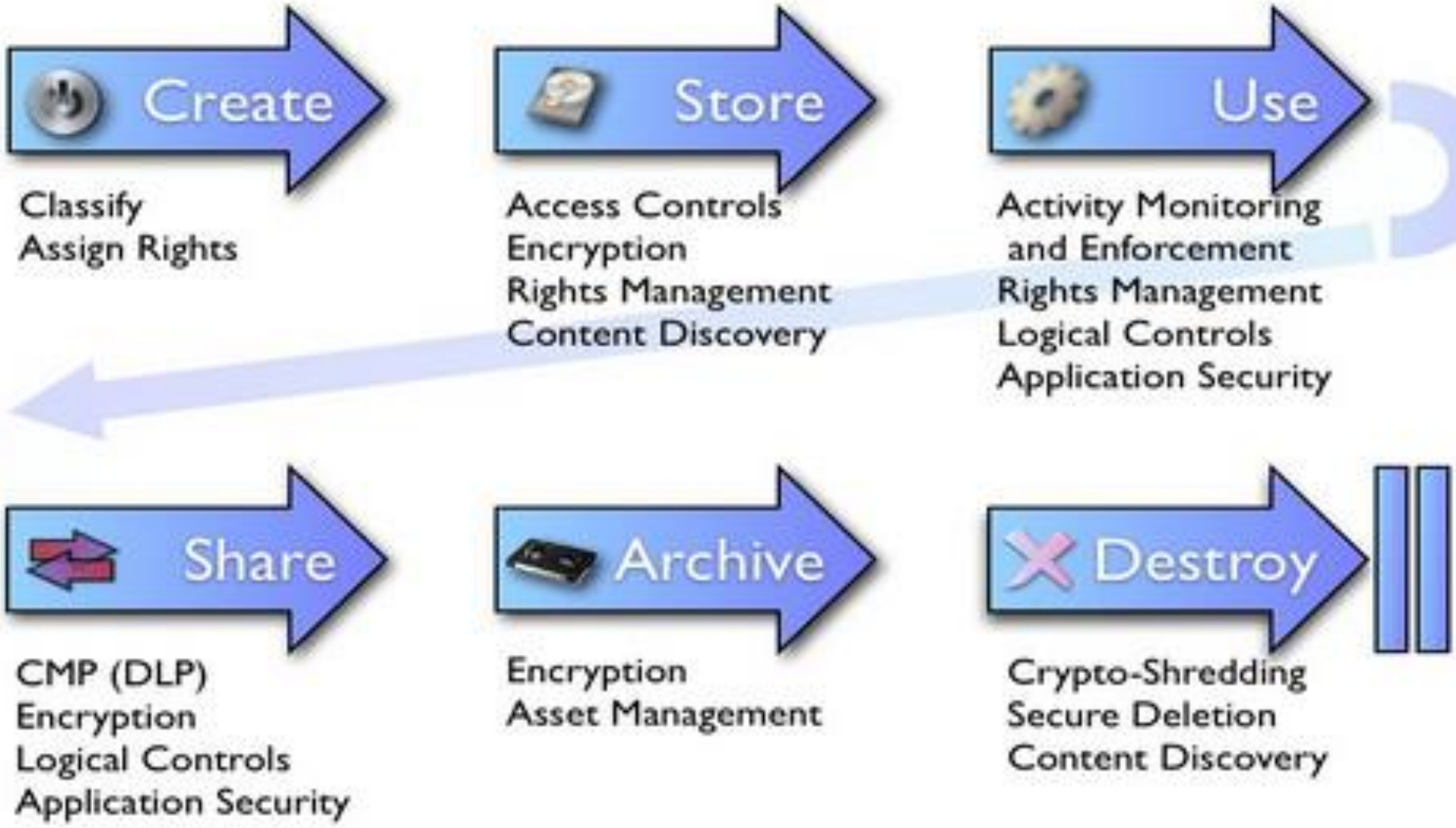
*Dopuszczalne pod warunkiem spełnienia określonych wymagań

