Ochrona sieci światowej klasy dzięki Sophos XG Firewall w wersji 18

Damian Przygodzki
SOPHOS System Engineer

12.03.2020

SophosLabs – Globalna Baza Danych o Zagrożeniach

Globalnie
~ 100 spamowych pułapek przetwarzanych w 22 krajach > 30 milionów wiadomości dziennie

Bogata wiedza specjalistyczna
znając krajobraz zagrożeń, metod ataku i produkty (punkty końcowe, sieć, chmura)

Pełne portfolio technologii
Szeroki wachlarz technik, procesów i systemów budowanych przez 30 lat

Threat Intelligence
Dane w czasie rzeczywistym zasilają produkty Sophos oraz partnerów technologicznych

Ciągłe innowacje
nieustanny rozwój i praca nad strategią, technikami i narzędziami przeciwko mikro i makro zagrożeniami

Zakres ochrony

Firewall Endpoint Server Mobile Email Wireless Encryption Web

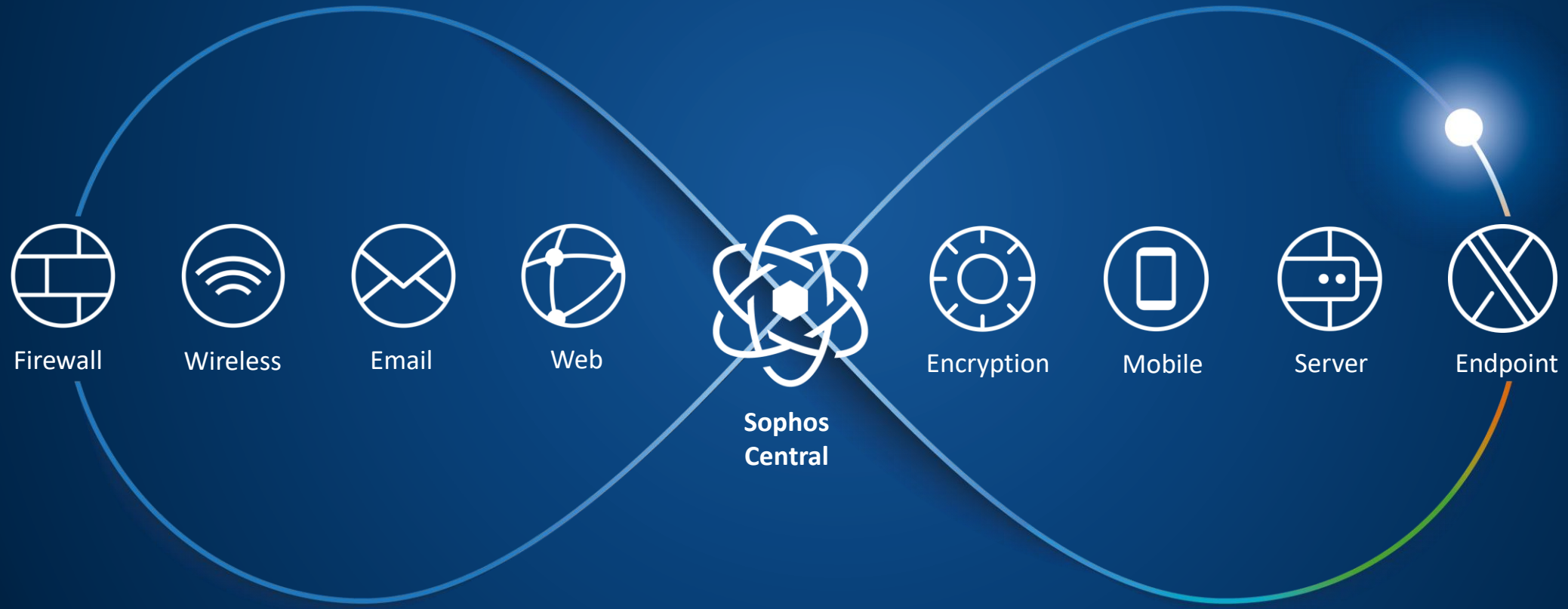
Integracja Produktów

Udostępniaj informacje o zagrożeniach, statusie i poziomie bezpieczeństwa poprzez Security Heartbeat™

+

Dynamiczne polityki reagujące na podstawie Security Heartbeat™

Zakres Ochrony + **Integracja Produktów** + **Efektywność Zarządzania**



Synchronized Security

Przykłady zastosowania

Ale jak działa Synchronized Security w praktyce?!

