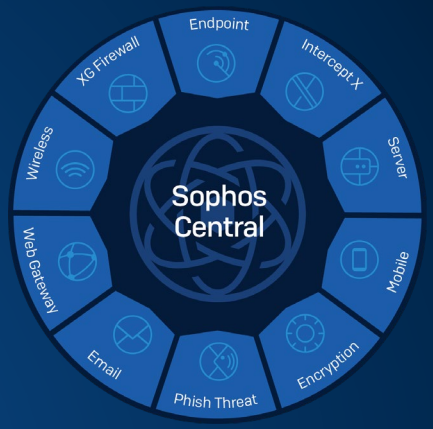
WEBINAR SERIES:

Bezpieczny wrzesień z Sophos Central

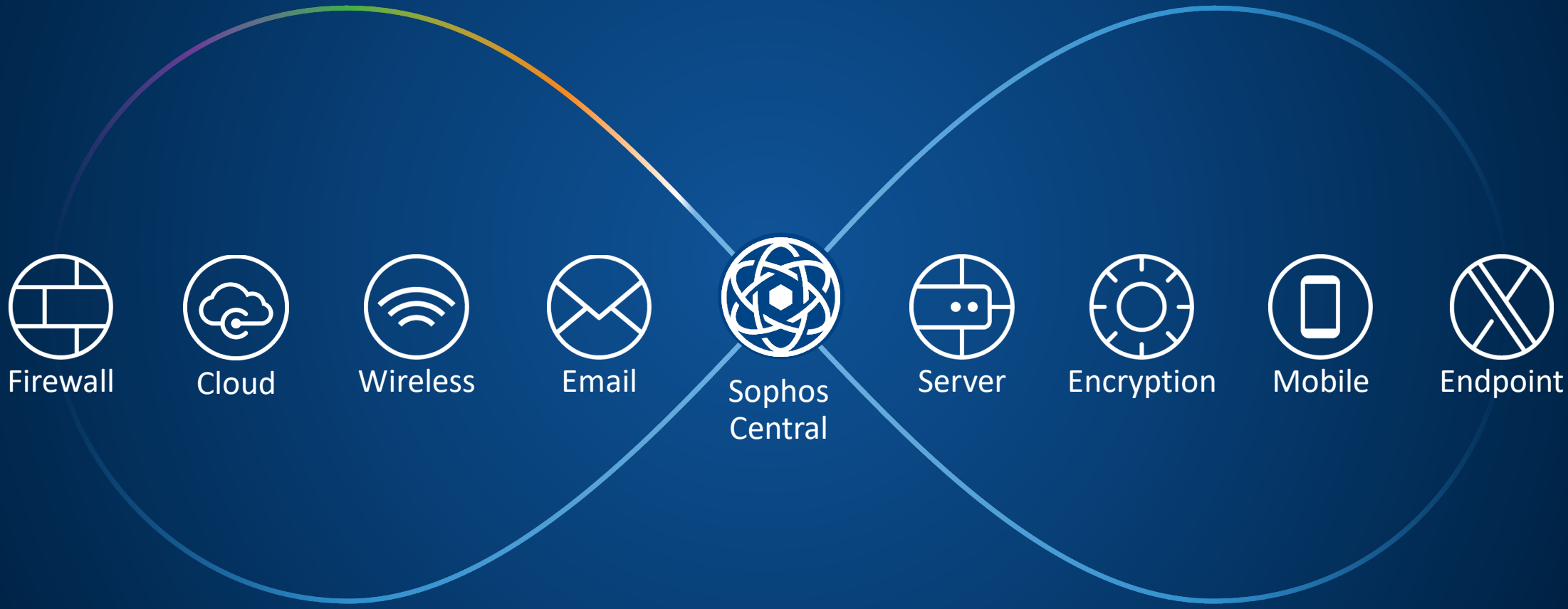


Sesja 1

Wprowadzenie do Sophos Central.
Centralna, intuicyjna konsola do zarządzania wszystkimi rozwiązaniami bezpieczeństwa (w tym Synchronized Security).

SOPHOS

Sophos Centralna Platforma



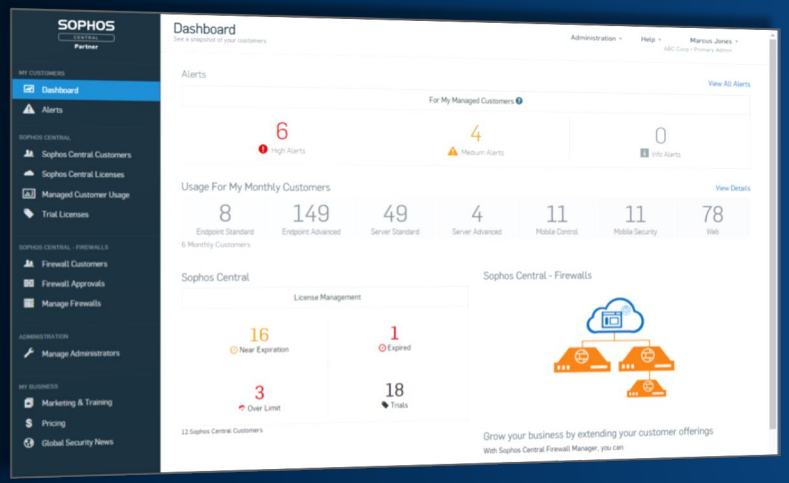
Sophos Centralna Platforma

Sophos Central - Przegląd

- Oparta o chmurę platforma zarządzająca całym środowiskiem bezpieczeństwa
- Zunifikowany interfejs użytkownika dedykowany dla wszystkich produktów
- Centralne zarządzanie wszystkimi użytkownikami, urządzeniami i politykami bezpieczeństwa
- Centralne rejestrowanie i raportowanie oraz analiza zdarzeń
- Bezpieczeństwo oparte o Sophos Synchronized Security. Komponenty bezpieczeństwa działają jak system i automatycznie reagują na zagrożenia wewnątrz sieci

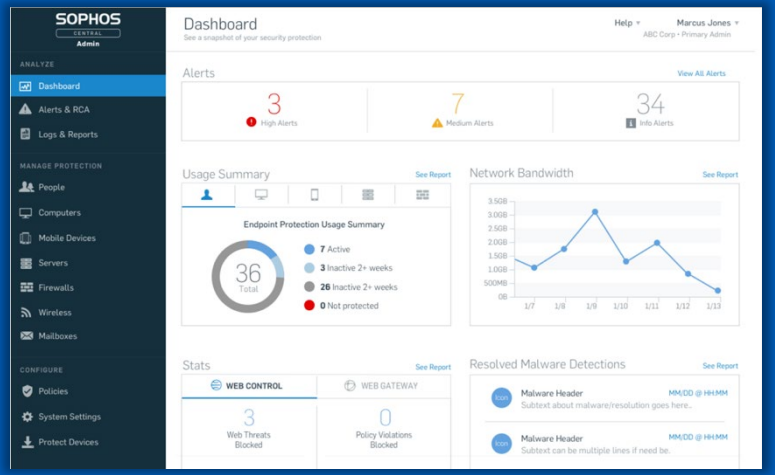
Sophos Central - zarządzanie

Partner Dashboard



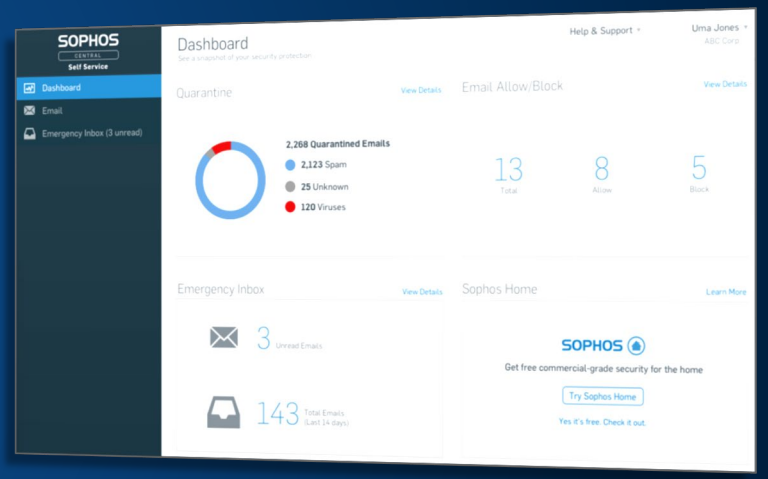
Pozwala partnerom na zarządzanie środowiskiem klientów

Admin



- Endpoint
- Mobile
- Server
- Encryption
- Cloud Optix
- Wireless
- Phish Threat
- Email Security
- XG Firewall

Self Service

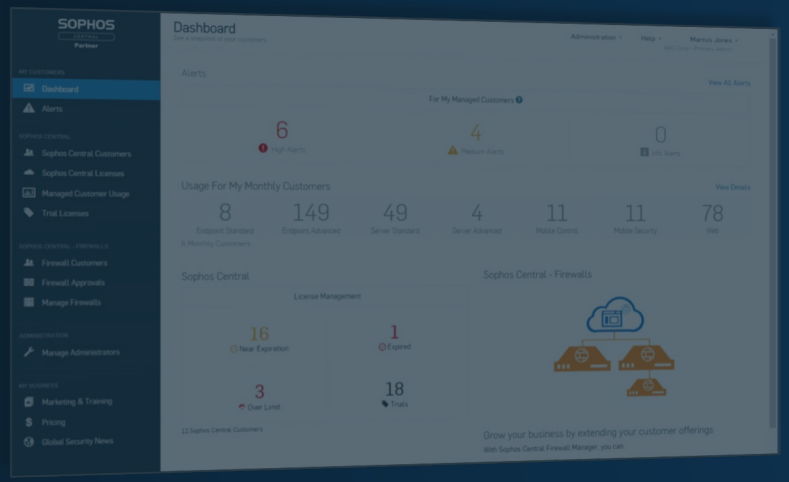


Pozwala użytkownikom na dostęp do ich poczty, rejestrować urządzenia mobilne i zarządzać dostępem do stacji

SOPHOS

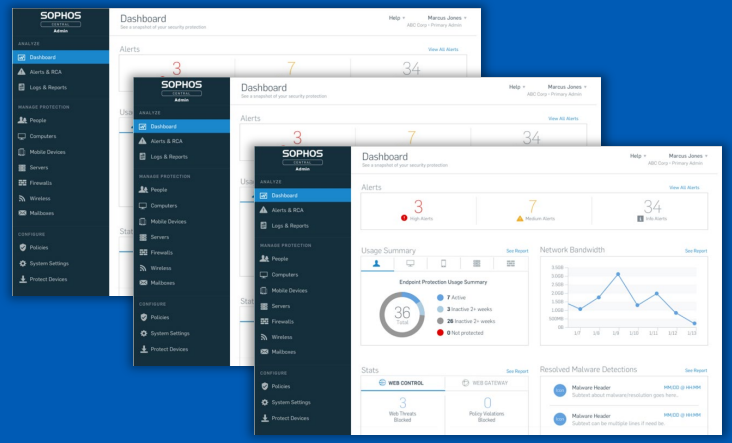
Sophos Central - Management

Partner Dashboard



Pozwala partnerom na zarządzanie środowiskiem klientów

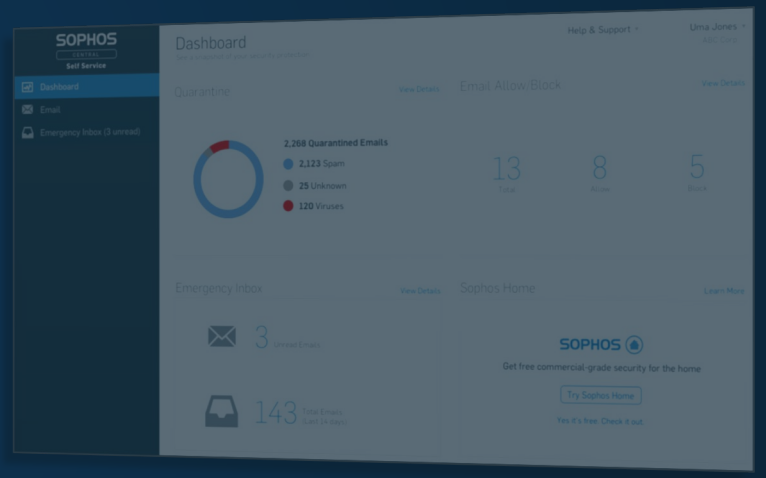
Enterprise Dashboard



Enterprise Console

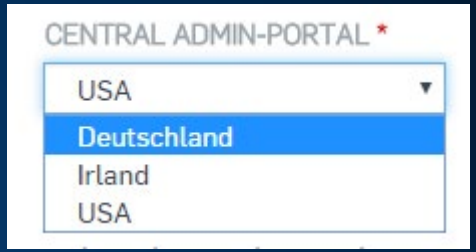
- Single dashboard for multiple sub-estates
- Aggregated alerts
- Immediate remediation
- Single license pool