	Create	Store	Use	Share	Archive	Destroy
Access	X	X	X	X	X	X
Process	X		X			
Store		X			X	

ZAUFANA TRZECIA STRONA.PL

Zabezpieczenia

aruba CLOUD

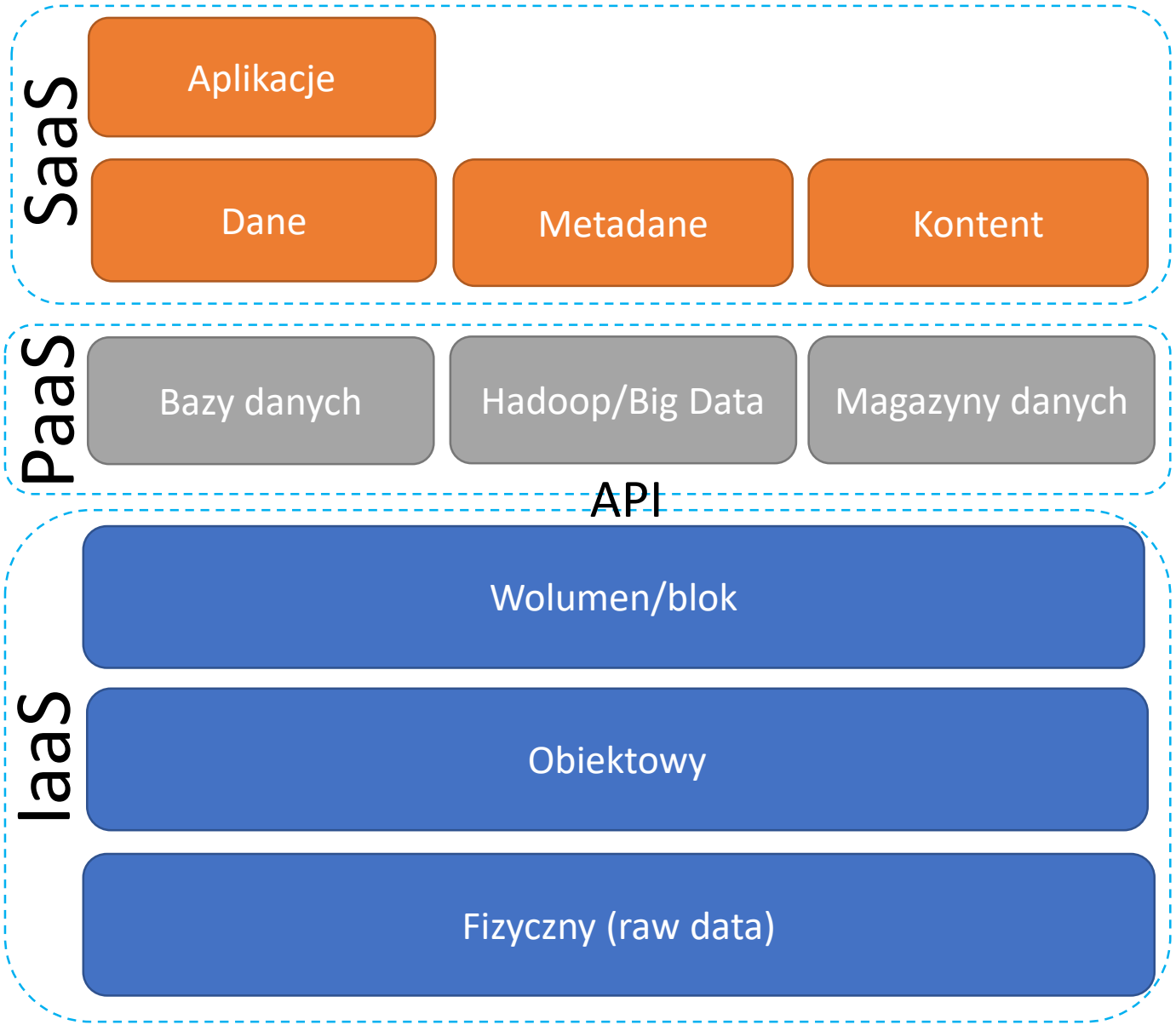


Źródło: www.cloudsecurityalliance.org

ZAUFANA TRZECIA STRONA.PL

Szyfrowanie danych w spoczynku

aruba CLOUD



- Provider-managed encryption: Dane są szyfrowane w aplikacji i generalnie zarządzane przez dostawcę
- Proxy encryption: Dane przechodzą przez szyfrujące proxy zanim trafią do SaaS.