Automatyzacja – Izolacja i usuwanie zagrożeń

1 Wykrycie złosliwego oprogramowania

2 Komunikacja pomiędzy produktami

3 Izolacja urządzenia

8 sekund

5 Dostęp Przywrócony

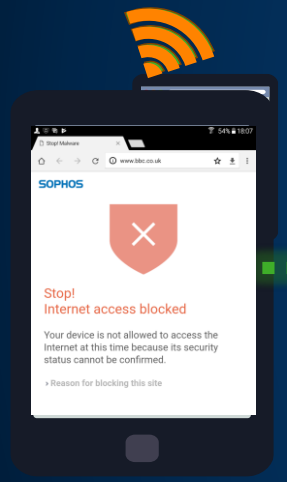
4 Proces czyszczenia

Automatyzacja – Ochrona sieci bezprzewodowej

1 Naruszenie polityki bezpieczeństwa

2 Komunikacja pomiędzy produktami

3 Ogranicz dostęp do WLAN



Security Heartbeat™

4 Agent: Alarm

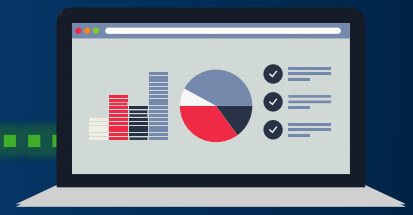
Automatyzacja – wykrycie skompromitowanej skrzynki