Self Service



Pozwala użytkownikom na dostęp do ich poczty, rejestrować urządzenia mobilne i zarządzać dostępem do stacji

Sophos Central Datacenter



- Sophos Central używa Amazon Web Services
- Central przechowuje metadane: nazwy komputerów, użytkowników, etc.
- W platformie Central nie przechowujemy haseł użytkowników oraz nieporządzanych plikó
- W chwili tworzenia konta, szyfrowana przestrzeń nie ulega zmianie
  - USA lub Irlandia (Dublin) lub Niemcy (Frankfurt)
- Amazon w różnych lokalizacjach używa różnych polityk bezpieczeństwa: np. Frankfurt
- Sophos Central Security Framework
  http://docs.sophos.com/central/Framework/security-framework/index.html
- Możliwość podpisania umowy o zachowaniu poufności

https://sophoslegal.na1.echosign.com/public/esignWidget?wid=CBFCIBAA3AAABLblqZhBQCgIMyN2K3xr5AyZWgZ-COf4FpVYN_-ksFT62r1H4SikgibGXkdYMDcFWfzywo1s*

Zaawansowane ustawienia

- Wielo-składnikowa autoryzacja
- Update caches oraz message relays
- Synchronizacja z usługą katalogową AD
- Zarządzanie rolami administracyjnymi
- SIEM API
- Azure AD Federated Sign In
- Enterprise Dashboard
  - Zarządzanie wieloma lokalizacjami przy pomocy centralnej platformy
  - Centralne zarządzanie alarmami
  - Lokalny i globalny administrator
  - Globalne szablony konfiguracyjne

Licencjonowanie – sposób liczenia licencji

Typ licencji	Licencja na:
Endpoint/Intercept X/Device Encryption	
Mobile	
Wireless	
Server/Intercept X	
Terminal Server	
Virtual Environments - Server - Clients	
PhishThreat	

Sophos Central – wartości dodane

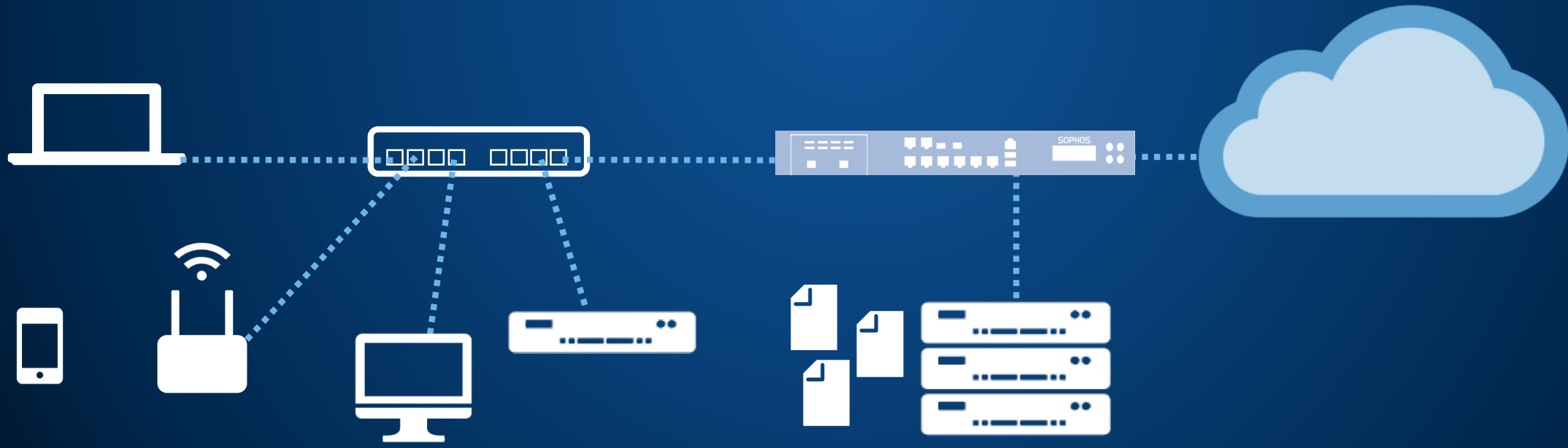
- Jedna konsola dla pełnego bezpieczeństwa (zarządzanie, raportowanie)
- Nie wymaga własnej infrastruktury
- Szybkie wdrożenie mechanizmów bezpieczeństwa – dla wszystkich urządzeń i użytkowników
- Prosty outsourcing
- Możliwe różne sposoby opłaty za licencję
  - Standardowa subskrypcja
  - Opłata miesięczna za licencję (via MSP with Flex Partner Status)
  - Specjalna oferta dla sektoru edukcji i organizacji publicznych
- Podstawowy element Synchronized Security

Dlaczego potrzebujemy Synchronized Security?

