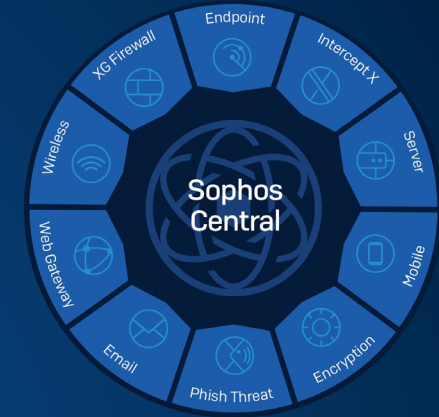


# Bezpieczny wrzesień z Sophos Central

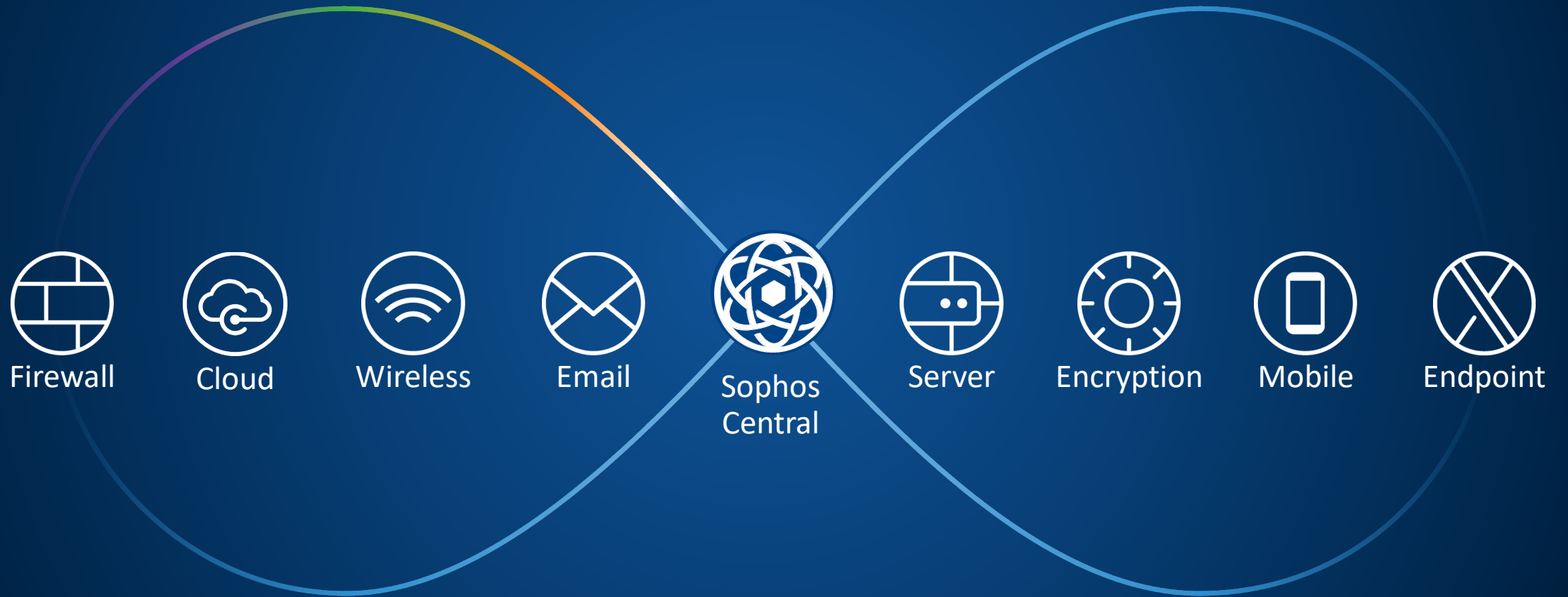


## Sesja 3

**Funkcje Sophos Central dla ochrony komputerów, serwerów i urządzeń mobilnych:**

**Intercept X z EDR dla stacji i serwerów, zarządzanie urządzeniami mobilnymi**

# Platforma Sophos Central



# Technologie ochrony punktów końcowych i serwerów

# 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

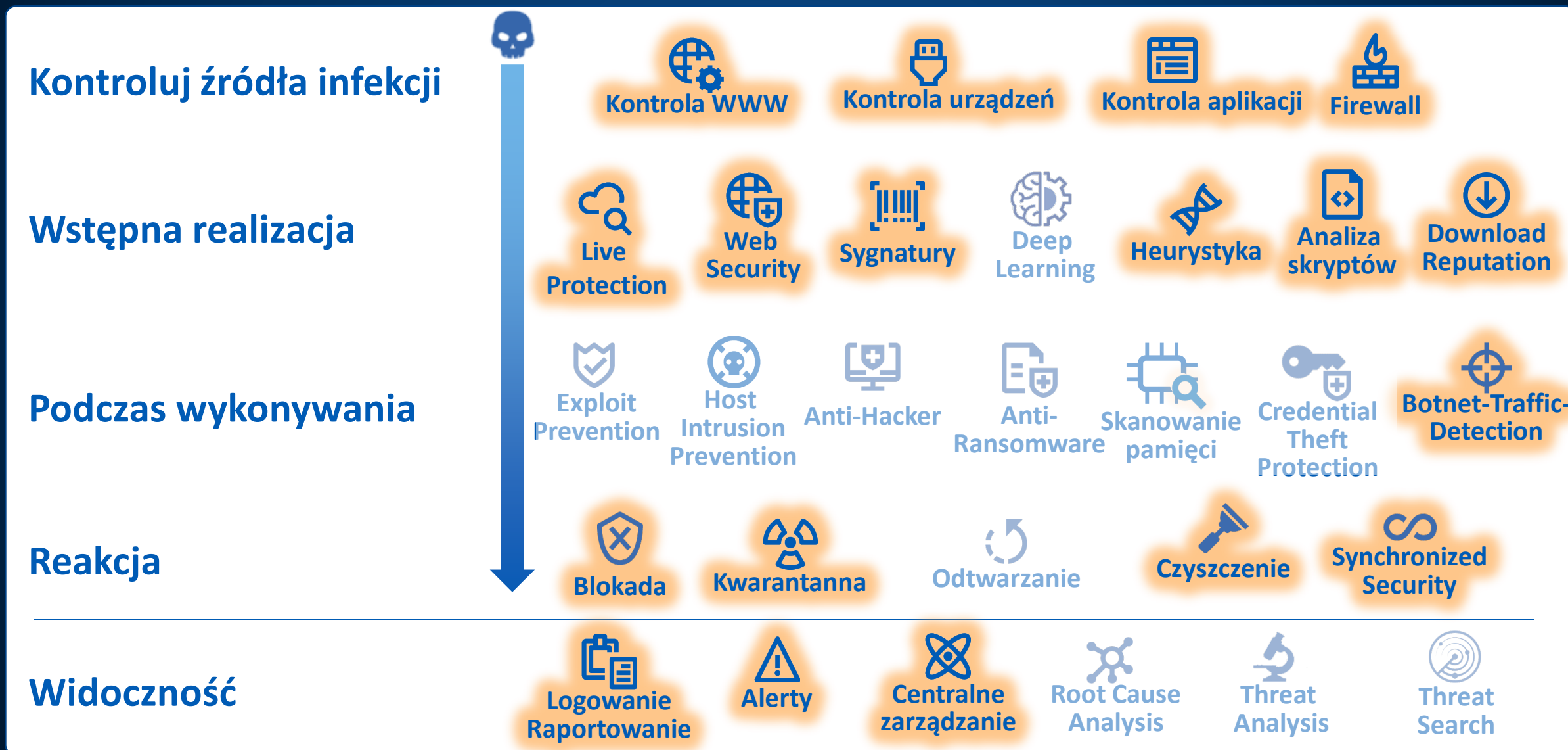
 Centralne zarządzanie

 Root Cause Analysis

 Threat Analysis