1 Skompromitowana skrzynka

2 Komunikacja pomiędzy produktami

3 Endpoint: Skanowanie

Security Heartbeat™



5 Skrzynka przywrócona

4 Endpoint: usunięcie zagrożenia

Automatyzacja – Ochrona danych

1 Wykrycie zagrożenia

2 Komunikacja pomiędzy komponentami

3 Klucze szyfrowania odwołane

Security Heartbeat™

5 Klucze szyfrowania Przywrócone

4 Usunięcie zagrożenia

Wcześniej nieokreślone aplikacje

1 Nieznana aplikacja

2 Informacje o aplikacji udostępnia Endpoint

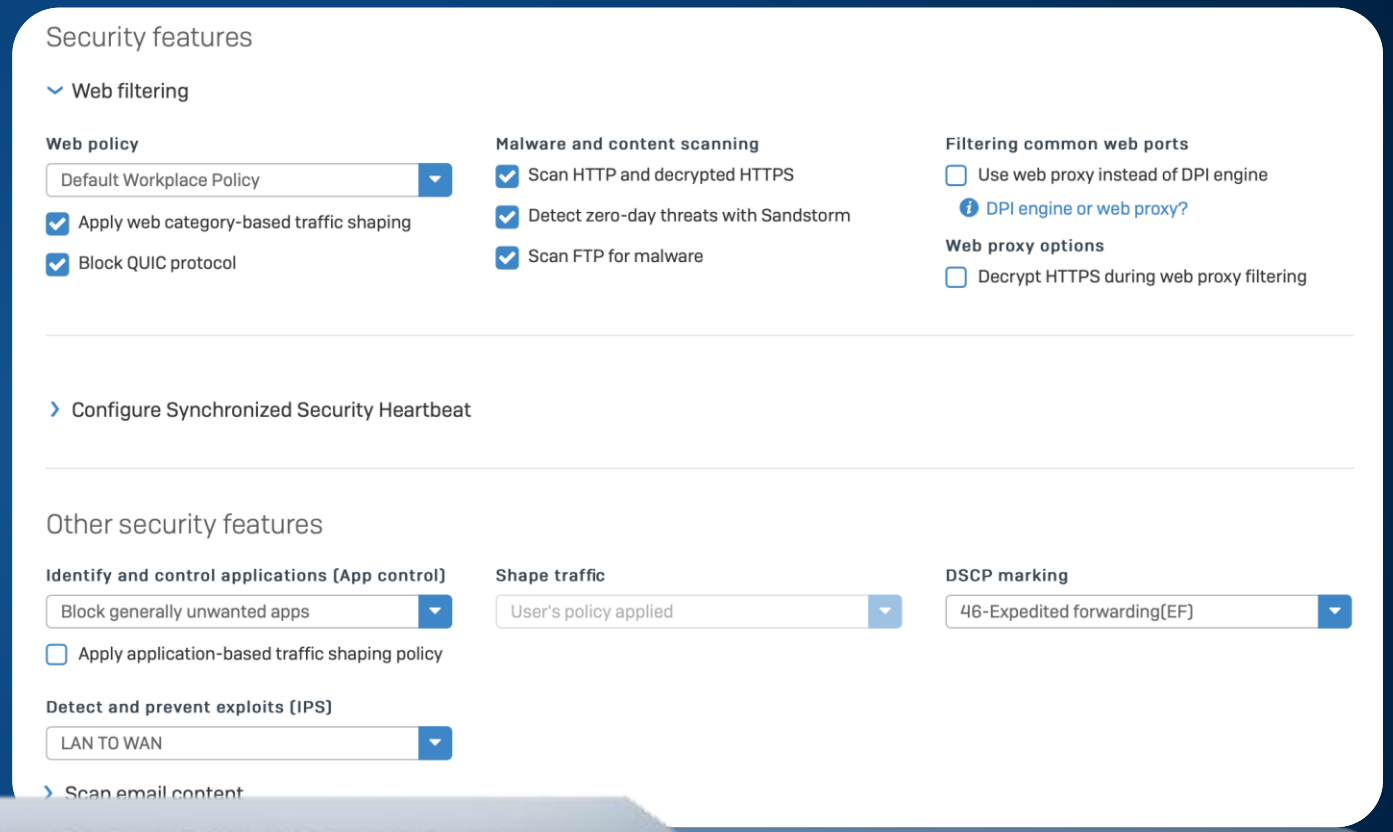
Security Heartbeat™

3 Aplikacja jest sklasyfikowana i kontrolowana

XG Firewall w wersji 18

XG Firewall – Pełny pakiet ochrony

- SSL Inspection
- AI Threat Intelligence & Sandboxing
- Web and Application Control
- Intrusion Prevention System
- Advanced Threat Protection
- Synchronized Security



Unikalne dla Sophos: wszystkie konfiguracje bezpieczeństwa zintegrowane na jednym ekranie

Nowa wersja SFOSv18

XG Firewall v18

Xstream

Architektura Xstream

Inspekcja SSL

Threat Intelligence

Akceleracja Aplikacji & SD-WAN

Central Management 2.0

Darmowe zarządzanie Sophos Central

Dostęp do firewal via Chmura

Polityki Group Firewall

Wdrożenie Zero-Touch

Central Reporting 1.0

Raportowanie Cloud Firewall

Packaged and dynamic reports

Unikalne reporty-to-log drill down

MTR Konektor

Architektura Xstream

Architektura Xtream rozwiązuje problemy…

Brak widoczności w zaszyfrowanym ruchu

SSL Inspection

Xstream SSL Inspection Engine

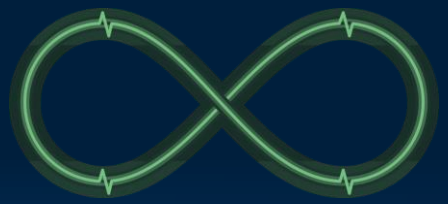
Ochrona przed Ransomware i zagrożeniami

SOPHOS labs

Threat Intelligence

Uczenie maszynowe, analiza plików

Krytyczna wydajność aplikacji



Application Acceleration

FastPath & Synchronized SD-WAN

Architektura Xstream

widoczność, ochrona i wydajność

Silnik przetwarzania pakietów w wersji 18

Firewall Stack
(Normal Path)

- Zarządzanie połączeniami
- Zezwalaj, blokuj, decyzja DPI
- DoS / QoS

DPI Engine
IPS, Web, AV, App, SSL

- Przetwarzanie strumieniowe DPI
- Inteligentny offloading
- Jednoprzebiegowe skanowanie bez proxy
- Polityka i kontrola SSL

