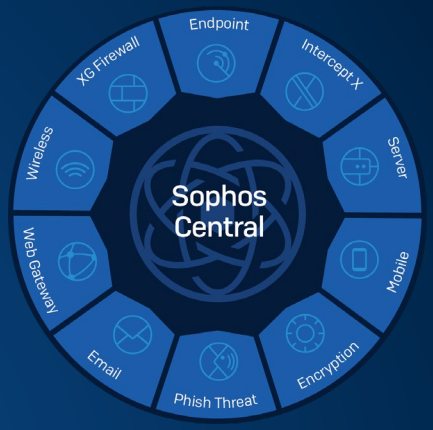
Bezpieczny wrzesień
z Sophos Central

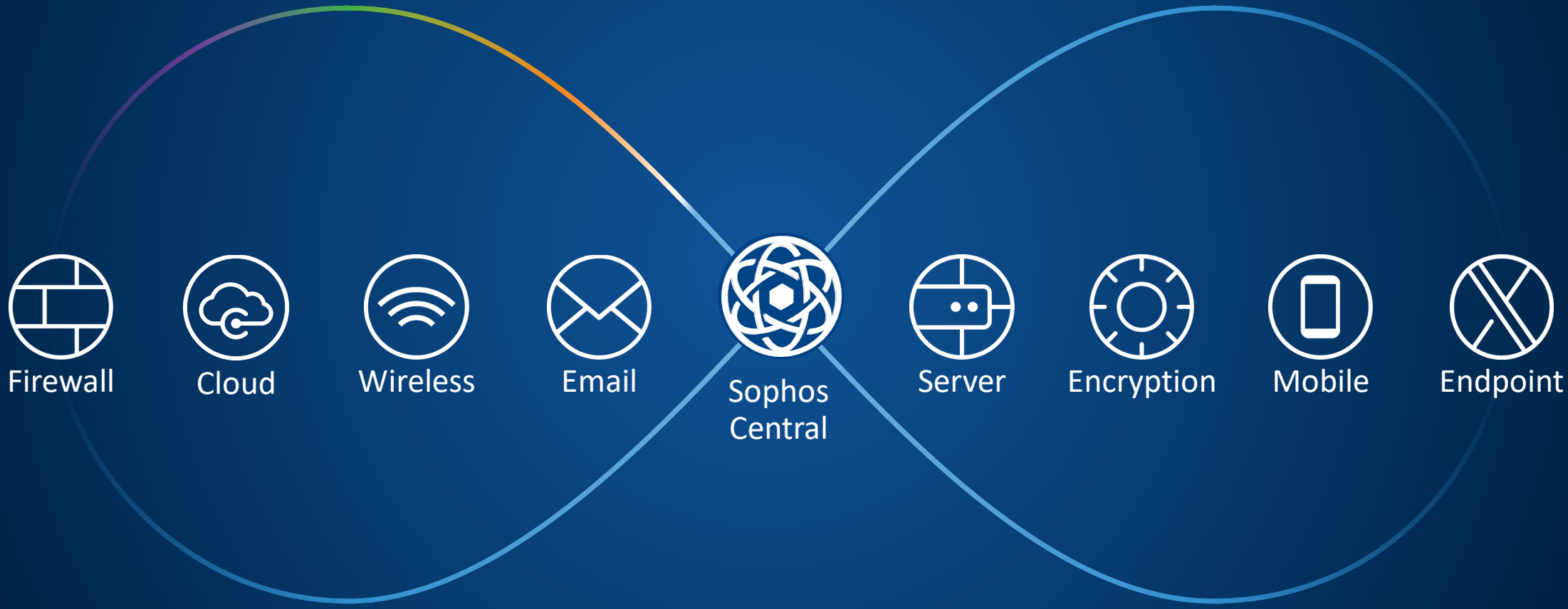


Sesja 3
Funkcje Sophos Central dla ochrony komputerów, serwerów i urządzeń mobilnych:
Intercept X z EDR dla stacji i serwerów, zarządzanie urządzeniami mobilnymi

Grzegorz Nocon
Sophos System Enginer

SOPHOS

Platforma Sophos Central



Technologie ochrony punktów końcowych i serwerów

SOPHOS

Wszystkie warstwy ochronne

Kontroluj źródła infekcji

- Kontrola WWW
- Kontrola urządzeń
- Kontrola aplikacji
- Firewall

Wstępna realizacja

- Live Protection
- Web Security
- Sygnatury
- Deep Learning
- Heurystyka
- Analiza skryptów
- Download Reputation

Podczas wykonywania

- Exploit Prevention
- Host Intrusion Prevention
- Anti-Hacker
- Anti-Ransomware
- Skanowanie pamięci
- Credential Theft Protection
- Botnet-Traffic-Detection

Reakcja

- Blokada
- Kwarantanna
- Odtwarzanie
- Czyszczenie
- Synchronized Security

Widoczność

- Logowanie Raportowanie
- Alerty
- Centralne zarządzanie
- Root Cause Analysis
- Threat Analysis
- Threat Search

SOPHOS

Central Endpoint/Server Protection

Kontroluj źródła infekcji

- Kontrola WWW
- Kontrola urządzeń
- Kontrola aplikacji
- Firewall

Wstępna realizacja

- Live Protection
- Web Security
- Sygnatury
- Deep Learning
- Heurystyka
- Analiza skryptów
- Download Reputation

Podczas wykonywania

- Exploit Prevention
- Host Intrusion Prevention
- Anti-Hacker
- Anti-Ransomware
- Skanowanie pamięci
- Credential Theft Protection
- Botnet-Traffic-Detection

Reakcja

- Blokada
- Kwarantanna
- Odtwarzanie
- Czyszczenie
- Synchronized Security

Widoczność

- Logowanie Raportowanie
- Alerty
- Centralne zarządzanie
- Root Cause Analysis
- Threat Analysis
- Threat Search

SOPHOS INTERCEPT X Advanced

Kontroluj źródła infekcji

- Kontrola WWW
- Kontrola urządzeń
- Kontrola aplikacji
- Firewall

Wstępna realizacja

- Live Protection
- Web Security
- Sygnatury
- Deep Learning
- Heurystyka
- Analiza skryptów
- Download Reputation

Podczas wykonywania

- Exploit Prevention
- Host Intrusion Prevention
- Anti-Hacker
- Anti-Ransomware
- Skanowanie pamięci
- Credential Theft Protection
- Botnet-Traffic-Detection

Reakcja

- Blokada
- Kwarantanna
- Odtwarzanie
- Czyszczenie
- Synchronized Security

Widoczność

- Logowanie Raportowanie
- Alerty
- Centralne zarządzanie
- Root Cause Analysis
- Threat Analysis
- Threat Search

SOPHOS INTERCEPT X Advanced z EDR

Kontroluj źródła infekcji

- Kontrola WWW
- Kontrola urządzeń
- Kontrola aplikacji
- Firewall

Wstępna realizacja

- Live Protection
- Web Security
- Sygnatury
- Deep Learning
- Heurystyka
- Analiza skryptów
- Download Reputation

Podczas wykonywania

- Exploit Prevention
- Host Intrusion Prevention
- Anti-Hacker
- Anti-Ransomware
- Skanowanie pamięci
- Credential Theft Protection
- Botnet-Traffic-Detection