 Threat Search

# 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

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

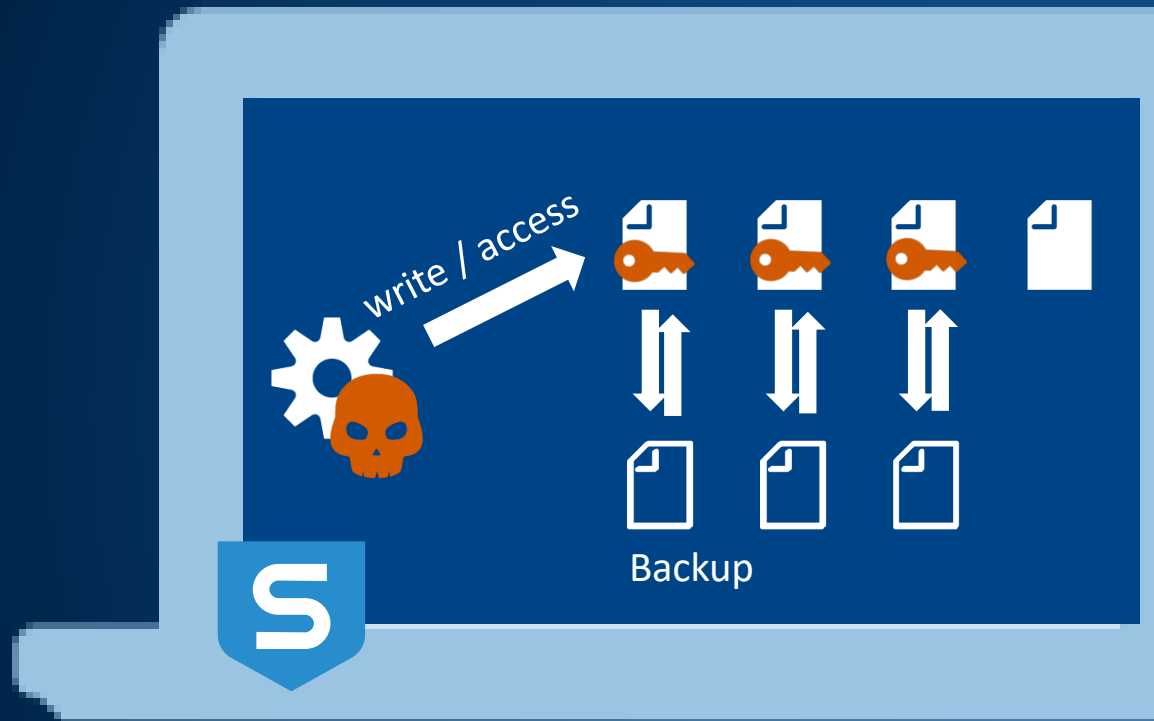
Centralne zarządzanie

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  [e. *yZe+N00Pi>0E
00000010 C4 D9 C3 F6 CB C4 D9 C3 C9 DA CD 9B 98 9F 98 F6  AUA0EAUA0EUÍ>~Y~0
00000020 CE CF CC CC 9A F6 CE CF CC C6 CB C4 CD 9B 9A 9E  iiii0iiiiEEAÍ>sz
00000030 99 D1 F6 CC C5 C4 DE DE C8 C6 D1 F6 CC 9A F6 CC  "NoiAApPEEñoisoi
00000040 C4 C3 C6 F6 CC C9 C2 CB D8 D9 CF DE 9A 8A FC CF  AA0eiEAE0UipšSuí
00000050 D8 CE CB C4 CB 91 D7 D7 F6 D8 F6 C4 F6 DC C3 CF  0iEAE`*x000A0UAI
00000060 DD C1 C3 C4 CE 9E F6 DF C9 9B F6 DA CB D8 CE F6  YAAAifz0BÉ>0UE0i0
00000070 D9 CB 98 9A 9A F6 D9 C6 98 9D 9C F6 D9 C6 C7 DF  UE~šš0UE".00UECB
00000080 C6 DE 9B F6 C6 CB C4 CD 93 F6 CC 9A F6 CC D9 98  EP>0EEAÍ"0i0oiU~
00000090 98 8A FE C2 CF 8A DB DF C3 C9 C1 8A C8 D8 C5 DD  ~ŠpAÍŠÜBÁEÁŠÈ0ÁY
000000A0 C4 8A CC C5 D2 8A C0 DF C7 DA D9 8A C5 DC CF D8  AŠiA0ŠAB0UŠAUI0
000000B0 8A DE C2 CF 8A C6 CB D0 D3 8A CE C5 CD 84 D7  ŠpAÍŠEE0ÓŠiAÍ„x
    