Network Flow FastPath

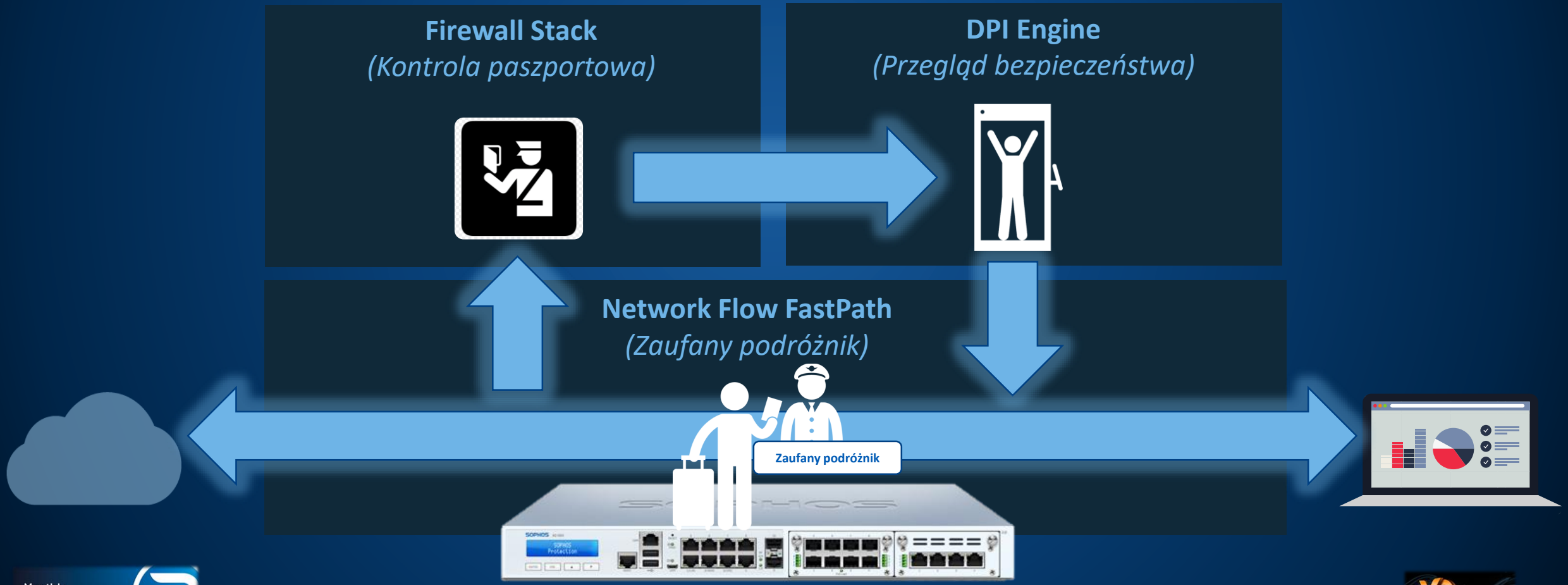
- Przyspieszenie zaufanego ruchu Aplikacji
- Bezpośrednia dostawa do DPI
- Odciążanie DoS / QoS

Ewolucja bezpieczeństwa podróży lotniczych

Ewolucja do szybszego, lepszego bezpieczeństwa

Firewall – przetwarzanie pakietów(i podróż lotnicza)

Kontrola Firewall jest podobna do kontroli podróży lotniczych



Jak działa?!

Wstępne połączenie

Firewall konfiguracja połączenia- Zezwalaj, Blokuj lub podejmuj decyzje dotyczące bezpieczeństwa

Firewall Stack
(Normalna ścieżka)

