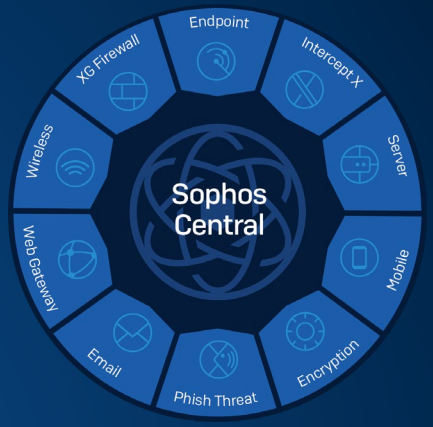
Bezpieczny wrzesień
z Sophos Central

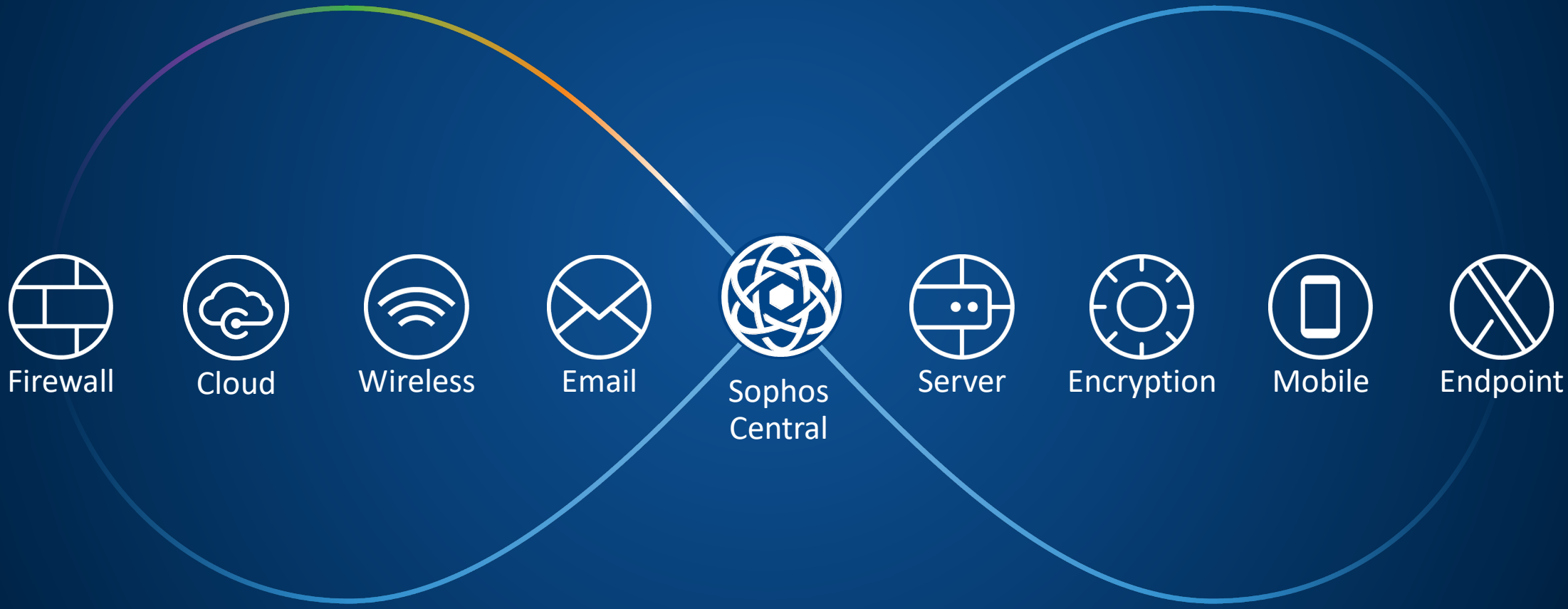


Sesja 4

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

SOPHOS

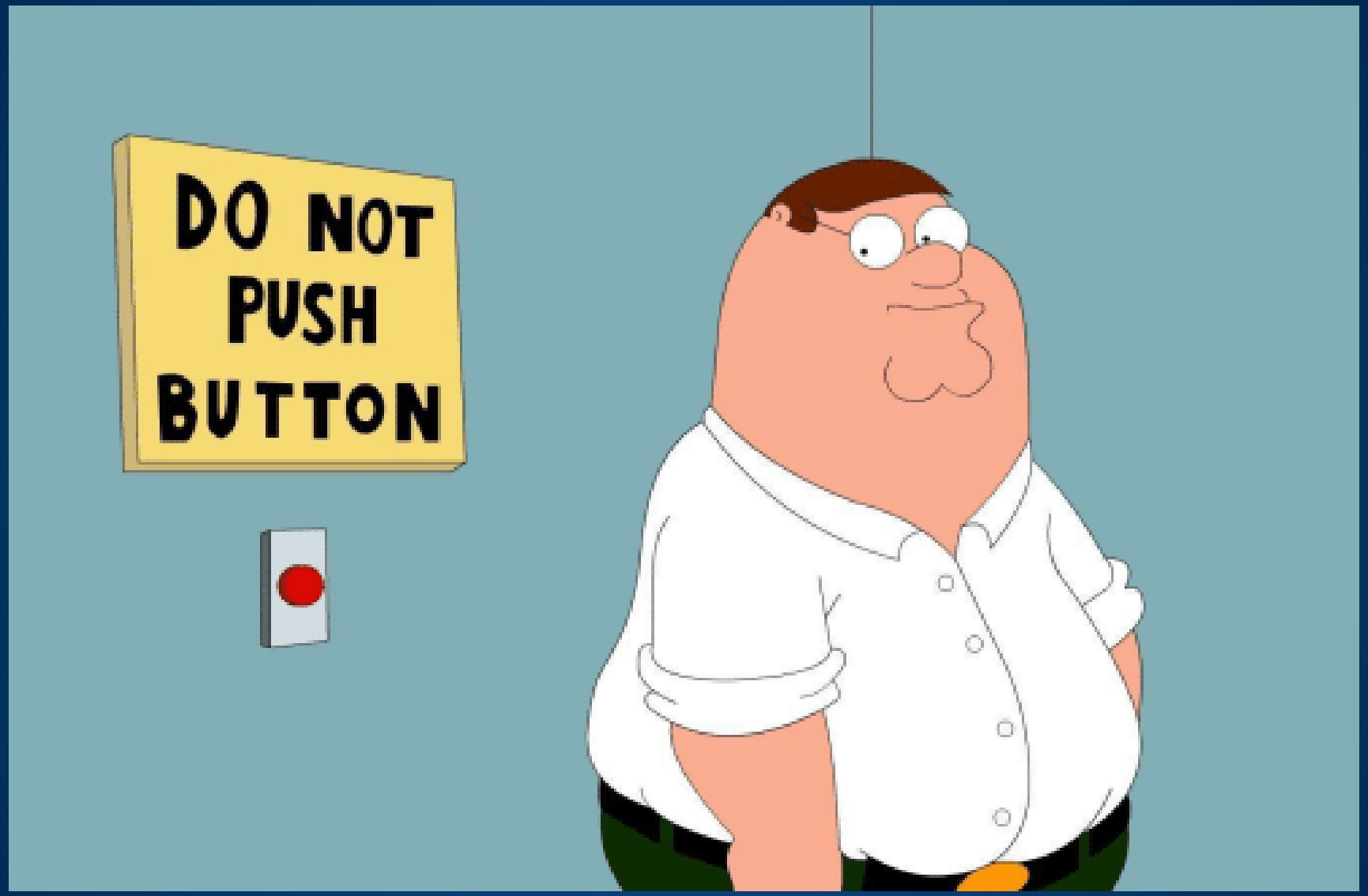
Platforma Sophos Central



Funkcje - Email/Cloud/Szyfrowanie

Phish Threat

SOPHOS


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

Szkolenia użytkowników

Ochrona w punkcie końcowym

Email & Web Protection

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

Central Email
Email Gateway
Web Gateway
XG/UTM
Sandstorm

Symulacja ataku

- Szkolenie
- Weryfikacja
- Raport

Phish Threat

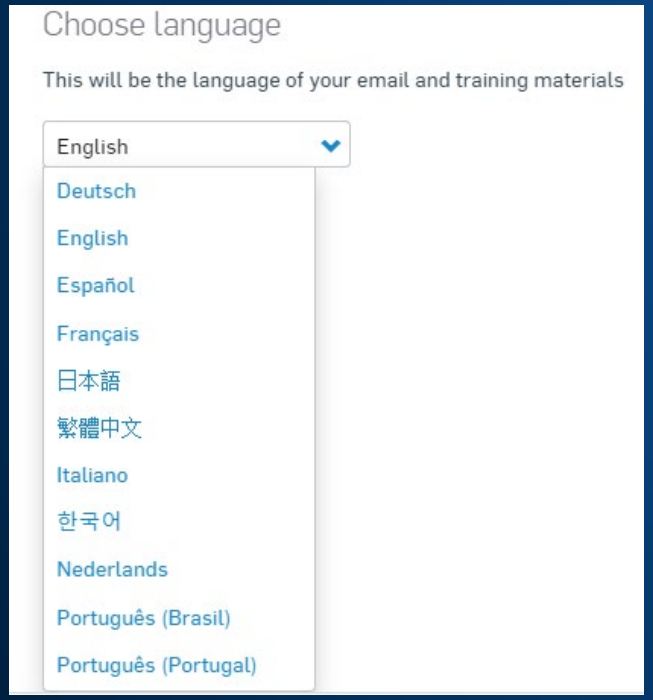
Endpoint Protection

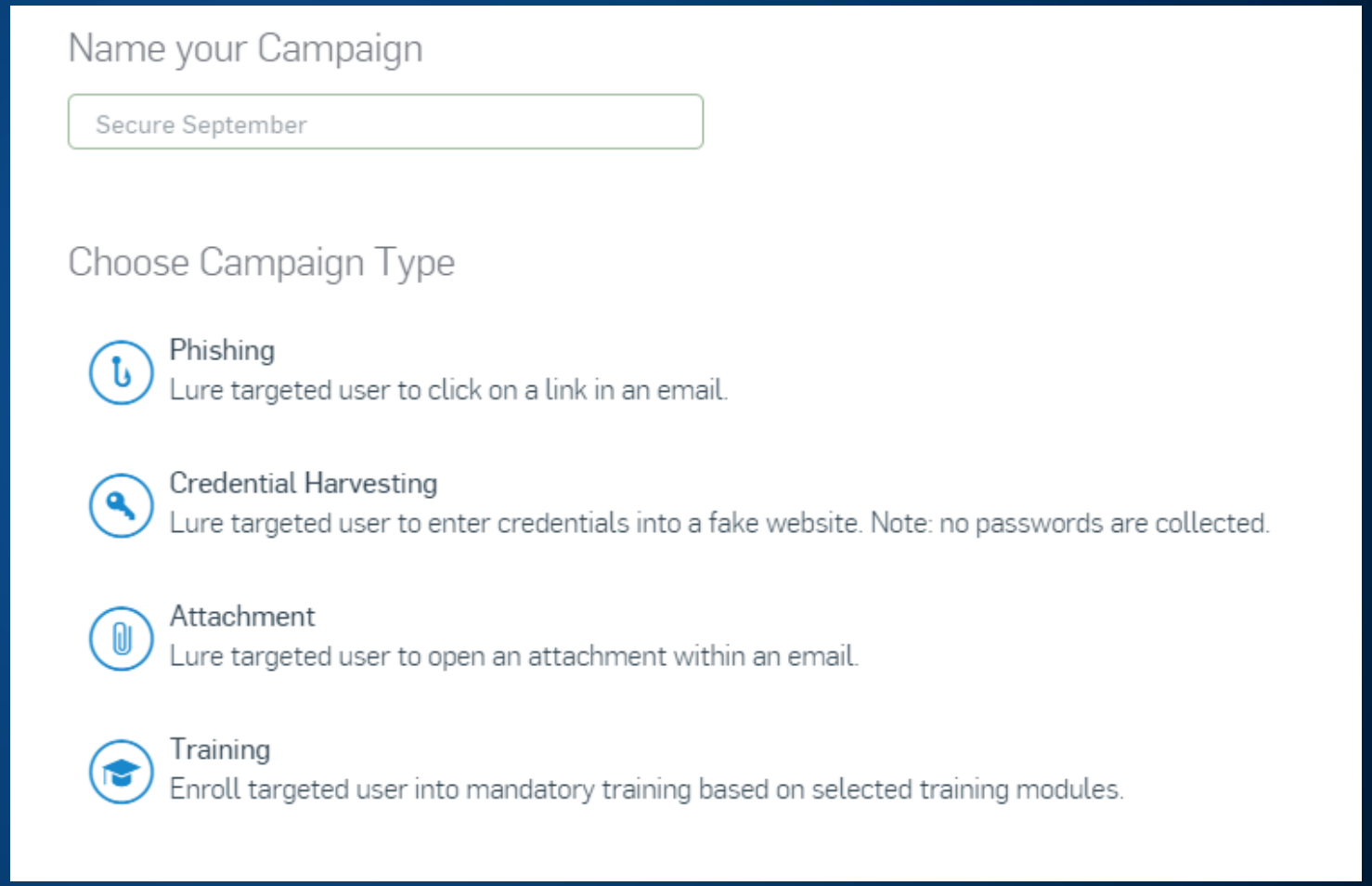
- Anti-Malware
- Anti-Exploit
- Anti-Ransomware
- Anti-Hacker