SOPHOS

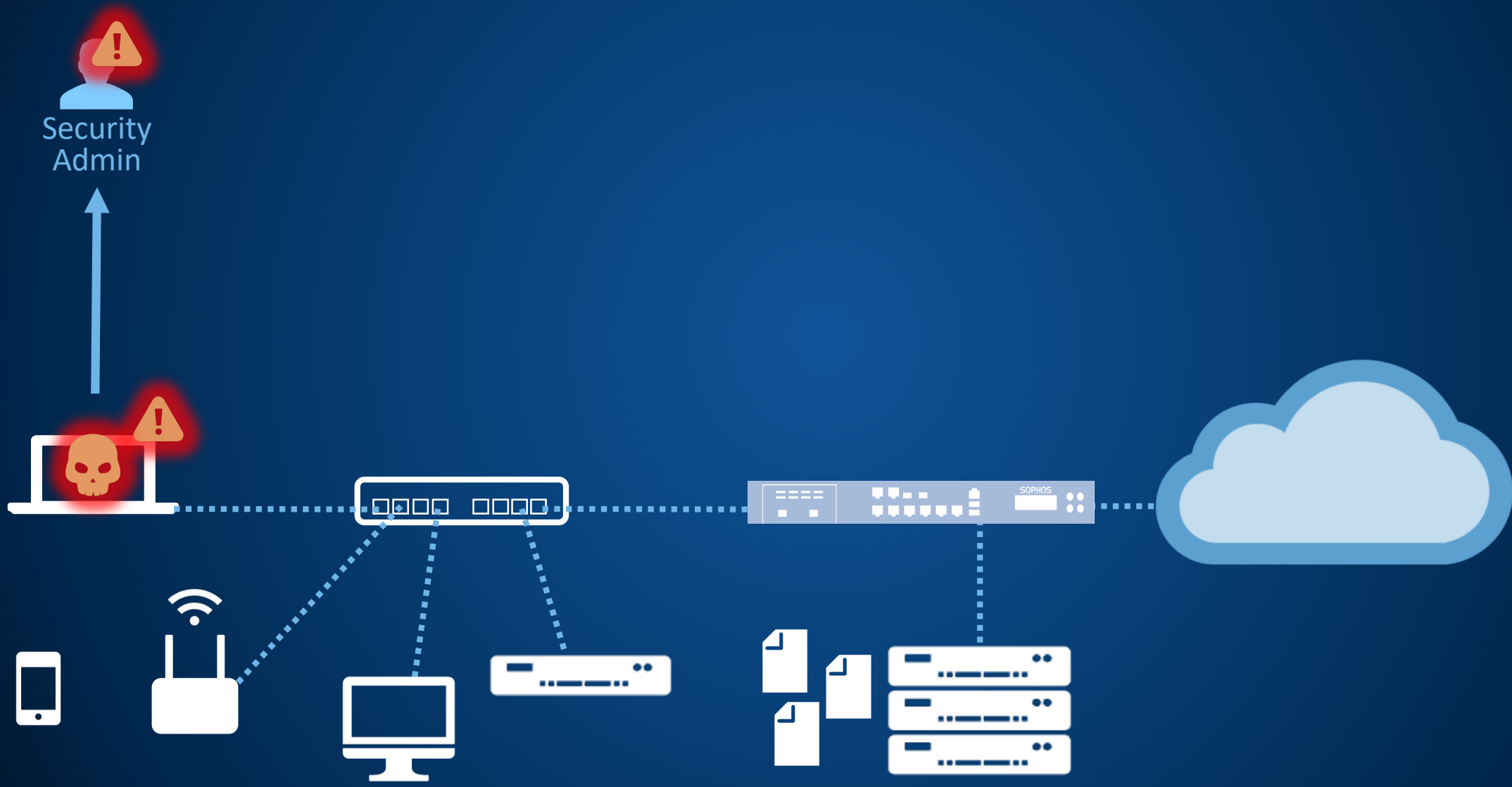

IN CASE OF
CYBERATTACK
BREAK GLASS
AND PULL CABLES

Zarządzanie incydentami bez Synchronized Security



SOPHOS

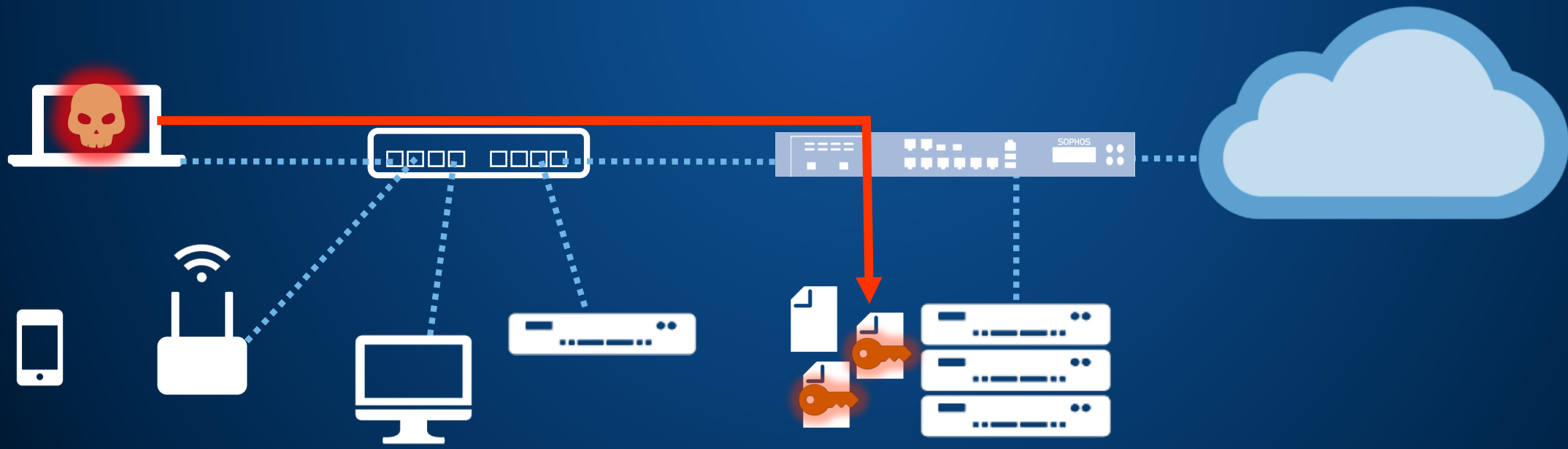
Zagrożenie zostaje rozpoznane



.. i analiza

Security Admin

Pliki na serwerze zostały zaszyfrowane

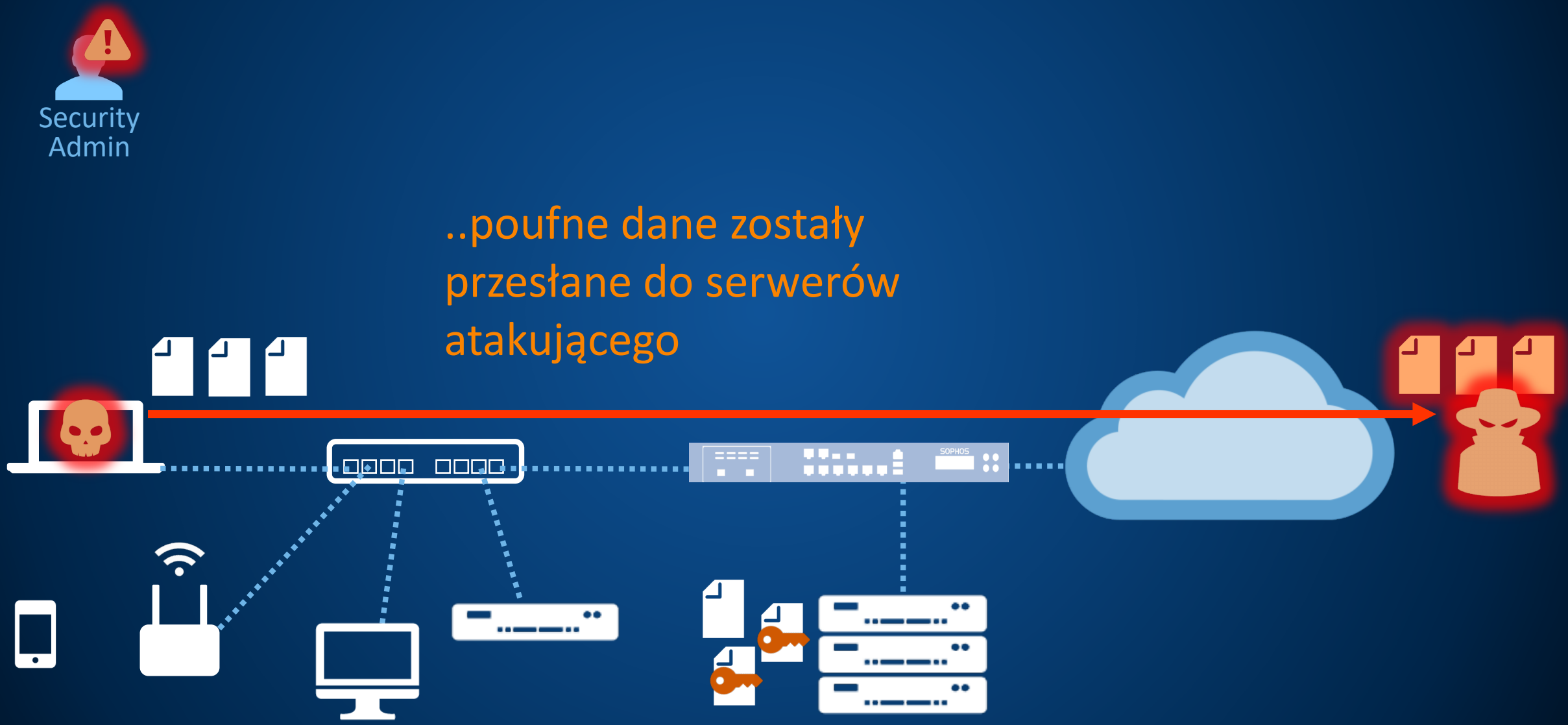


SOPHOS

.. i analiza

Security Admin

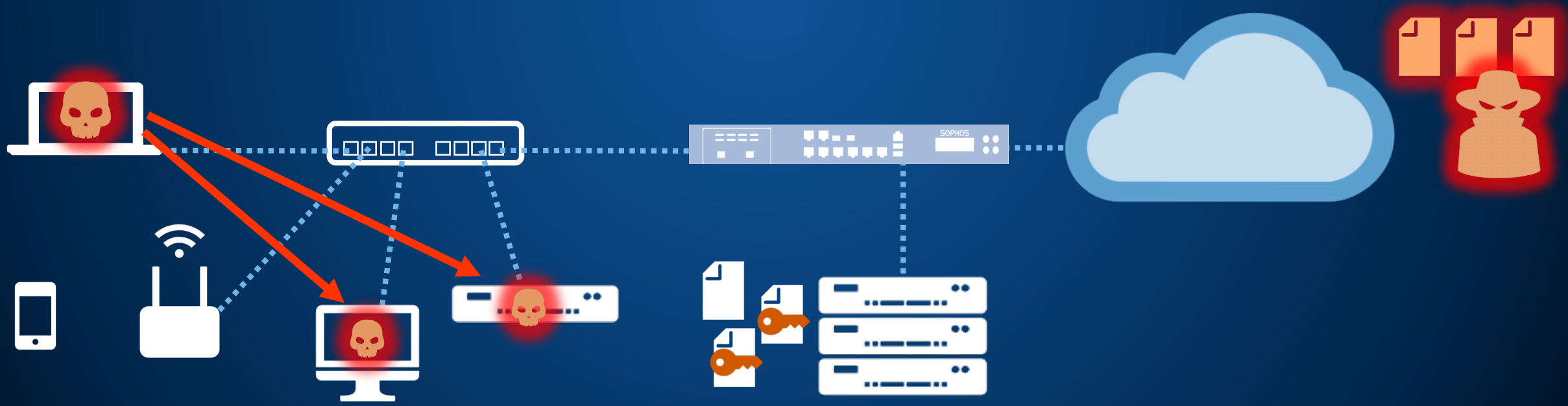
..poufne dane zostały przesłane do serwerów atakującego



.. i analiza

Security Admin

.. pozostałe stacje i serwery zostały zainfekowane



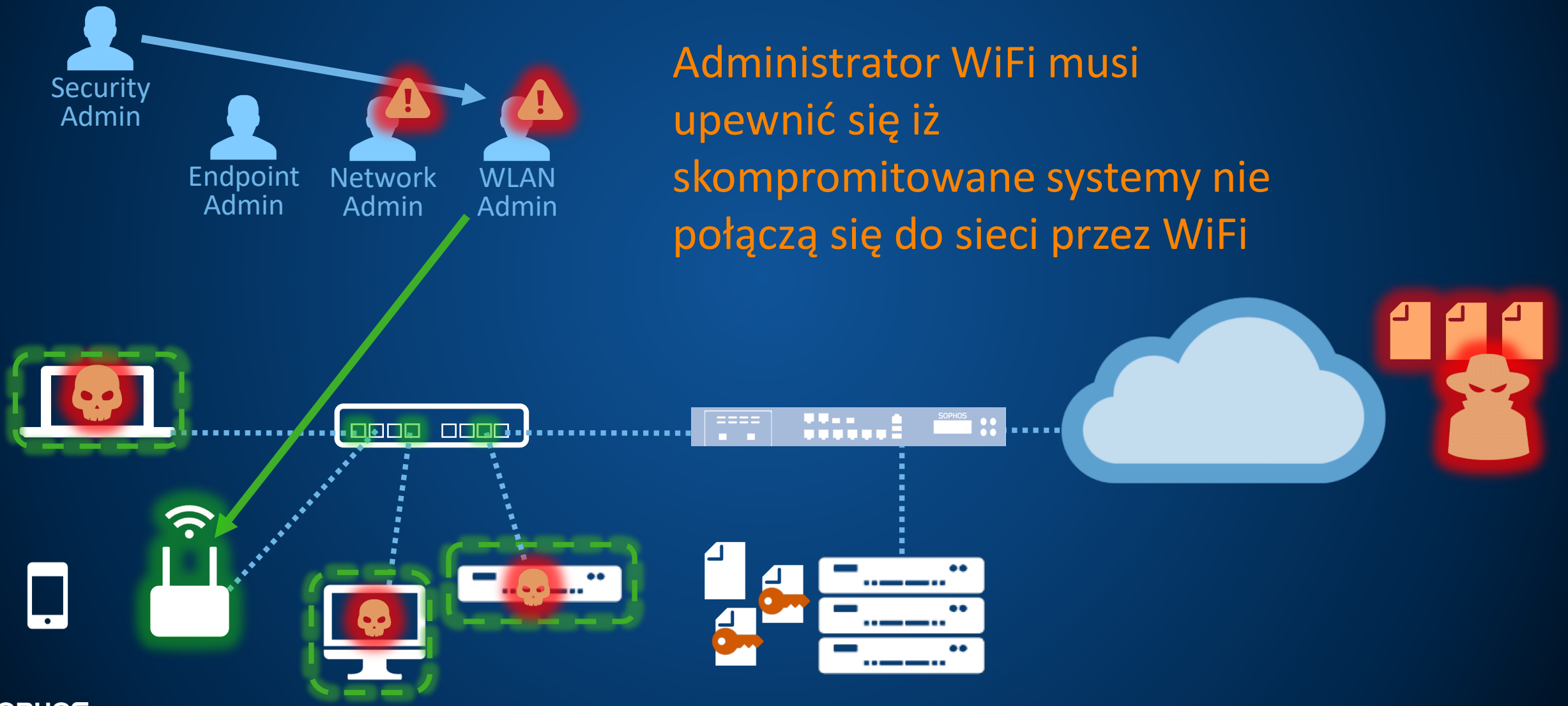
Akcja!!!


Security Admin
Endpoint Admin
Administrator musi odszukać zainfekowane systemy
SOPHOS

Akcja!!!

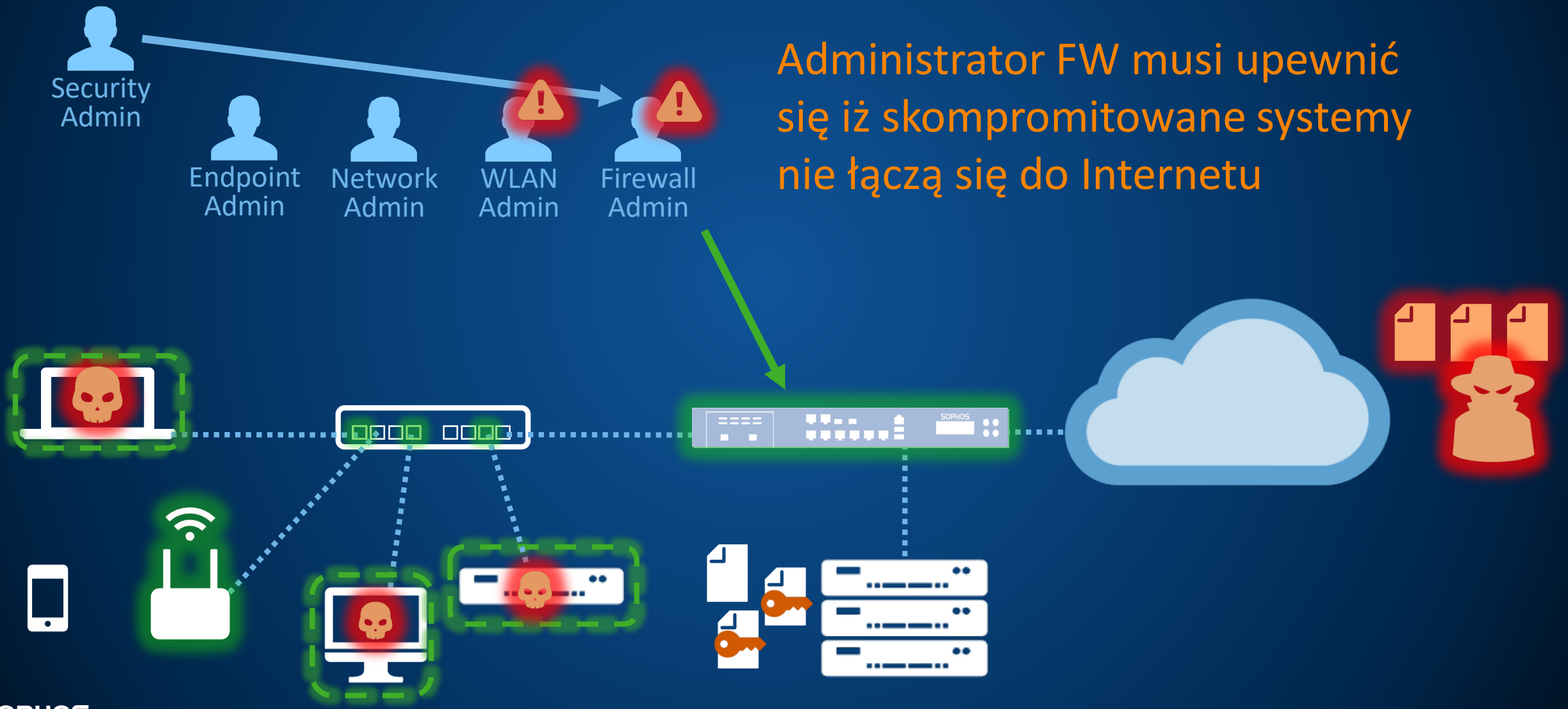

Security Admin
Endpoint Admin
Network Admin
Administrator musi zablokować komunikacje dla skompromitowanych stacji
SOPHOS

Akcja!!!