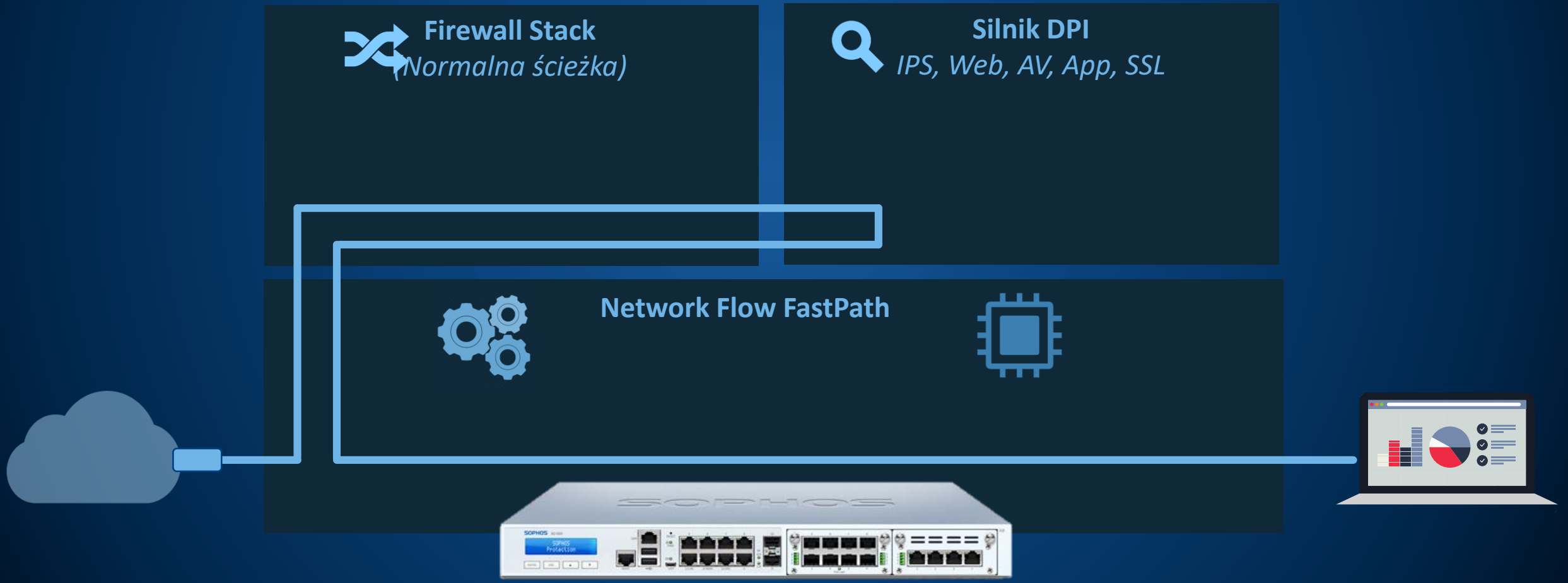
Silnik DPI
IPS, Web, AV, App, SSL

Network Flow FastPath

Jak działa?!

Inspekcja DPI

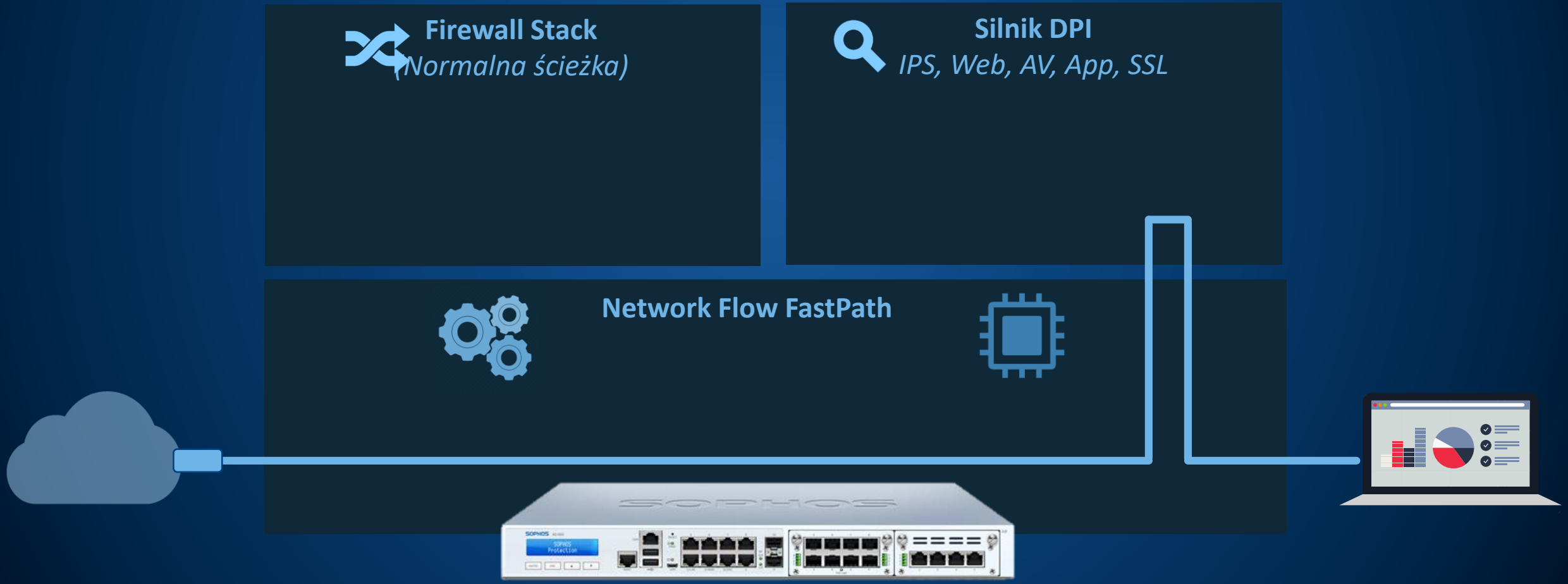
Wstępna dostawa pakietów do DPI Engine przez SlowPath