Intercept X
Sophos Endpoint Protection
Mobile Security

Phish Threat przegląd kampanii

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

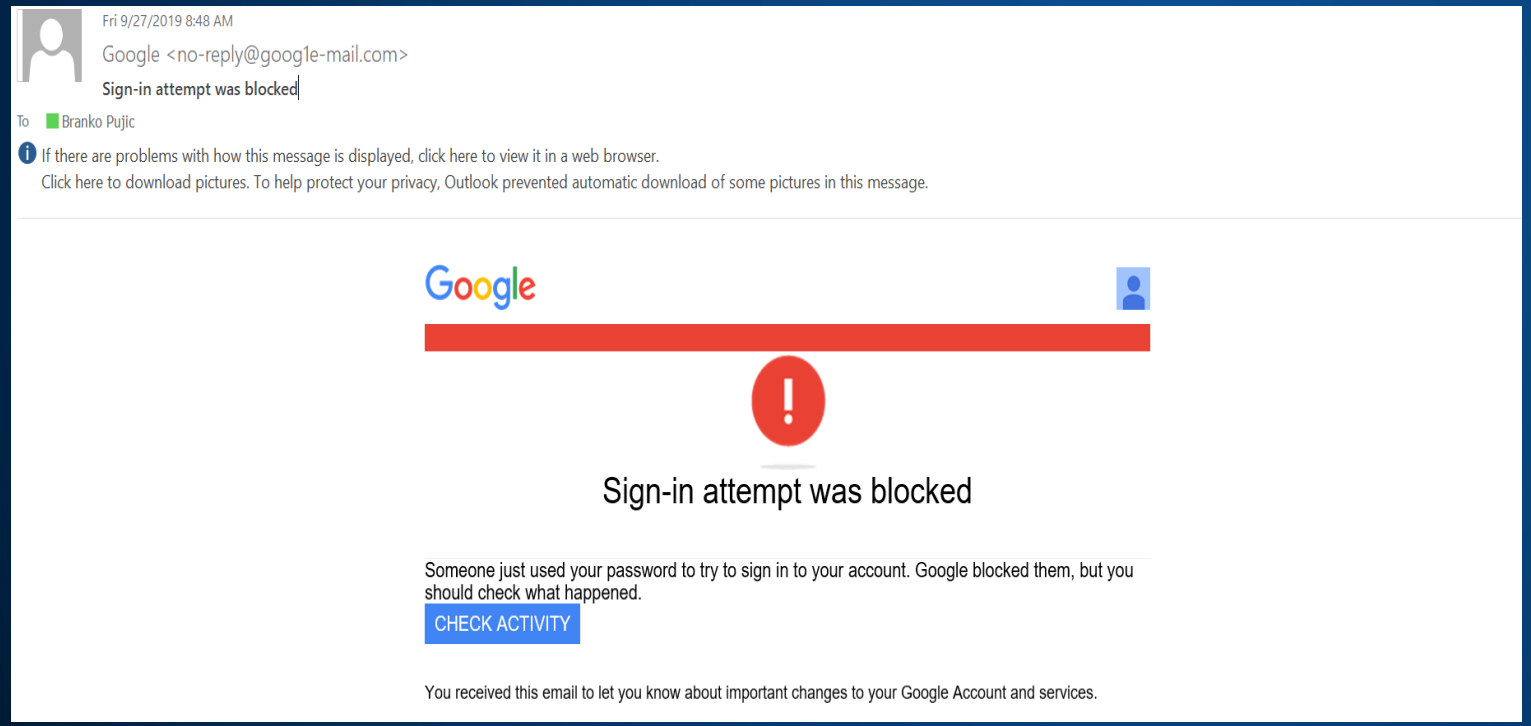


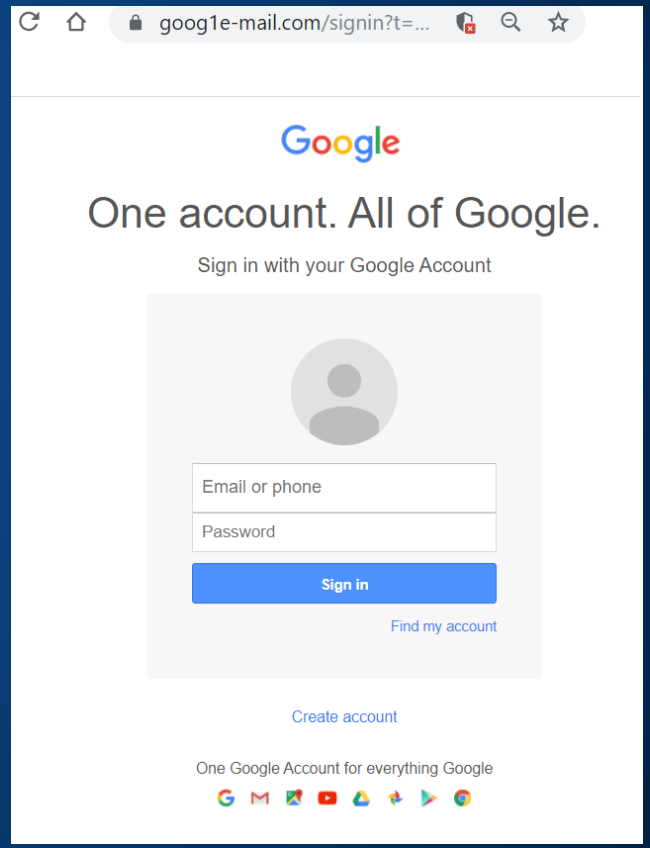


Phish Threat – kampania: Access data theft

Pozwala na weryfikację:

