

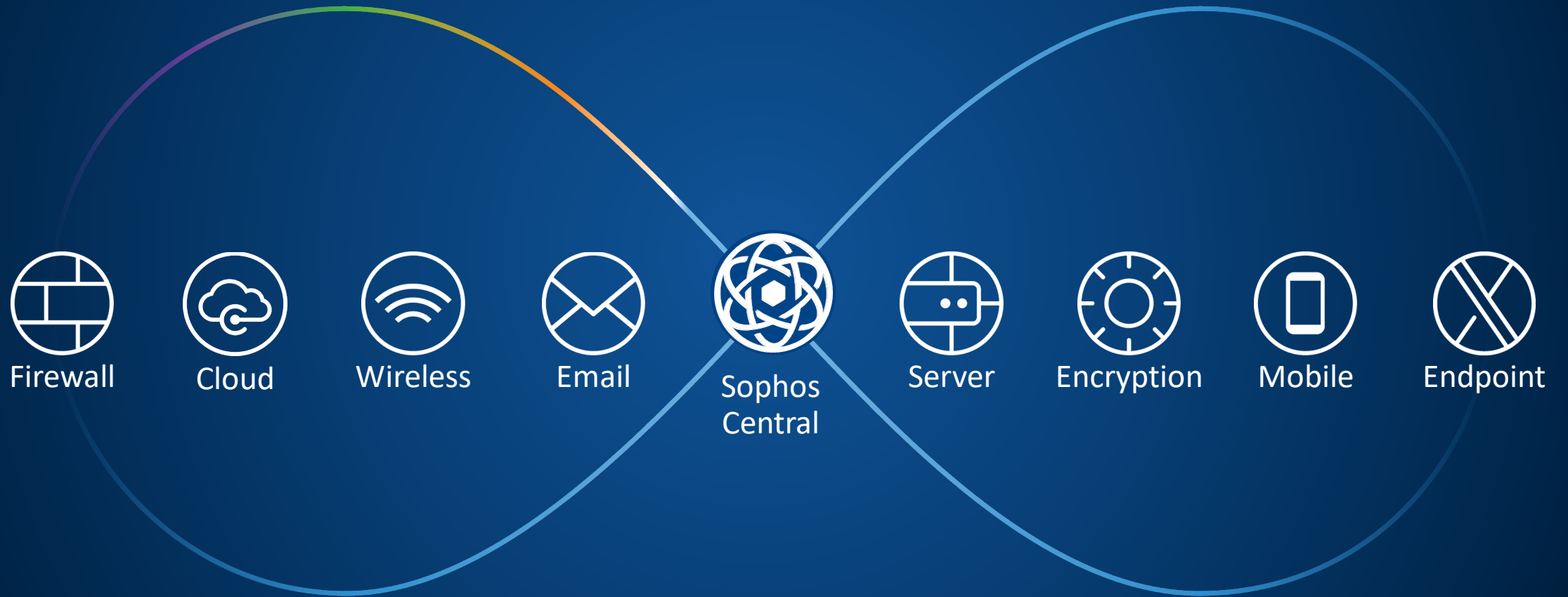
# Bezpieczny wrzesień z Sophos Central



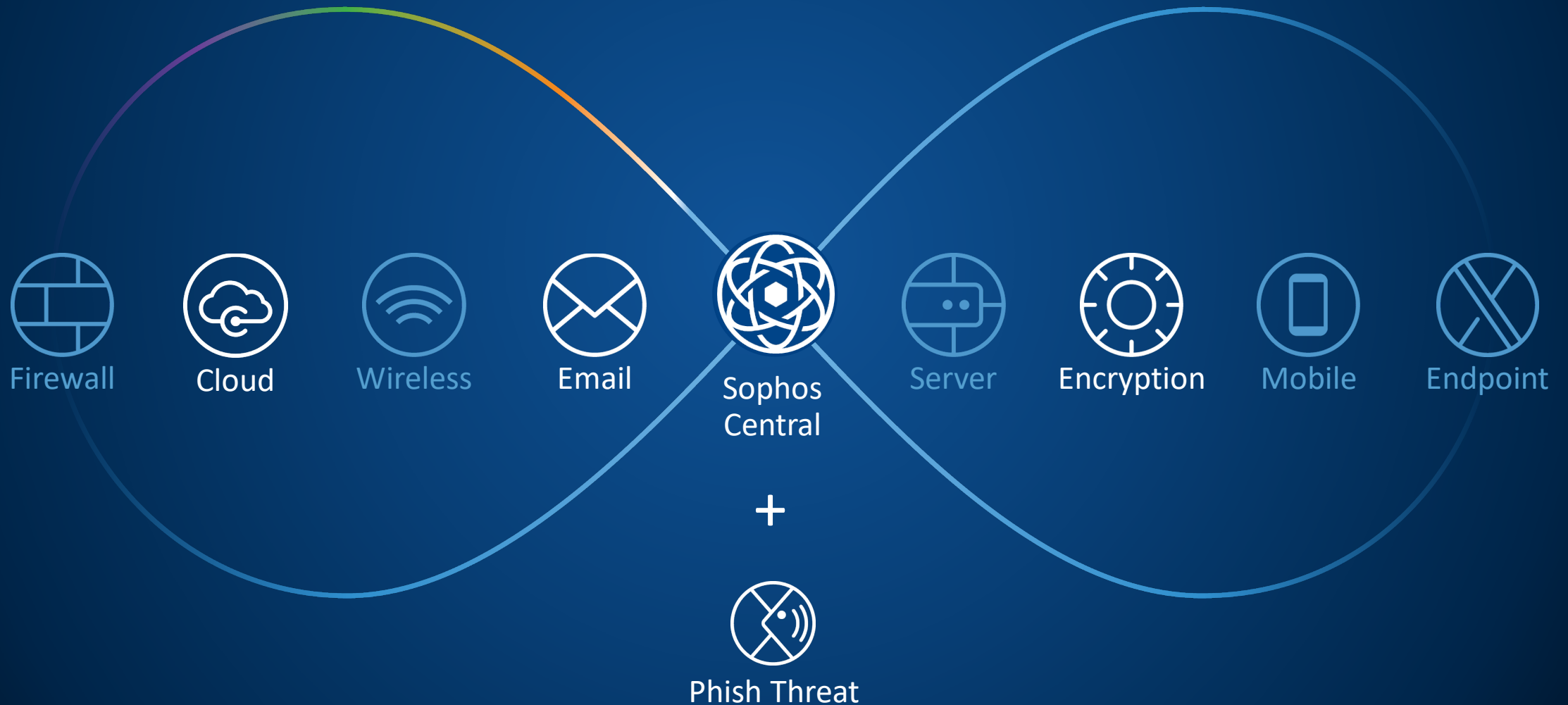
## Sesja 4

**Sophos Central funkcje: Szyfrowanie, Poczta, Chmura publiczna (Cloud Optix), oraz symulator ataków phishing (Phish threat)**

# Platforma Sophos Central



# Funkcje - Email/Cloud/Szyfrowanie



# Phish Threat



**DO NOT  
PUSH  
BUTTON**



# Ochrona przed zagrożeniami e-mail



## Ochrona na bramie

### Email & Web Protection

- Anti-Virus & Anti-SPAM
- Niebezpieczna zawartość+ typ pliku
- Filtrowanie URL
- Time-of-click URL protection

Central Email  
Email Gateway  
Web Gateway  
XG/UTM  
Sandstorm



## Ochrona w punkcie końcowym

### Endpoint protection

- Anti-Malware
- Anti-Exploit
- Anti-Ransomware
- Anti-Hacker

Intercept X  
Sophos Endpoint Protection  
Mobile Security

# Ochrona przed zagrożeniami e-mail



## Ochrona na bramie

### Email & Web Protection

- Anti-Virus & Anti-SPAM
- Filtrowanie URL
- Niebezpieczna zawartość+ typ pliku
- Time-of-click URL protection
- Sandboxing

Central Email  
Email Gateway  
Web Gateway  
XG/UTM  
Sandstorm



## Szkolenia użytkowników

### Symulacja ataku

- Szkolenie
- Weryfikacja
- Raport

Phish Threat



## Ochrona w punkcie końcowym

### Endpoint Protection

- Anti-Malware
- Anti-Exploit
- Anti-Ransomware
- Anti-Hacker

Intercept X  
Sophos Endpoint Protection  
Mobile Security



# Phish Threat przegląd kampanii



- Różne scenariusze, a także zwykłe kampanie szkoleniowe
- Obecnie obsługiwane 11 języków

Choose language

This will be the language of your email and training materials





English ▼

- Deutsch
- English
- Español
- Français
- 日本語
- 繁體中文
- Italiano
- 한국어
- Nederlands
- Português (Brasil)
- Português (Portugal)

Name your Campaign

Secure September

Choose Campaign Type

-  **Phishing**  
Lure targeted user to click on a link in an email.
-  **Credential Harvesting**  
Lure targeted user to enter credentials into a fake website. Note: no passwords are collected.
-  **Attachment**  
Lure targeted user to open an attachment within an email.
-  **Training**  
Enroll targeted user into mandatory training based on selected training modules.