```

Zaszyfrowane pliki



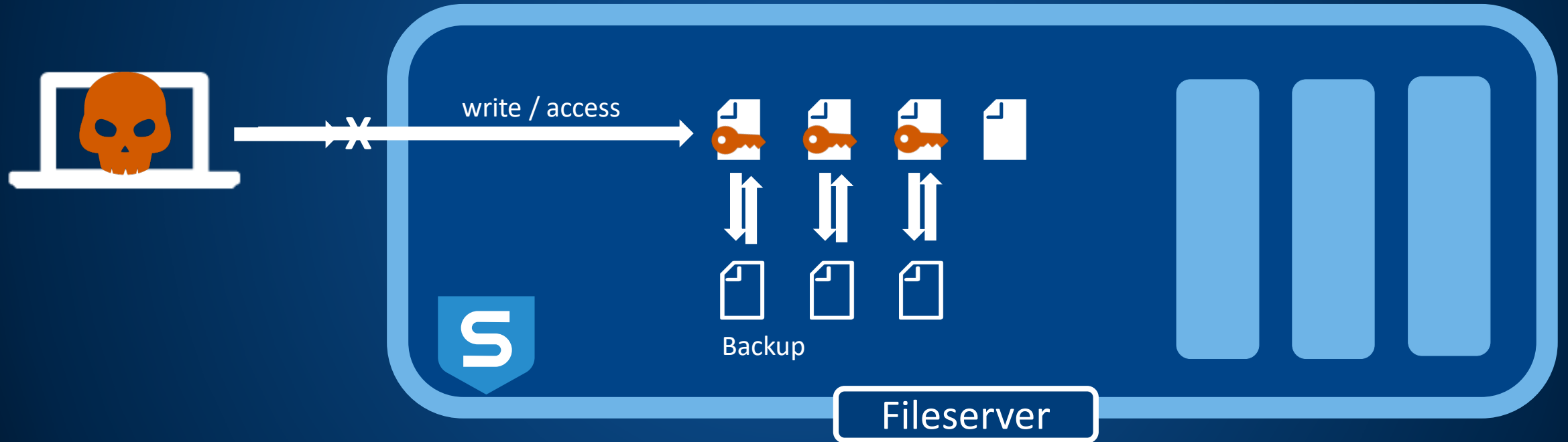
Root Cause Analysis



Extended Cleanup z Sophos Clean



# CryptoGuard – ochrona przeciwko stacji z aktywną infekcją ransomware



# CryptoGuard - analiza

**SOPHOS**



**SOPHOS**

Intercept

*For Server with EDR* 



# Funkcje NextGen z

SOPHOS  
Intercept  
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

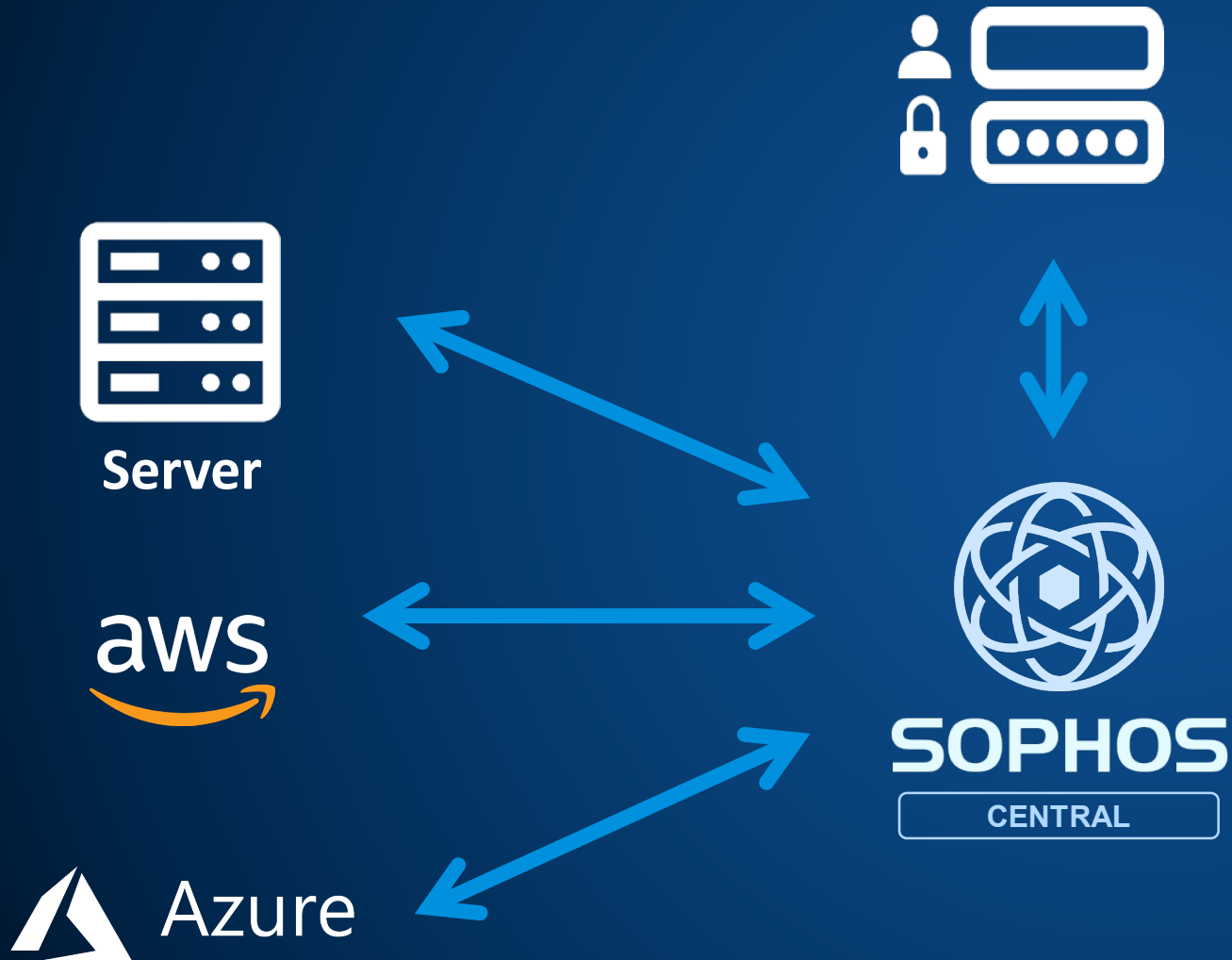


Zarządzanie aplikacjami i  
wykrywanie obciążeń aplikacji  
chmurowych



Elastyczne opcje wdrażania

# 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

**SOPHOS CENTRAL Admin**

## Server Protection - AWS Workload Security

Overview / Server Protection Dashboard / Map

Help Administrator Super Admin

Map AWS Instances S3 storage

Location: North America Resource type: S3 storage only AWS account: Show all accounts

Resource Summary: 4 Bad health 1 Good health Total: 6 S3 Storage

Canada (Central)

US West (Oregon) 2 US West (N. California) 2

### Server Protection - AWS Workload Security

Overview / Server Protection Dashboard / S3 storage

Map AWS Instances S3 storage

S3 storage health: All items AWS region: Show all regions

Name	AWS region	AWS account	Default encryption	Versioning	Access control list (public access)	Policy	CloudTrail logging