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

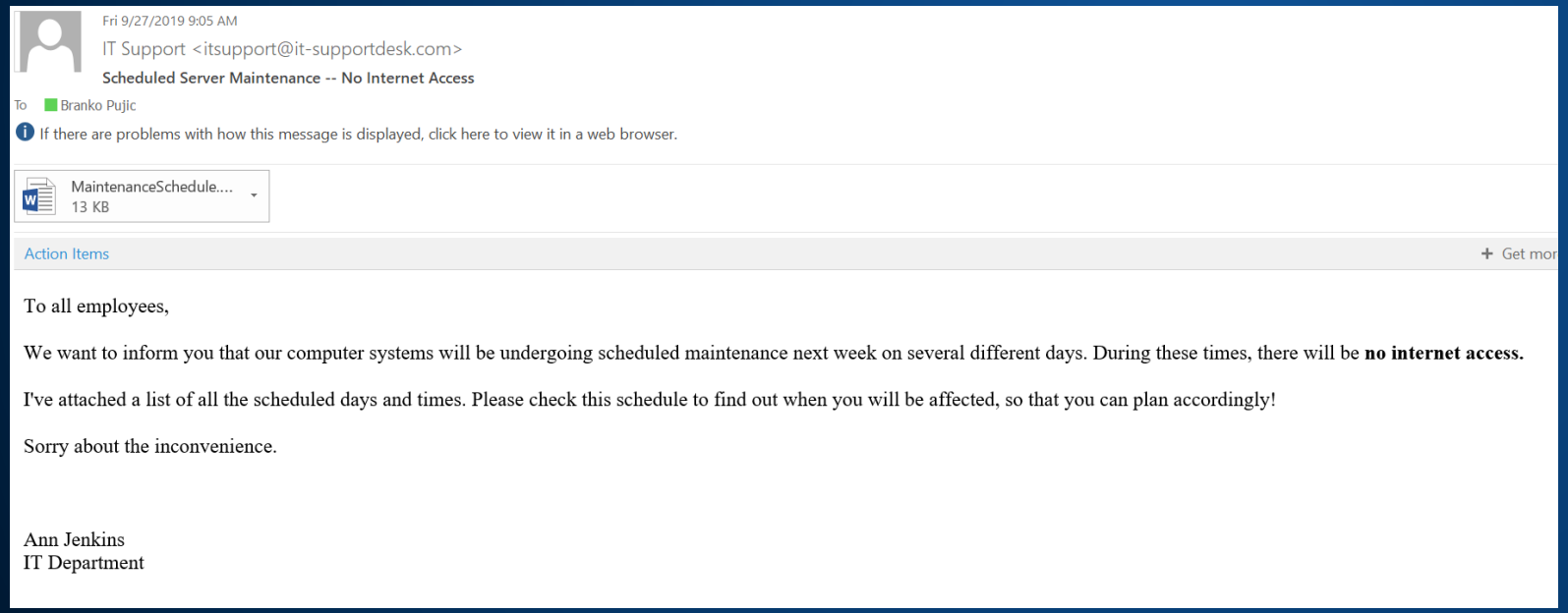


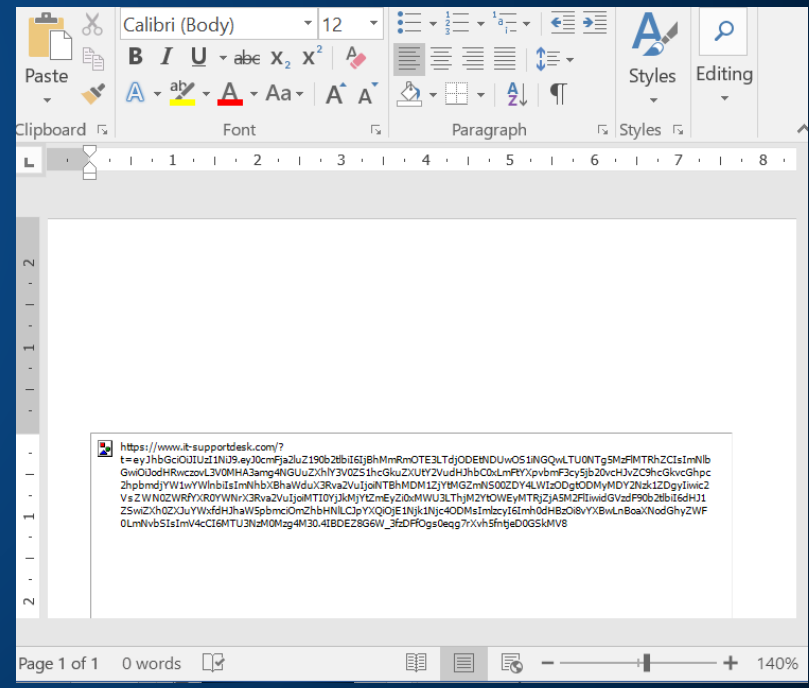


Phish Threat – kampania: Office Attachment

Sprawdza, czy użytkownik wykonała akcję z załącznikiem MS Office

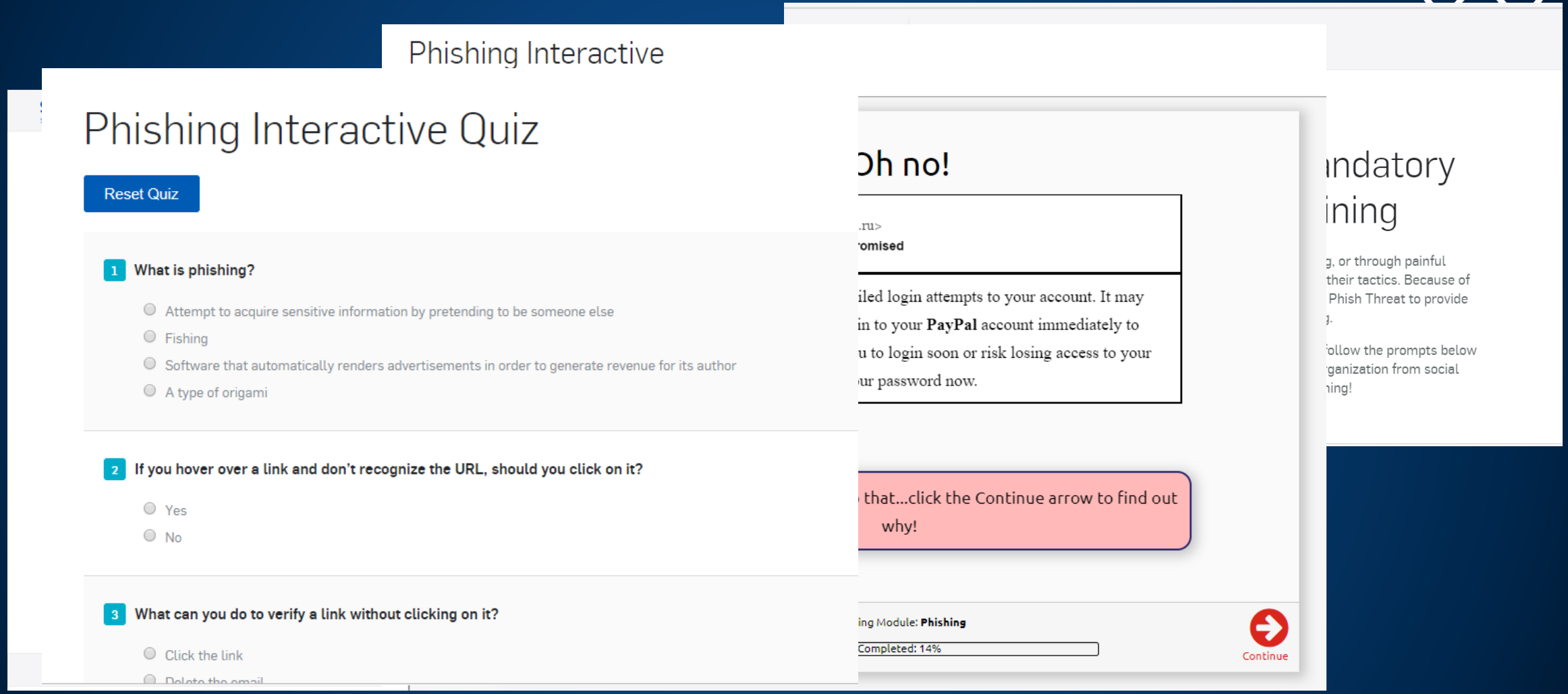
- Pobranie pliku
- otwarcie





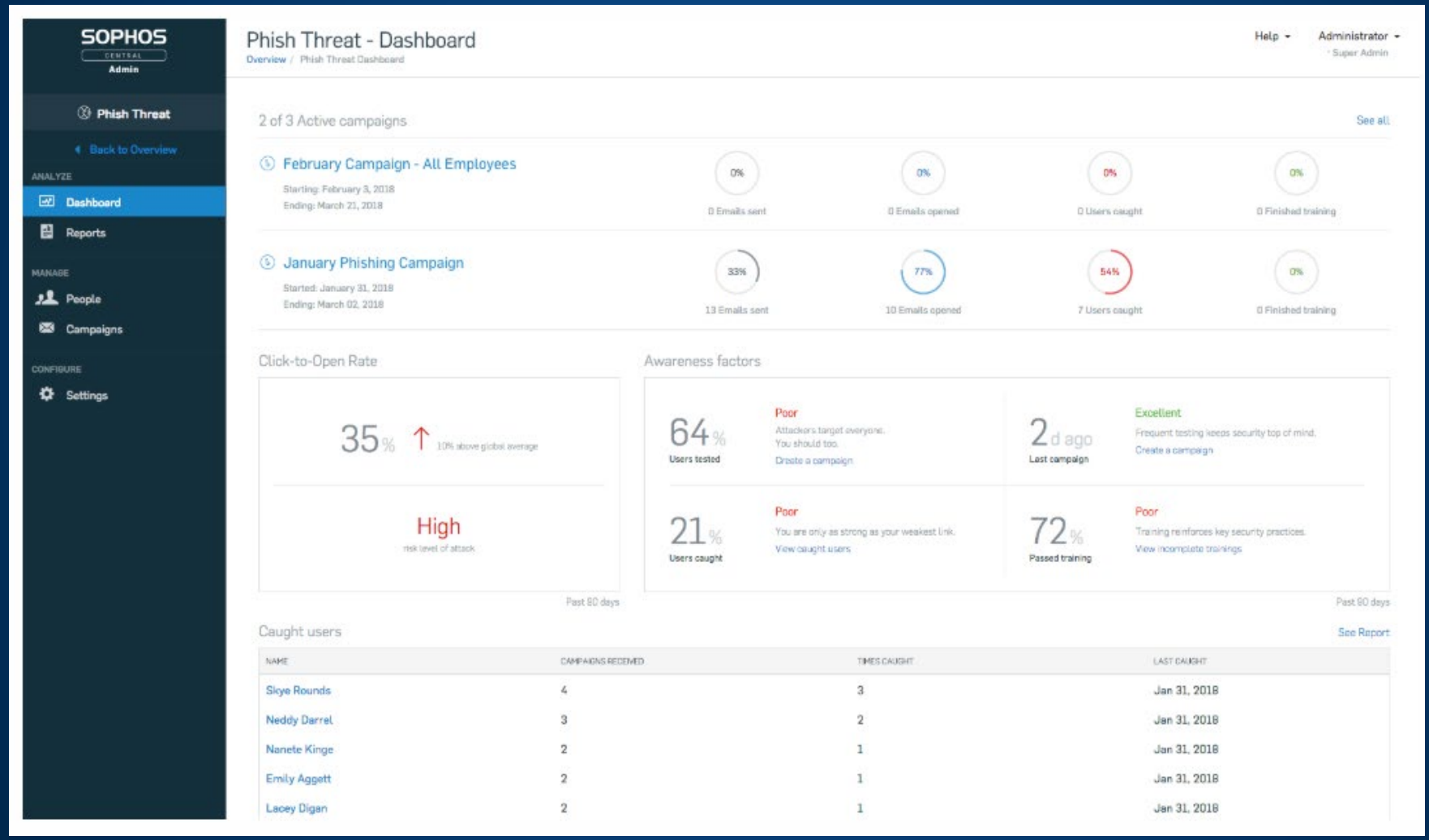
SOPHOS

Phish Threat szkolenie



SOPHOS

Phish Threat - konsola

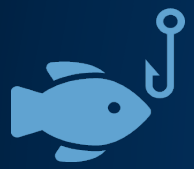


Synchronized Security

Sophos Phish Threat

Łańcuch Cyber Ataku

1. *Dostarczenie*
2. *Wykonanie i Exploitowanie*
3. *BOOM!* $$$



Phishing

Zainfeowany URL

Command & Control

Kradież haseł

Eskalacja uprawnień

Wykonanie złośliwego kodu

Poszukiwanie danch

Ransomware

Atak na serwer

Phishing Training

Email | Web | Firewall | Endpoint | Firewall | Endpoint | Server

SOPHOS

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

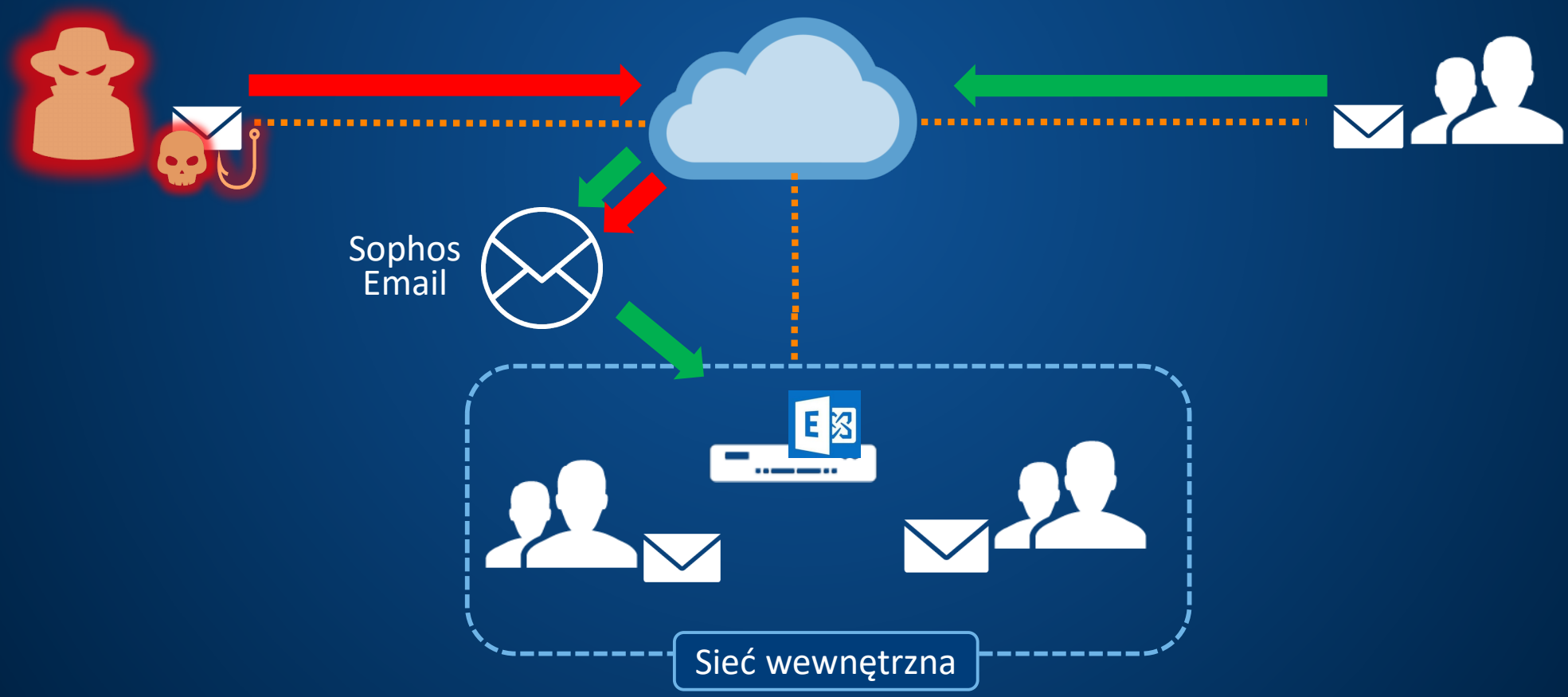
Central Email

SOPHOS

Central Email - przegląd

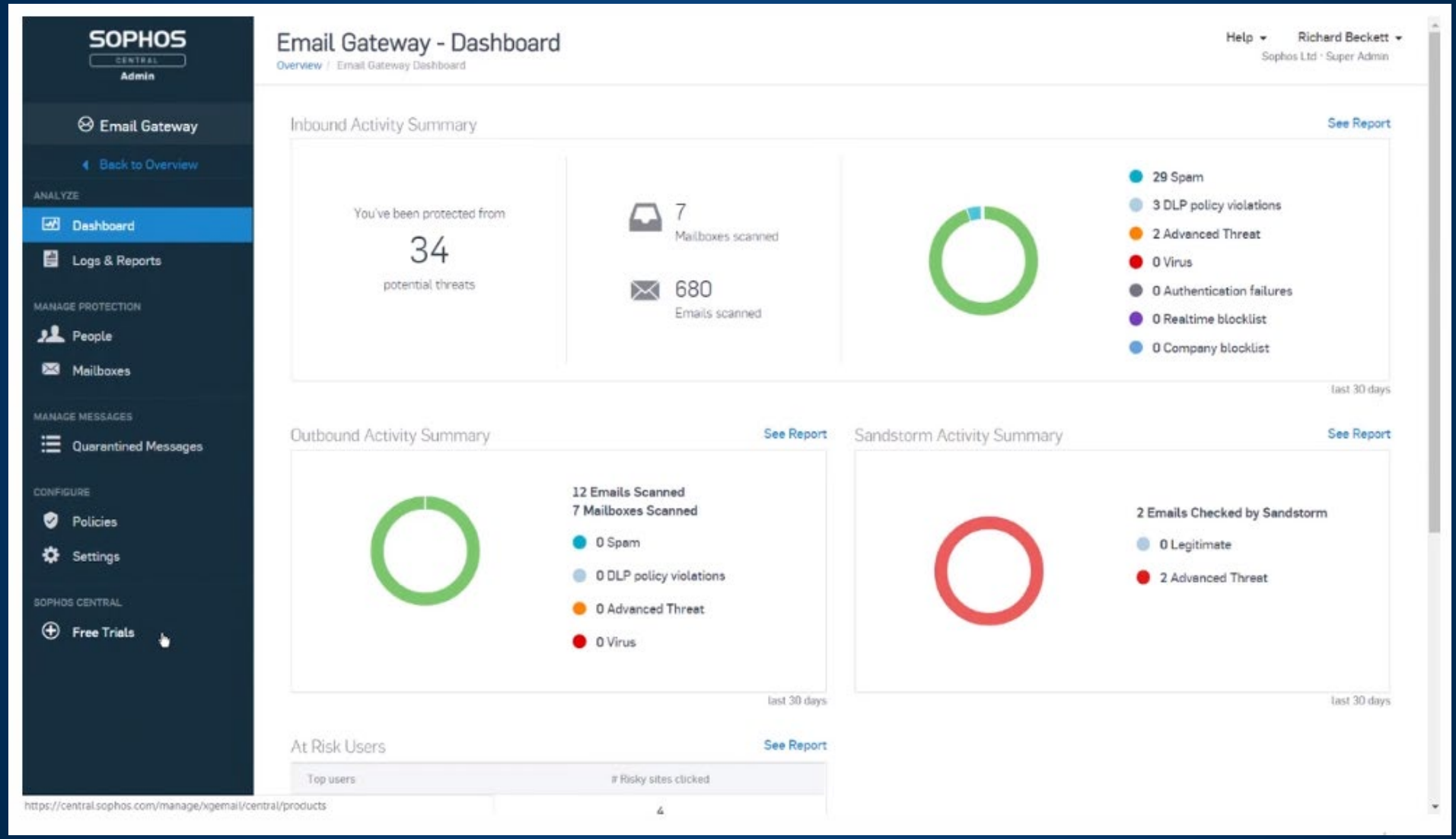
- Oparte na chmurze rozwiązanie bramy e-mail
- Dodatkowa ochrona usług e-mail w chmurze (Office365 / Gmail) lub lokalnych serwerów poczty (Exchange / Notes)
- Administracja za pośrednictwem Sophos Central
- Inteligentniejsze zabezpieczenia poczty e-mail
- Sandboxing z głębokim uczeniem się
- Time of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

Email – środowisko pocztowe u klienta

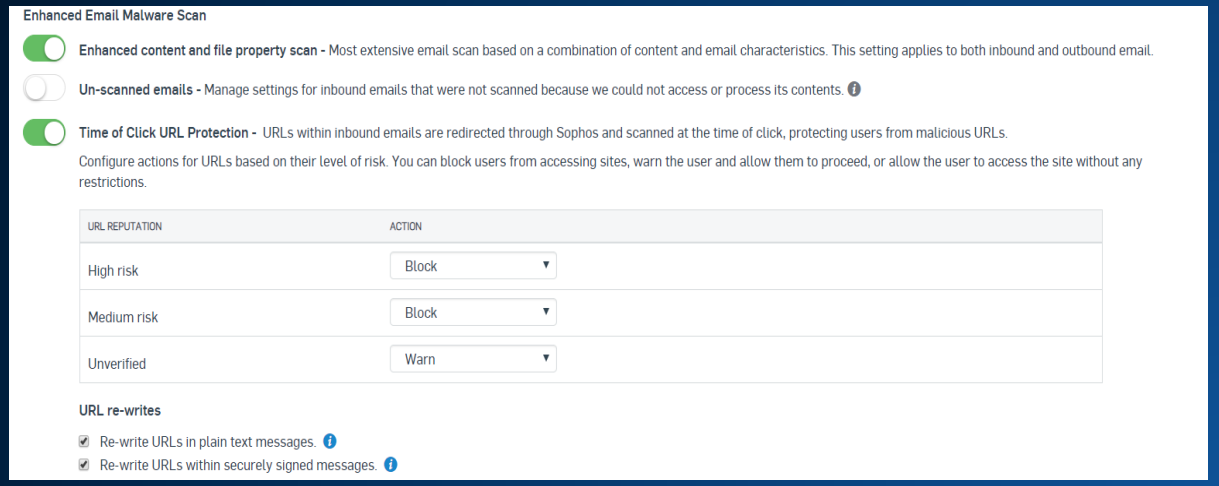


Email - Office 365

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



Link zostanie sprawdzony w momencie kliknięcia

Klick

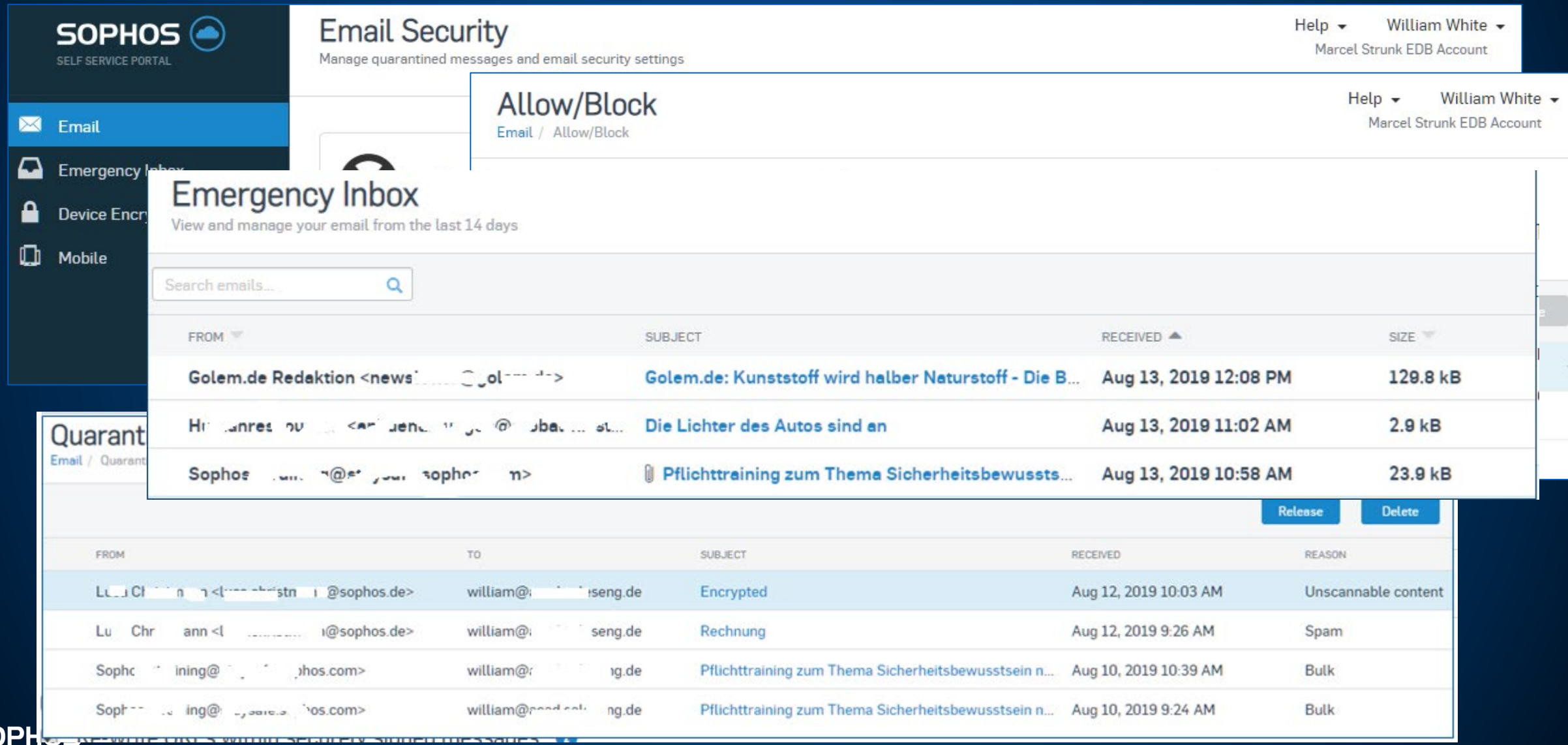
sophosXY12

Sophos Email

Link początkowy jest zastąpiony przez urządzenie

SOPHOS

Self Service



Szyfrowanie SPX

Hasło dostępne?