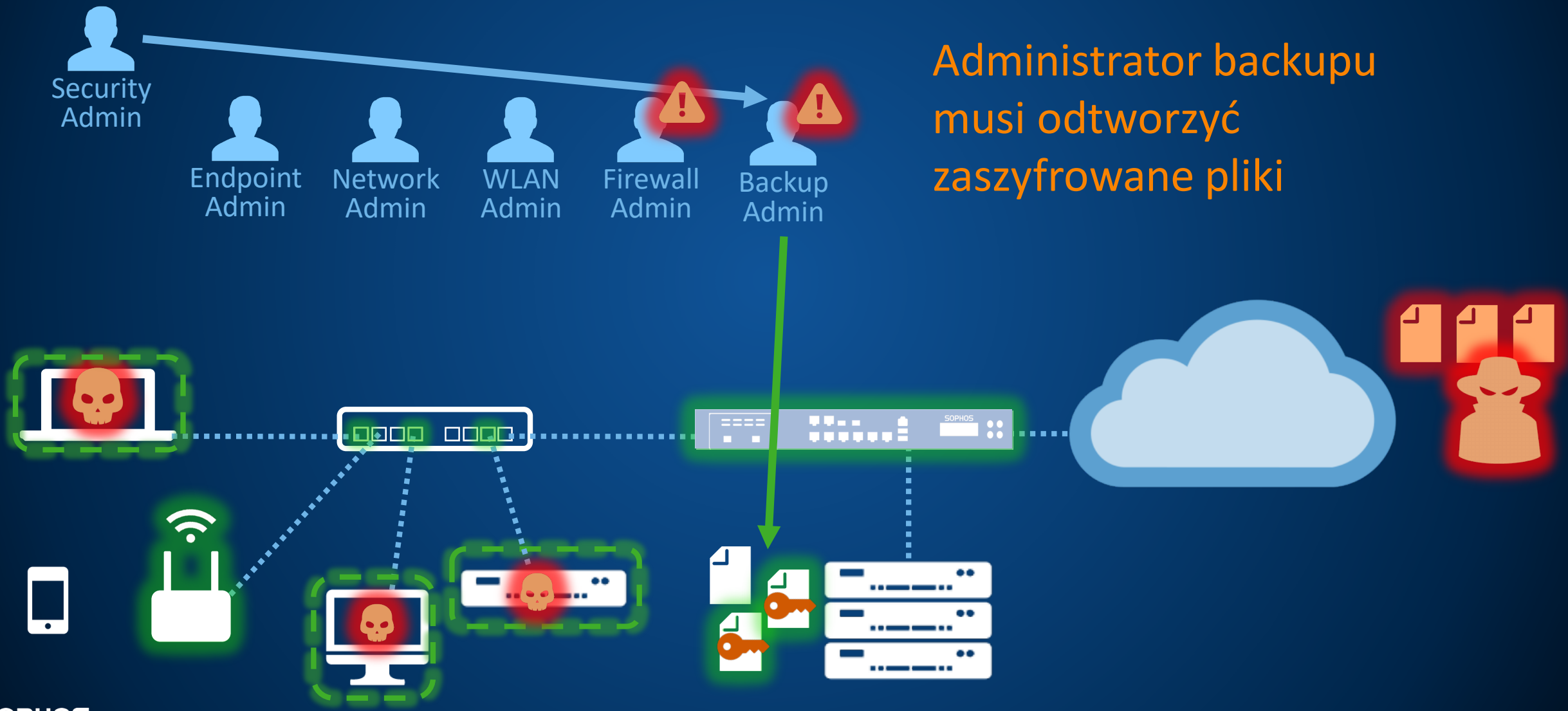


Administrator WiFi musi upewnić się iż skompromitowane systemy nie połączą się do sieci przez WiFi

Akcja!!!

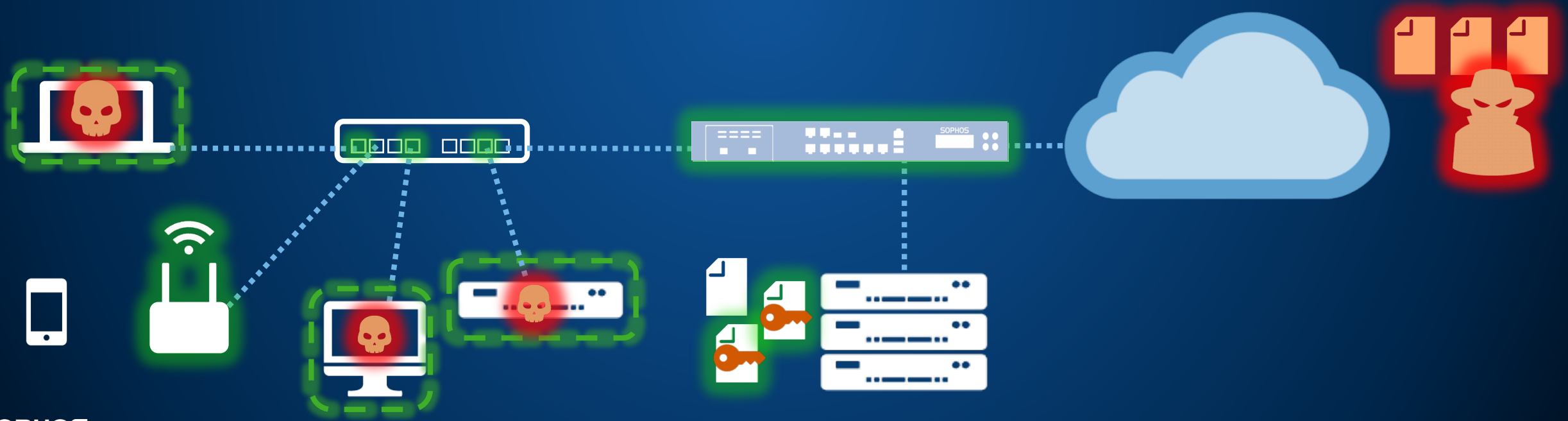

Security Admin
Endpoint Admin
Network Admin
WLAN Admin
Firewall Admin
Administrator FW musi upewnić się iż skompromitowane systemy nie łączą się do Internetu
SOPHOS

Akcja!!!


Security Admin
Endpoint Admin
Network Admin
WLAN Admin
Firewall Admin
Backup Admin
Administrator backupu musi odtworzyć zaszyfrowane pliki
SOPHOS

Akcja!!!

Właśnie został poinformowany CISO



Akcja!!!