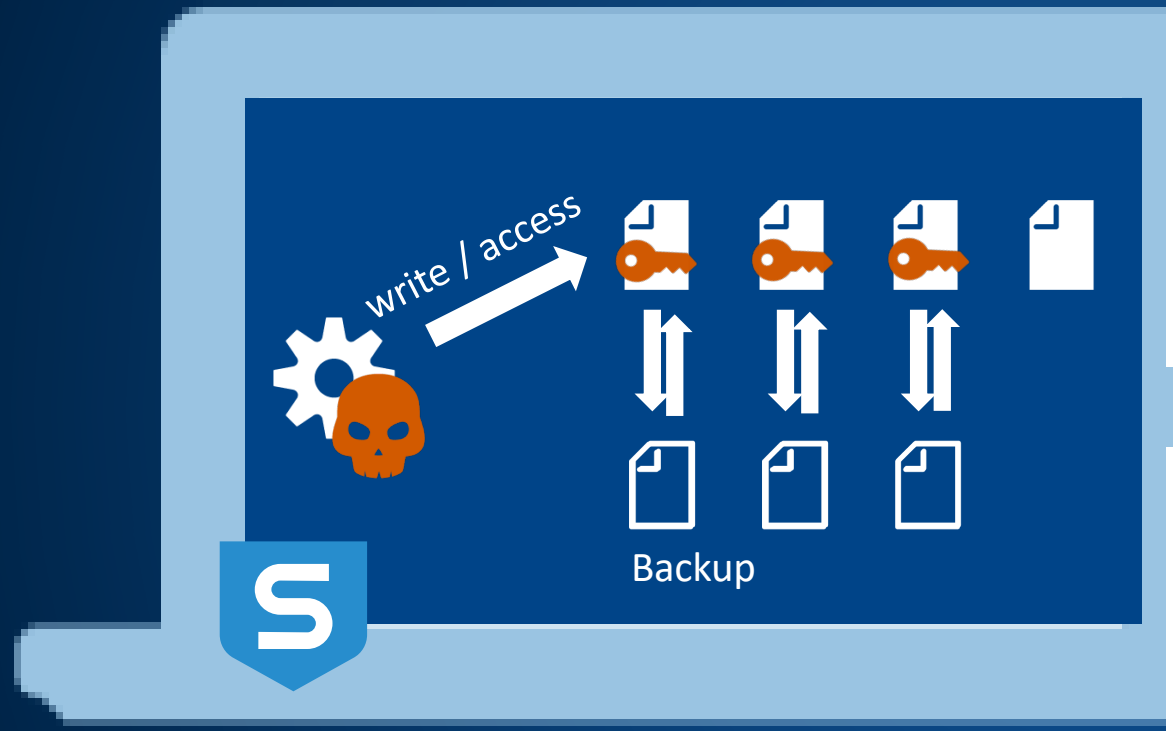
Reakcja

- Blokada
- Kwarantanna
- Odtwarzanie
- Czyszczenie
- Synchronized Security

Widoczność

- Logowanie Raportowanie
- Alerty
- Centralne zarządzanie
- Root Cause Analysis
- Threat Analysis
- Threat Search

CryptoGuard – ochrona przeciw ransomware



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	7B	5C	72	74	66	31	5C	61	6E	73	69	5C	61	6E	73	69	{\rtf1\ansi\ansi
00000010	63	70	67	31	32	35	32	5C	64	65	66	66	30	5C	64	65	cpg1252\deff0\de
00000020	66	6C	61	6E	67	31	30	34	33	7B	5C	66	6F	6E	74	74	flang1043{\fontt
00000030	62	6C	7B	5C	66	30	5C	66	6E	69	6C	5C	66	63	68	61	bl{\f0\fnil\fcha
00000040	72	73	65	74	30	20	56	65	72	64	61	6E	61	3B	7D	7D	rset0 Verdana;}}
00000050	5C	72	5C	6E	5C	76	69	65	77	6B	69	6E	64	34	5C	75	\r\n\viewkind4\u
00000060	63	31	5C	70	61	72	64	5C	73	61	32	30	30	5C	73	6C	c1\pard\sa200\sl
00000070	32	37	36	5C	73	6C	6D	75	6C	74	31	5C	6C	61	6E	67	276\slmult1\lang
00000080	39	5C	66	30	5C	66	73	32	32	20	54	68	65	20	71	75	9\f0\fs22 The qu
00000090	69	63	6B	20	62	72	6F	77	6E	20	66	6F	78	20	6A	75	ick brown fox ju
000000A0	6D	70	73	20	6F	76	65	72	20	74	68	65	20	6C	61	7A	mps over the laz
000000B0	79	20	64	6F	67	2E	7D										y dog.}

Niezaszyfrowane pliki

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	7D	EB	10	B2	FD	8E	EB	B9	D1	F6	D8	DE	CC	9B	F6	CB	}ë.²ýŽë¹ÑöØÞÌ›öË
00000010	C4	D9	C3	F6	CB	C4	D9	C3	C9	DA	CD	9B	98	9F	98	F6	ÄÙÃöËÄÙÃÉÚÍ›˜Ÿ˜ö
00000020	CE	CF	CC	CC	9A	F6	CE	CF	CC	C6	CB	C4	CD	9B	9A	9E	ÎÏÌÌšöÎÏÌÆËÄÍ›šž
00000030	99	D1	F6	CC	C5	C4	DE	DE	C8	C6	D1	F6	CC	9A	F6	CC	™ÑöÌÅÄÞÞÈÆÑöÌšöÌ
00000040	C4	C3	C6	F6	CC	C9	C2	CB	D8	D9	CF	DE	9A	8A	FC	CF	ÄÃÆöÌÉÂËØÙÏÞšŠüÏ
00000050	D8	CE	CB	C4	CB	91	D7	D7	F6	D8	F6	C4	F6	DC	C3	CF	ØÎËÄË'××öØöÄöÜÃÏ
00000060	DD	C1	C3	C4	CE	9E	F6	DF	C9	9B	F6	DA	CB	D8	CE	F6	ÝÁÃÄÎžößÉ›öÚËØÎö
00000070	D9	CB	98	9A	9A	F6	D9	C6	98	9D	9C	F6	D9	C6	C7	DF	ÙË˜ššöÙÆ˜.œöÙÆÇß
00000080	C6	DE	9B	F6	C6	CB	C4	CD	93	F6	CC	9A	F6	CC	D9	98	ÆÞ›öÆËÄÍ"öÌšöÌÙ˜
00000090	98	8A	FE	C2	CF	8A	DB	DF	C3	C9	C1	8A	C8	D8	C5	DD	˜ŠþÂÏŠÛßÃÉÁŠÈØÅÝ
000000A0	C4	8A	CC	C5	D2	8A	C0	DF	C7	DA	D9	8A	C5	DC	CF	D8	ÄŠÌÅÒŠÀßÇÚÙŠÅÜÏØ
000000B0	8A	DE	C2	CF	8A	C6	CB	D0	D3	8A	CE	C5	CD	84	D7		ŠÞÂÏŠÆËÐÓŠÎÅÍ„×