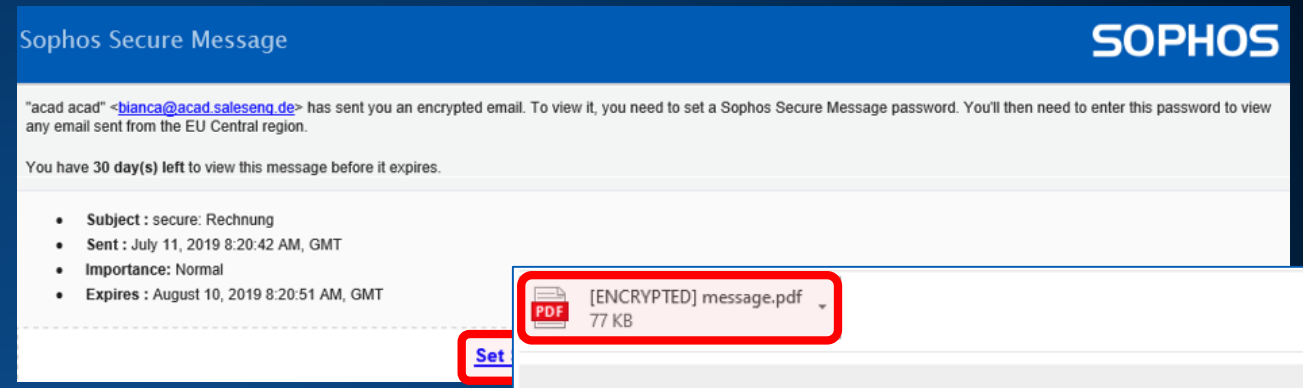
Sophos Email

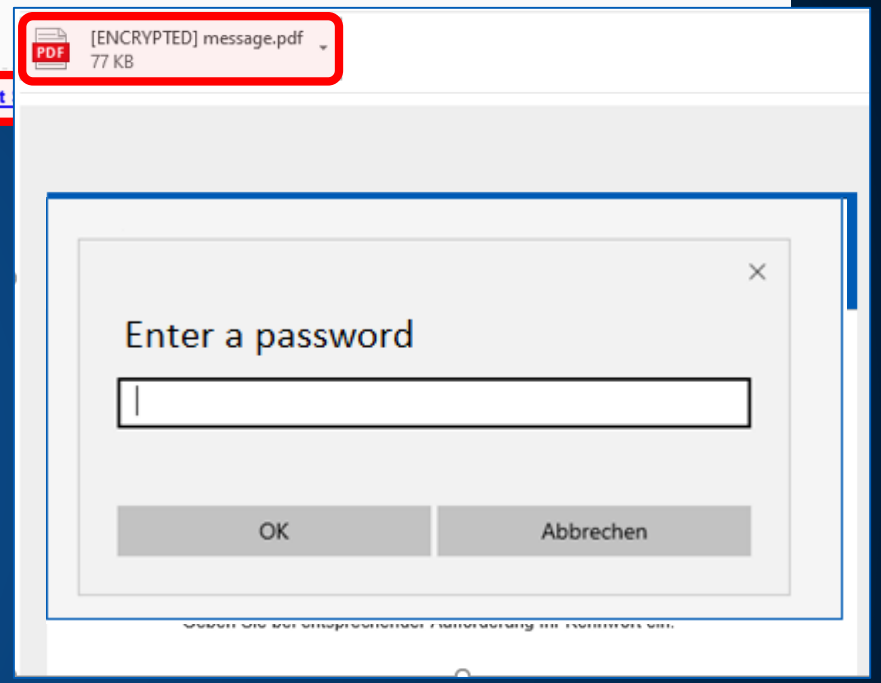
Żądanie rejestracji

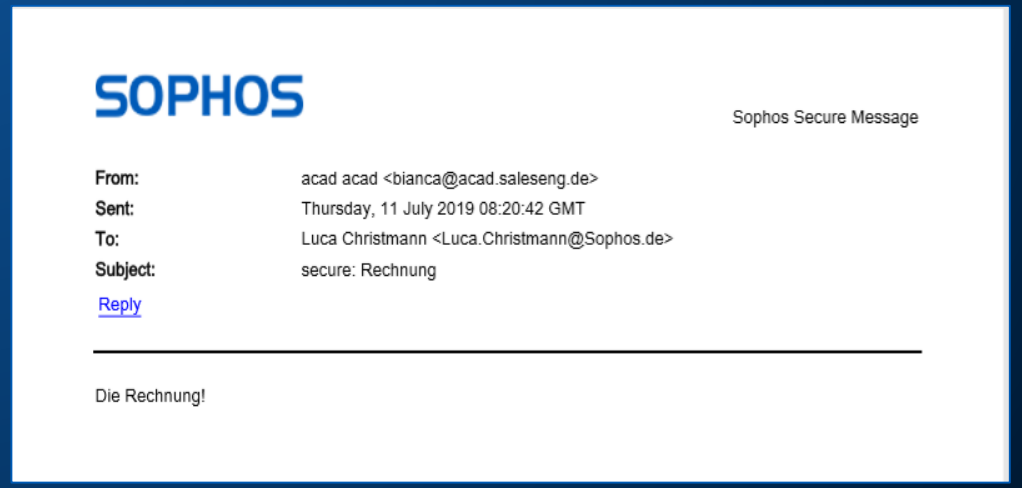
Odbiorca

Zaszyfroway email

Nadawca





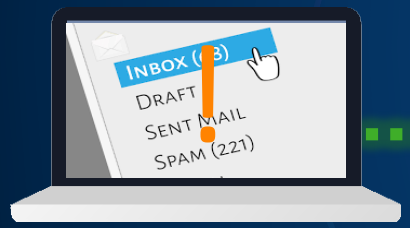


Email i integracja Phish Threat

1 **Podejrzany lik 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™

SOPHOS

** Available Q4 2018*

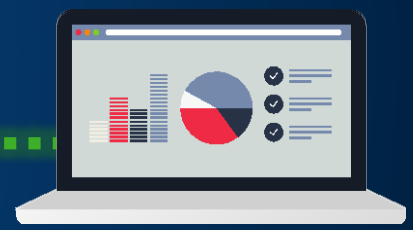
Email i integracja z Endpoint

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: Skanownaie urządzenie**
Sophos Endpoint identyfikuje i skanuje wszystkie znane urządzenia powiązane ze skrzynką pocztową

Security Heartbeat™

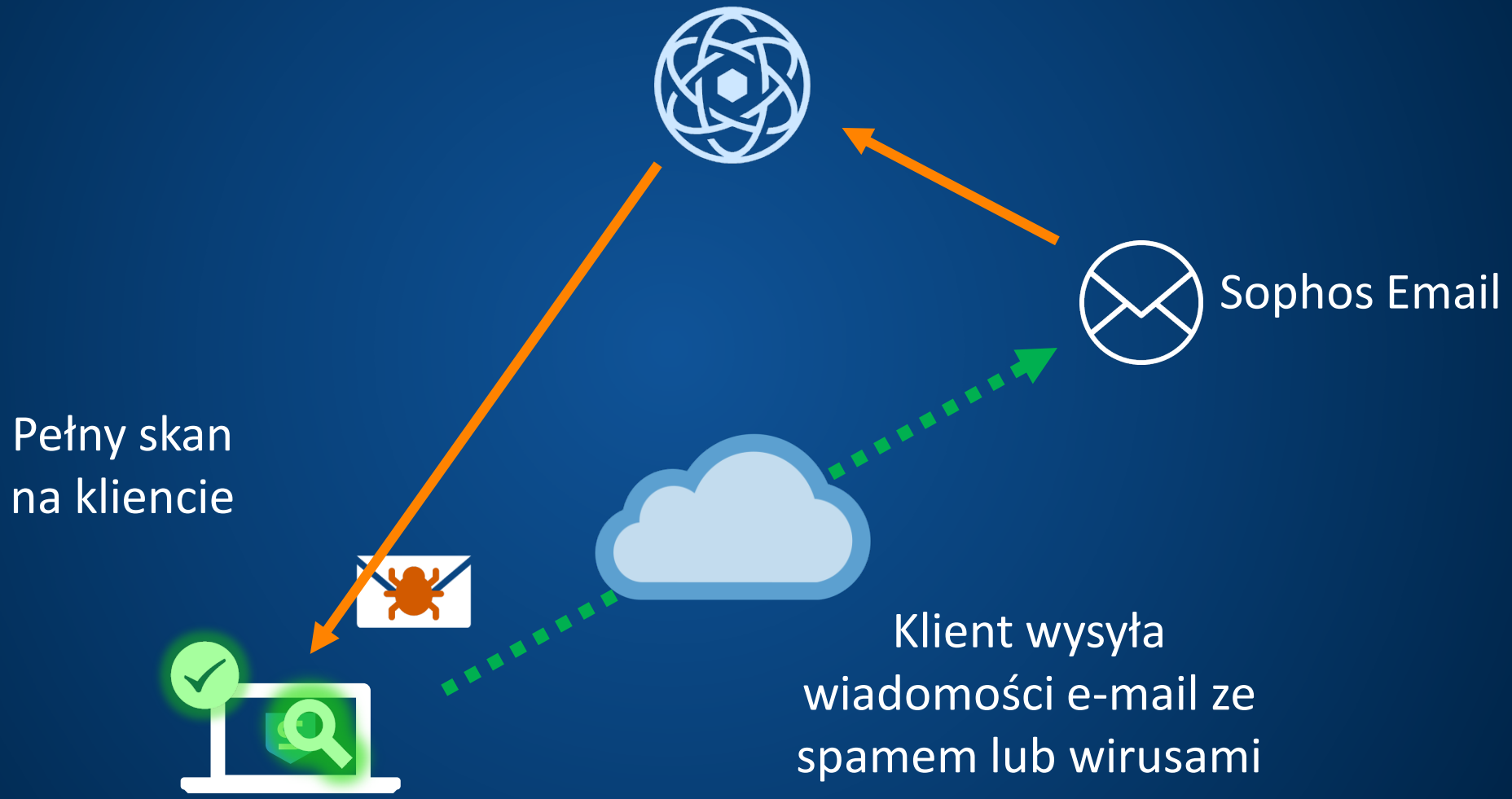


5 **Przywrócenie dostępu do skrzynki**

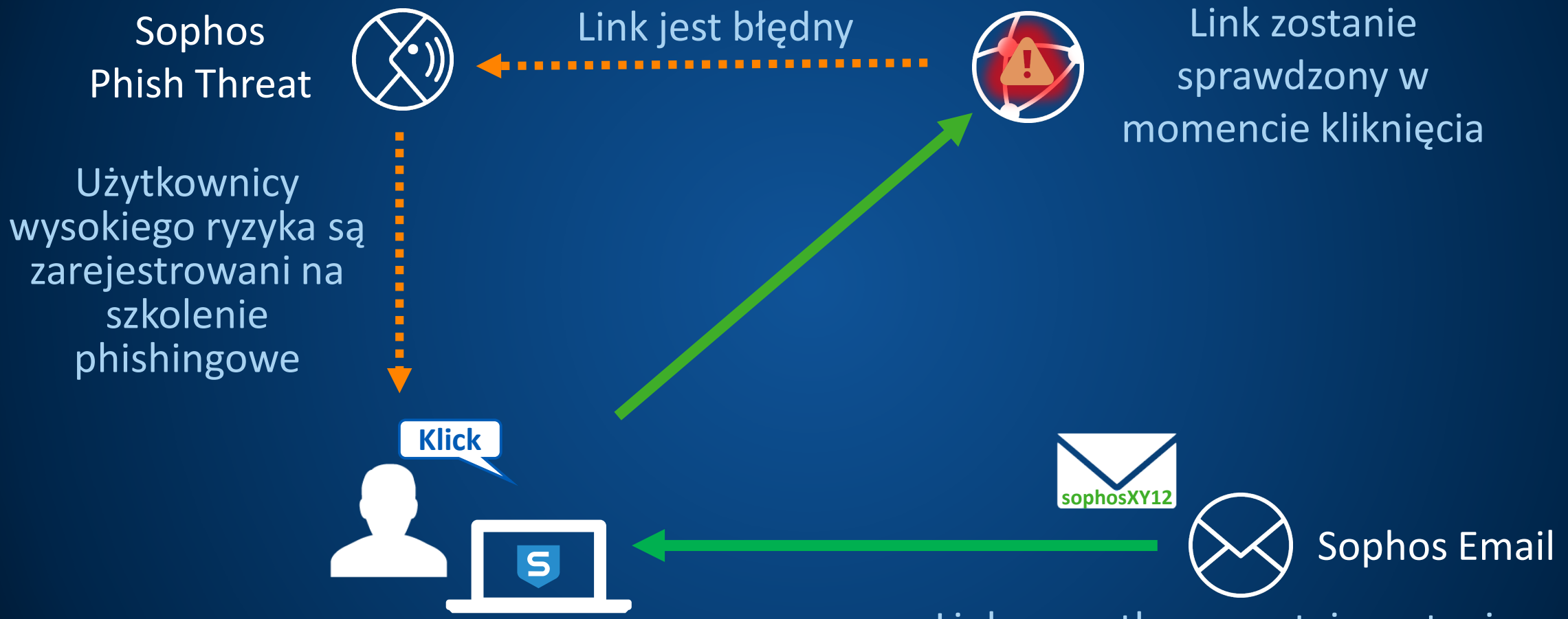
4 **Endpoint: Clean-up**
Sophos Endpoint automatycznie usuwa wszelkie infekcje