Security Admin

Endpoint Admin

Network Admin

WLAN Admin

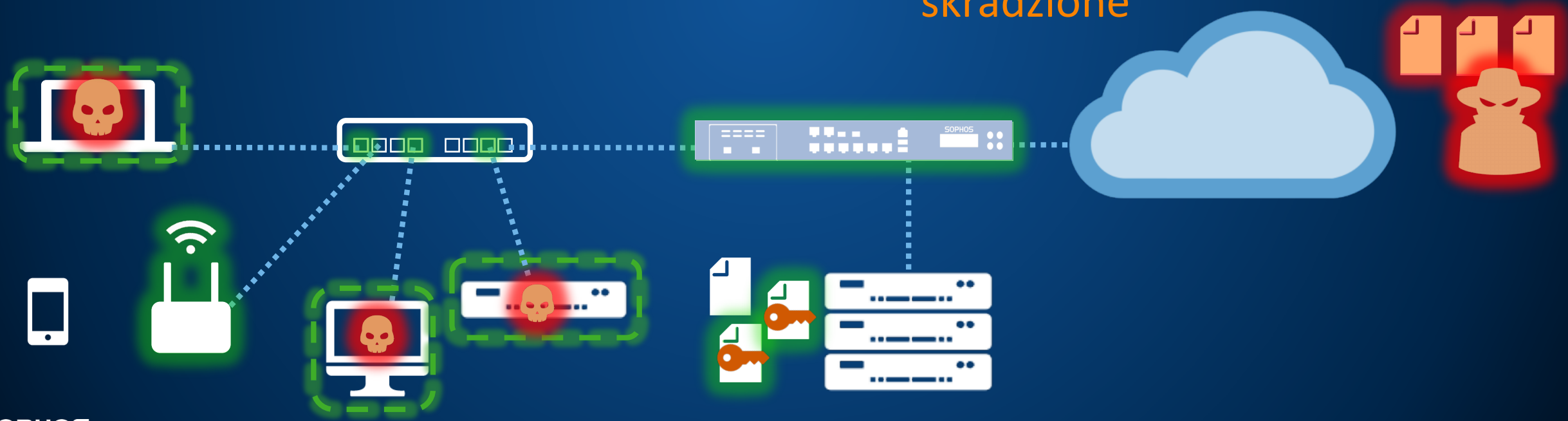
Firewall Admin

Backup Admin

CISO

CEO

.. I na końcu manager dowiaduje się iż dane zostały skradzione



Procedura na wypadek incydentu

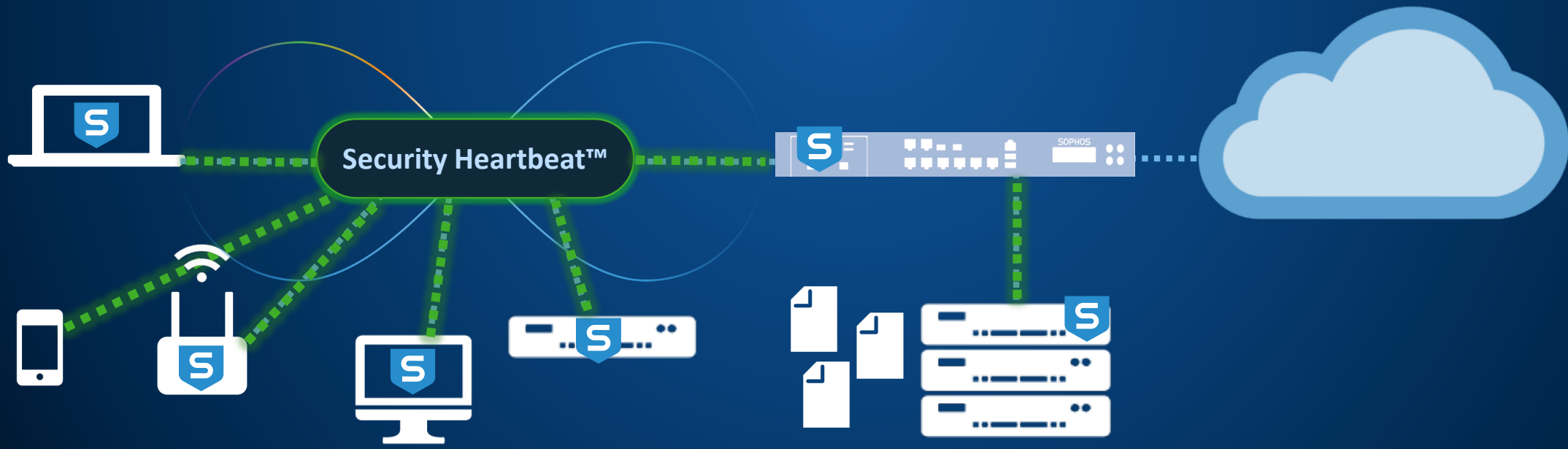
z

Synchronized Security

SOPHOS

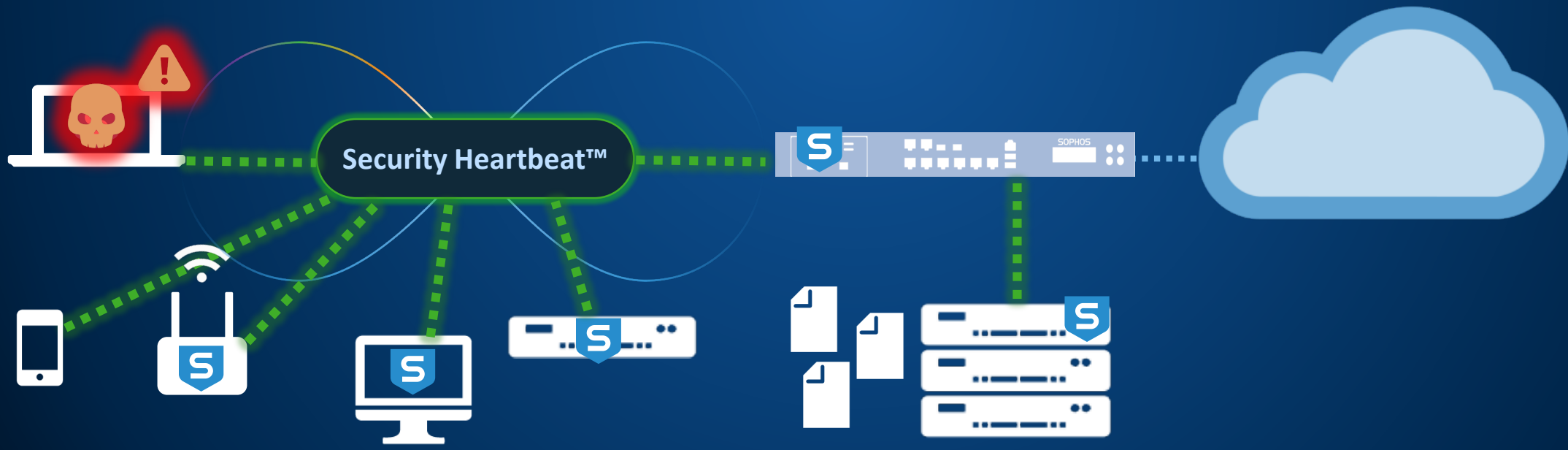
Rozwiązywanie problemów z zagrożeniamu przy uzyciu Synchronized Security

Stacje, serwery, urządzenia mobilne,
WiFi i Firewall komunikują się
bezpośrednio przy pomocy
SecurityHeartbeat



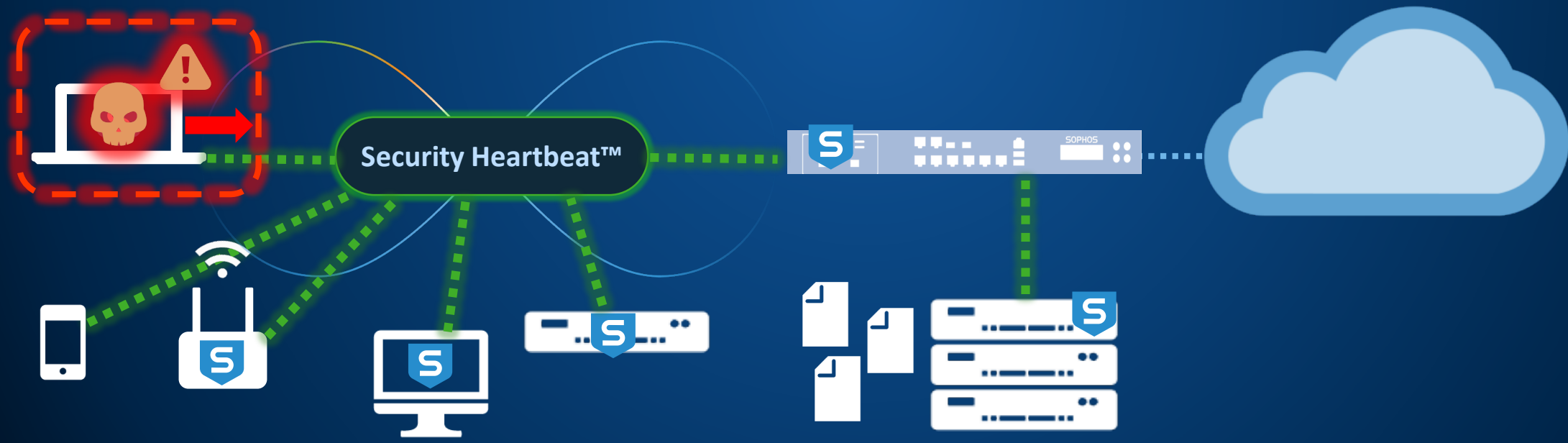
Rozwiązywanie problemów z zagrożeniami przy uzyciu Synchronized Security

Na wypadek zdarzenia wszystkie komponenty są informowane o incydencie



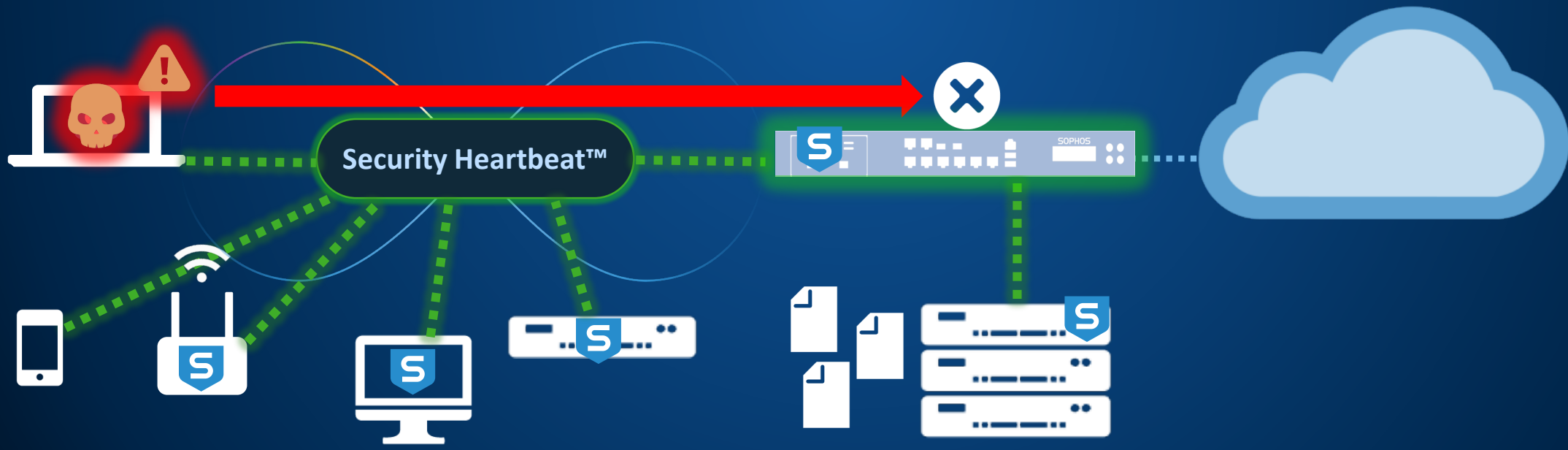
Rozwiązywanie problemów z zagrożeniami przy uzyciu Synchronized Security

Klient dokonuje samo-izolacji



Rozwiązywanie problemów z zagrożeniami przy uzyciu Synchronized Security

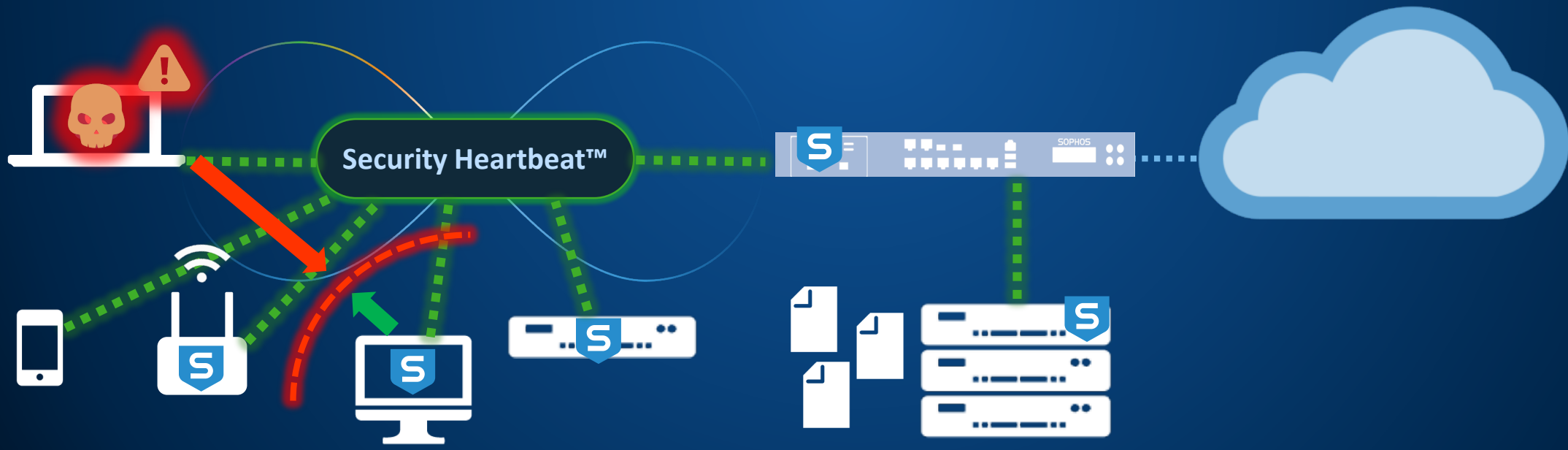
Firewall blokuje komunikacje dla stacji aby zapobiec rozprzestrzenieniu się infekacji