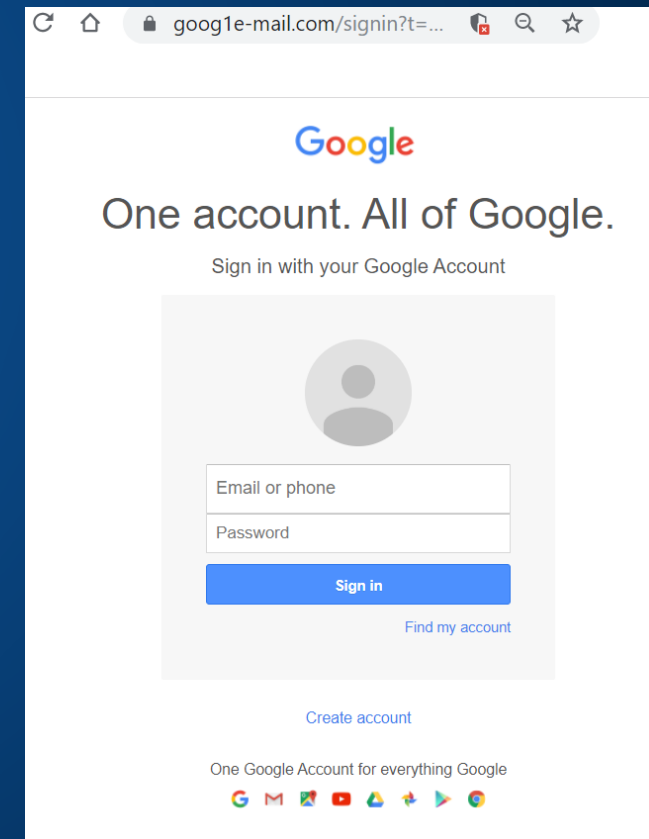
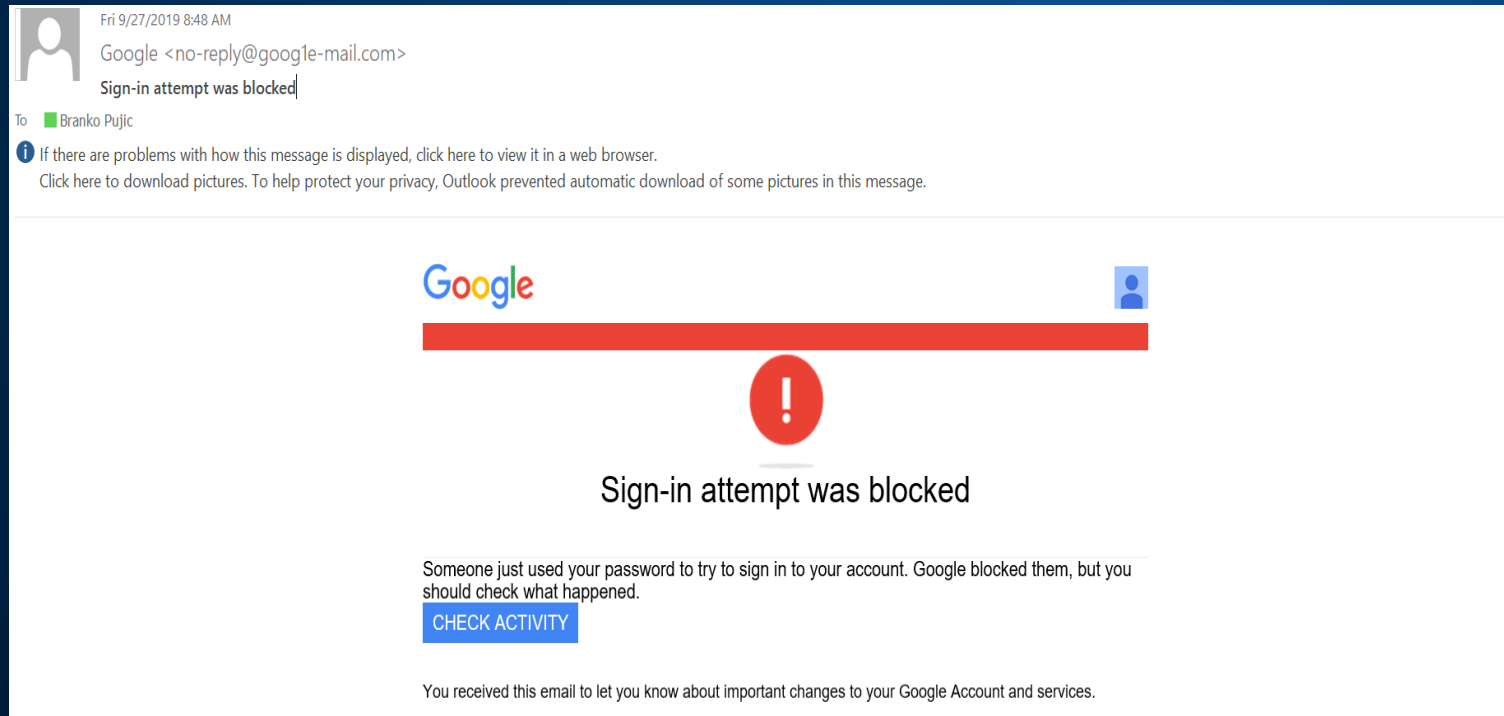


# Phish Threat – kampania: Access data theft



Pozwala na weryfikację:

- Czy użytkownik kliknie link
- czy wprowadzono dane dostępowe (WAŻNE: dane logowania nie są przechowywane!)





# Phish Threat szkolenie



## Phishing Interactive

### Phishing Interactive Quiz

Reset Quiz

**1** What is phishing?

- Attempt to acquire sensitive information by pretending to be someone else
- Fishing
- Software that automatically renders advertisements in order to generate revenue for its author
- A type of origami

**2** If you hover over a link and don't recognize the URL, should you click on it?

- Yes
- No

**3** What can you do to verify a link without clicking on it?

- Click the link
- Delete the email

Oh no!

.ru>  
omised

iled login attempts to your account. It may  
in to your **PayPal** account immediately to  
u to login soon or risk losing access to your  
our password now.

that...click the Continue arrow to find out why!

ing Module: **Phishing**

Completed: 14%



Continue

andatory  
ining

g, or through painful  
their tactics. Because of  
Phish Threat to provide  
J.

ollow the prompts below  
ganization from social  
ing!

# Phish Threat - konsola



**SOPHOS**  
CENTRAL  
Admin

**Phish Threat**

Back to Overview

ANALYZE

- Dashboard
- Reports

MANAGE

- People
- Campaigns

CONFIGURE

- Settings

## Phish Threat - Dashboard

Overview / Phish Threat Dashboard

Help - Administrator - Super Admin

2 of 3 Active campaigns [See all](#)

### February Campaign - All Employees

Starting: February 3, 2018  
Ending: March 21, 2018

- 0% 0 Emails sent
- 0% 0 Emails opened
- 0% 0 Users caught
- 0% 0 Finished training

### January Phishing Campaign

Started: January 31, 2018  
Ending: March 02, 2018

- 33% 13 Emails sent
- 77% 10 Emails opened
- 54% 7 Users caught
- 0% 0 Finished training

#### Click-to-Open Rate

35% ↑ 10% above global average

**High**  
risk level of attack

Past 60 days

#### Awareness factors

**64%** **Poor**  
Users tested  
Attacker's target everyone. You should too.  
[Create a campaign](#)

**2 d ago** **Excellent**  
Last campaign  
Frequent testing keeps security top of mind.  
[Create a campaign](#)

**21%** **Poor**  
Users caught  
You are only as strong as your weakest link.  
[View caught users](#)

**72%** **Poor**  
Passed training  
Training reinforces key security practices.  
[View incomplete trainings](#)

Past 60 days

#### Caught users

[See Report](#)

NAME	CAMPAIGNS RECEIVED	TIMES CAUGHT	LAST CAUGHT
Skye Rounds	4	3	Jan 31, 2018
Neddy Darrel	3	2	Jan 31, 2018
Nanete Kinge	2	1	Jan 31, 2018
Emily Aggett	2	1	Jan 31, 2018
Laocy Digan	2	1	Jan 31, 2018