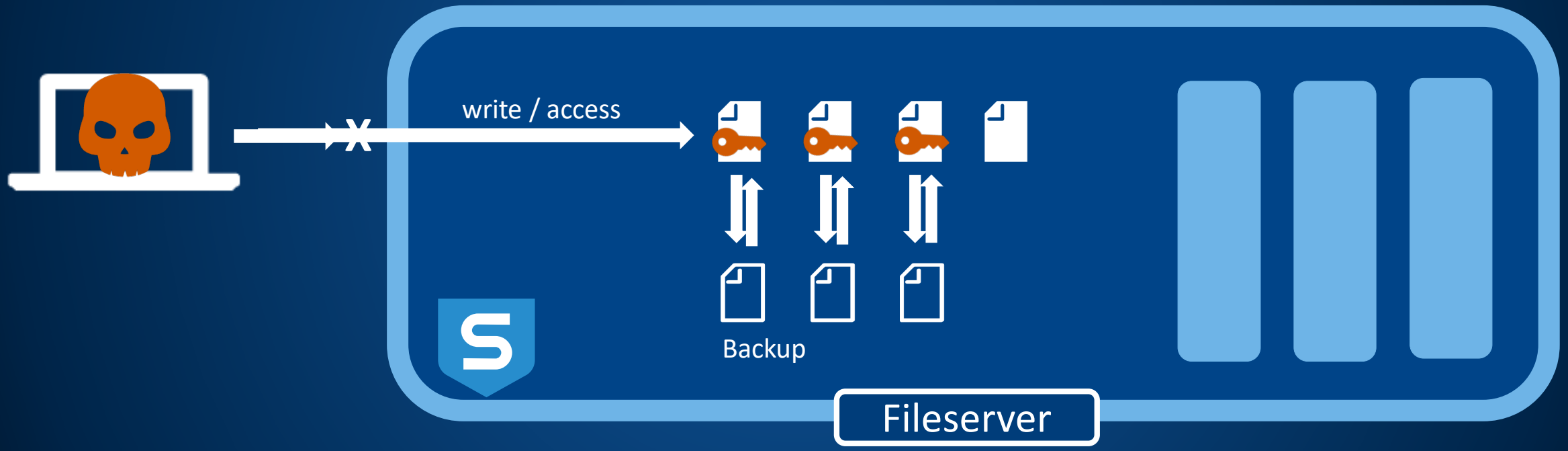
Zaszyfrowane pliki

Root Cause Analysis

Extended Cleanup z Sophos Clean

SOPHOS

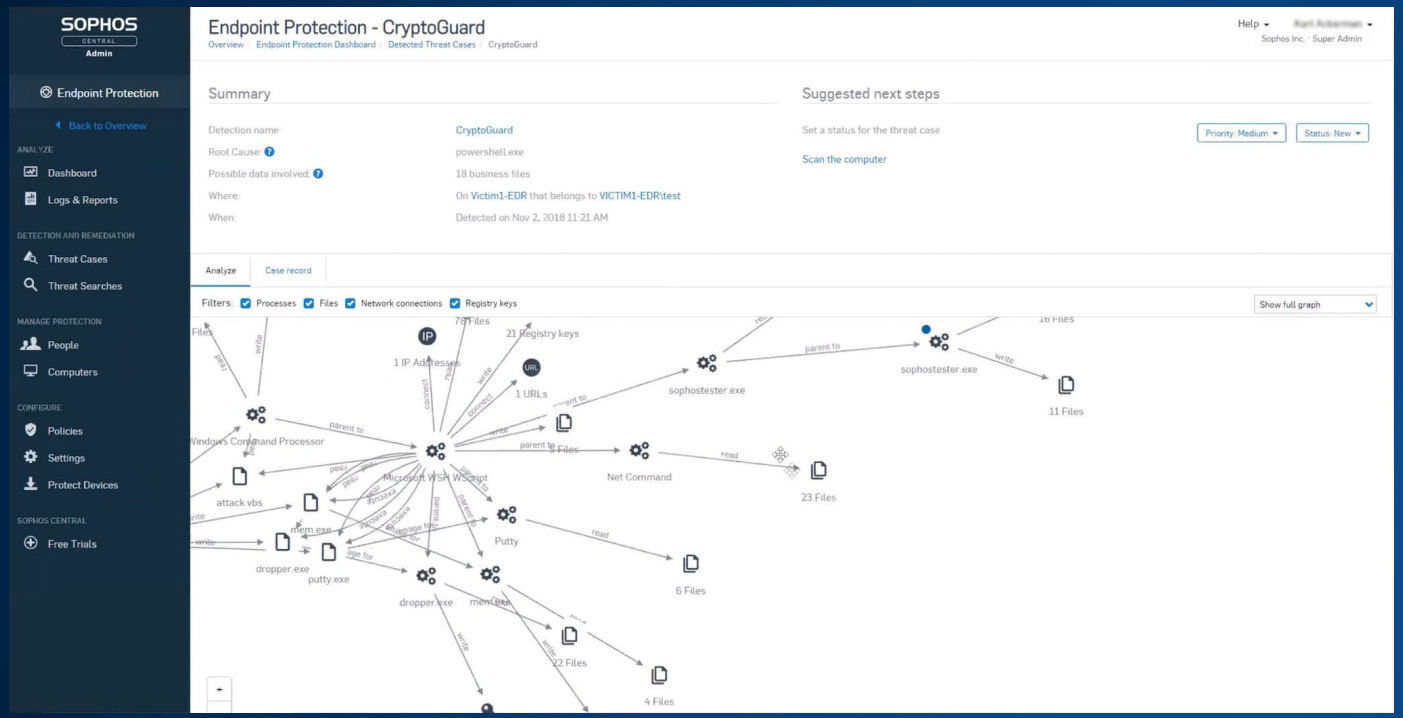
CryptoGuard – ochrona przeciwko stacji z aktywną infekcją ransomware