769009662912-awsmacietrail-data...	US East (N. Virginia)	769009662912	Off	Off	None	Not public	Read and write events
sophos-pm-s3	US East (N. Virginia)	769009662912	Off	On	None	Not public	Read and write events
sophos-pm-s3-sm	US West (Oregon)	769009662912	Off	On	None	Not public	Read and write events
web-pm-docs	US West (Oregon)	769009662912	Off	Off	Read	Not public	Read and write events
web-pm-logs	US West (N. Califor...)	769009662912	On	On	Read	Not public	Read and write events
customer-data-pm-logs	US West (N. Califor...)	769009662912	On	On	None	Not public	Read and write events

1 - 6 of 6

# 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?



Integruje wszystkie elementy EDR  
w jednym rozwiązaniu



# Demo




## EDR

**SOPHOS**

# Podsumowując...

SOPHOS

# Sophos Endpoint Protection (Licencja per użytkownik)

	CENTRAL ENDPOINT PROTECTION		 Advanced	 Advanced with EDR
AV Signatures / 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 Server Protection (Licencja per serwer)

	CENTRAL SERVER PROTECTION	SOPHOS Intercept For Server 	SOPHOS Intercept For Server with EDR III 
AV Signatures / 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





# 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



**SOPHOS**  
CENTRAL  
Admin

**Mobile**

[Back to Overview](#)

INFORM

- Dashboard**