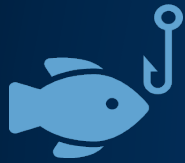
SOPHOS

# Synchronized Security

Sophos Phish Threat



# Łańcuch Cyber Ataku



Phishing



Zainfeowany URL



Command & Control



Kradzież haseł



Eskalacja uprawnień



Wykonanie złośliwego kodu



Poszukiwanie danych



Ransomware



Atak na serwer

Phishing Training

Email

Web

Firewall

Endpoint

Firewall

Endpoint

Server



# Synchronized Security: Phish Threat + Email/Endpoint

1

Kliknięty podejrzany link w wiadomości email

Naruszenie polityk na stacji końcowej

2

Email: Identyfikuje ryzykownych użytkowników

Endpoint: Identyfikuje ryzykownych użytkowników

3

Dodanie do platformy szkoleniowej PhishThreat



# Phish Threat wartości dodane



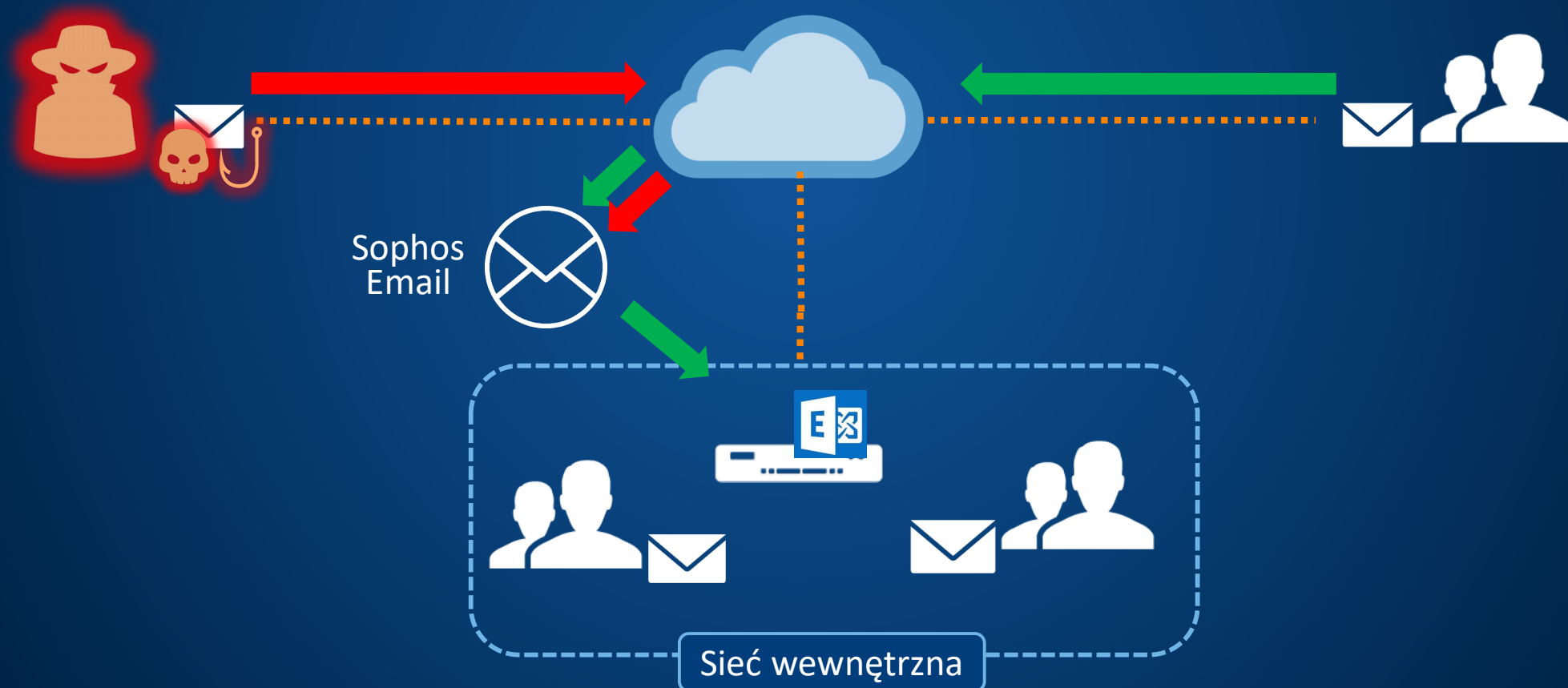
- Holistyczne bezpieczeństwo - uwzględnienie czynnika ludzkiego
- Zwiększa świadomość menedżerów budżetu na temat potrzeby bezpieczeństwa NextGen
- Nie wymaga instalacji, może być używany od razu po wyjęciu z pudełka
- Możliwa natychmiastowa realizacja testu, potrzebne są tylko adresy e-mail
- Test może również zrobić partner

# Central Email

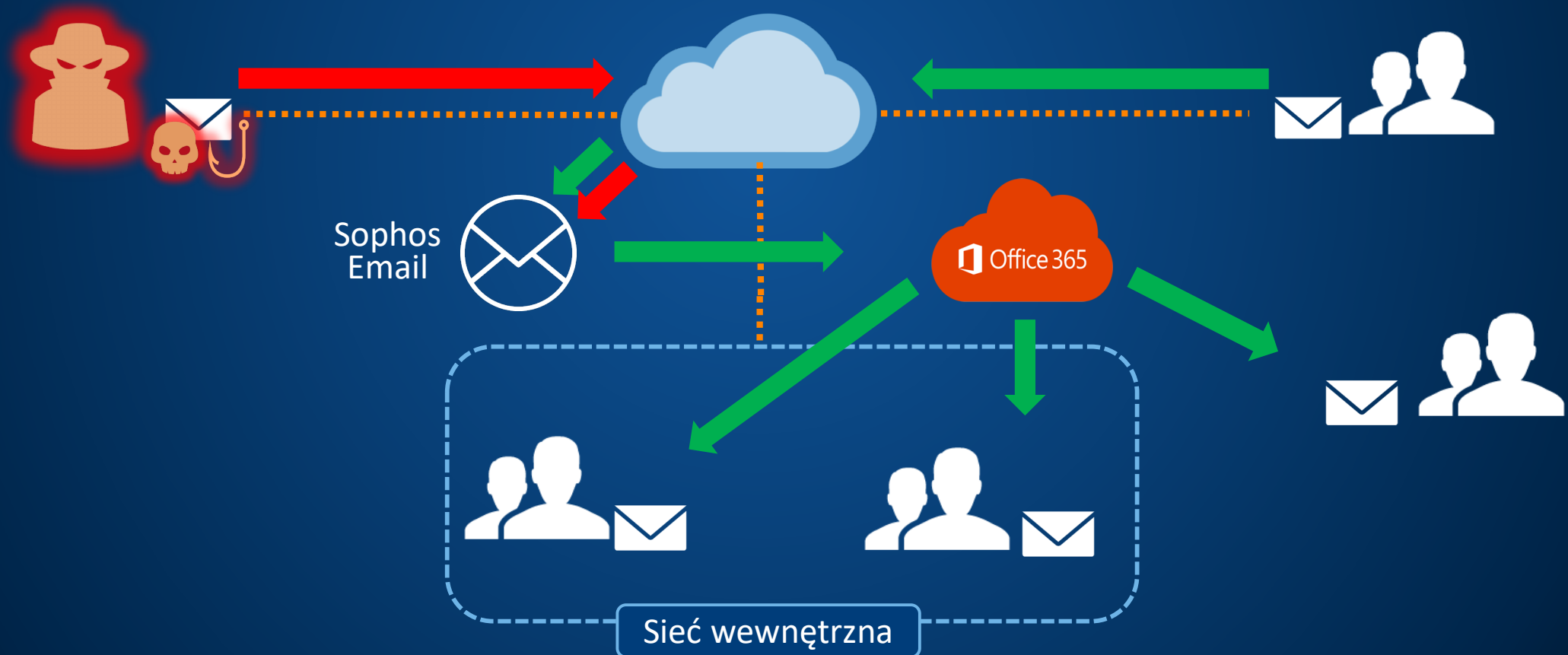
# Central Email - przegląd

- Oparte na chmurze rozwiązanie bramy e-mail
- Dodatkowa ochrona usług e-mail w chmurze (Office365 / Gmail) lub lokalnych serwerów poczty (Exchange / Notes)
- Administracja za pośrednictwem Sophos Central
- Inteligentniejsze zabezpieczenia poczty e-mail
- Sandboxing z głębokim uczeniem się
- Time of Click
- Ochrona przed oszustwami typu phishing
- SPF, DKIM, DMARC i analiza nagłówek
- Szyfrowanie PDF i DLP

# Email – środowisko pocztowe u klienta



# Email - Office 365





# Konsola

**SOPHOS**  
CENTRAL  
Admin

Email Gateway

Back to Overview

ANALYZE

- Dashboard
- Logs & Reports

MANAGE PROTECTION

- People
- Mailboxes

MANAGE MESSAGES

- Quarantined Messages

CONFIGURE

- Policies
- Settings

SOPHOS CENTRAL

- Free Trials

## Email Gateway - Dashboard

Overview / Email Gateway Dashboard

Help Richard Beckett  
Sophos Ltd · Super Admin

### Inbound Activity Summary

See Report

You've been protected from  
**34**  
potential threats

7 Mailboxes scanned

680 Emails scanned

- 29 Spam
- 3 DLP policy violations
- 2 Advanced Threat
- 0 Virus
- 0 Authentication failures
- 0 Realtime blocklist
- 0 Company blocklist

last 30 days

### Outbound Activity Summary

See Report

12 Emails Scanned  
7 Mailboxes Scanned

- 0 Spam
- 0 DLP policy violations
- 0 Advanced Threat
- 0 Virus

last 30 days

### Sandstorm Activity Summary

See Report

2 Emails Checked by Sandstorm

- 0 Legitimate
- 2 Advanced Threat

last 30 days

### At Risk Users

See Report

Top users	# Risky sites clicked
	4

https://central.sophos.com/manage/xgemail/central/products

# Time-of-Click

Enhanced Email Malware Scan

- Enhanced content and file property scan** - Most extensive email scan based on a combination of content and email characteristics. This setting applies to both inbound and outbound email.
- Un-scanned emails** - Manage settings for inbound emails that were not scanned because we could not access or process its contents. ⓘ
- Time of Click URL Protection** - URLs within inbound emails are redirected through Sophos and scanned at the time of click, protecting users from malicious URLs.  
Configure actions for URLs based on their level of risk. You can block users from accessing sites, warn the user and allow them to proceed, or allow the user to access the site without any restrictions.