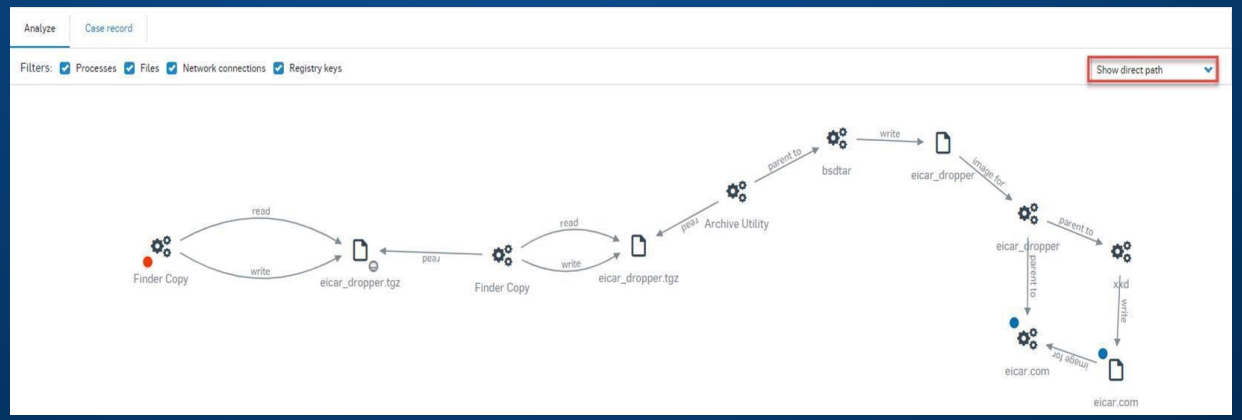


CryptoGuard - analiza

SOPHOS

Root Cause Analysis





SOPHOS

SOPHOS

Intercept X

For Server with EDR

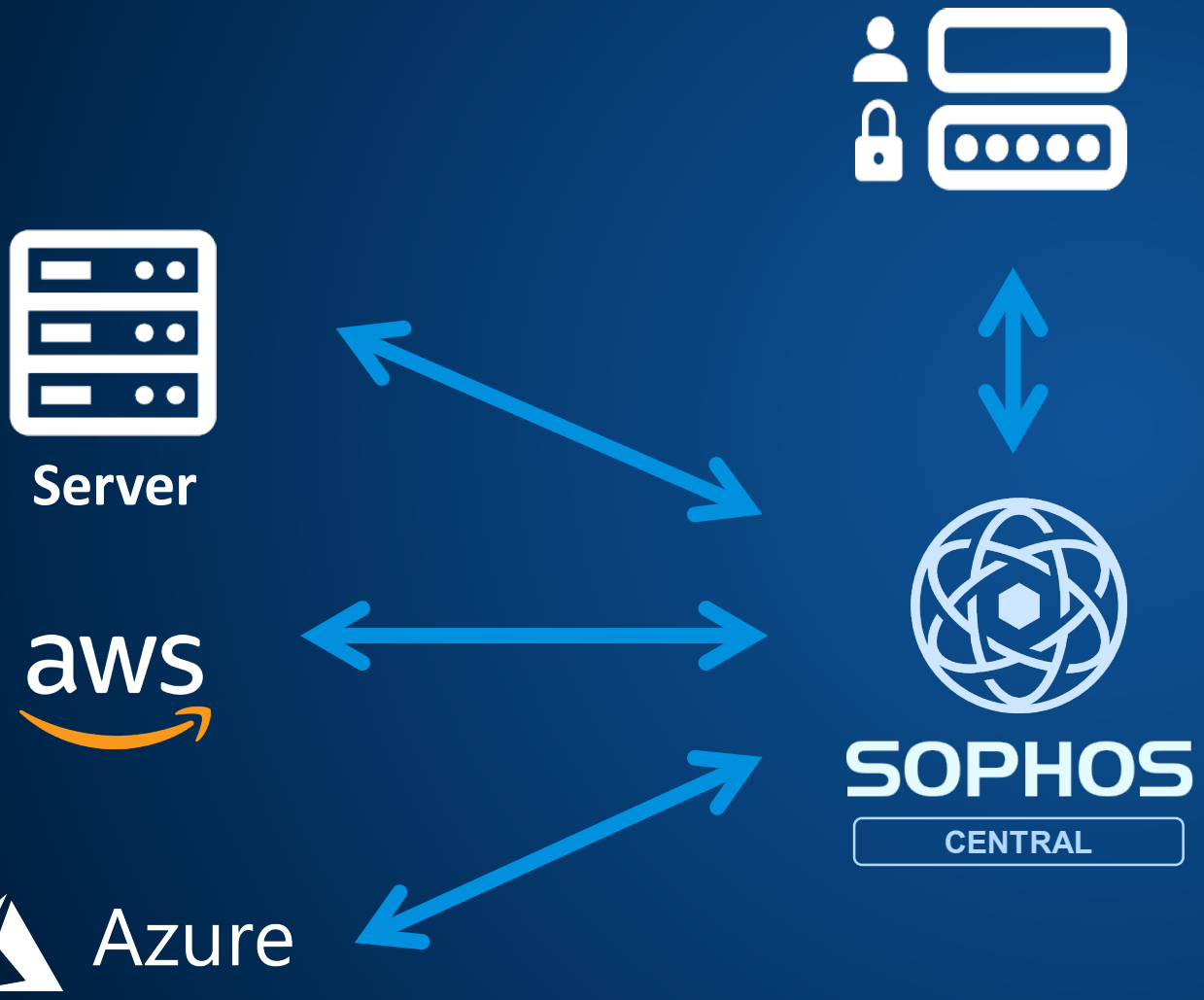
Funkcje NextGen z

SOPHOS Intercept X For Server with EDR

- Deep Learning
- Exploit Prevention
- Anti-Ransomware
- Technologia Anti-Hacker
- Server Lockdown wraz z File Integrity Monitoring
- Analiza ataku wspomagana AI
- Wyszukiwanie i ograniczanie zagrożeń w firmie
- Synchronized Security
- Zarządzanie aplikacjami i wykrywanie obciążeń aplikacji chmurowych
- Elastyczne opcje wdrażania

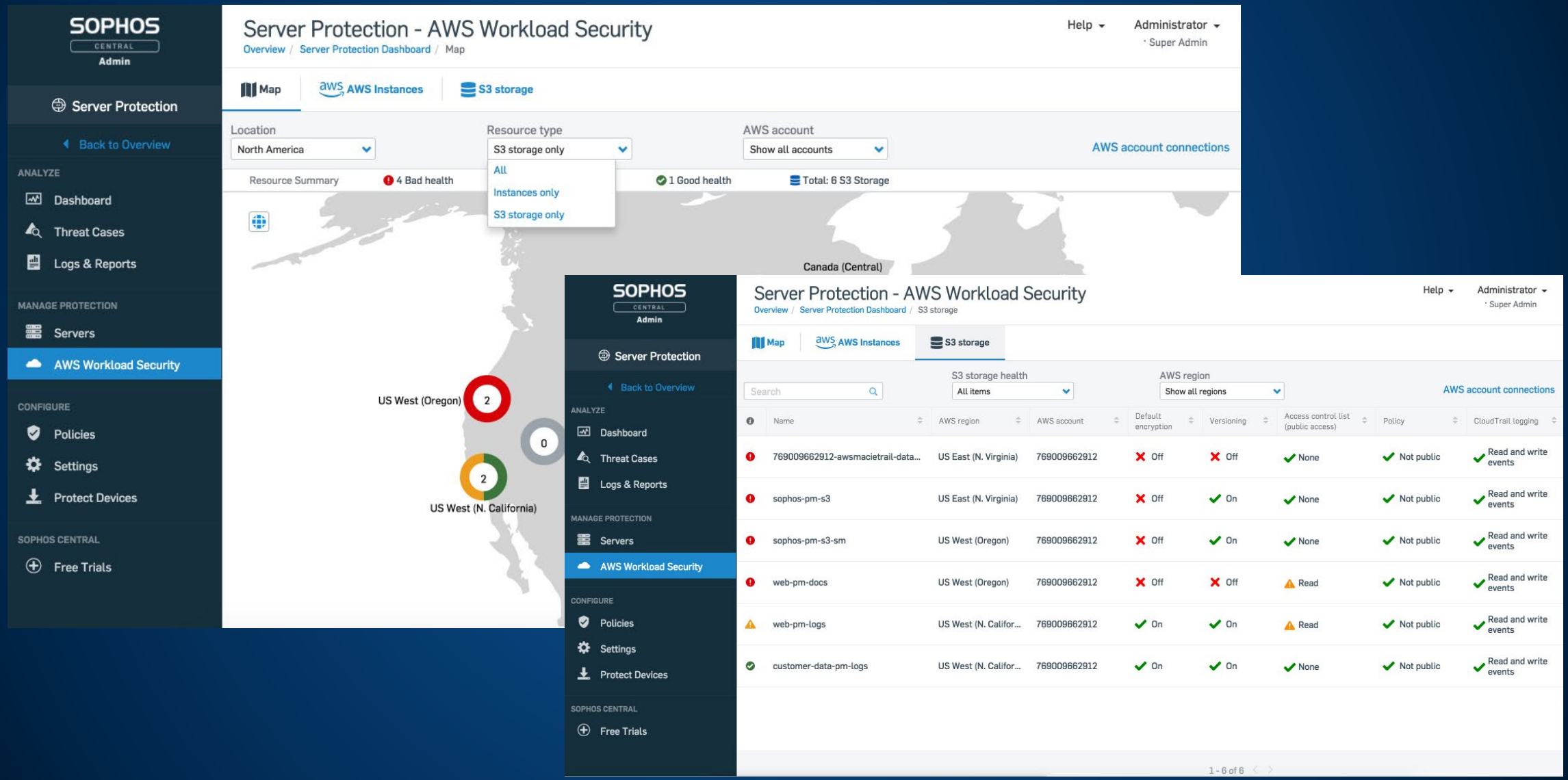
SOPHOS

Wsparcie dla chmury hybrydowej



- Zarządzaj zasadami i widocznością obciążeń w różnych środowiskach
- Integracja z interfejsami API
- Konsola zarządzania reaguje na automatyczne skalowanie i przejściowe maszyny wirtualne
- Obsługa instalacji skryptowej i automatycznej
- Zasady są automatycznie stosowane do instancji automatycznego skalowania

Serwer w ramach AWS



Najlepsza ochrona i najniższy całkowity koszt

Dlaczego warto inwestować w Intercept X?