SOPHOS

Synchronized Security z Sophos Email i ochronie Endpoint



Synchronized Security z Sophos Email Advanced i PhishThreat



SOPHOS

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

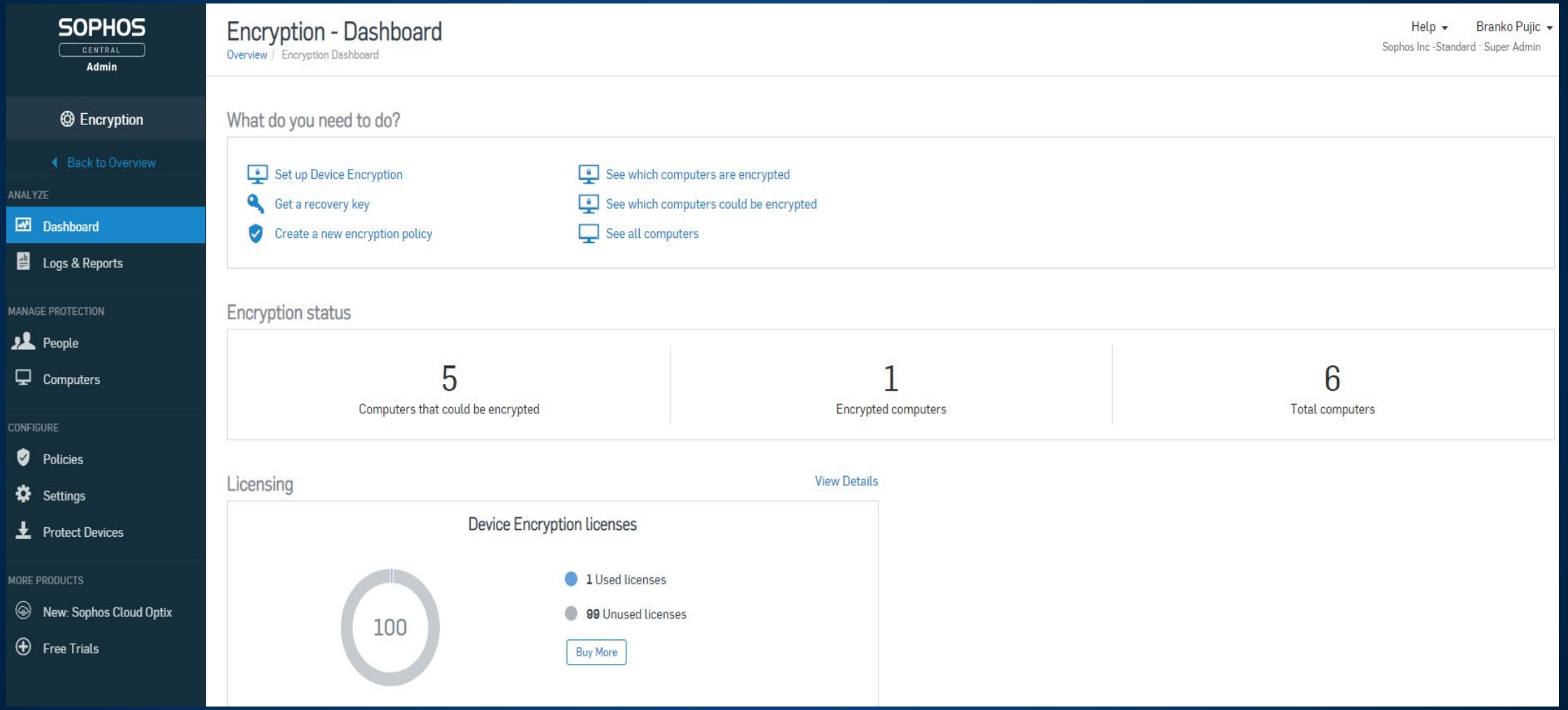
Central Device Encryption

SOPHOS

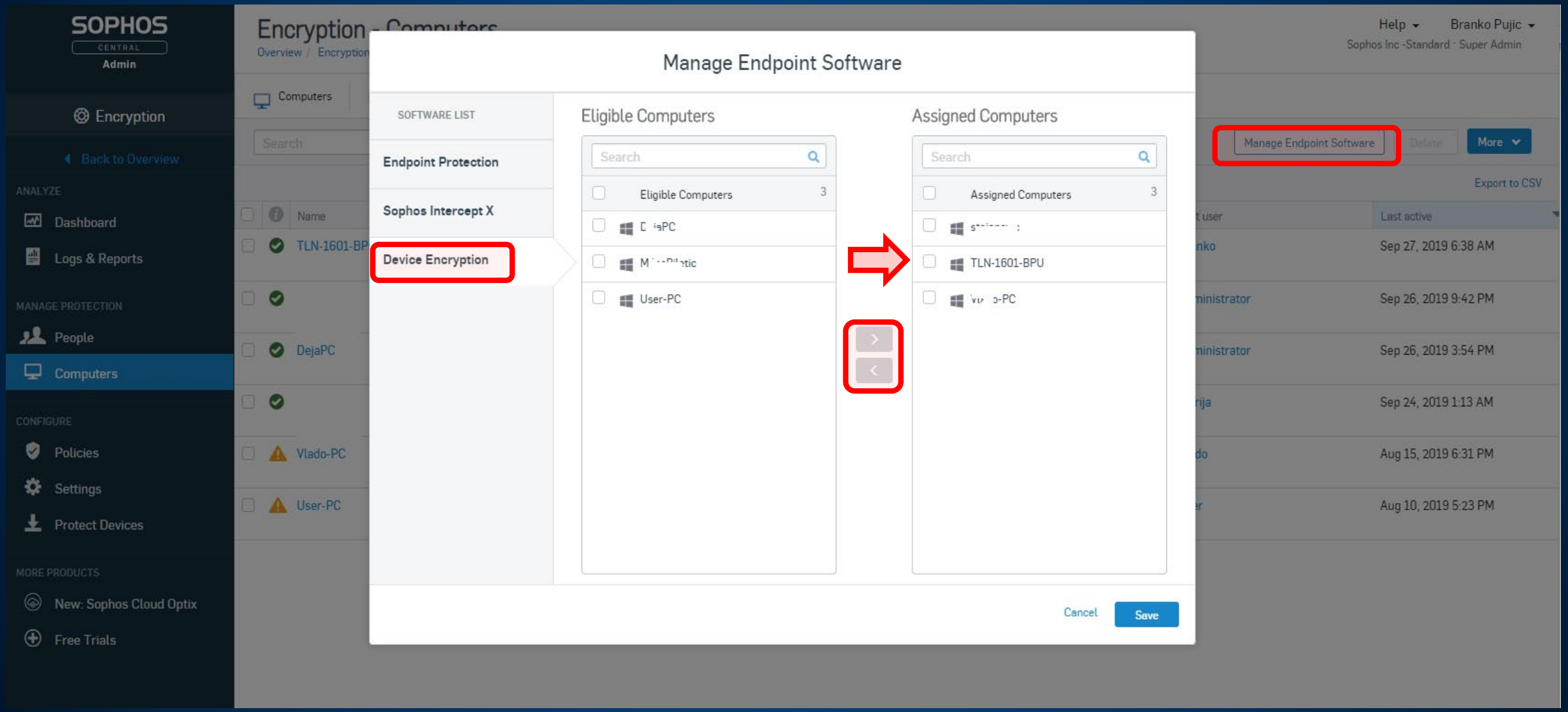
Central Device Encryption - przegląd

- 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

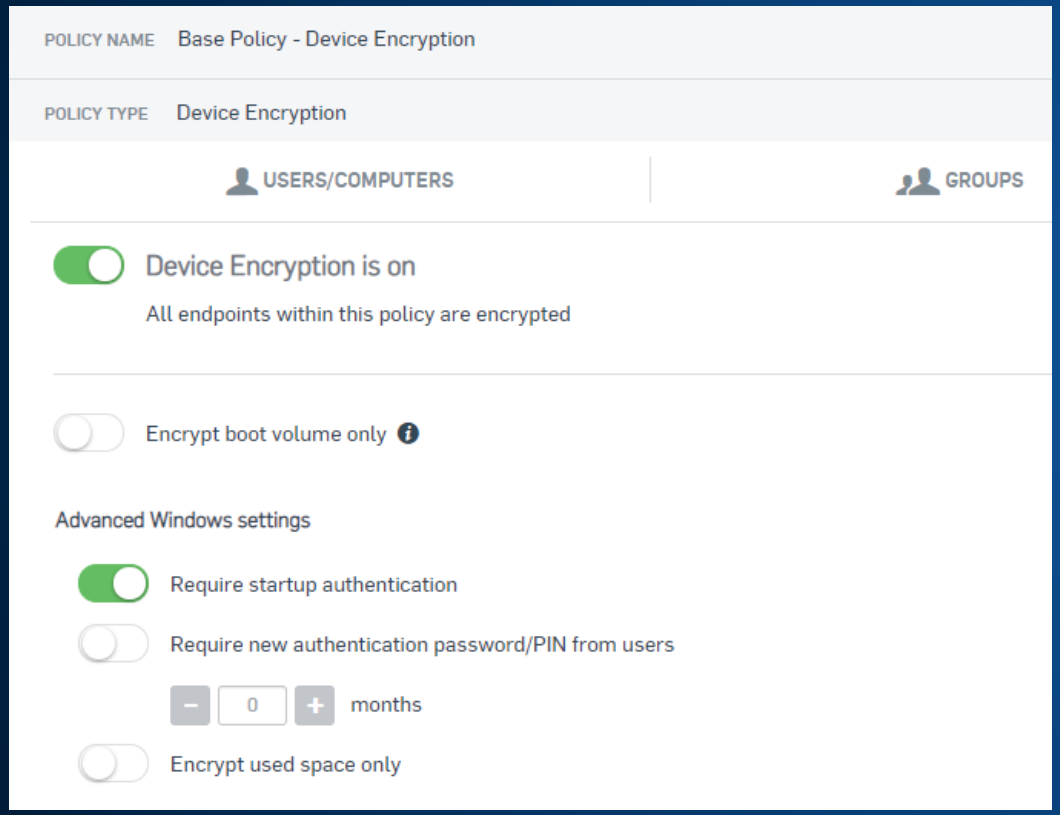
Central Device Encryption - Dashboard



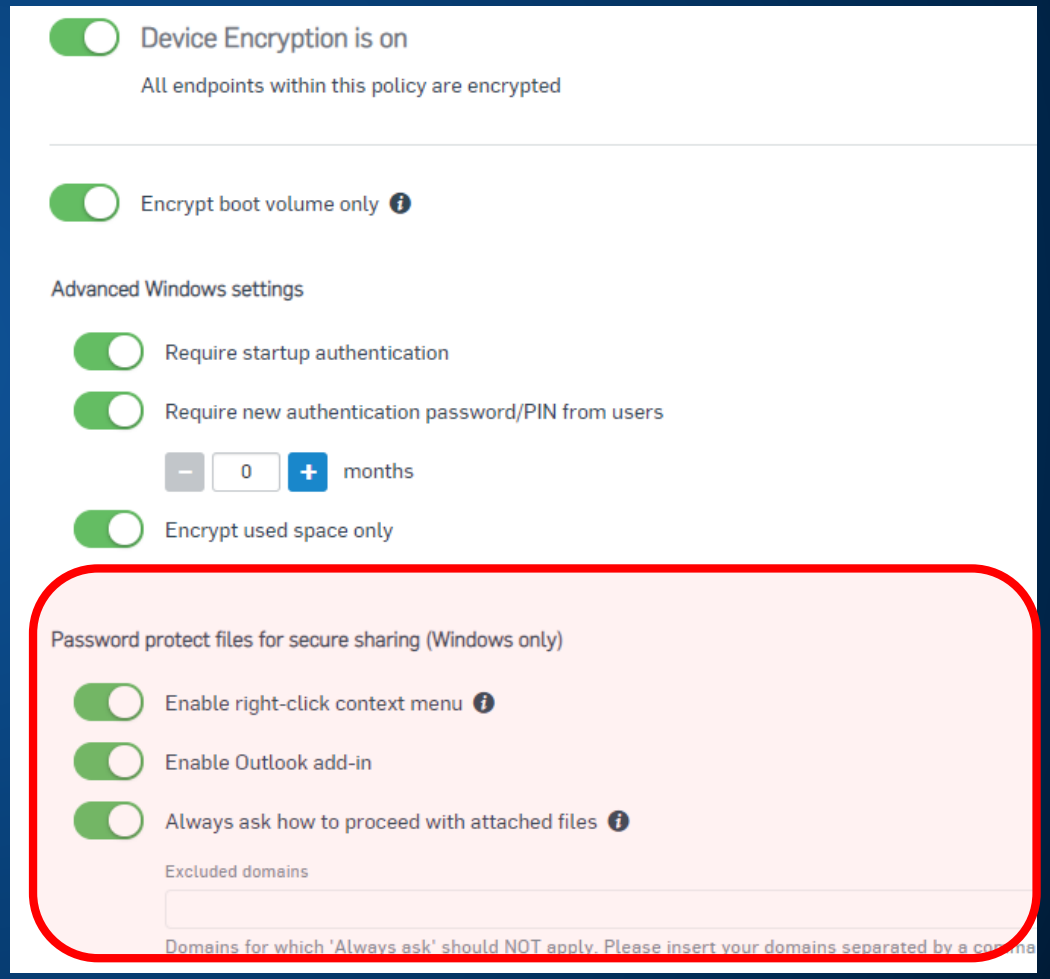
Device Encryption dodanie/usunięcie urządzenia