- Reports
- Tasks

MANAGE

- Devices
- Device groups
- People

CONFIGURE

- Profiles, policies
- Task bundles
- Apps
- Documents
- Compliance policies

SETTINGS

- App groups
- Setup

## Dashboard

[+ Add widget](#) [Restore default layout](#)

### Getting started videos

- Quick tour
- Initial setup
- Configuration
- Device enrollment
- Day-to-day tasks

### Compliance status - All

Status	Count
Non-compliant	6
Compliant	6

### Compliance violation severity

Severity	Count
Low	0
Medium	2
High	1

### Add device wizard

**Add device**

### Managed status - All

Status	Count
Managed	6
Not managed	0

### Compliance status - Android

Status	Count
Non-compliant	3
Compliant	3

### Split by platform

Platform	Count
iOS	6
Android	6

### Compliance status - iOS

Status	Count
Non-compliant	3
Compliant	3

### Versions - iOS

Version	Count
12.4.1	3
12.4	3

SOPHOS

26

# Central Mobile – konsola



**SOPHOS**  
CENTRAL  
Admin

**Mobile**  
[Back to Overview](#)

INFORM  
Dashboard  
Reports  
Tasks

MANAGE  
**Devices**  
Device groups  
Users

CONFIGURE  
Profiles, policies  
Task bundles  
Apps  
Documents  
Compliance policies

SETTINGS  
App groups  
Setup

## Devices

Help Administrator

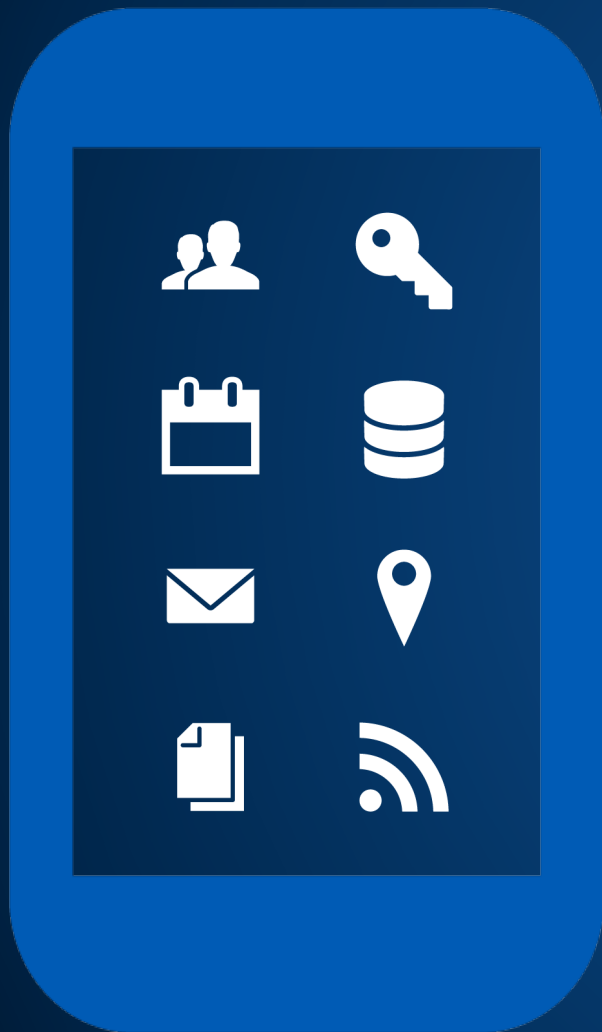
+ Add Actions Settings Saved filters Extended filter Search all fields