SOPHOS

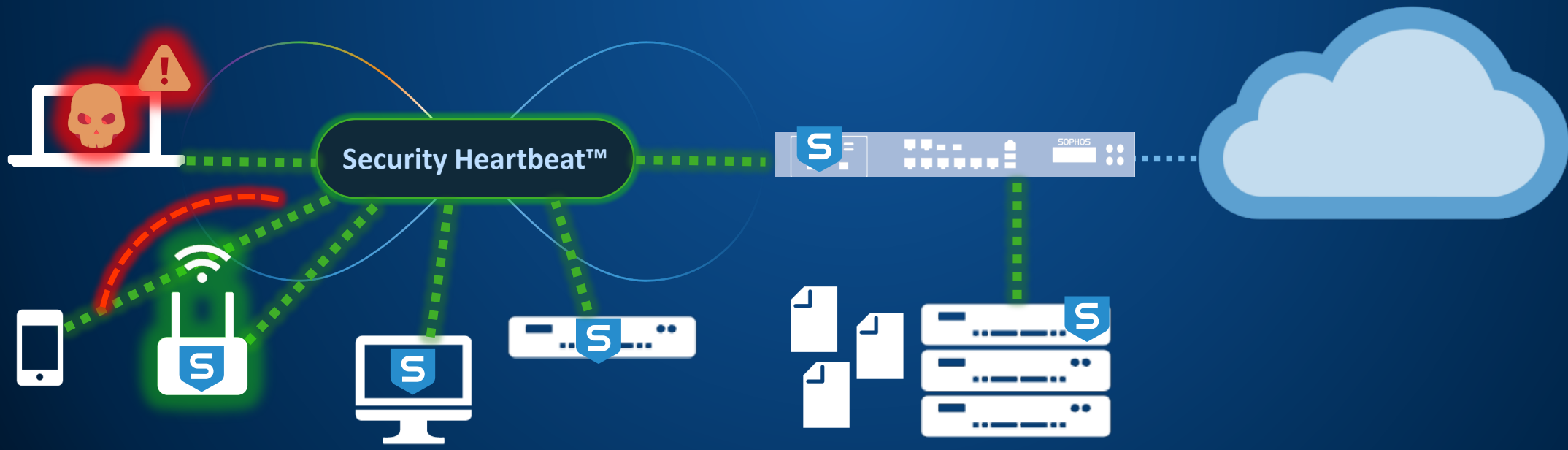
Rozwiązywanie problemów z zagrożeniami przy uzyciu Synchronized Security

Na stacjach w ramach tej samej domeny broadcastowej następuje blokada połączeń do zainfekowanego systemu



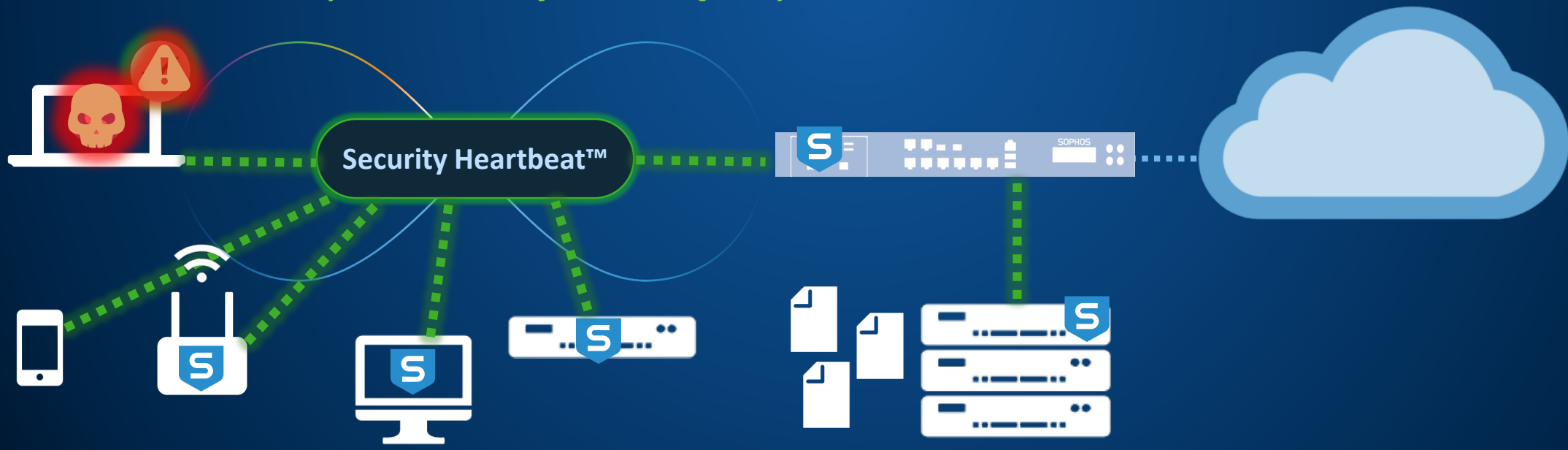
Rozwiązywanie problemów z zagrożeniami przy uzyciu Synchronized Security

AP WiFi blokuje komunikacje
dla zainfekowanej stacji

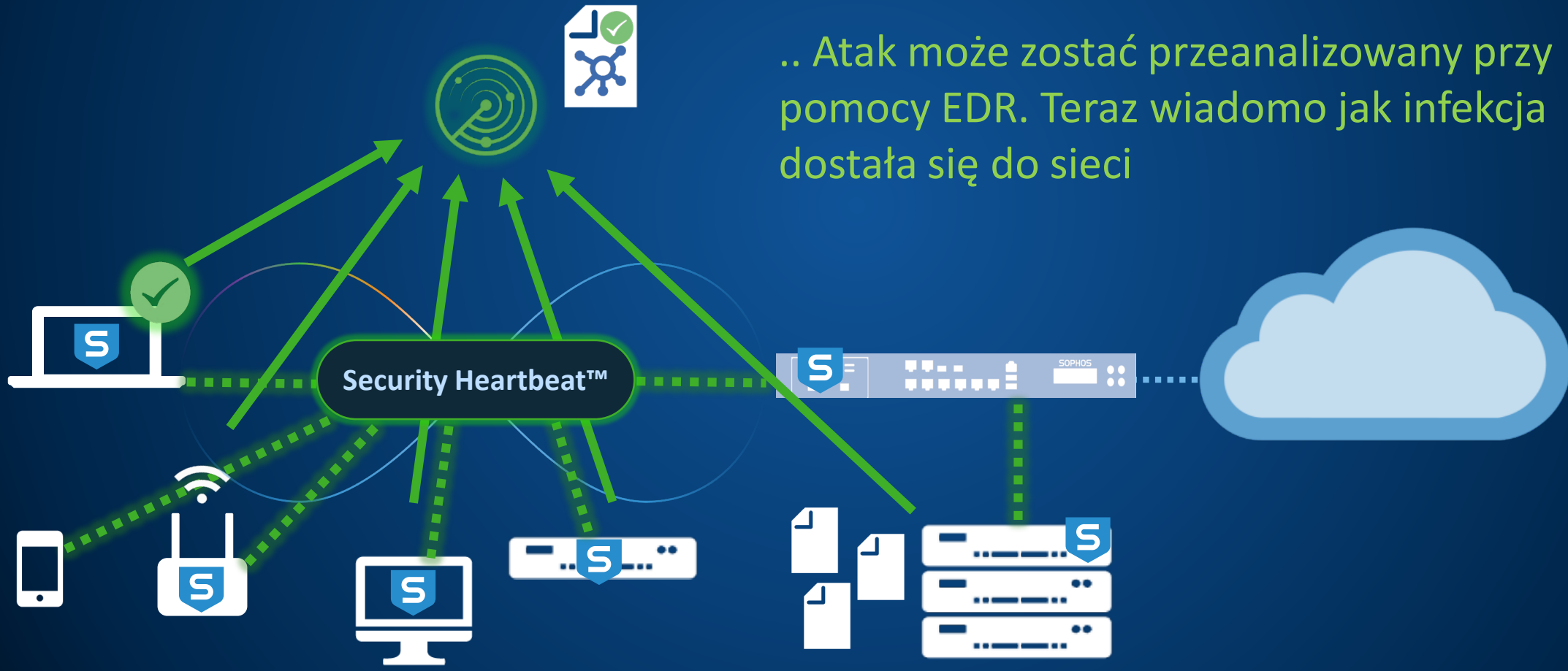


Rozwiązywanie problemów z zagrożeniami przy uzyciu Synchronized Security

..Incydent zostaje rozwiązany..

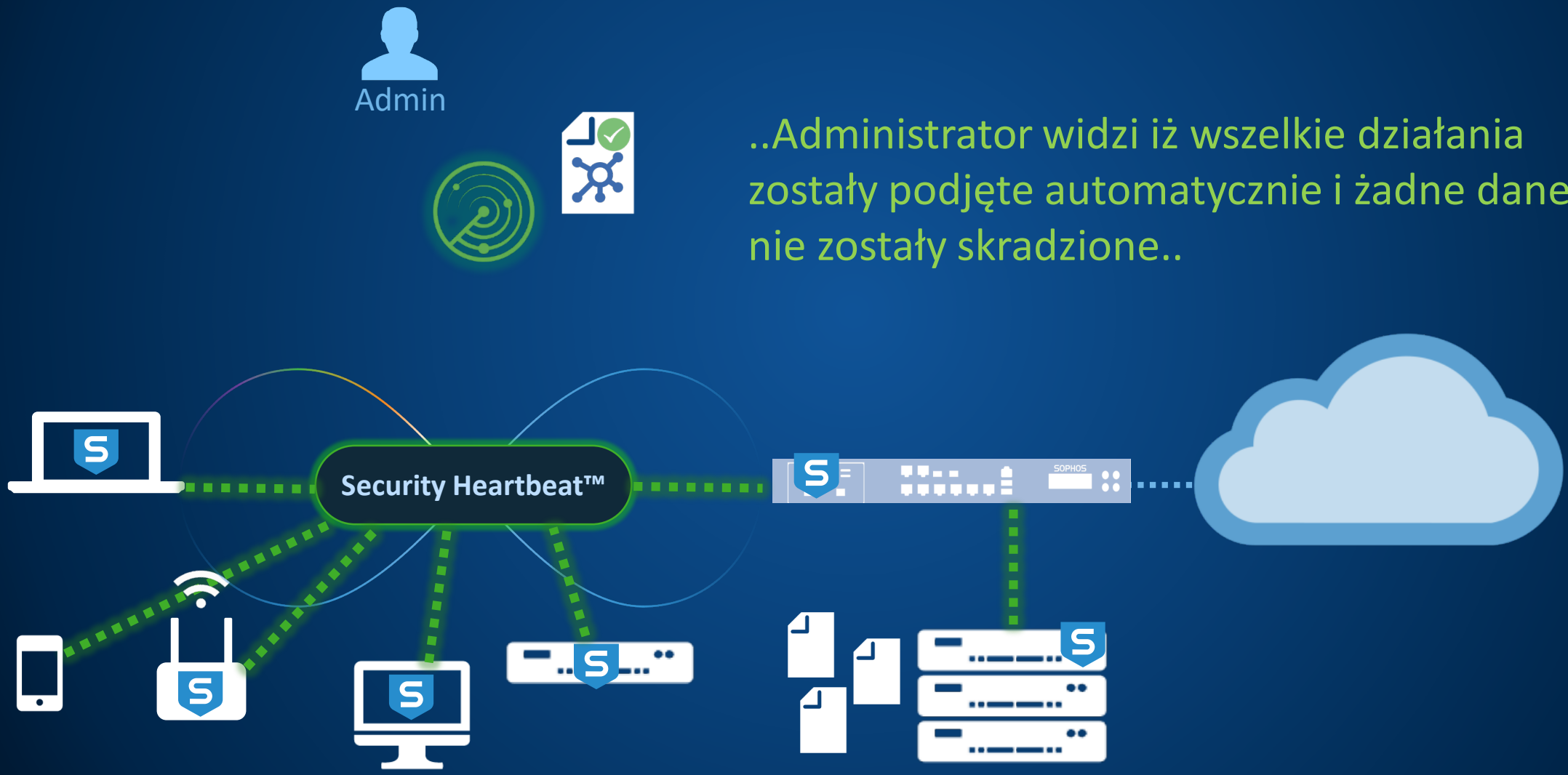


Rozwiązywanie problemów z zagrożeniami przy uzyciu Synchronized Security



.. Atak może zostać przeanalizowany przy pomocy EDR. Teraz wiadomo jak infekcja dostała się do sieci

Rozwiązywanie problemów z zagrożeniami przy uzyciu Synchronized Security



..Administrator widzi iż wszelkie działania zostały podjęte automatycznie i żadne dane nie zostały skradzione..