- Szyfrowanie warstwy aplikacyjnej - Dane są szyfrowane w aplikacji lub kliencie uzyskującym dostęp do platformy.
- Szyfrowanie bazy danych - Dane są szyfrowane wykorzystując mechanizmy wbudowane I wspierane przez platformę bazodanową
- Proxy encryption: Dane przechodzą przez szyfrujące proxy zanim trafią do platformy

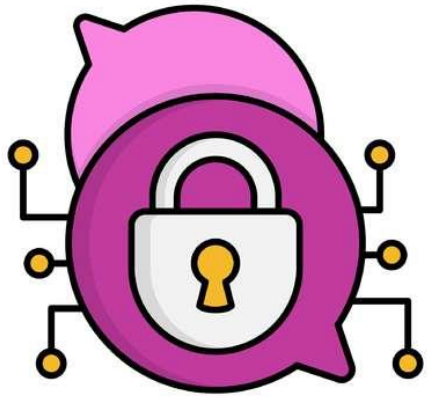
- Instance-managed encryption (TrueCrypt, dm-crypt Linuxa)
- Externally-managed encryption (HSM, SecaaS, Serwer)

- Szyfrowanie po stronie klienta (client-side encryption)
- Szyfrowanie po stronie serwera (server-side encryption)

ZAUFANA TRZECIA STRONA.PL

Szyfrowanie podczas przesyłu

aruba CLOUD



OS	Client	S/MIME	PGP		
			-MDC	+MDC	SE
Windows	Outlook 2007	∠	∠	∠	√
	Outlook 2010	∠	√	√	√
	Outlook 2013	⊥	√	√	√
	Outlook 2016	⊥	√	√	√
	Win. 10 Mail	∠	–	–	–
	Win. Live Mail	∠	–	–	–
	The Bat!	⊥	√	√	√
	Postbox	∠	∠	∠	∠
	eM Client	∠	√	∠	√
	IBM Notes	∠	–	–	–
Linux	Thunderbird	∠	∠	∠	∠
	Evolution	∠	√	√	√
	Trojitá	∠	√	√	√
	KMail	⊥	√	√	√
	Claws	√	√	√	√
	Mutt	√	√	√	√
macOS	Apple Mail	∠	∠	∠	∠
	MailMate	∠	√	√	√
	Airmail	∠	∠	∠	∠
iOS	Mail App	∠	–	–	–
	Canary Mail	–	√	√	√
Android	K-9 Mail	–	√	√	√
	R2Mail2	∠	√	∠	√
	MailDroid	∠	√	∠	√
	Nine	∠	–	–	–
Webmail	United Internet	–	√	√	√
	Mailbox.org	–	√	√	√
	ProtonMail	–	√	√	√
	Mailfence	–	√	√	√
	GMail	∠	–	–	–
Webapp	Roundcube	–	√	√	∠
	Horde IMP	⊥	√	∠	∠
	AfterLogic	–	√	√	√
	Rainloop	–	√	√	√
	Mailpile	–	√	√	√

∠ Exfiltration (no user interaction) √ No exfiltration channel
⊥ Exfiltration (with user interaction) – Encryption not supported

kolor czerwony - możliwość deszyfrowania tylko przy otwarciu spreparowanego listu
pomarańczowy - wymaga pewnej interakcji ze strony ofiary

https://zaufanatrzeciastrona.pl/post/uzywacie-szyfrowania-poczty-lepiej-wylaczcie-od-razu-swoje-wtyczki/