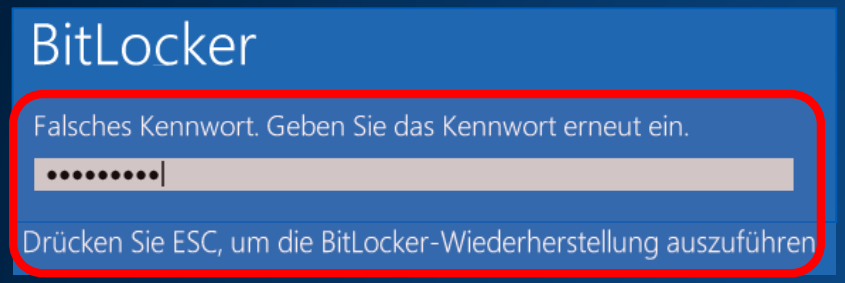
Konfiguracja polityk

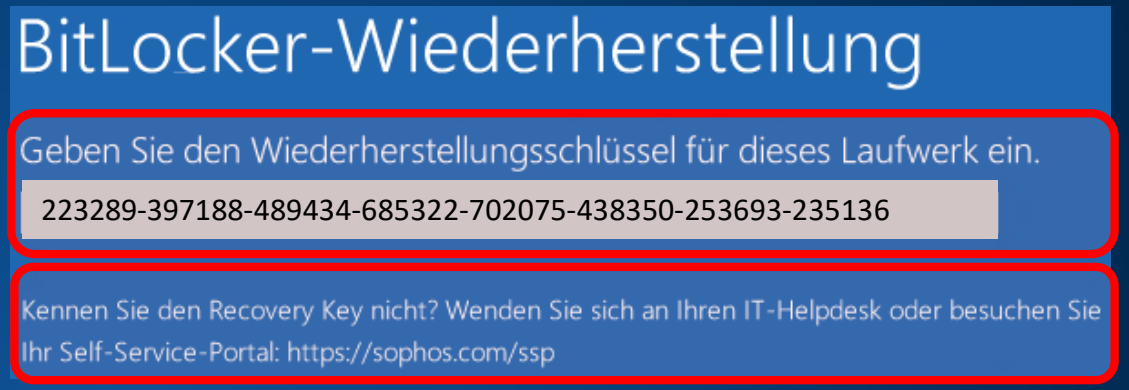


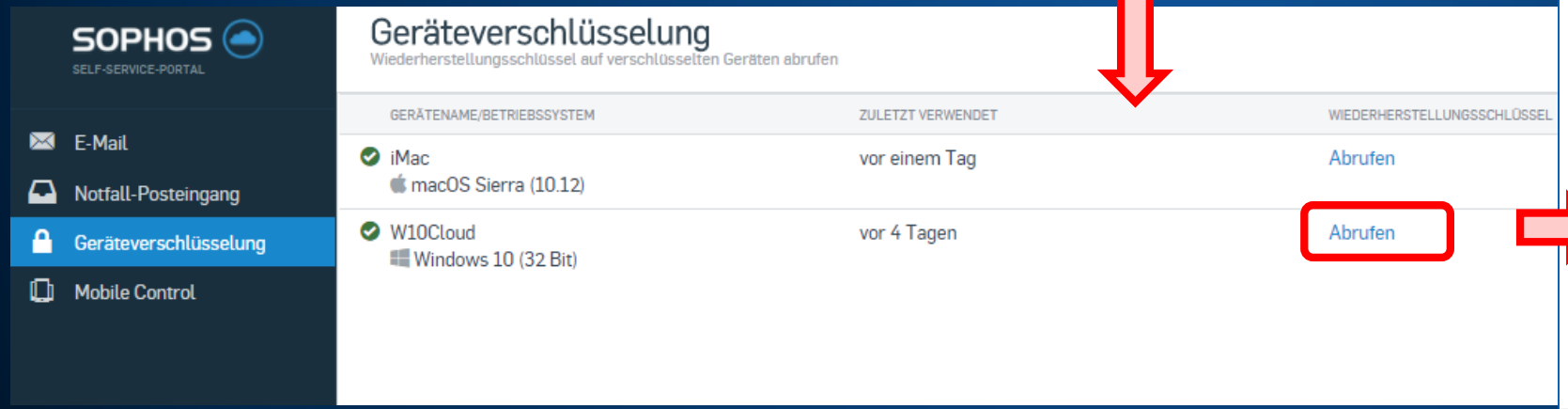
Outlook: Central Device Encryption v2

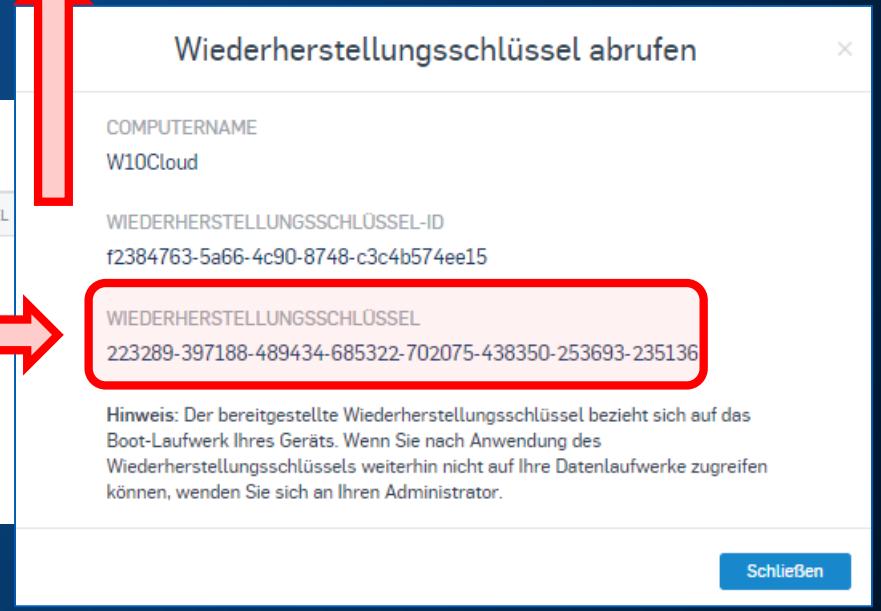


Password Recovery: Self-Service





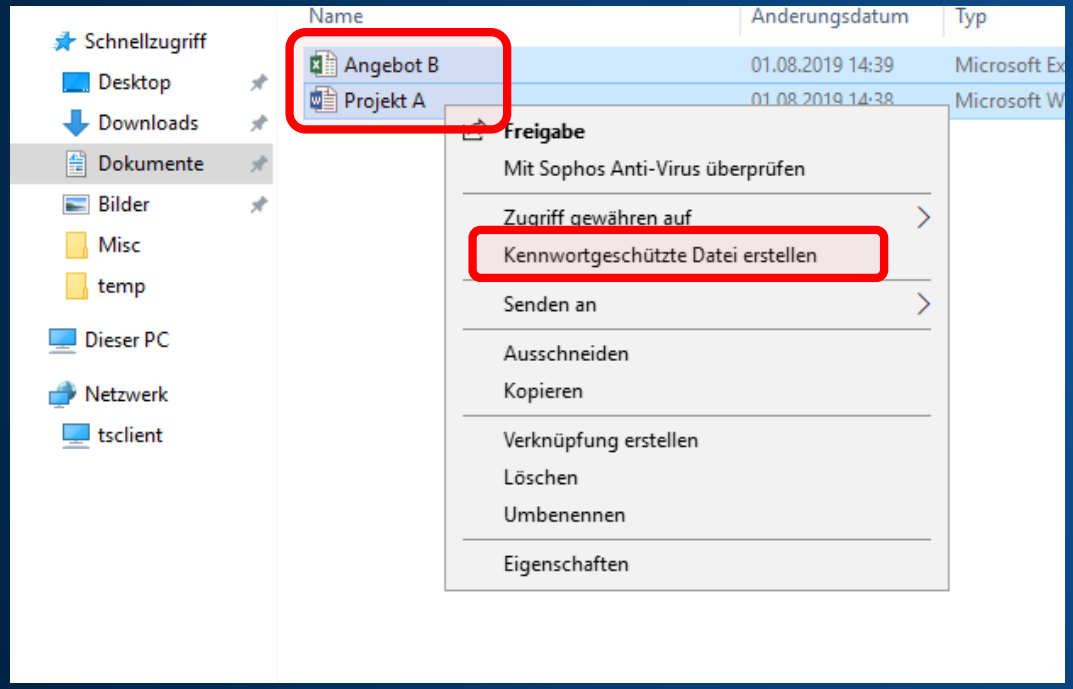


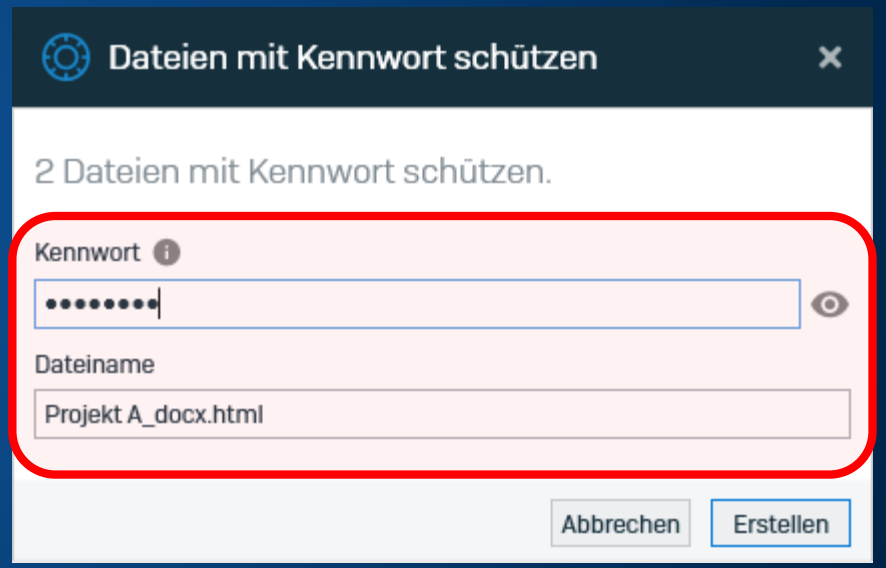


Outlook: Central Device Encryption v2
Pliki chronione hasłem

SOPHOS

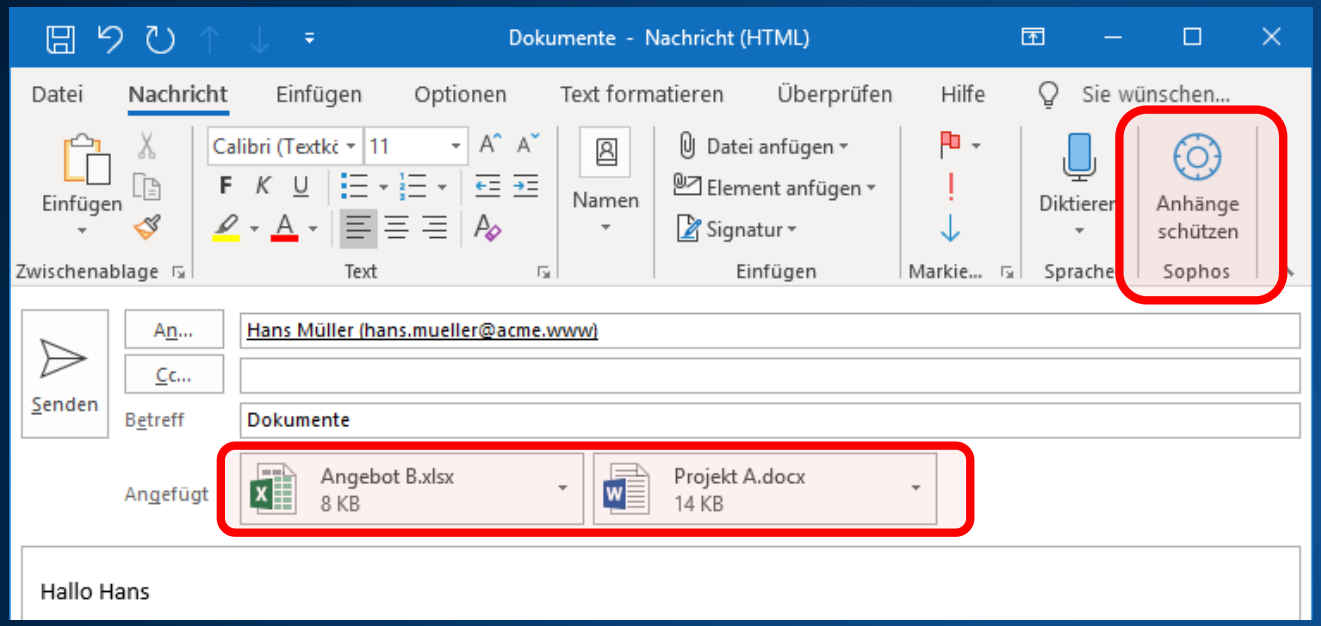
Pliki chronione hasłem

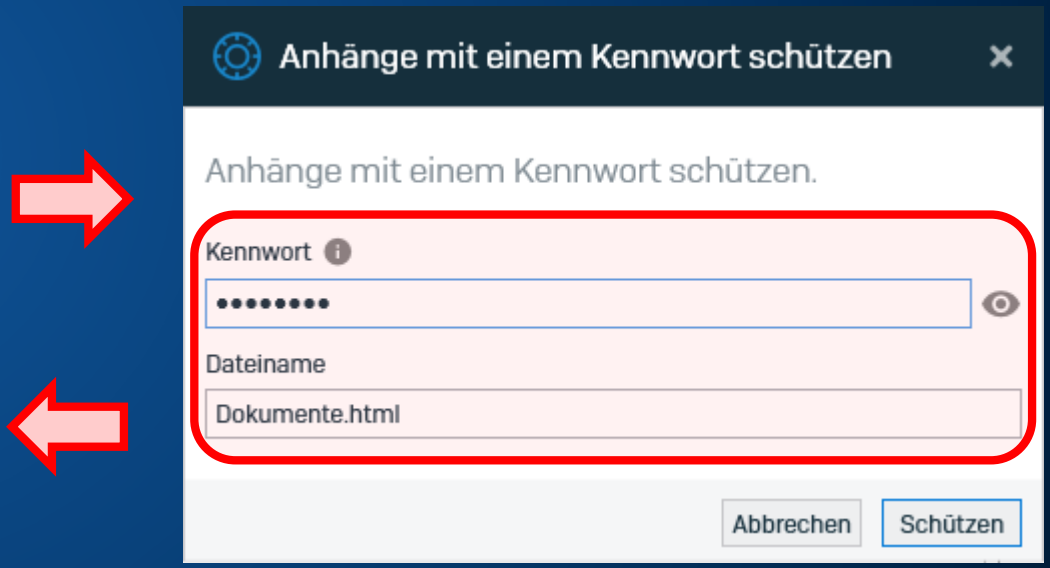


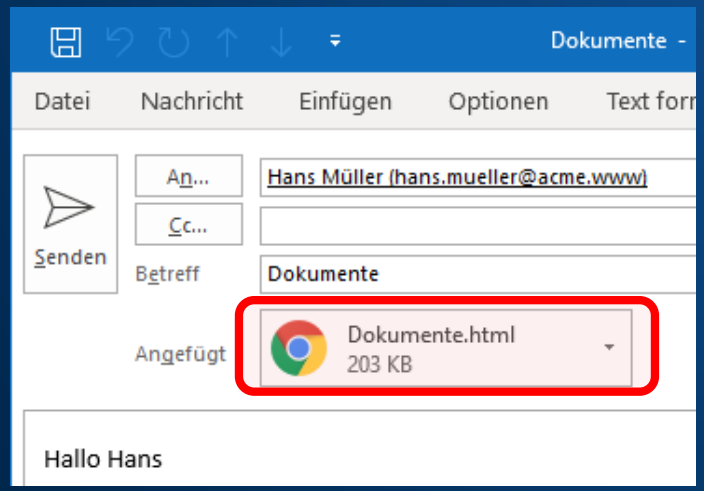


SOPHOS

Outlook Plugin: Szyfrowanie w razie potrzeby lub według zasad





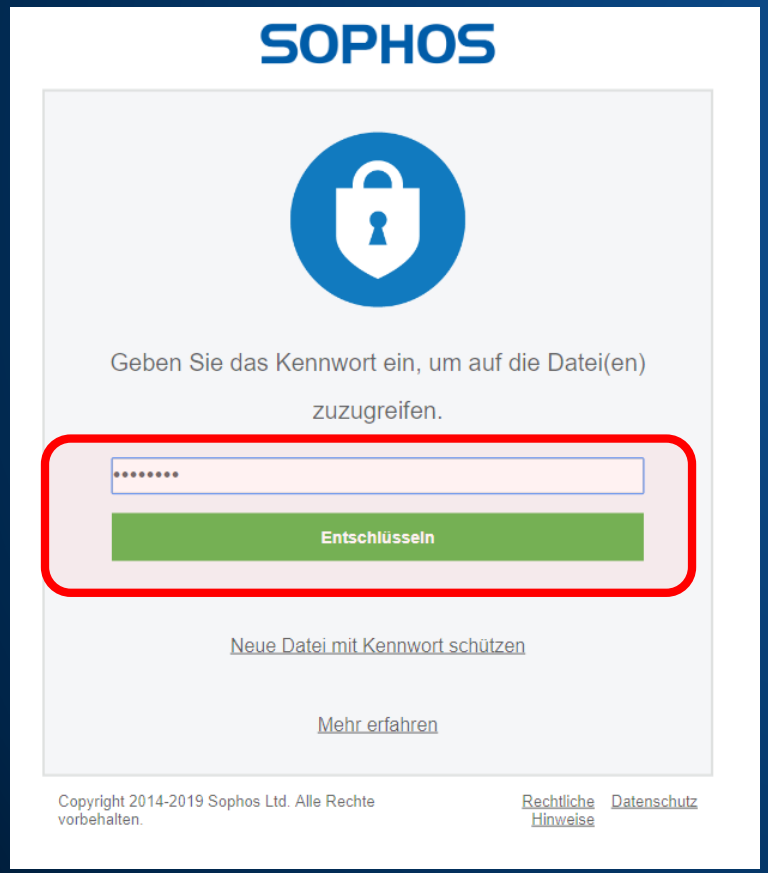


SOPHOS

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.