Jak działa?!

Odciążenie Firewall

Odciążenie zapory ogniowej, flow analizowany tylko w silniku DPI w celu skanowania bezpieczeństwa



Jak działa?!

Pełne odciążenie FastPath

Kiedy ruch bezpieczny silnik DPI zostaje odciążony do FastPath

Firewall Stack

(Normalna ściezka)

Silnik DPI

IPS, Web, AV, App, SSL

Network Flow FastPath

Inspekcja SSL

Inspekcja SSL jest niezwykle ważna

SSL / TLS trendy i ich wpływ

Widoczność

Google

80%

ruchu jest Zaszyfrowana

Ogromny ślepy punkt

Zagrożenia

SOPHOS labs

32%

Połączenia złośliwego oprograwmoania i PUA csą szyfrowane (TLS)

Cyberkryminaliści to wykorzystują

Wydajność

VansonBourne

96%

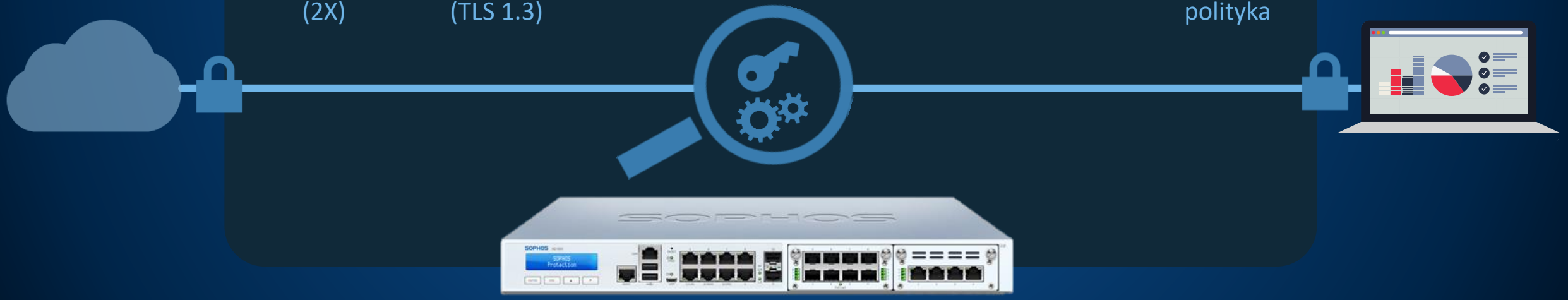
NIE używa analizy SSL

Organizacje są bezsilne

Xstream SSL Inspection

Widoczność SSL– Bezpieczeństwo - Wydajność

- Wysoka wydajność (2X)
- Koncentracja na bezpieczeństwie (TLS 1.3)
- Analiza całego ruchu
- At-a-Glance Health
- Nie zepsuje internetu ☺
- Prosta i elastyczna polityka



Reguły inspekcji SSL/TLS

Mechanizm kontroli SSL, który jest niezależny od portu i aplikacji

Reguły SSL są niezależne od reguł na zaporze

Odszyfrowane pakiety są wysyłane do IPS, kontroli aplikacji, filtrowania sieci i antywirusa

Threat Intelligence

Architektura Xstream

widoczność, ochrona i wydajność

Silnik przetwarzania pakietów w wersji 18

Firewall Stack
(Normal Path)

- Zarządzanie połączeniami
- Zezwalaj, blokuj, decyzja DPI
- DoS / QoS

DPI Engine
IPS, Web, AV, App, SSL

- Przetwarzanie strumieniowe DPI
- Inteligentny offloading
- Jednoprzebiegowe skanowanie bez proxy
- Polityka i kontrola SSL