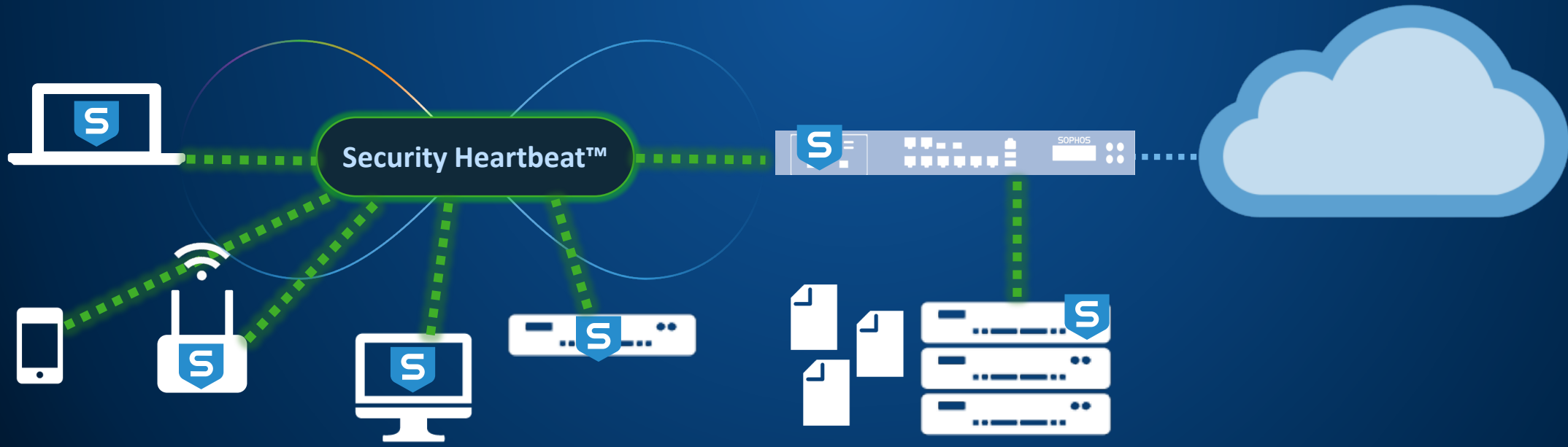
SOPHOS

Rozwiązywanie problemów z zagrożeniami przy uzyciu Synchronized Security

Admin

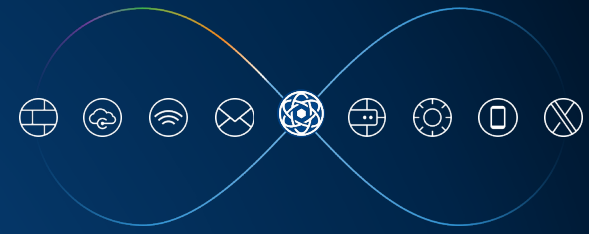
CEO

..a szef jest usatysfakcjonowany iż dział bezpieczeństwa działa należycie.



SOPHOS

Synchronized Security - koncepcja

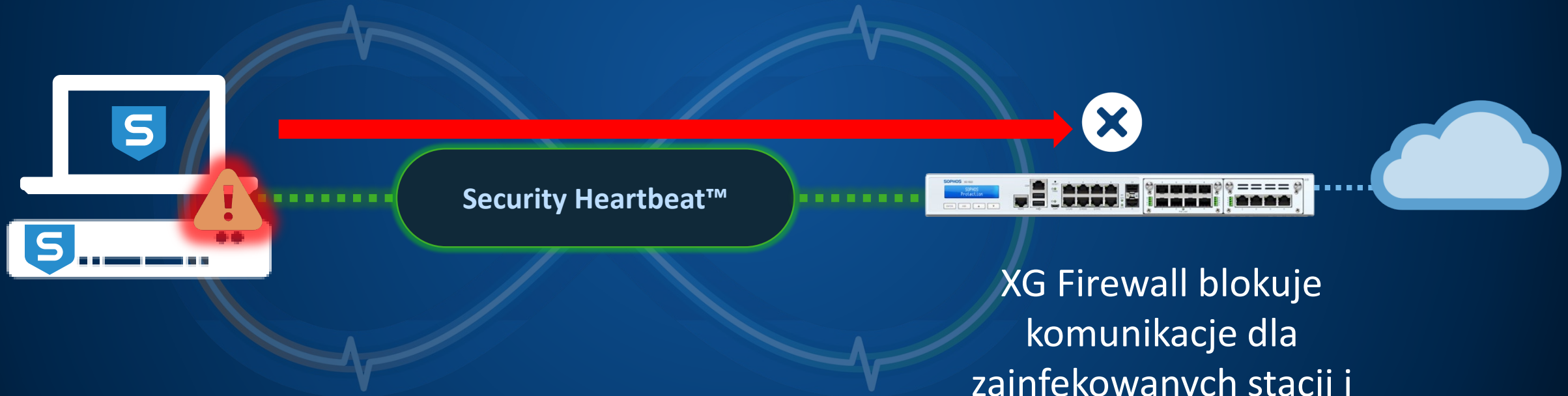


- Komponenty bezpieczeństwa (firewall i endpoint) działają jako system
- Komponenty wymieniają się informacjami
  - Status bezpieczeństwa
  - Ruchem aplikacji
  - użytkownikiem
- Cele:
  - Lepsza detekcja zagrożeń i aktywności hakerów
  - Automatyczna eliminacja zagrożeń
  - Ochrona krytycznych danych
  - Lepsza widoczność ruchu aplikacji

Synchronized Security wszystkie komponenty z XG Firewall-em

SOPHOS

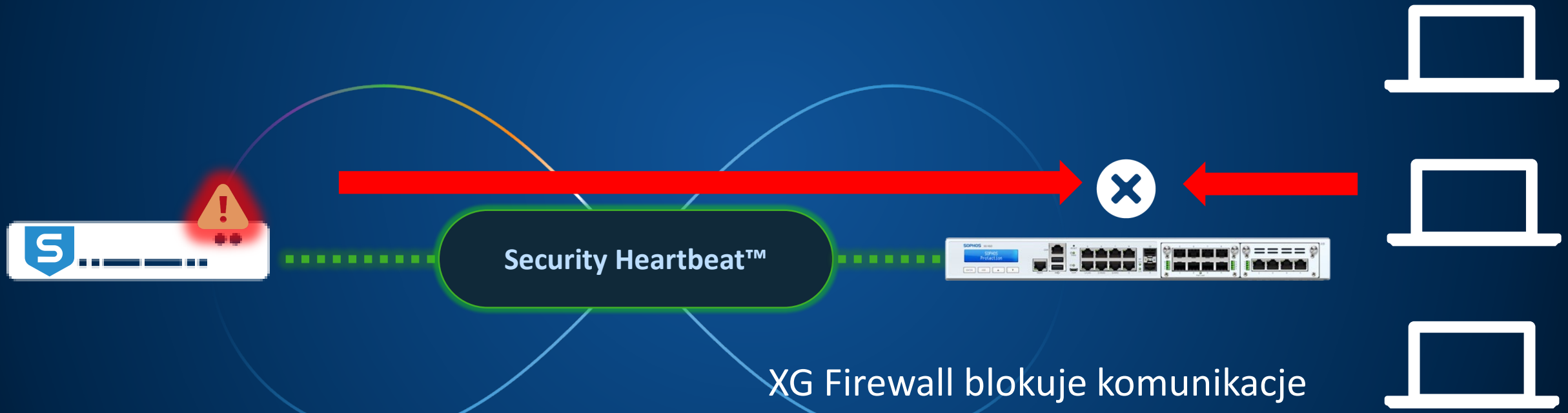
Security Heartbeat – Automatyczna kwarantanna