- Wiodąca na rynku ochrona NextGen - antywirus nie chroni przed nowoczesnymi, ukierunkowanymi atakami
- Zgodność - RODO itp. Wymagają ochrony zgodnie z „najnowszym stanem wiedzy”
- Root cause analysis:
  - aby znaleźć sposoby występowania i rozprzestrzeniania się zagrożeń
  - aby dowiedzieć się, czy dane zostały skradzione
- Predefiniowane wytyczne dotyczące najlepszych praktyk
- Ochrona przed oprogramowaniem ransomware, w tym odzyskiwanie zaszyfrowanych plików
- Synchronized security wraz z innymi komponentami Sophos

EDR

Co to jest EDR (Endpoint Detection and Response)?

EDR to całościowe podejście do bezpieczeństwa punktów końcowych, z naciskiem na

- Wykrywanie i ochrona przed współczesnymi zagrożeniami
- Reakcja na zdarzenia związane z bezpieczeństwem
- Szukaj zagrożeń
- Dochodzenie kryminalistyczne - czy mamy naruszenie zasad zgodności?

SOPHOS INTERCEPT X Advanced with EDR

Integruje wszystkie elementy EDR w jednym rozwiązaniu

Demo

EDR

SOPHOS

Podsumowując...

SOPHOS

Sophos Endpoint Protection (Licencja per użytkownik)

	Central Endpoint Protection	Intercept X	Intercept X Advanced	Intercept X Advanced with EDR
AV Signaturs / HIPS / Live Protection	✓	Dowolna konkurencyjna ochrona AV	✓	✓
Device / Web / App Control	✓		✓	✓
Data Loss Protection (DLP)	✓		✓	✓
Malicious Traffic Detection (MTD)	✓	✓	✓	✓
Security Heartbeat	✓	✓	✓	✓
Deep Learning		✓	✓	✓
CryptoGuard		✓	✓	✓
WipeGuard		✓	✓	✓
Anti-Hacker-Technolies (CredGuard etc.)		✓	✓	✓
Exploit Protection		✓	✓	✓
Root cause analysis		✓	✓	✓
Automatic / Manual Client-Isolation	✓/-	✓/-	✓/-	✓/✓
Malware-Analysis by SophosLabs				✓
Search & contain threats				✓

SOPHOS

Sophos Server Protection (Licencja per serwer)

	Central Server Protection	Sophos Intercept X For Server	Sophos Intercept X For Server with EDR with EDR
AV Signaturs / HIPS / Live Protection	✓	✓	✓
Device / Web / App Control / DLP	✓	✓	✓
Automatic exclusions	✓	✓	✓
Cloud Workload Discovery	✓	✓	✓
Security Heartbeat	✓	✓	✓
Server Lockdown		✓	✓
Deep Learning		✓	✓
Anti-Ransomware (CryptoGuard, WipeGuard)		✓	✓
Anti-Hacker-Technologies (CredGuard etc.)		✓	✓
Exploit Protection		✓	✓
Root cause analysis		✓	✓
Automatic / Manual Client-Isolation	✓/-	✓/-	✓/✓
Malware-Analysis by SophosLabs			✓
Search & contain threats			✓