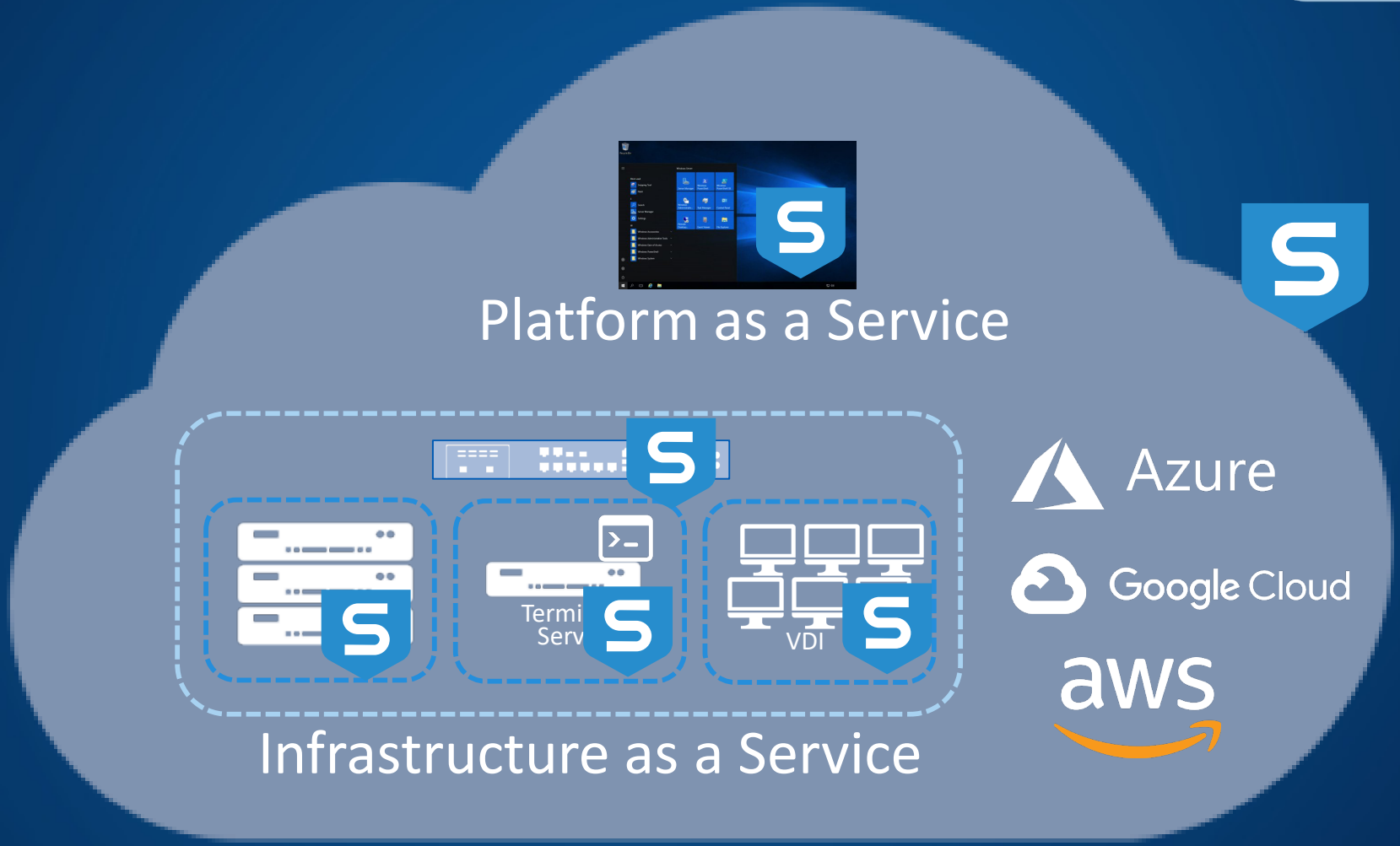
4 **Clean-up**
Sophos Endpoint automatycznie usuwa infekcję.

SOPHOS

Cloud

SOPHOS

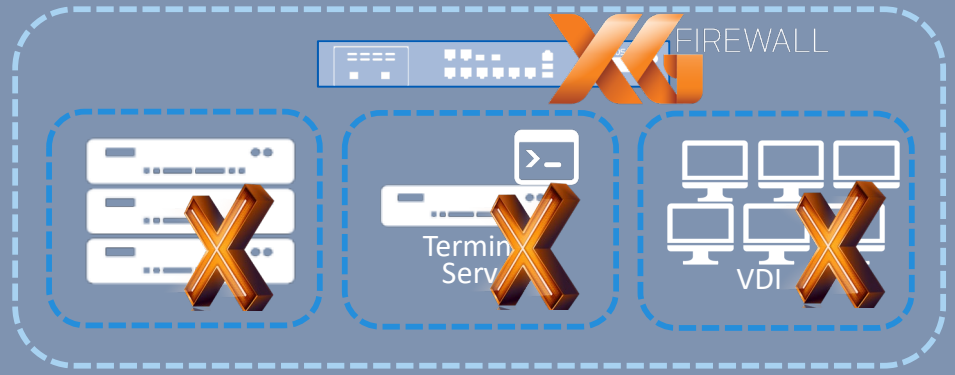
Gdzie Sophos chroni w chmurze



Gdzie Sophos chroni w chmurze

Platform as a Service

Cloud Optix



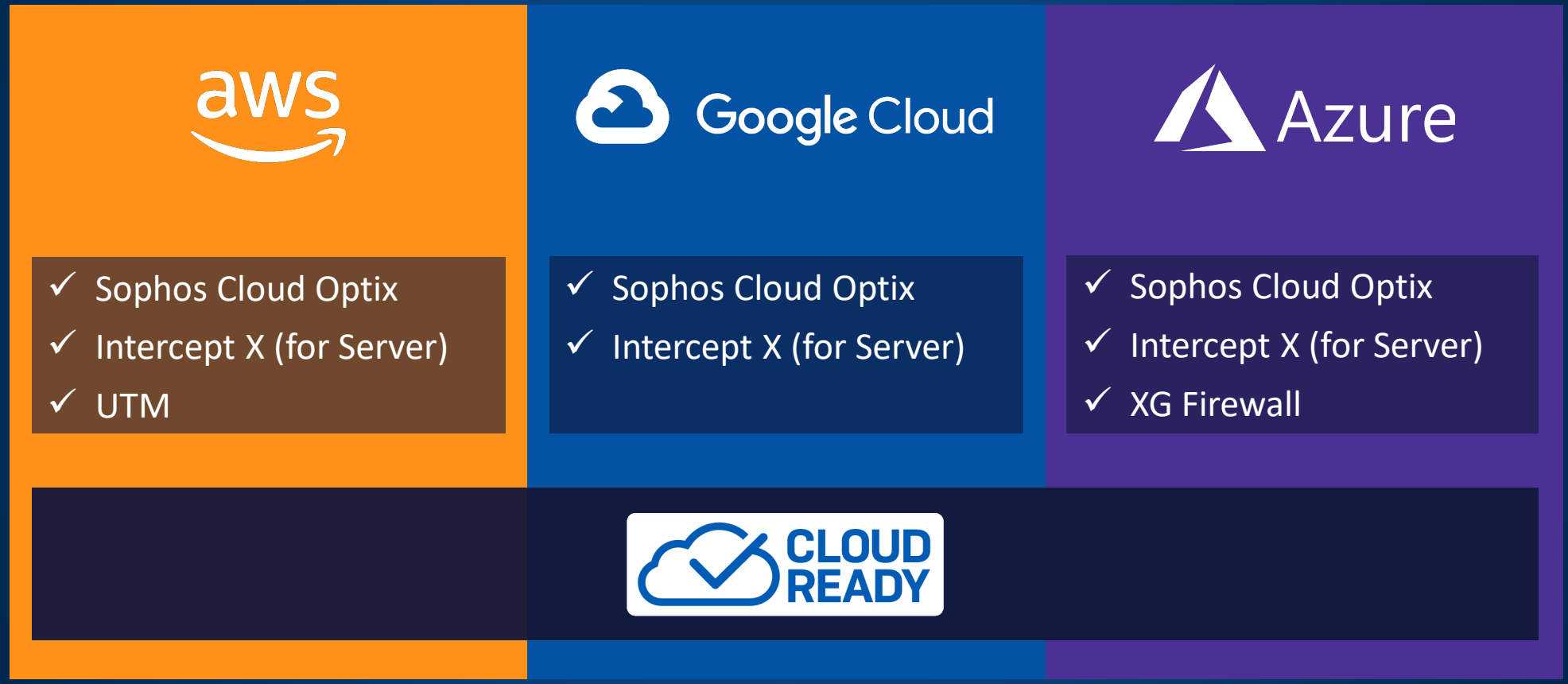
Infrastructure as a Service

Azure

Google Cloud

aws

Sophos Cloud rozwiązania



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%

SOPHOS Cloud Optix

Azure Google Cloud aws

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?

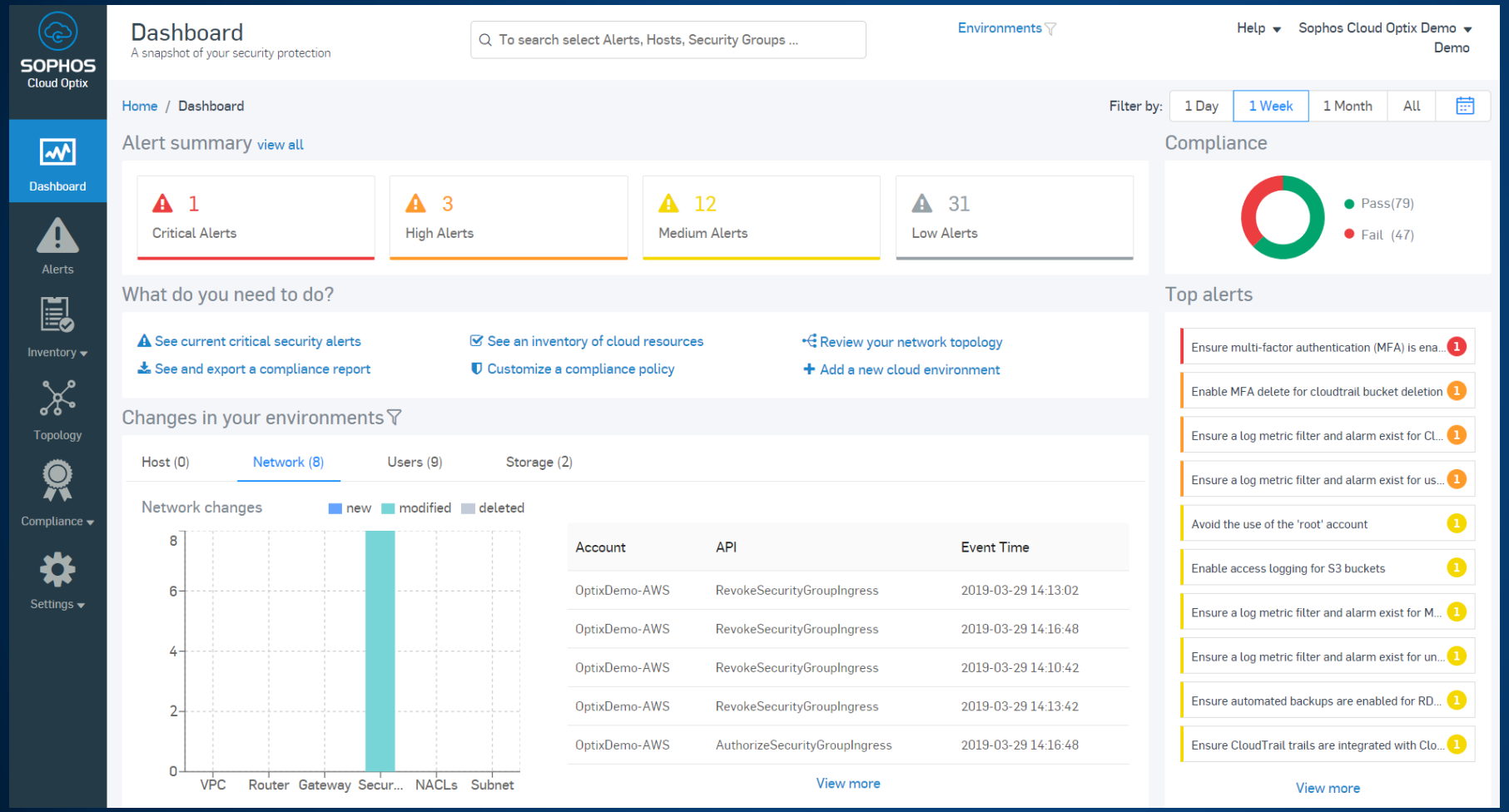
Czy uwierzytelnianie i logowanie są poprawnie skonfigurowane?

Reakcja

Czy współczesne ataki AI można wykryć i zatrzymać?

Czy błędne konfiguracje można korygować automatycznie?