<input type="checkbox"/>	Name	Model	Operating system	Management mode	Managed	Compliant	EAS	CON	Owner	Last seen
<input type="checkbox"/>	Conrad's iPhone	iPhone 4S	iOS 9.3.5	Sophos container	✓	✓	✓	✓	Corporate	> 3 days ago
<input type="checkbox"/>	Dave Malarky	MacBook Pro	macOS 10.13.3	Device	✓	✓	✓	⊘	Corporate	> 3 days ago
<input type="checkbox"/>	Dave's Droid	Galaxy J5	Android 6.0.1	Device	✓	✗	✓	✓	Personal	> 3 days ago
<input type="checkbox"/>	Lenovo T430	innotek GmbH VirtualBox	Win 10.0.10586.0	Device	✓	✗	✗	⊘	Personal	> 1 month ago
<input type="checkbox"/>	PN-VM-W10RS2	innotek GmbH VirtualBox	Win 10.0.15063.726	Device	✓	✓	✓	⊘	Personal	> 1 month ago
<input type="checkbox"/>	Thomas' iPhone	iPhone 5s Silver 16 GB	iOS 10.3.2	Not managed	✗	✗	✓	✓	Corporate	> 6 months ago
<input type="checkbox"/>	Tom Lippert_1	Sony Xperia Z5	Android 5.1.1	Device	✓	✗	✗	✗	Corporate	> 1 month ago
<input type="checkbox"/>	Tom Lippert_2	LGE LG G4	Android 5.1	Device	✓	✓	✓	✓	Corporate	> 1 month ago
<input type="checkbox"/>	Tom Lippert_4	Sony Xperia XZ1	Android 8.0.0	Not managed	✗	✗	✓	✓	Corporate	> 1 month ago
<input type="checkbox"/>	Tom Lippert_5	iPad (4th generation) White 16 GB	iOS 10.3.3	Not managed	✗	✗	✓	✓	Corporate	> 1 month ago