Sophos Mobile

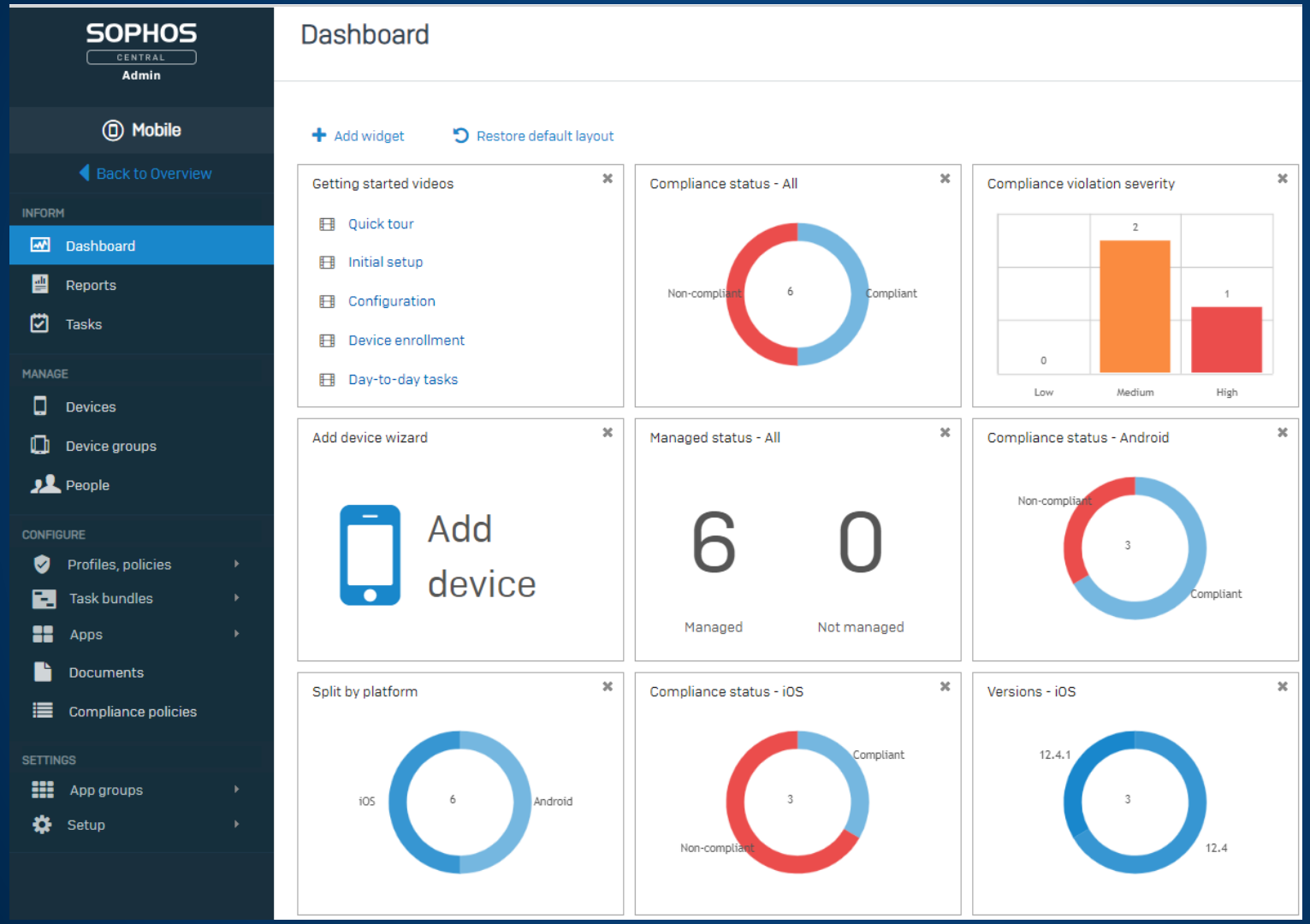
Unified Endpoint Management

SOPHOS

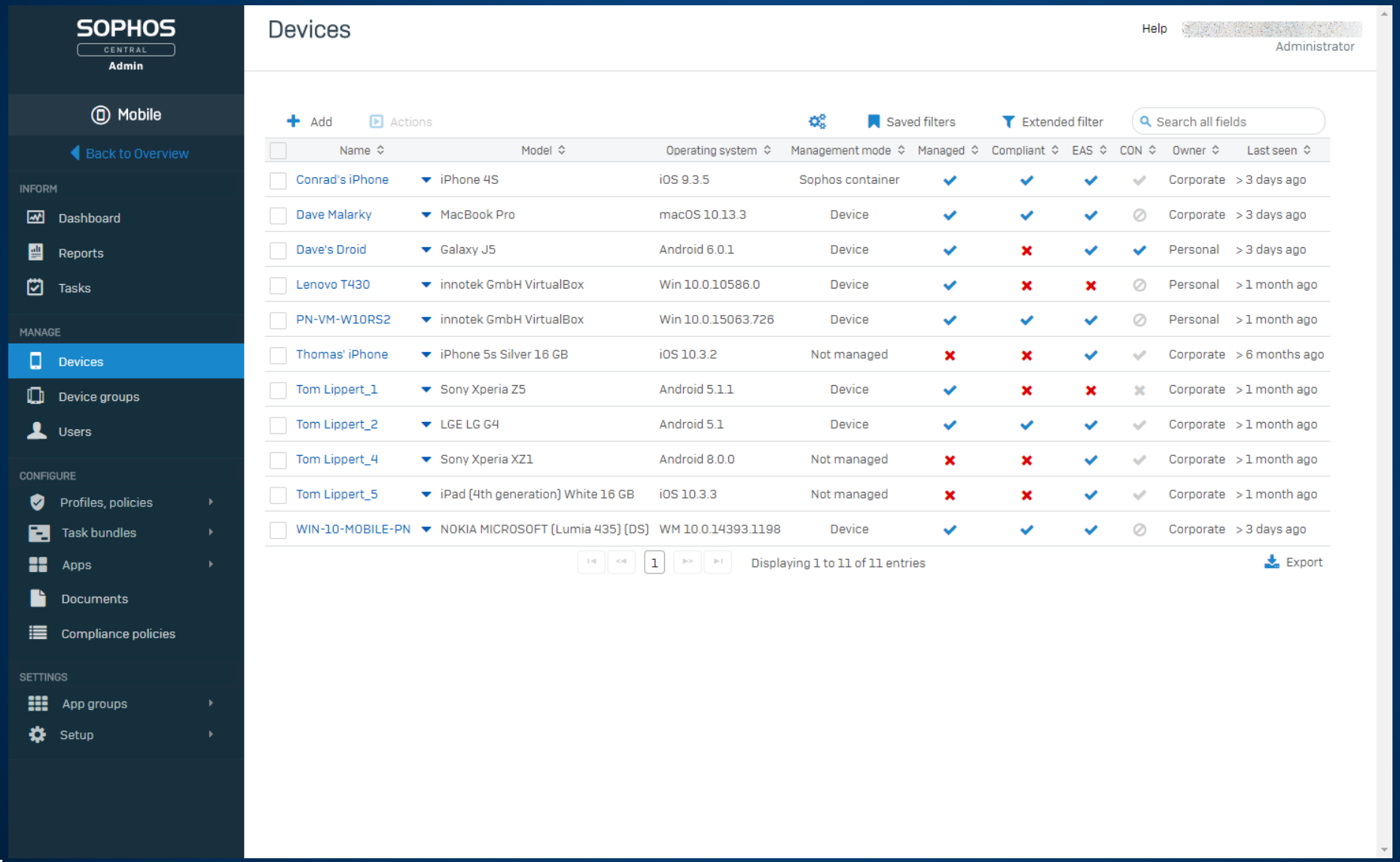
Co to jest Central Mobile?

- Dostarczanie poczty elektronicznej, sieci WLAN, VPN i aplikacji na urządzeniach korporacyjnych i prywatnych
- Integracja smartfonów, tabletów i notebooków z infrastrukturą korporacyjną
- Centralna administracja i zarządzanie urządzeniami mobilnymi niezależnie od lokalizacji
- Funkcje bezpieczeństwa w przypadku utraty i kradzieży urządzeń (blokowanie, lokalizacja i usuwanie)
- Jailbreak, rootowanie, polityka haseł, niechciane aplikacje ...

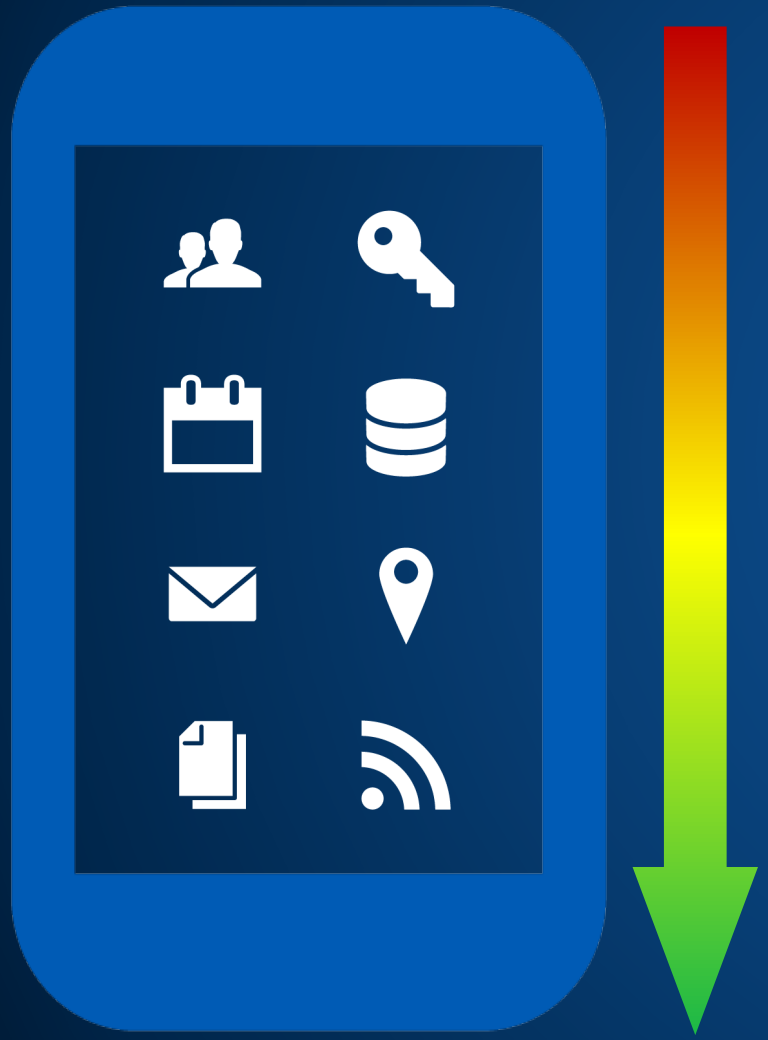
Central Mobile – konsola



Central Mobile – konsola



Jakie dane dotyczące RODO znajdują się na urządzeniu mobilnym?



Kontakty

Elementy kalendarza

E-maile

Dokumenty firmowe

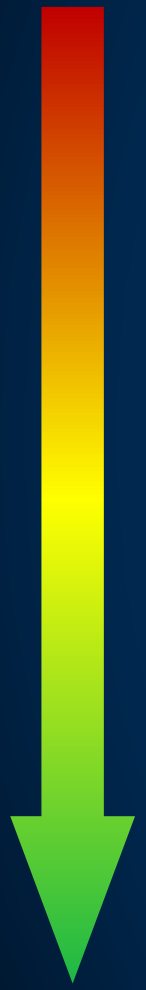
Dostęp do danych dla aplikacji i usług

Lokalnie przechowywane dane w aplikacjach firmy

Dane lokalizacji

Adresy IP

Jakie dane dotyczące RODO znajdują się na urządzeniu mobilnym?