URL REPUTATION	ACTION
High risk	Block ▼
Medium risk	Block ▼
Unverified	Warn ▼

URL re-writes

- Re-write URLs in plain text messages. ⓘ
- Re-write URLs within securely signed messages. ⓘ



Link zostanie sprawdzony w momencie kliknięcia



Sophos Email

Link początkowy jest zastąpiony przez urządzenie

# Self Service

The screenshot displays the Sophos Self Service Portal interface. On the left is a dark navigation sidebar with the Sophos logo and menu items: Email, Emergency Inbox, Device Encryption, and Mobile. The main content area is divided into several sections:

- Email Security:** A header section with the title "Email Security" and subtitle "Manage quarantined messages and email security settings". It includes a user profile for William White (Marcel Strunk EDB Account) and a "Help" dropdown.
- Allow/Block:** A sub-section with the title "Allow/Block" and subtitle "Email / Allow/Block".
- Emergency Inbox:** A section titled "Emergency Inbox" with the subtitle "View and manage your email from the last 14 days". It features a search bar and a table of email entries.
- Quarantined:** A section titled "Quarantined" with the subtitle "Email / Quarantined". It contains a table of quarantined messages.

**Emergency Inbox Table:**

FROM	SUBJECT	RECEIVED	SIZE
Golem.de Redaktion <news@golem.de>	Golem.de: Kunststoff wird halber Naturstoff - Die B...	Aug 13, 2019 12:08 PM	129.8 kB
Hilfeschreiber <mailto:help@sofistik.de>	Die Lichter des Autos sind an	Aug 13, 2019 11:02 AM	2.9 kB
Sophos <mailto:training@sophos.com>	Pflichttraining zum Thema Sicherheitsbewusstse...	Aug 13, 2019 10:58 AM	23.9 kB

**Quarantined Table:**

FROM	TO	SUBJECT	RECEIVED	REASON
Luca Christmann <luca.christmann@sophos.de>	william@...seng.de	Encrypted	Aug 12, 2019 10:03 AM	Unscannable content
Luca Christmann <luca.christmann@sophos.de>	william@...seng.de	Rechnung	Aug 12, 2019 9:26 AM	Spam
Sophos <mailto:training@sophos.com>	william@...g.de	Pflichttraining zum Thema Sicherheitsbewusstsein n...	Aug 10, 2019 10:39 AM	Bulk
Sophos <mailto:training@sophos.com>	william@...g.de	Pflichttraining zum Thema Sicherheitsbewusstsein n...	Aug 10, 2019 9:24 AM	Bulk

# Szyfrowanie SPX



"acad acad" <bianca@acad.saleseng.de> has sent you an encrypted email. To view it, you need to set a Sophos Secure Message password. You'll then need to enter this password to view any email sent from the EU Central region.

You have 30 day(s) left to view this message before it expires.

- Subject : secure: Rechnung
- Sent : July 11, 2019 8:20:42 AM, GMT
- Importance: Normal
- Expires : August 10, 2019 8:20:51 AM, GMT

[ENCRYPTED] message.pdf  
77 KB

Set

Enter a password

OK Abbrechen

**From:** acad acad <bianca@acad.saleseng.de>  
**Sent:** Thursday, 11 July 2019 08:20:42 GMT  
**To:** Luca Christmann <Luca.Christmann@Sophos.de>  
**Subject:** secure: Rechnung

[Reply](#)

Die Rechnung!

# Email i integracja Phish Threat

1

## **Podważony link został kliknięty**

Użytkownik Sophos Email klika łącze e-mail sklasyfikowane jako ryzyko dla organizacji

2

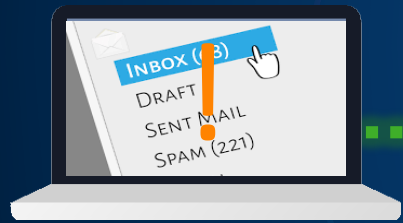
## **Identyfikuje ryzykownych użytkowników**

Natychmiast przeglądaj użytkowników wysokiego ryzyka w raporcie Sophos Email „At Risk Users”

3

## **Dodanie do platformy szkoleniowej PhishThreat**

Zarejestruj użytkowników Sophos e-mail wysokiego ryzyka bezpośrednio w symulacjach phishing Threat i szkoleniach uświadamiających za pomocą jednego kliknięcia.



**Security Heartbeat™**





# Email i integracja z Endpoint

1

## Wykrycie skompromitowanego konta email

Sophos Email wykrywa zainfekowaną skrzynkę pocztową wysyłającą spam wychodzący lub wiadomości phishingowe

2

## Izolacja skrzynki

Sophos Email izoluje skrzynkę pocztową, ostrzega Centralnego Administratora i dzieli się informacjami z Punktem końcowym. Zapobieganie rozprzestrzenianiu się ataku poprzez usunięcie uprawnień nadawcy

3

## Endpoint: Skanowanie urządzenia

Sophos Endpoint identyfikuje i skanuje wszystkie znane urządzenia powiązane ze skrzynką pocztową