Data Loss Prevention

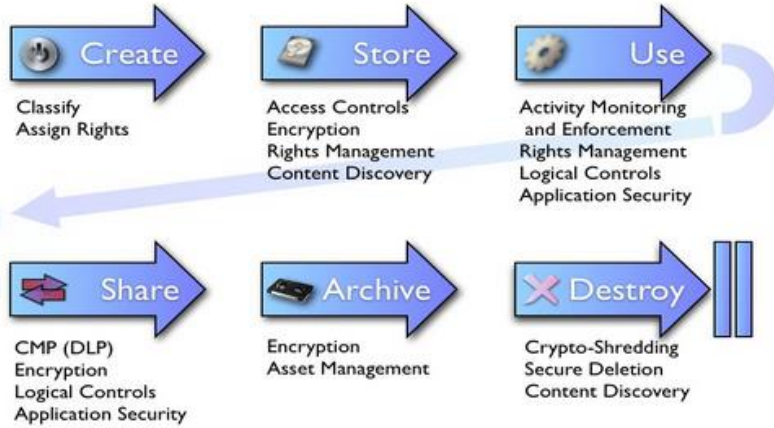
- Monitorowanie. Umożliwienie transferu danych przy jednoczesnym rejestrowaniu i zbieraniu dowodów ze zdarzeń świadczących o naruszeniu polityki bezpieczeństwa.
- Zapobieganie. Blokowanie nieuprawnionego transferu danych.
- Alarmowanie. Powiadamianie administratorów i użytkowników o incydentach naruszenia bezpieczeństwa.
- Kwarantanna. Zatrzymywanie danych w oczekiwaniu na autoryzację przed wysłaniem.
- Inwentaryzowanie. Wyszukiwanie plików zawierających dane podlegające ochronie na dyskach komputerów oraz udostępnionych zasobach.

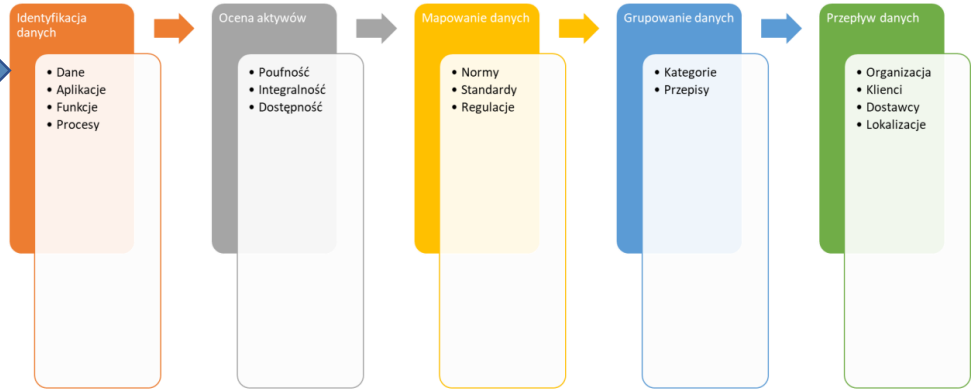
ZAUFANA TRZECIA STRONA.PL

Podsumowanie

aruba CLOUD

Kategoria	Funkcje	Aktorzy								Lokalizacja									
		Admin		Internal		Aplikacja		External		SaaS		PaaS		Iaas		EU		Non EU	
	Możliwe(M)/ Dopuszczalne (D)	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
Dane osobowe	Access	✓	✓	✓	✓	×	×	✓	×	×	✓	×	✓	×	✓	✓	✓	✓	
	Process	✓	✓	✓	✓	×	×	✓	✓	×	✓	×	✓	×	✓	✓	✓	✓	×
	Store	✓	✓	✓	✓	✓	✓	×	×	×	✓	×	✓	×	✓	✓	✓	✓	×





ZAUFANA TRZECIA STRONA.PL

Data Loss Prevention

aruba CLOUD

Pytania

Dziękuję za uwagę