- **Aplikacje z niechcianymi danymi**

  Biała lub czarna lista aplikacji, kontrola dostępu do danych

- **Aplikacje złośliwego oprogramowania**

  Rozwiązanie Mobile Security wyszukuje i usuwa wszystkie złośliwe oprogramowanie

- **Utrata lub kradzież urządzenia**

  Zablokuj, zlokalizuj i usuń dane urządzenia lub firmy

- **Utrata danych z powodu błędu użytkownika**

  Konteneryzacja danych firmy

- **Złośliwy użytkownik**

  Konteneryzacja danych firmy, ograniczenie dostępu do danych

Dwa warianty wdrożenia

W pełni zarządzane urządzenie firmowe

- Scenariusze aplikacji:
  - Urządzenie do pojedynczej aplikacji
  - Wykorzystanie czysto biznesowe

Lock Down

1. iOS Supervised
2. Android Enterprise Full Device

Aplikacja do przechowywania danych w kontenerach

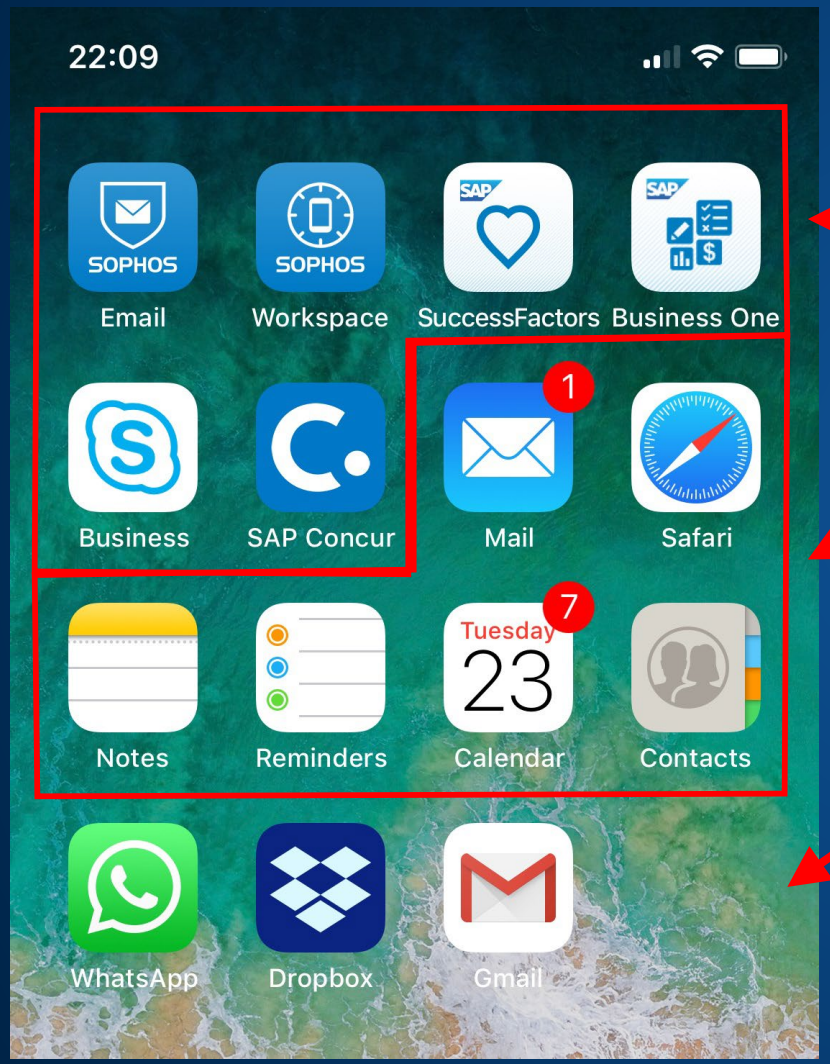
Scenariusz:

- Urządzenie firmowe do użytku prywatnego
- Prywatne urządzenie do użytku firmowego (BYOD)
- Partnerzy i konsultanci

Container

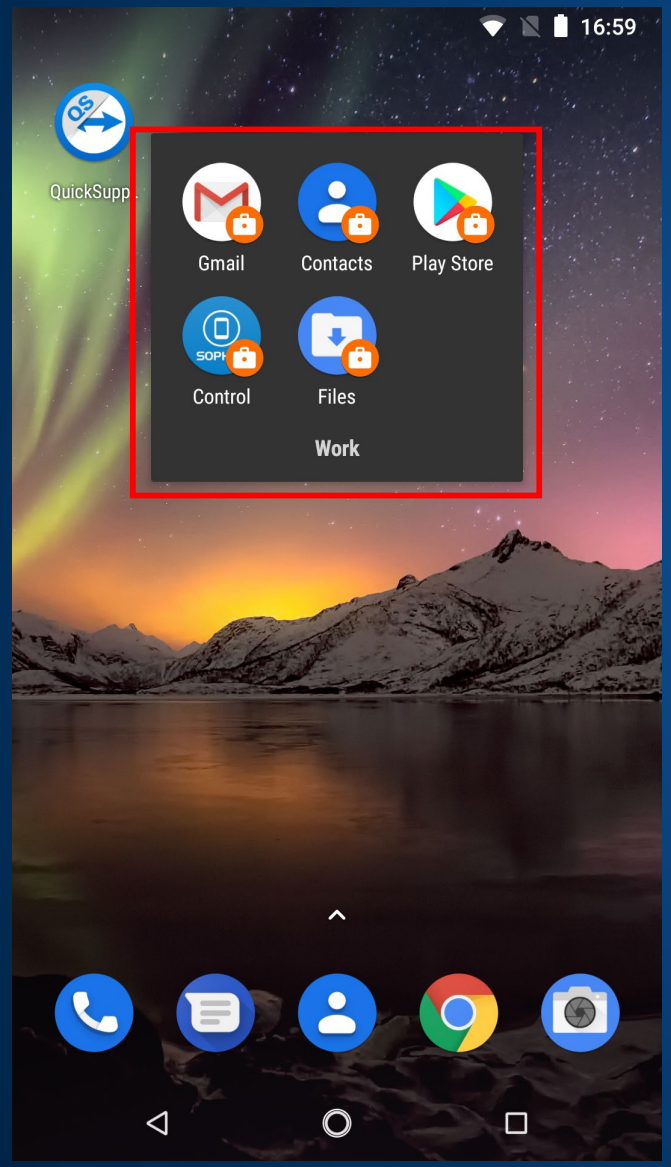
3. iOS Managed Profile
4. Android Enterprise Work Profile
5. Sophos Container

Konteneryzacja w systemie iOS - widok urządzenia



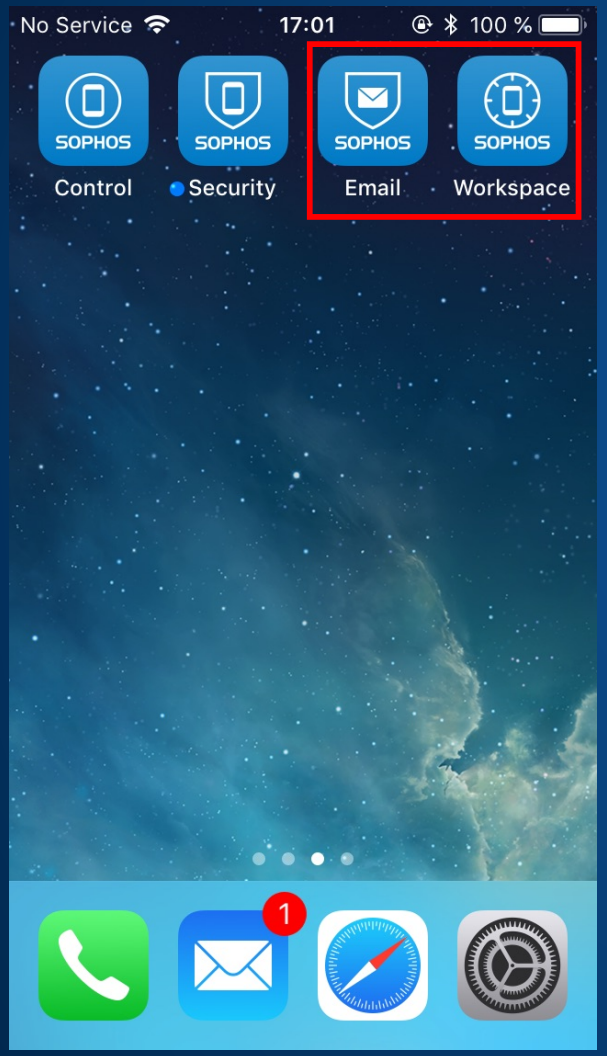
- Aplikacje z danymi firmy (aplikacje zarządzane)
- Aplikacje z osobnymi danymi firmowymi i prywatnymi (dane / konta zarządzane)
- Aplikacje osobiste (niezarządzane aplikacje i dane)