Security Heartbeat™

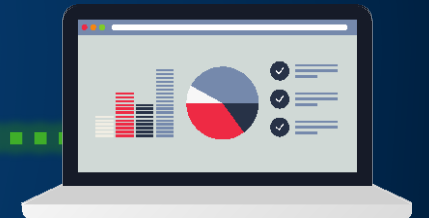
5

## Przywrócenie dostępu do skrzynki

4

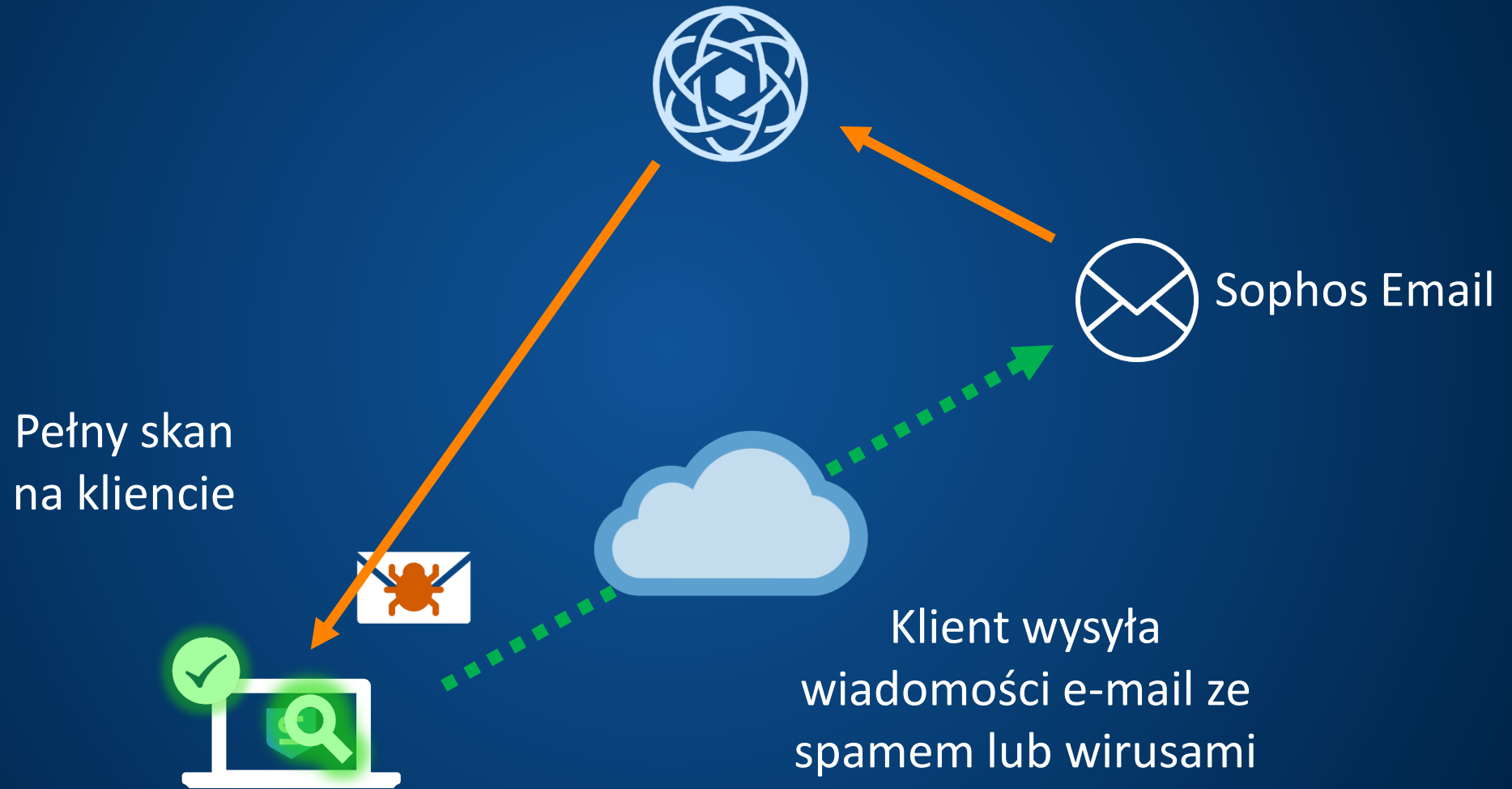
## Endpoint: Clean-up

Sophos Endpoint automatycznie usuwa wszelkie infekcje

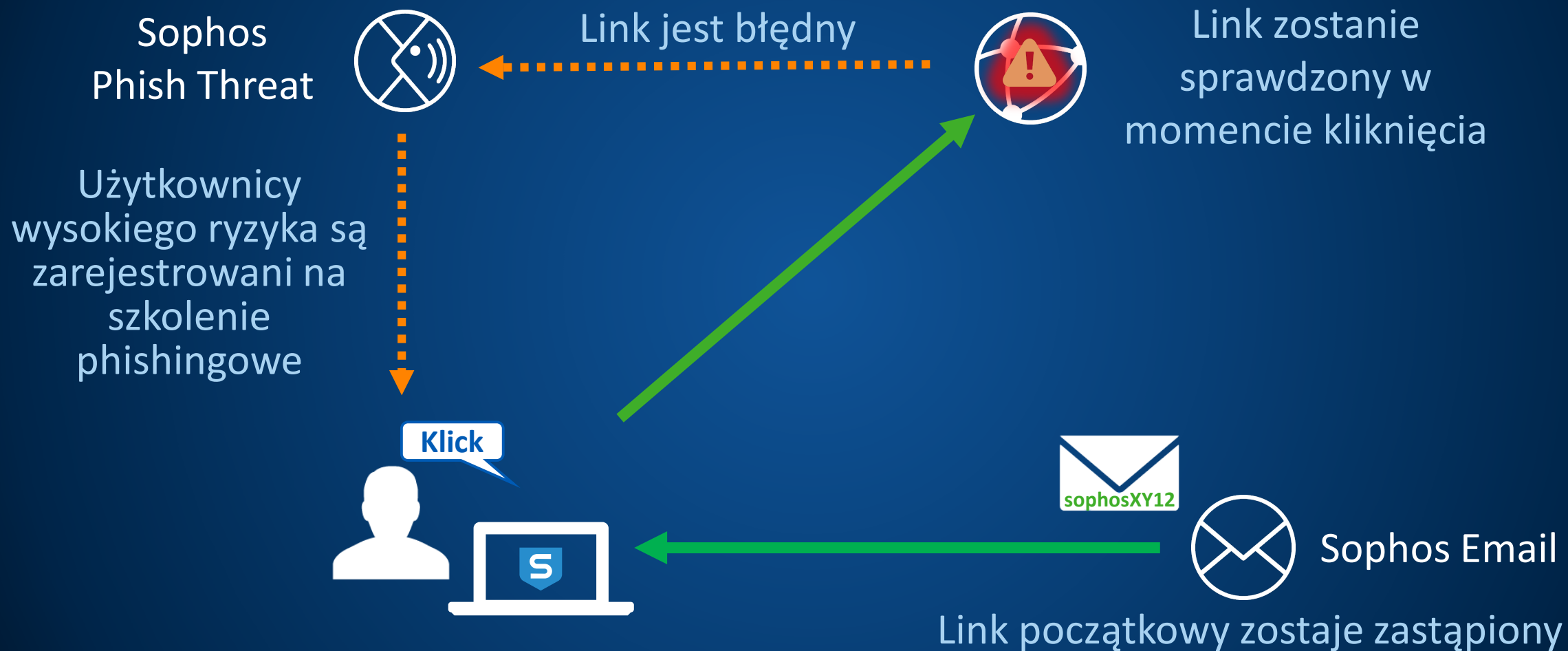




# Synchronized Security z Sophos Email i ochronie Endpoint



# Synchronized Security z Sophos Email Advanced i PhishThreat



# Licencja (per user)

Ochrona i administracja	Email Standard	Email Advanced
Exchange 2003+, Office365, Google App	✓	✓
Filtrowanie spamu	✓	✓
User / Admin "Allow" / "Block"	✓	✓
Portal Self-service z dostępem do kwarantanny	✓	✓
Spooling / Emergency Inbox ()	✓	✓
Ochrona phishing	✓	✓
SPF/DKIM/DMARC - Anti-Spoofing	✓	✓
Time-of-Click URL Protection		✓
Sophos Sandstorm		✓
Szyfrowanie		✓
Obsługa załączników		✓
Inteligentne banery		✓

# Central Email – wartości dodane

- Nie jest wymagana własna infrastruktura
- Przygotowano integrację ze systemami poczty elektronicznej, w tym. Office365, Gsuite, MS Exchange
- Ochrona NextGen dzięki Sandboxing i time-of-Click
- Szyfrowanie PDF i DLP
- Portal Self-Service dla użytkowników końcowych do administrowania kwarantanną i czarną listą / białą listą
- Awaryjna skrzynka odbiorcza w przypadku awarii / niedostępności serwera pocztowego
- Zsynchronizowane zabezpieczenia z platformą Sophos Phish i ochroną Endpoint

# Central Device Encryption

# Central Device Encryption - przegląd

- Szyfrowanie dysku twardego dla klientów Windows 7+ i Mac 10.12+
- Chroni twoje dane w przypadku utraty i kradzieży
- Zarządzanie szyfrowaniem dysków twardych funkcją BitLocker i FileVault
- Weryfikowalność szyfrowania
- Przyjazne dla użytkownika odzyskiwanie hasła
- Ochrona przed deszyfrowaniem
- Łatwe wdrożenie



# Central Device Encryption - Dashboard

**SOPHOS**  
CENTRAL  
Admin

Encryption

[Back to Overview](#)

ANALYZE

Dashboard

Logs & Reports

MANAGE PROTECTION

People

Computers

CONFIGURE

Policies

Settings

Protect Devices

MORE PRODUCTS

New: Sophos Cloud Optix

Free Trials

## Encryption - Dashboard

Overview / Encryption Dashboard

Help ▾ Branko Pujic ▾  
Sophos Inc -Standard · Super Admin

### What do you need to do?

- Set up Device Encryption
- Get a recovery key
- Create a new encryption policy
- See which computers are encrypted
- See which computers could be encrypted
- See all computers

### Encryption status

5 Computers that could be encrypted	1 Encrypted computers	6 Total computers
--	--------------------------	----------------------

### Licensing

View Details

#### Device Encryption licenses

100

- 1 Used licenses
- 99 Unused licenses

[Buy More](#)

# Device Encryption dodanie/usunięcie urządzenia

The screenshot displays the Sophos Central Admin interface for managing endpoint software. A modal window titled "Manage Endpoint Software" is open, showing two columns: "Eligible Computers" and "Assigned Computers".

In the background, the "Manage Endpoint Software" button is highlighted with a red box. The "Device Encryption" option in the left sidebar is also highlighted with a red box. A red arrow points from the "Device Encryption" option to the "Eligible Computers" list. A red box highlights the right arrow button between the "Eligible Computers" and "Assigned Computers" lists.

The "Manage Endpoint Software" dialog box contains the following information:

- SOFTWARE LIST:** Endpoint Protection, Sophos Intercept X, **Device Encryption** (highlighted).
- Eligible Computers:** 3 computers listed: Eligible Computers, E 19PC, M 19-PC, and User-PC.
- Assigned Computers:** 3 computers listed: Assigned Computers, TLN-1601-BPU, and User-PC.

Buttons at the bottom of the dialog include "Cancel" and "Save".

# Konfiguracja polityk

POLICY NAME Base Policy - Device Encryption

POLICY TYPE Device Encryption

USERS/COMPUTERS | GROUPS

Device Encryption is on  
All endpoints within this policy are encrypted

Encrypt boot volume only ⓘ

Advanced Windows settings

Require startup authentication

Require new authentication password/PIN from users

months

Encrypt used space only

## Outlook: Central Device Encryption v2

Device Encryption is on  
All endpoints within this policy are encrypted

Encrypt boot volume only ⓘ

Advanced Windows settings

Require startup authentication

Require new authentication password/PIN from users

months

Encrypt used space only

Password protect files for secure sharing (Windows only)

Enable right-click context menu ⓘ

Enable Outlook add-in

Always ask how to proceed with attached files ⓘ

Excluded domains

Domains for which 'Always ask' should NOT apply. Please insert your domains separated by a comma

# Password Recovery: Self-Service

## BitLocker

Falsches Kennwort. Geben Sie das Kennwort erneut ein.

.....

Drücken Sie ESC, um die BitLocker-Wiederherstellung auszuführen

## BitLocker-Wiederherstellung

Geben Sie den Wiederherstellungsschlüssel für dieses Laufwerk ein.