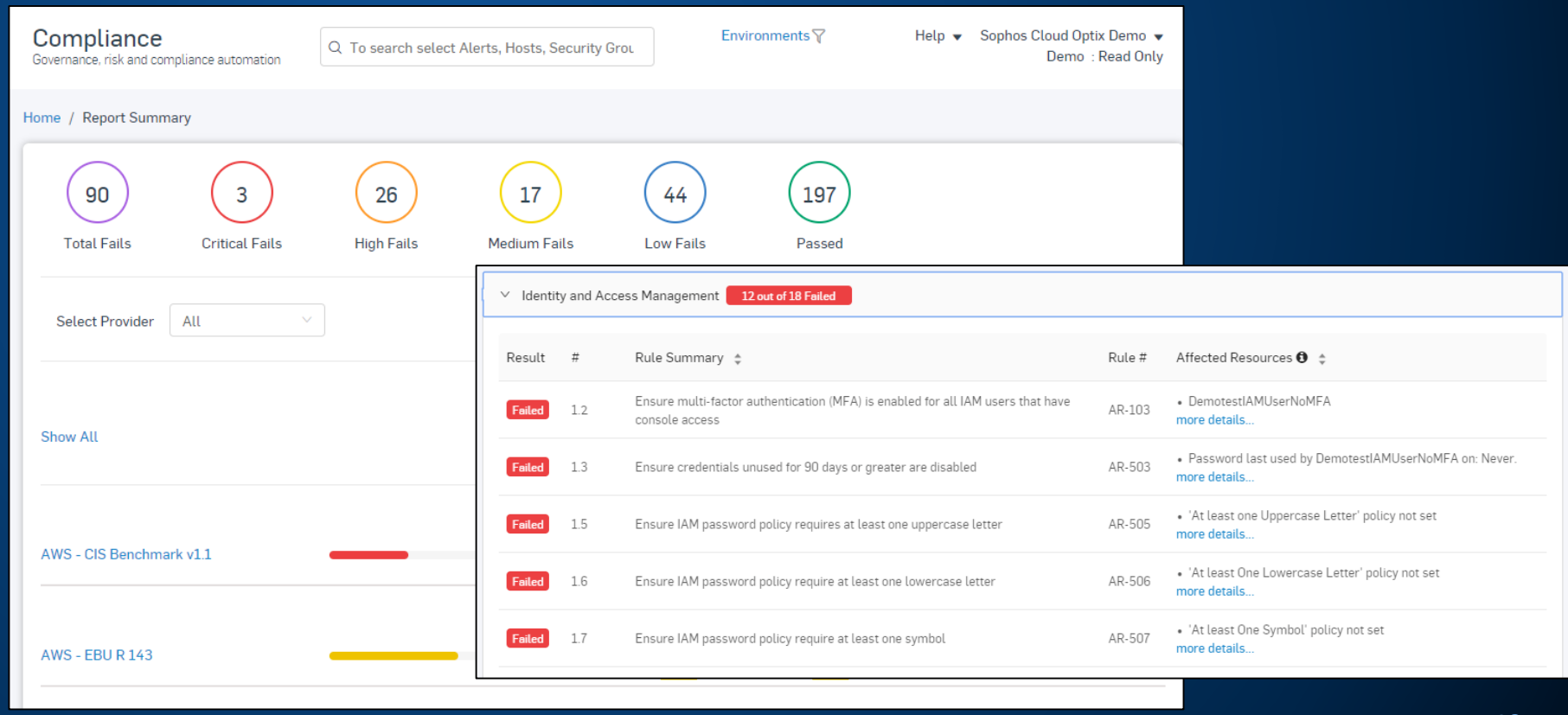
Intuicyjna konsola



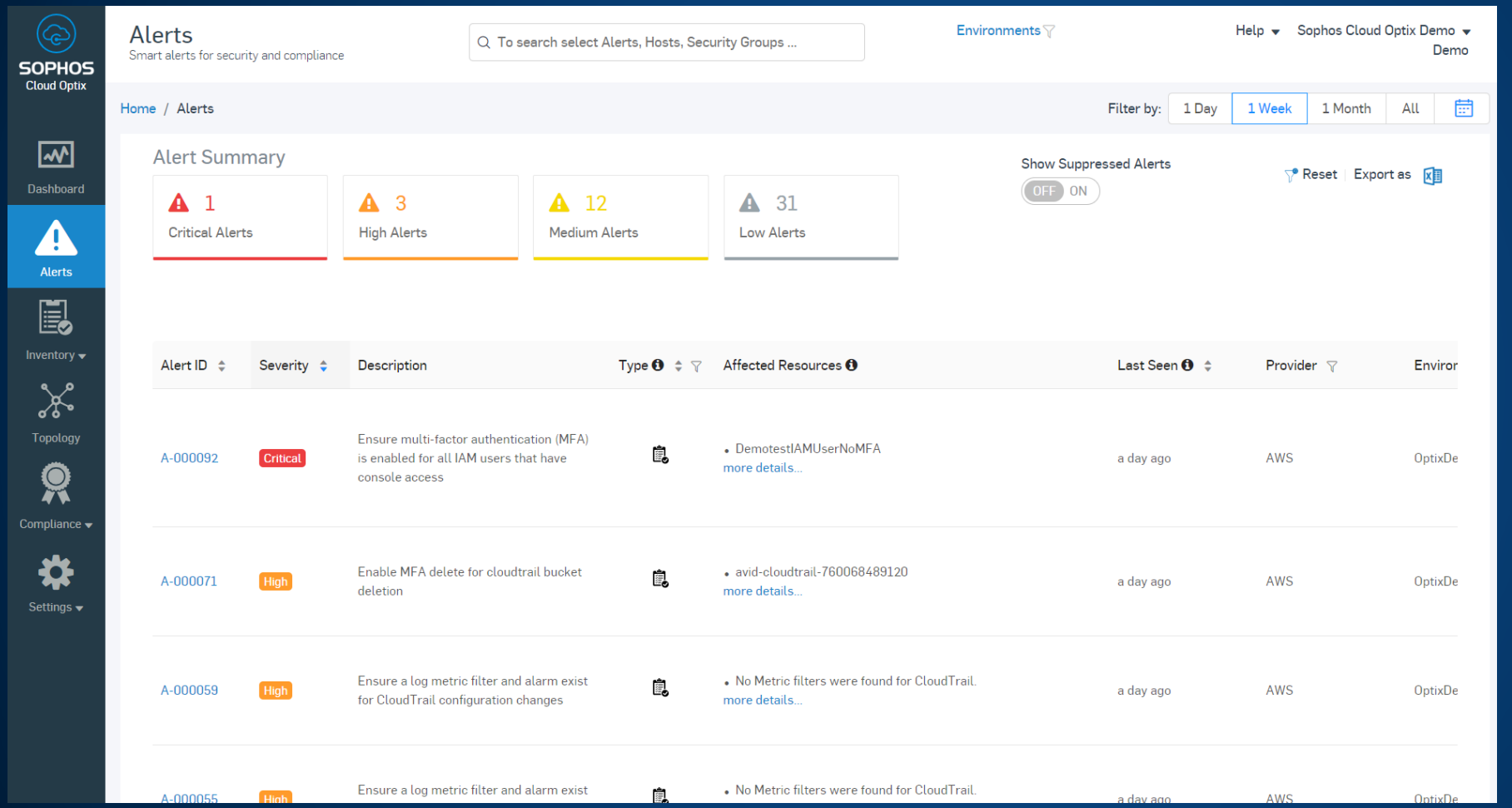
- Przegląd alarmów
- Status zgodności
- Raporty zgodności
- Inwentaryzacja
- Topologia sieci
- Prezentacja zmian

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
  - ...



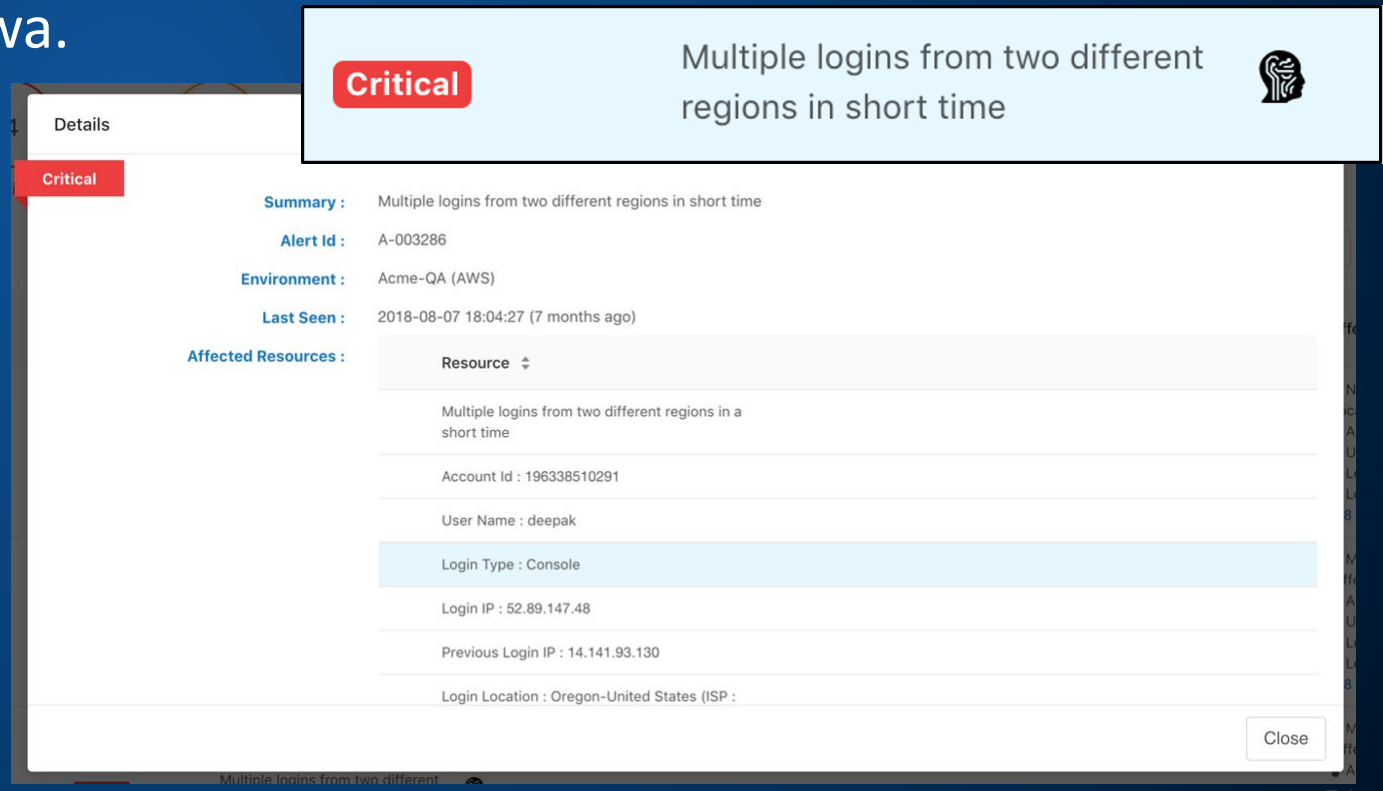
Ostrzeżenia i reakcje ze wsparciem AI



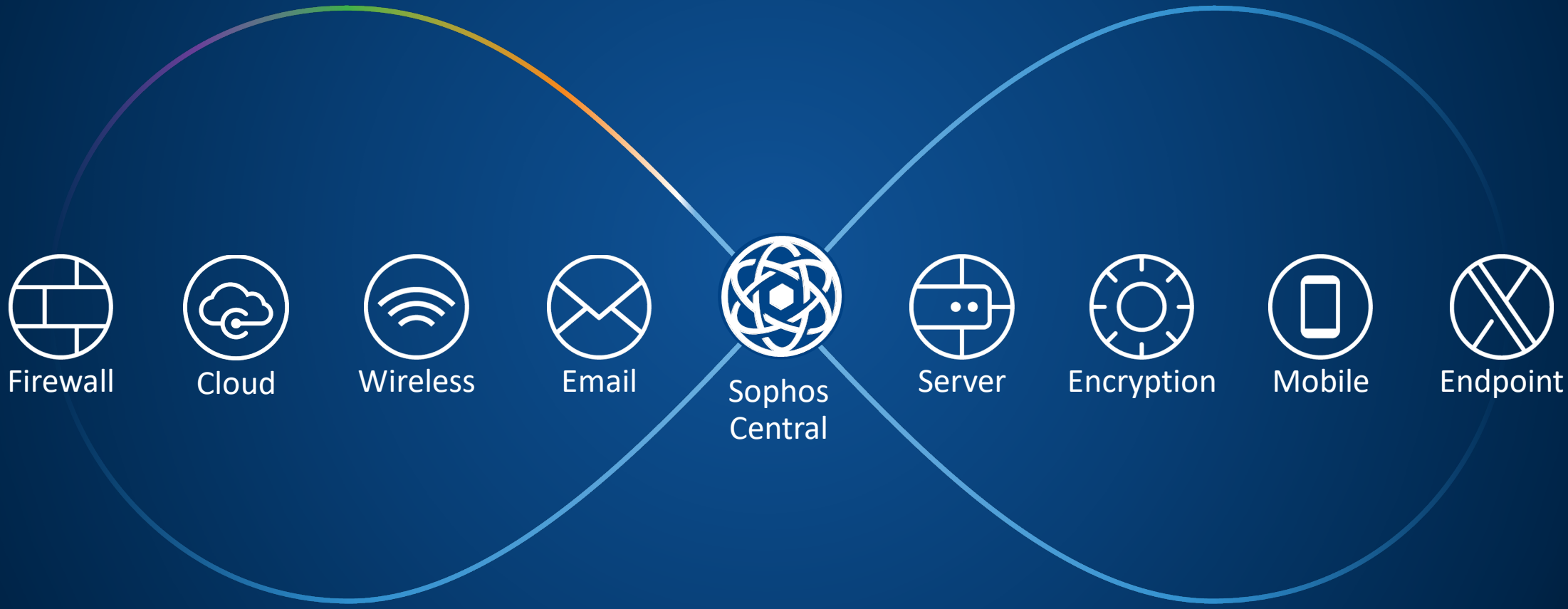
- Podejrzany ruch
- Przegląd infrastruktury jako szablonów kodu
- Identyfikuje wiele kluczy dostępu
- Zamyka otwarte porty
- Odkrywa odchylenie od normalnej konfiguracji
- Ustaw profilaktycznych „strażników”

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

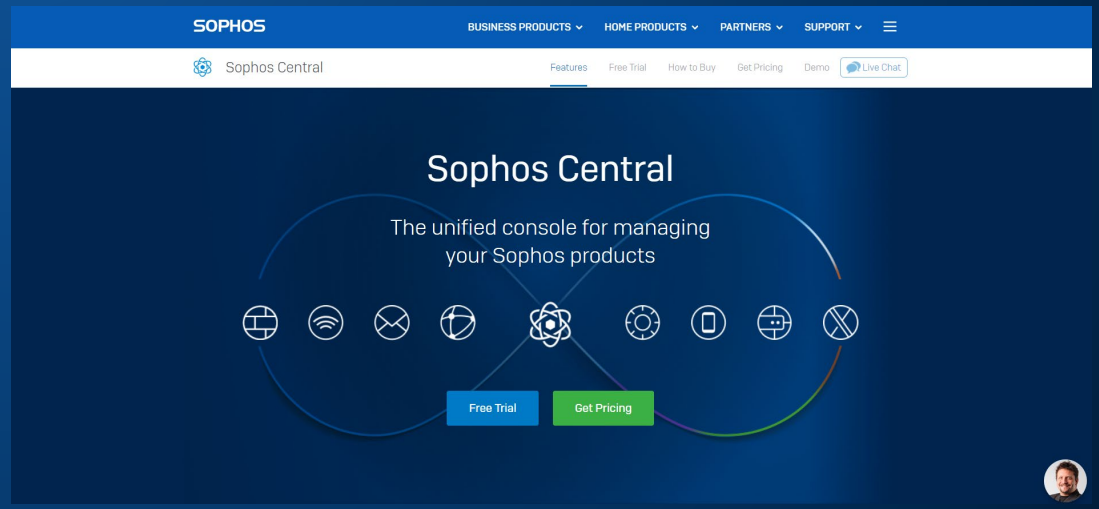


Sophos Central



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.