XG Firewall blokuje komunikacje dla zainfekowanych stacji i serwerów

Security Heartbeat – wykrywanie ruchu Botnet C&C

Security Heartbeat – Serwer Heartbeat

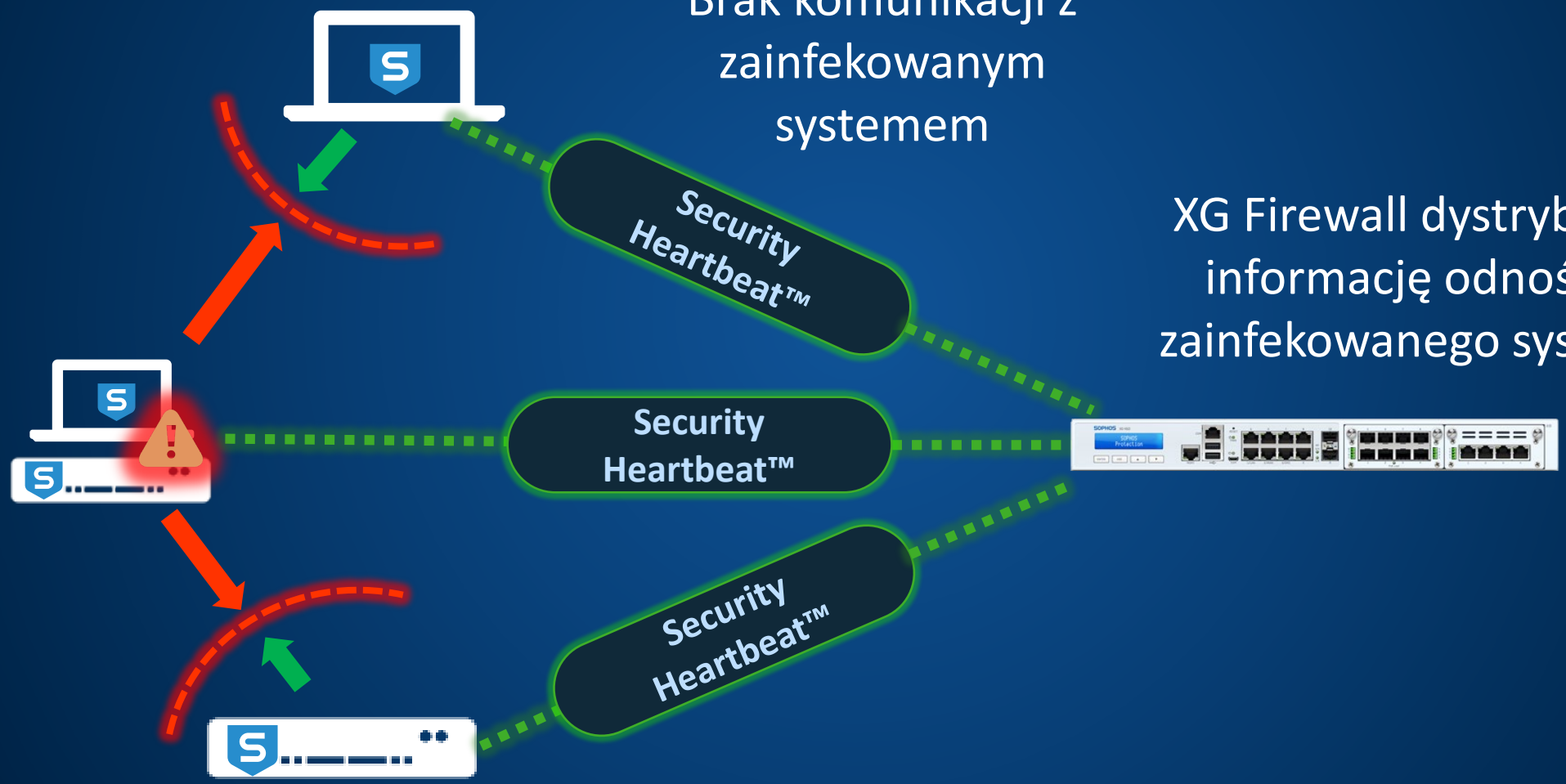


XG Firewall blokuje komunikacje
dla zainfekowanych serwerów

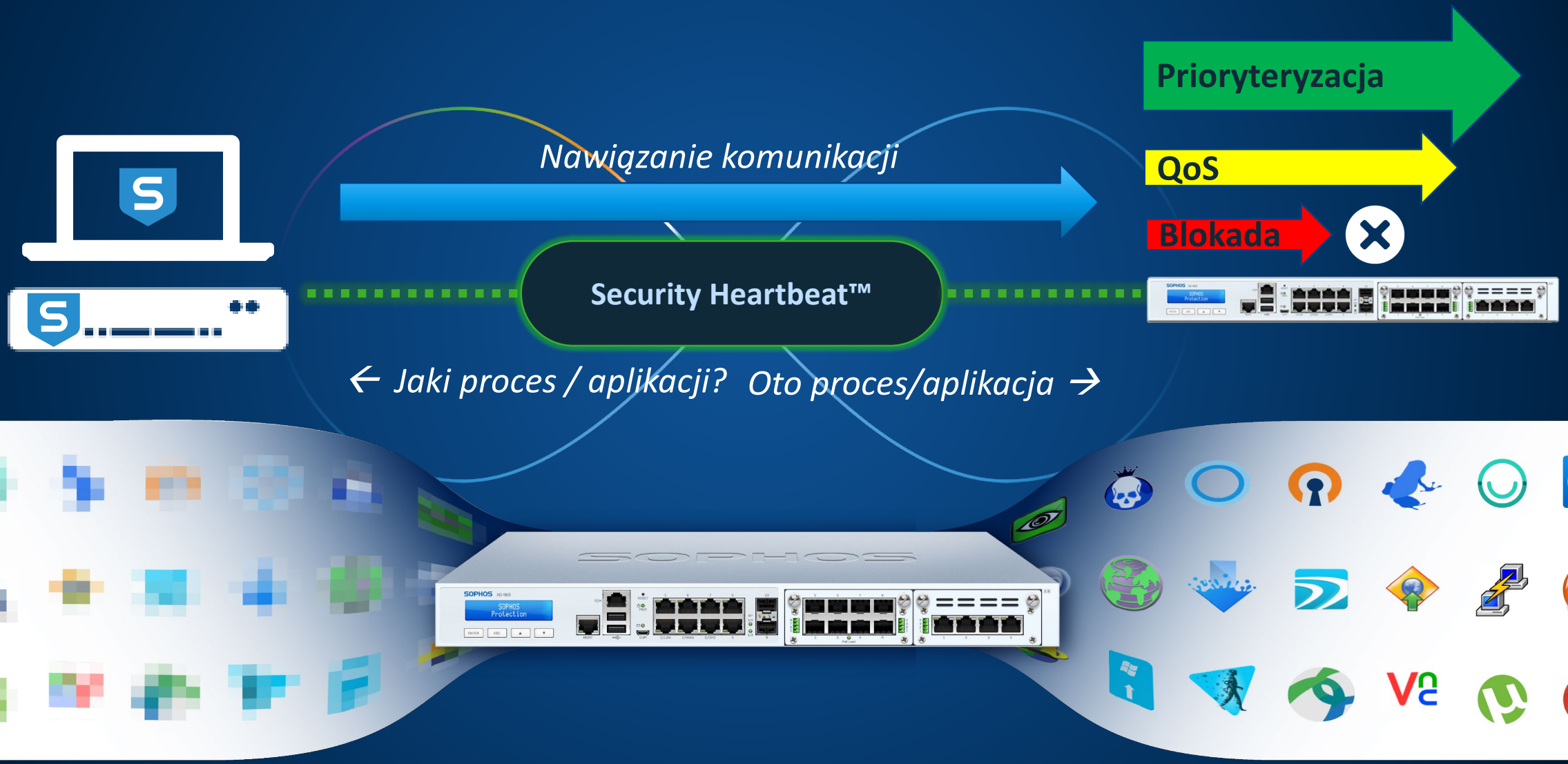
Security Heartbeat – brak komunikacji Heartbeat

XG Firewall blokuje komunikacje dla potencjalnie zainfekowanych stacji i serwerów

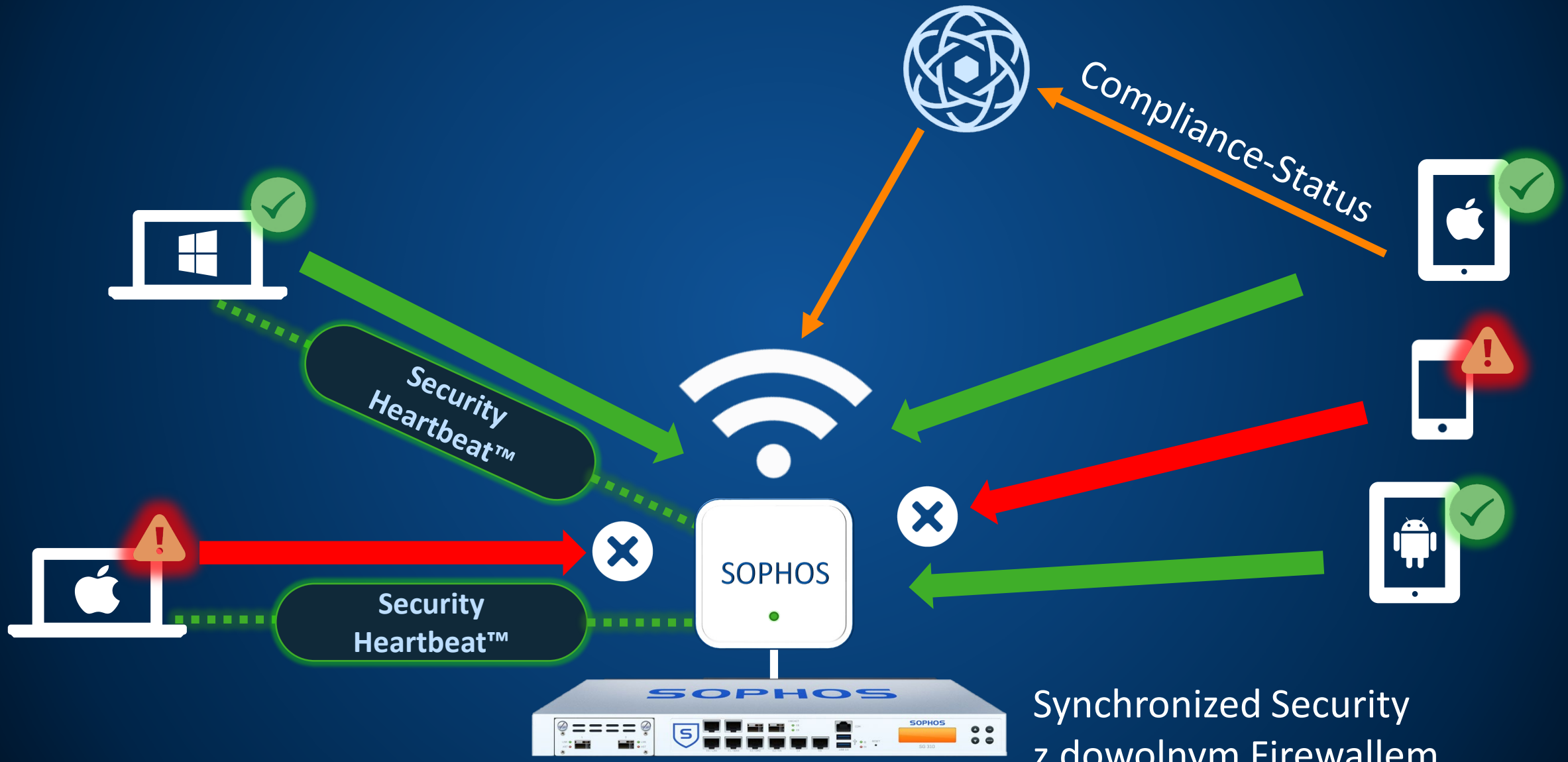
Lateral Movement Protection wraz z XG Firewall



Security Heartbeat – Synchronized App Control



Security Heartbeat – z WiFi AP i dowolnym Firewallem



Demo

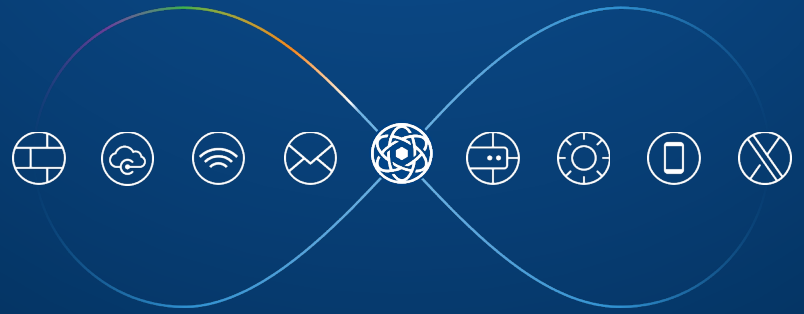
SOPHOS

Synchronized Security - Przegląd

	Sophos Email	APX Access Point	XG Firewall
SOPHOS INTERCEPT X NOW WITH EDR for Workstations	• Endpoint skanuje stację wysyłającą spam i malware	• Automatyczna kwarantanna w sieci	• Automatyczna kwarantanna w sieci • Missing Heartbeat • Synchronized AppControl • Lateral Movement Protection
SOPHOS Intercept X For Server with EDR for Servers		• Automatyczna kwarantanna w sieci	• Automatyczna kwarantanna w sieci • Missing Heartbeat • Synchronized AppControl • Lateral Movement Protection
Sophos Mobile		• Automatyczna kwarantanna w sieci	
PhishThreat	• Szkolenia dla użytkowników		

Synchronized Security – wartości dodane

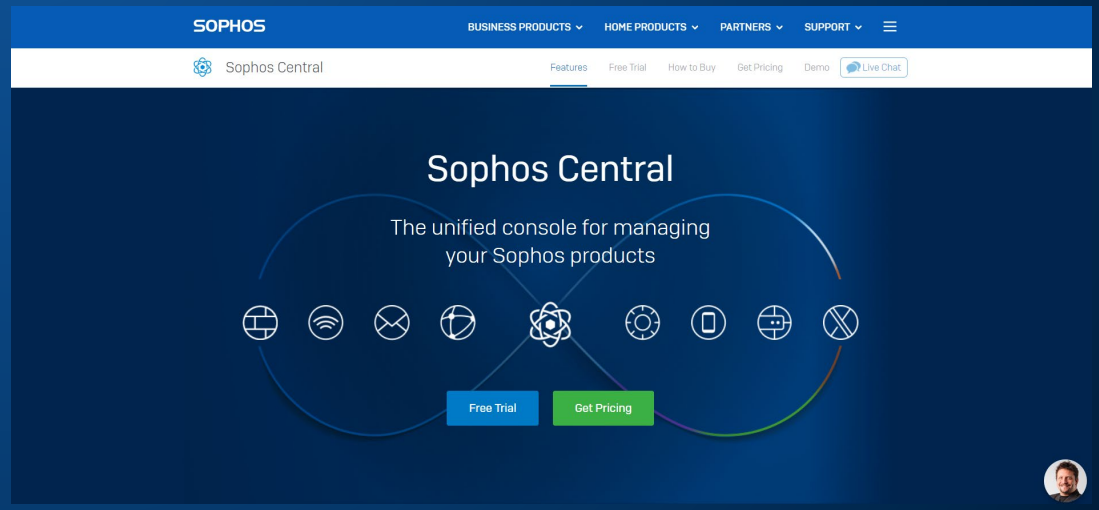
- Niezrównana widoczność – pokazuje co dzieje się w sieci
- Automatyczna reakcja kupuje czas
- Nie jest wymagana gotowość 24x7 -> Pracownicy mogą być efektywniej wykorzystywani
- Bezstresowe IT!
- System modułowy - im więcej komponentów Sophos, tym łatwiejsze zarządzanie bezpieczeństwem IT i automatyzacją procesów



SOPHOS

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.