223289-397188-489434-685322-702075-438350-253693-235136

Kennen Sie den Recovery Key nicht? Wenden Sie sich an Ihren IT-Helpdesk oder besuchen Sie Ihr Self-Service-Portal: <https://sophos.com/ssp>

**SOPHOS**  
SELF-SERVICE-PORTAL

- E-Mail
- Notfall-Posteingang
- Geräteverschlüsselung**
- Mobile Control

## Geräteverschlüsselung

Wiederherstellungsschlüssel auf verschlüsselten Geräten abrufen

GERÄTENAME/BETRIEBSSYSTEM	ZULETZT VERWENDET	WIEDERHERSTELLUNGSSCHLÜSSEL
✓ iMac macOS Sierra (10.12)	vor einem Tag	<a href="#">Abrufen</a>
✓ W10Cloud Windows 10 (32 Bit)	vor 4 Tagen	<a href="#">Abrufen</a>

### Wiederherstellungsschlüssel abrufen

COMPUTERNAME  
W10Cloud

WIEDERHERSTELLUNGSSCHLÜSSEL-ID  
f2384763-5a66-4c90-8748-c3c4b574ee15

**WIEDERHERSTELLUNGSSCHLÜSSEL**  
223289-397188-489434-685322-702075-438350-253693-235136

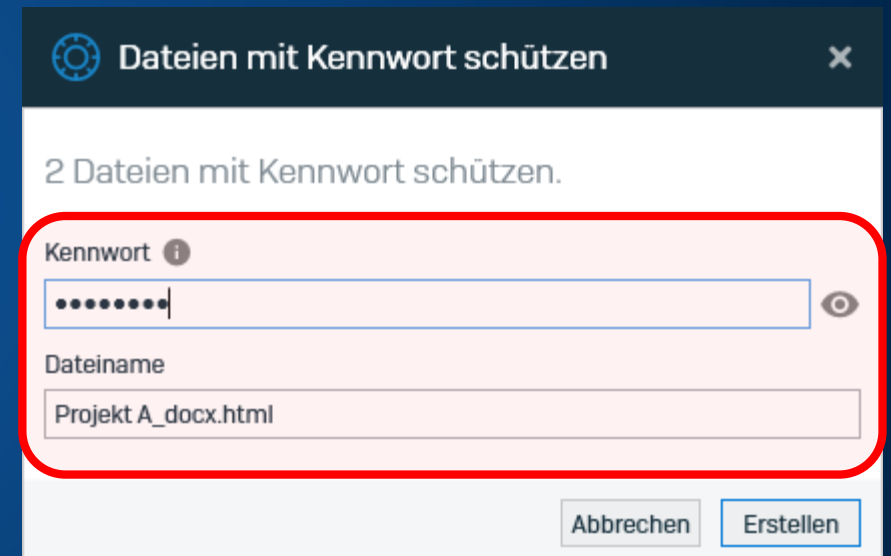
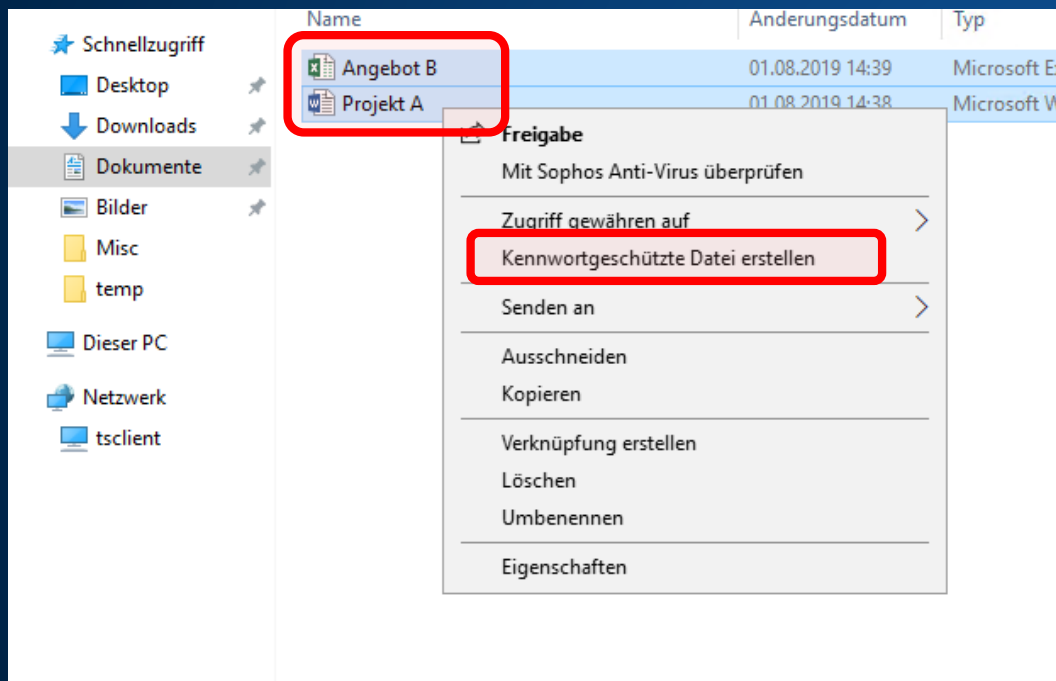
Hinweis: Der bereitgestellte Wiederherstellungsschlüssel bezieht sich auf das Boot-Laufwerk Ihres Geräts. Wenn Sie nach Anwendung des Wiederherstellungsschlüssels weiterhin nicht auf Ihre Datenlaufwerke zugreifen können, wenden Sie sich an Ihren Administrator.

Schließen

# Outlook: Central Device Encryption v2

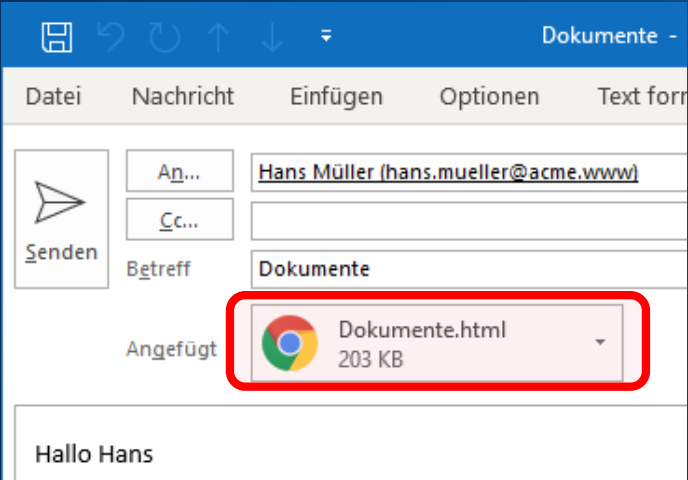
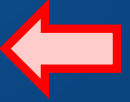
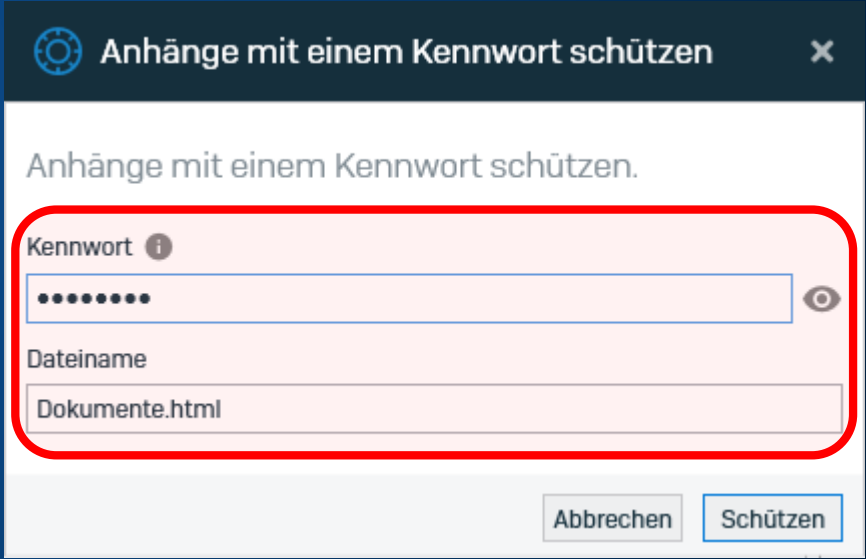
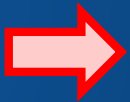
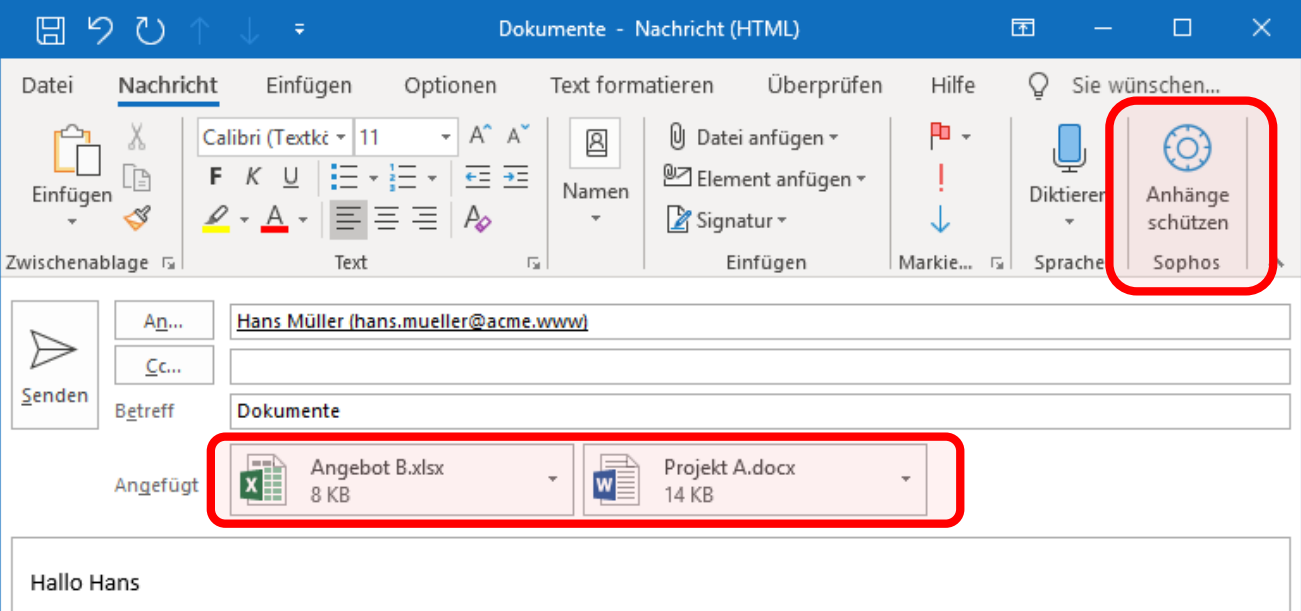
## Pliki chronione hasłem