<input type="checkbox"/>	WIN-10-MOBILE-PN	NOKIA MICROSOFT (Lumia 435) (DS)	WM 10.0.14393.1198	Device	✓	✓	✓	⊘	Corporate	> 3 days ago

« « 1 » » Export

Displaying 1 to 11 of 11 entries

# 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

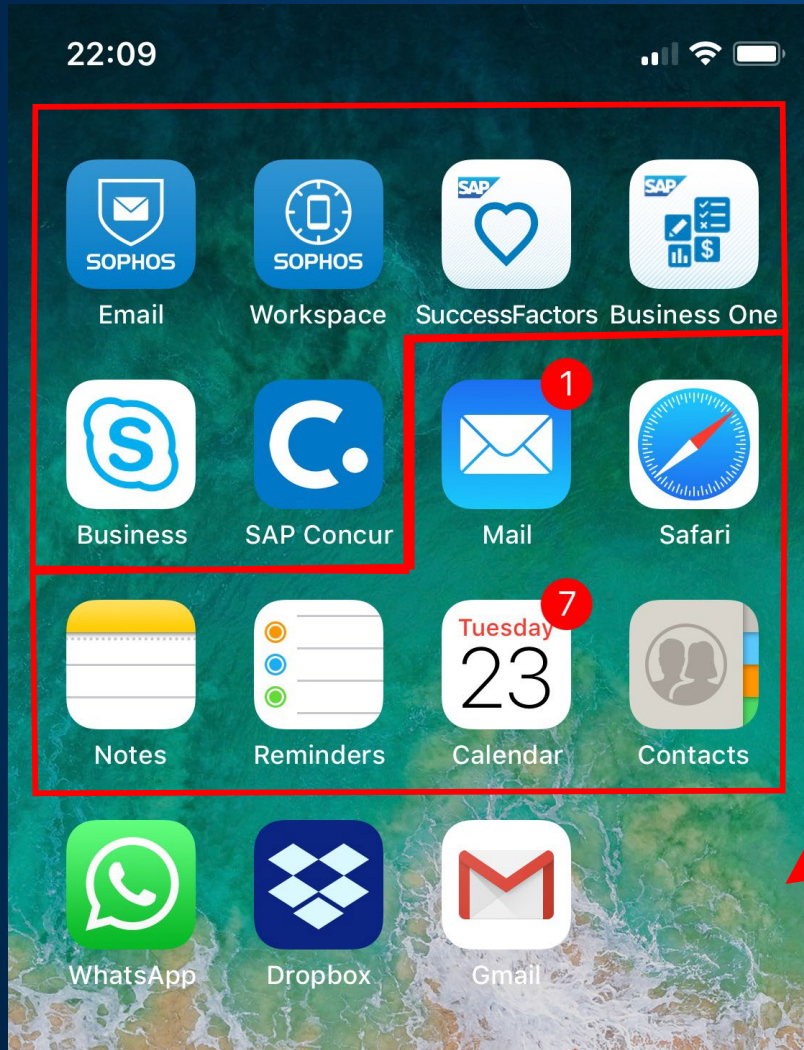
### Scenariusz:

- 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

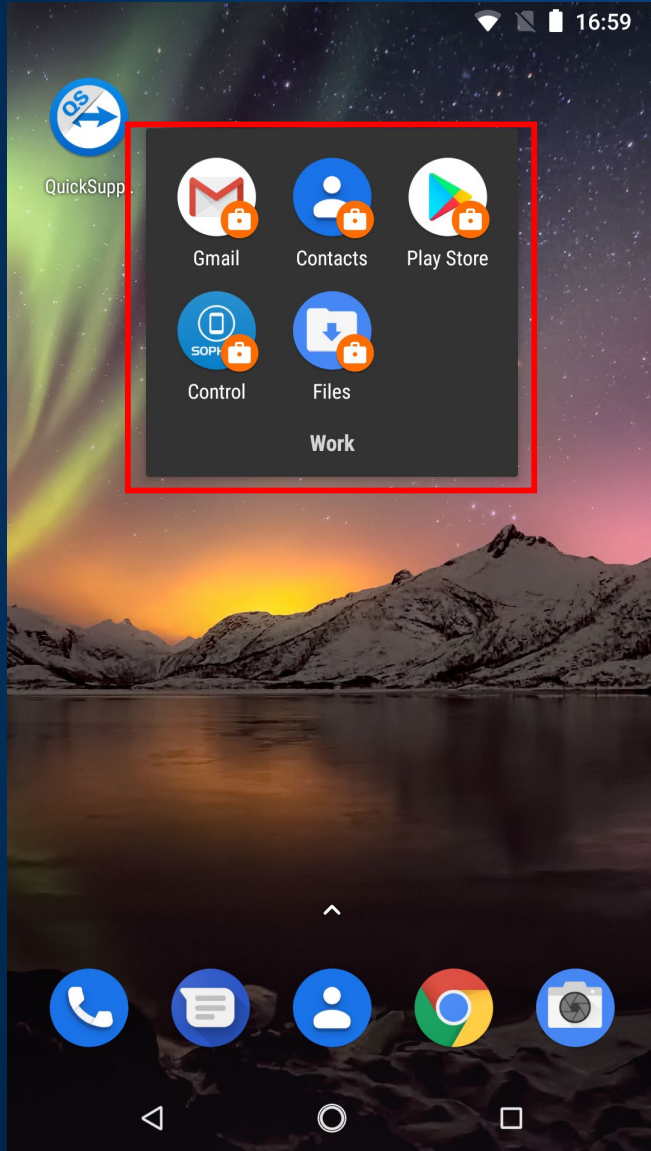


• Aplikacje z danymi firmy (aplikacje zarządzane)

• 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 teczki
- Aplikacje w kontenerze mogą udostępniać dane
- Żadne dane nie mogą opuścić kontenera
- Zwróć uwagę na ustawienia kontaktów i dzwoniących



# Konteneryzacja z kontenerem Sophos



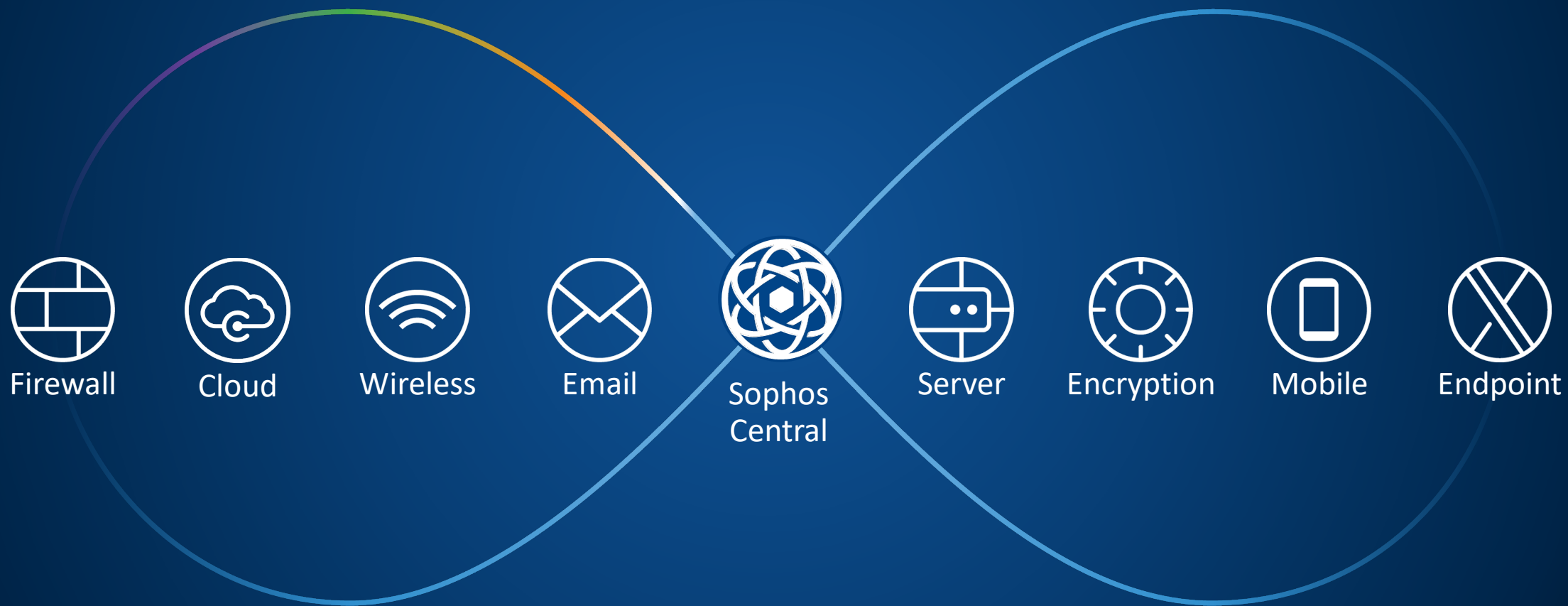
- Wszystkie dane istotne dla RODO znajdują się w kontenerze
- Obie aplikacje mogą wymieniać dane
- Kontakty są opcjonalnie wydawane tylko w ograniczonym zakresie

# Sophos Central Mobile – porównanie



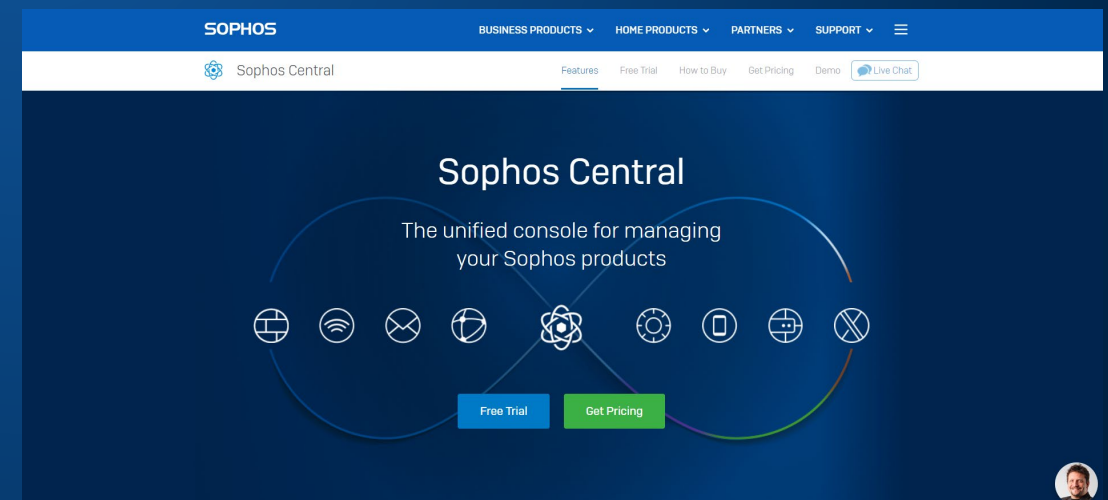
	CENTRAL MOBILE STANDARD	CENTRAL MOBILE ADVANCED	CENTRAL MOBILE SECURITY	Windows	MacOS	iOS	Android
Mobile Device Management	✓	✓		✓	✓	✓	✓
Mobile Application Management	✓	✓		✓	✓	✓	✓
Mobile Email Management	✓	✓		✓	✓	✓	✓
Mobile Content Management		✓				✓	✓
Sophos Container		✓				✓	✓
Mobile Security		✓	✓			✓	✓
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**  
Cybersecurity evolved.