Konteneryzacja w profilach roboczych Android Enterprise



- Folder zawiera wszystkie aplikacje do pracy
- Wszystkie aplikacje robocze mają ikonę teczek
- Aplikacje w kontenerze mogą udostępniać dane
- Żadne dane nie mogą opuścić kontenera
- Zwróć uwagę na ustawienia kontaktów i dzwoniących

Konteneryzacja z kontenerem Sophos

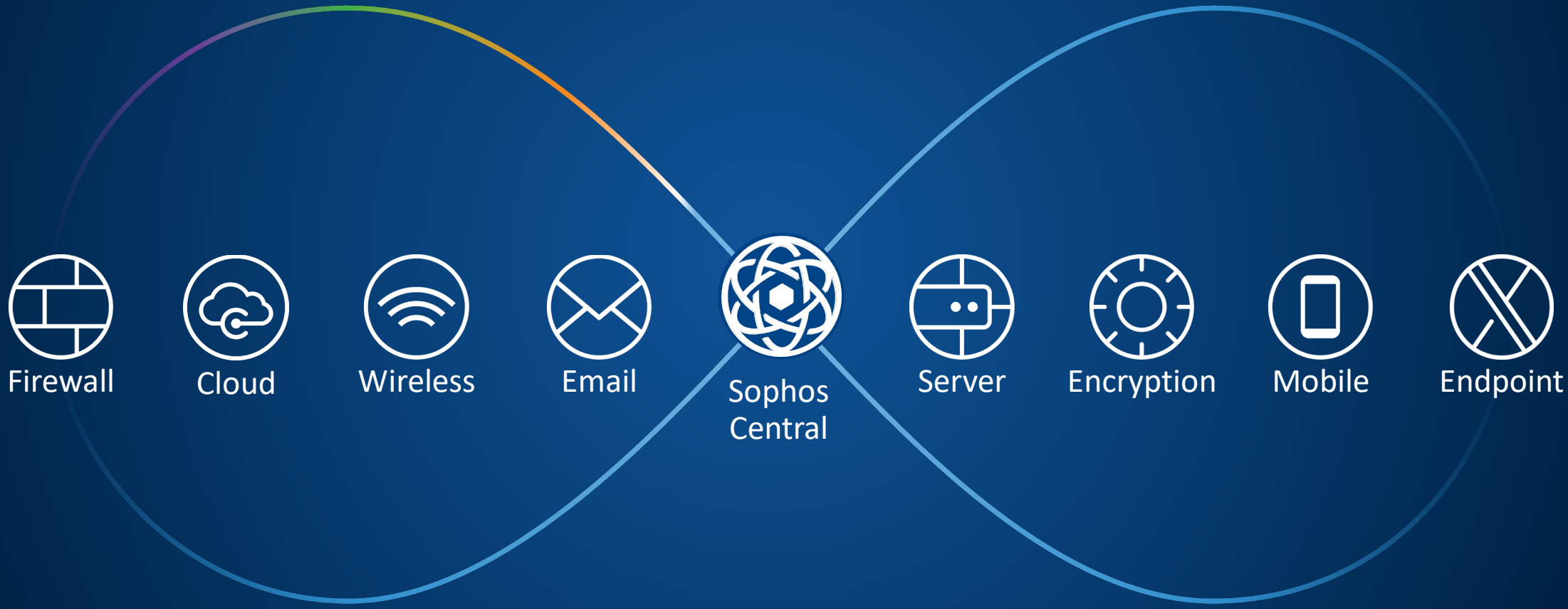


- Wszystkie dane istotne dla RODO znajdują się w kontenerze
- Obie aplikacje mogą wymieniać dane
- Kontakty są opcjonalnie wydawane tylko w ograniczonym zakresie

Sophos Central Mobile – porównanie

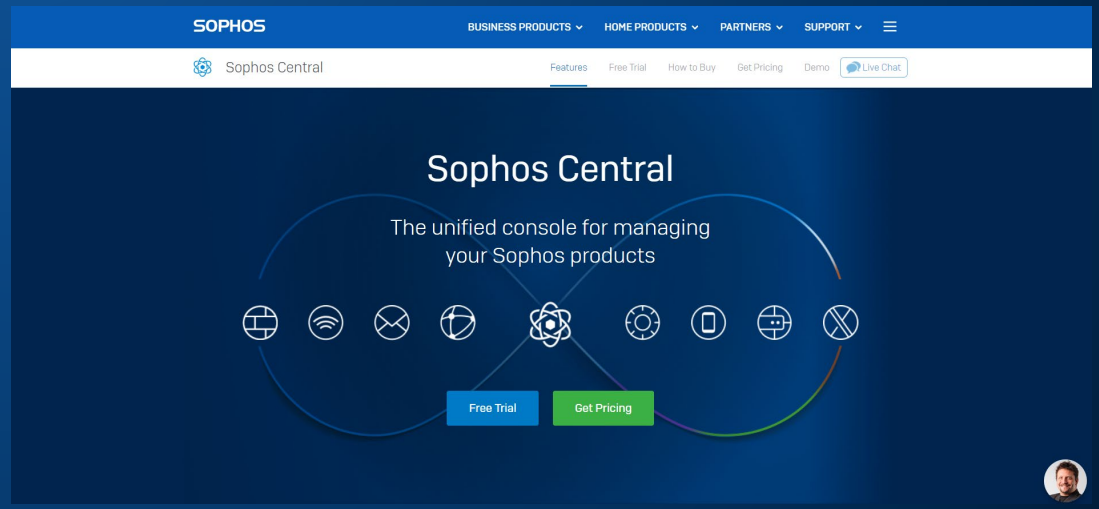
	CENTRAL MOBILE STANDARD	CENTRAL MOBILE ADVANCED	CENTRAL MOBILE SECURITY	Windows	MacOS	iOS	Android
Mobile Device Management	✓	✓		✓	✓	✓	✓
Mobile Application Management	✓	✓		✓	✓	✓	✓
Mobile Email Management	✓	✓		✓	✓	✓	✓
Mobile Content Management		✓				✓	✓
Sophos Container		✓				✓	✓
Mobile Security		✓	✓			✓	✓
Security Heartbeat via Central Wireless	✓	✓	✓	✓ via Endpoint	✓ via Endpoint	✓	✓

Sophos Central



Jak przetestować Sophos Central

- Istnieją dwie drogi rozpoczęcia wersji testowej
    1. Poprzez stronę www
    2. Poprzez swojego dystrybutora
- Każda nowo utworzona wersja trial ma dostęp do wszystkich produktów przez okres 30 dni. (Central Wireless wymaga Sophos APX)
- Każde konto Sophos Central pozwala na uruchomienie wersji trial.



SOPHOS

SOPHOS

Cybersecurity evolved.