# Pliki chronione hasłem





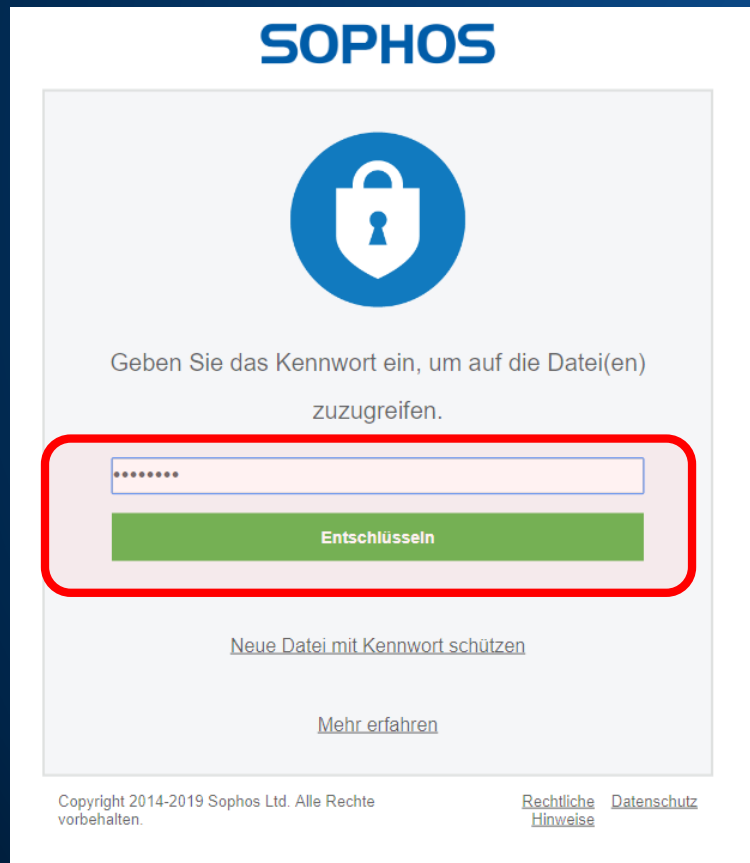
# Outlook Plugin: Szyfrowanie w razie potrzeby lub według zasad



# Pliki chronione hasłem

## Opis

- Wsparcie dla: Google Chrome, Microsoft Edge, Mozilla Firefox, Internet Explorer 11
- Na iOS lub Android: Sophos Secure Workspace



# Endpoint I integracja z szyfrowaniem

1

## Wykrycie zagrożenia

Sophos Endpoint wykrywa malware

2

## Komunikacja systemów

Sophos Endpoint przy pomocy Security Heartbeat™ współdzieli informacje z SafeGuard Enterprise

3

## Odwołanie kluczy szyfrujących

SafeGuard Encryption odwołuje klucze szyfrujące

Security Heartbeat™

5

## Przywrócenie kluczy szyfrujących

SafeGuard Enterprise przywraca klucze szyfrowania, a dostęp do danych wraca do normy.

4

## Clean-up

Sophos Endpoint automatycznie usuwa infekcję.



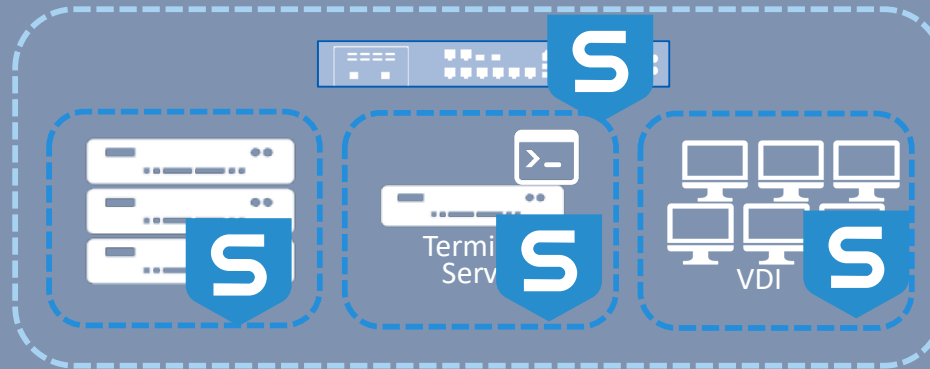
# Cloud

**SOPHOS**

# Gdzie Sophos chroni w chmurze



Platform as a Service



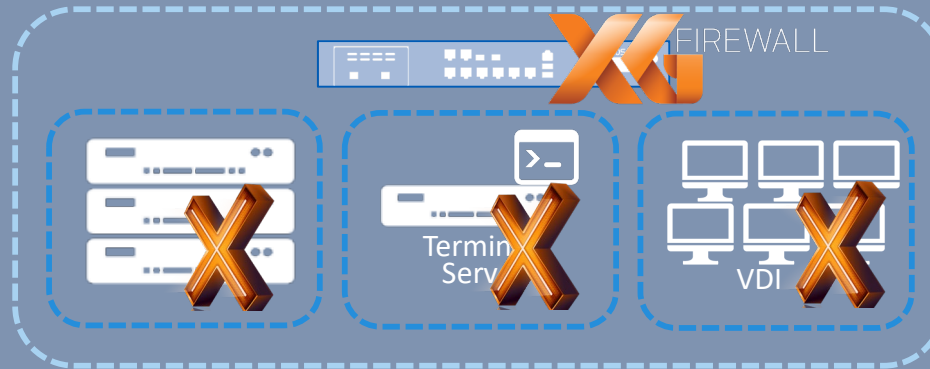
Infrastructure as a Service



# Gdzie Sophos chroni w chmurze



Platform as a Service



Infrastructure as a Service





# Sophos Cloud rozwiązania



- ✓ Sophos Cloud Optix
- ✓ Intercept X (for Server)
- ✓ UTM



Google Cloud

- ✓ Sophos Cloud Optix
- ✓ Intercept X (for Server)



Azure

- ✓ Sophos Cloud Optix
- ✓ Intercept X (for Server)
- ✓ XG Firewall



# Naruszenie bezpieczeństwa w chmurze publicznej

*Do 2023 r. co najmniej 99% awarii zabezpieczeń w chmurze będzie spowodowanych błędem konfiguracyjnym klienta*



**Do 2024 r. organizacje wdrażające ofertę CSPM ograniczą związane z chmurą incydenty związane z błędną konfiguracją o 80%**



Google Cloud



## Widoczność



Z jakich zasobów chmury korzystam obecnie?

Jakie zmiany zachodzą teraz i czy tego właśnie chcesz?

## Wymagania



Czy moje środowiska są zgodne z RODO, ISO?

Czy uwierzytelnianie i logowanie są poprawnie skonfigurowane?

## Reakcja



Czy współczesne ataki AI można wykryć i zatrzymać?

Czy błędne konfiguracje można korygować automatycznie?

# Intuicyjna konsola

The screenshot displays the Sophos Cloud Optim dashboard. At the top, there's a search bar and navigation options. The main content is divided into several sections:

- Alert summary:** Shows counts for Critical Alerts (1), High Alerts (3), Medium Alerts (12), and Low Alerts (31).
- What do you need to do?:** A list of actionable items like 'See current critical security alerts' and 'Review your network topology'.
- Changes in your environments:** A bar chart and table showing network changes. The bar chart shows 8 new network items. The table lists API events for 'OptixDemo-AWS'.
- Compliance:** A donut chart showing 79 passes and 47 fails.
- Top alerts:** A list of specific alerts, such as 'Ensure multi-factor authentication (MFA) is enabled'.

Account	API	Event Time
OptixDemo-AWS	RevokeSecurityGroupIngress	2019-03-29 14:13:02
OptixDemo-AWS	RevokeSecurityGroupIngress	2019-03-29 14:16:48
OptixDemo-AWS	RevokeSecurityGroupIngress	2019-03-29 14:10:42
OptixDemo-AWS	RevokeSecurityGroupIngress	2019-03-29 14:13:42
OptixDemo-AWS	AuthorizeSecurityGroupIngress	2019-03-29 14:16:48

- Przegląd alarmów
- Status zgodności
- Raporty zgodności
- Inwentaryzacja
- Topologia sieci
- Prezentacja zmian

# Monitoring zgodności / wymagań

- Szybki przegląd zgodności i stanu bezpieczeństwa
- Zmniejsza koszty i złożoność zarządzania, analizy ryzyka i zgodności
- Konfigurowalne szablony zgodności
  - RODO
  - PCI DSS
  - SOC2
  - CIS benchmarks
  - HIPAA
  - ...

The screenshot displays the Sophos Compliance dashboard. At the top, it shows the 'Compliance' header with a search bar and navigation options. Below this, a 'Report Summary' section features six circular gauges representing different failure categories: Total Fails (90), Critical Fails (3), High Fails (26), Medium Fails (17), Low Fails (44), and Passed (197). A 'Select Provider' dropdown is set to 'All'. Below the gauges, there are progress bars for 'AWS - CIS Benchmark v1.1' and 'AWS - EBU R 143'. A modal window is open, showing a table of failed rules under the 'Identity and Access Management' category, with 12 out of 18 rules failed.

Result	#	Rule Summary	Rule #	Affected Resources
Failed	1.2	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have console access	AR-103	DemotestIAMUserNoMFA <a href="#">more details...</a>
Failed	1.3	Ensure credentials unused for 90 days or greater are disabled	AR-503	Password last used by DemotestIAMUserNoMFA on: Never. <a href="#">more details...</a>
Failed	1.5	Ensure IAM password policy requires at least one uppercase letter	AR-505	'At least one Uppercase Letter' policy not set <a href="#">more details...</a>
Failed	1.6	Ensure IAM password policy require at least one lowercase letter	AR-506	'At least One Lowercase Letter' policy not set <a href="#">more details...</a>
Failed	1.7	Ensure IAM password policy require at least one symbol	AR-507	'At least One Symbol' policy not set <a href="#">more details...</a>



# Ostrzeżenia i reakcje ze wsparciem AI

**Alerts**  
Smart alerts for security and compliance

Search: To search select Alerts, Hosts, Security Groups ...

Environments: [dropdown]

Help | Sophos Cloud Optix Demo | Demo

Filter by: 1 Day | **1 Week** | 1 Month | All

**Alert Summary**

- Critical Alerts: 1
- High Alerts: 3
- Medium Alerts: 12
- Low Alerts: 31

Show Suppressed Alerts: OFF ON

Reset | Export as [icon]

Alert ID	Severity	Description	Type	Affected Resources	Last Seen	Provider	Enviro
A-000092	Critical	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have console access	[icon]	• DemotestIAMUserNoMFA <a href="#">more details...</a>	a day ago	AWS	OptixDe
A-000071	High	Enable MFA delete for cloudtrail bucket deletion	[icon]	• avid-cloudtrail-760068489120 <a href="#">more details...</a>	a day ago	AWS	OptixDe
A-000059	High	Ensure a log metric filter and alarm exist for CloudTrail configuration changes	[icon]	• No Metric filters were found for CloudTrail. <a href="#">more details...</a>	a day ago	AWS	OptixDe
A-000055	High	Ensure a log metric filter and alarm exist	[icon]	• No Metric filters were found for CloudTrail.	a day ago	AWS	OptixDe

- Podejrzany ruch
- Przegląd infrastruktury jako szablonów kodu
- Identyfikuje wiele kluczy dostępu
- Zamyka otwarte porty
- Odkrywa odchylenie od normalnej konfiguracji
- Ustaw profilaktycznych „strażników”



# Detekcja anomalii

- Cloud Optix stale uczy się i monitoruje zasoby w chmurze (segmenty S3, grupy zabezpieczeń, klucze dostępu użytkowników), konfiguracje, dzienniki grup zabezpieczeń i ruch sieciowy.
- Inteligentne alerty wspierane przez AI skracają czas reakcji i umożliwiają szybsze rozwiązywanie zagrożeń bezpieczeństwa.
- Wykrywanie anomalii
  - Logowanie użytkowników
  - Anomalie ruchu sieciowego

The screenshot displays a security alert interface. At the top, a red 'Critical' badge is visible. The alert title is 'Multiple logins from two different regions in short time', accompanied by a brain icon. Below the title, the alert details are shown:

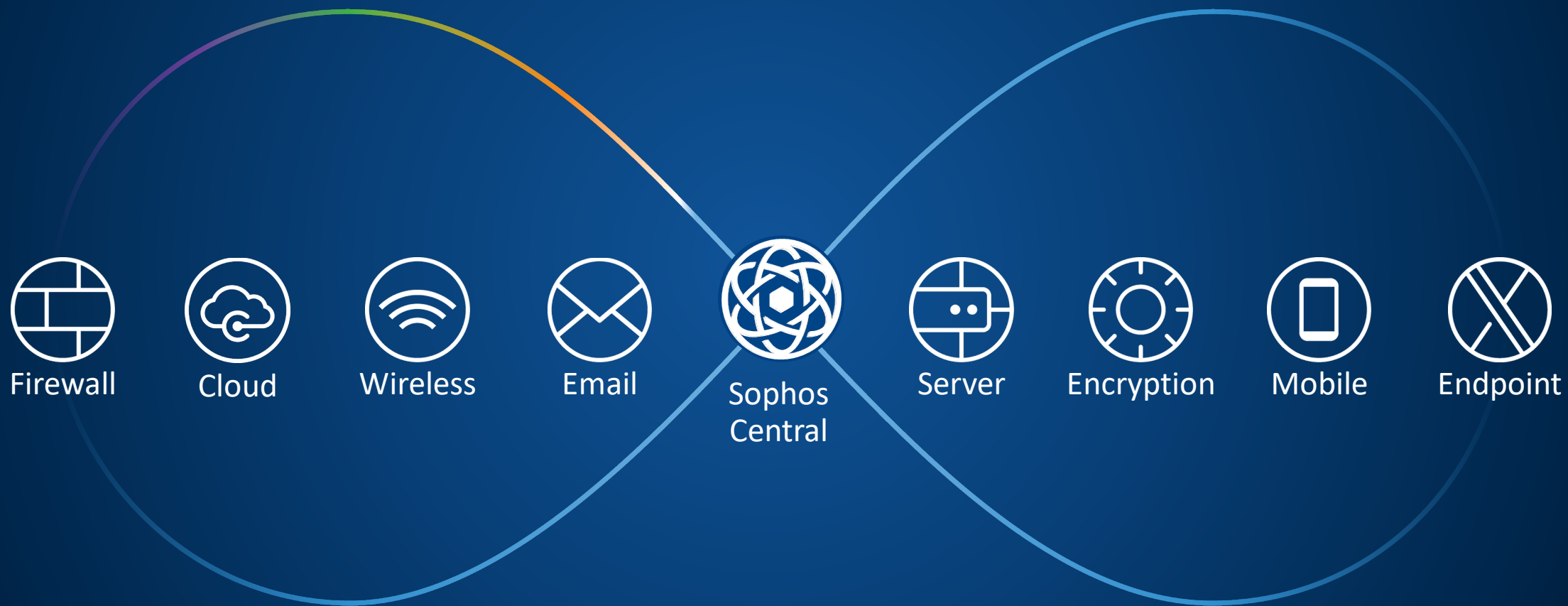
- Summary:** Multiple logins from two different regions in short time
- Alert Id:** A-003286
- Environment:** Acme-QA (AWS)
- Last Seen:** 2018-08-07 18:04:27 (7 months ago)

The 'Affected Resources' section contains a table with the following details:

Resource
Multiple logins from two different regions in a short time
Account Id : 196338510291
User Name : deepak
Login Type : Console
Login IP : 52.89.147.48
Previous Login IP : 14.141.93.130
Login Location : Oregon-United States (ISP :

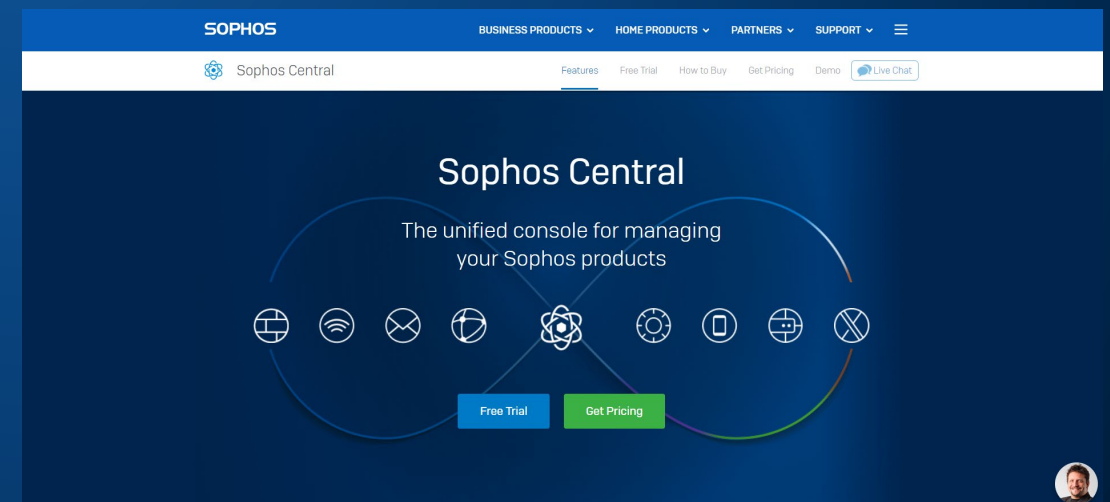
A 'Close' button is located at the bottom right of the alert details panel.

# 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.