Network Flow FastPath

- Przyspieszenie zaufanego ruchu Aplikacji
- Bezpośrednia dostawa do DPI
- Odciążanie DoS / QoS

Architektura Xstream

widoczność, ochrona i wydajność

DPI Engine

IPS, Web, AV, App, SSL

- Przetwarzanie strumieniowe DPI
- Inteligentny offloading
- Jednoprzebiegowe skanowanie bez proxy
- Polityka i kontrola SSL

Threat Intelligence

Powered by SophosLabs and Deep Learning

Threat Intelligence

SOPHOS labs

Sophos Sandstorm

- Chmurowy sandbox
- Dynmiczna analiza
- Technologia Intercept X
- Memory, Registry, File System, Network Analysis

Silnik DPI

IPS, Web, AV, App, SSL

- Analiza plików AV

Threat Intelligence

SOPHOS labs

New Threat Intelligence

- Chmurowa anliza Threat Intelligence
- Wiele technik modelowania zagrożeń
- Deep Learning & Artificial Intelligence

Sophos Sandstorm

- Chmurowy sandbox
- Dynmiczna analiza
- Technologia Intercept X
- Memory, Registry, File System, Network Analysis

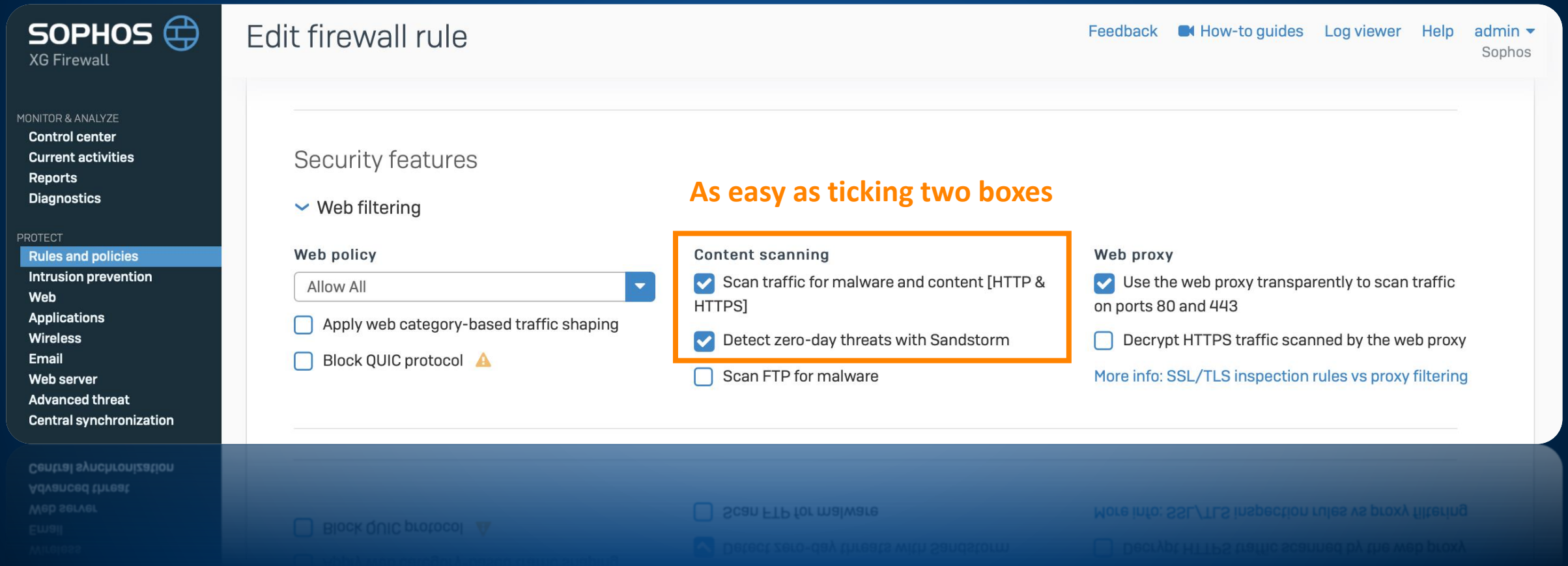
Silnik DPI

IPS, Web, AV, App, SSL

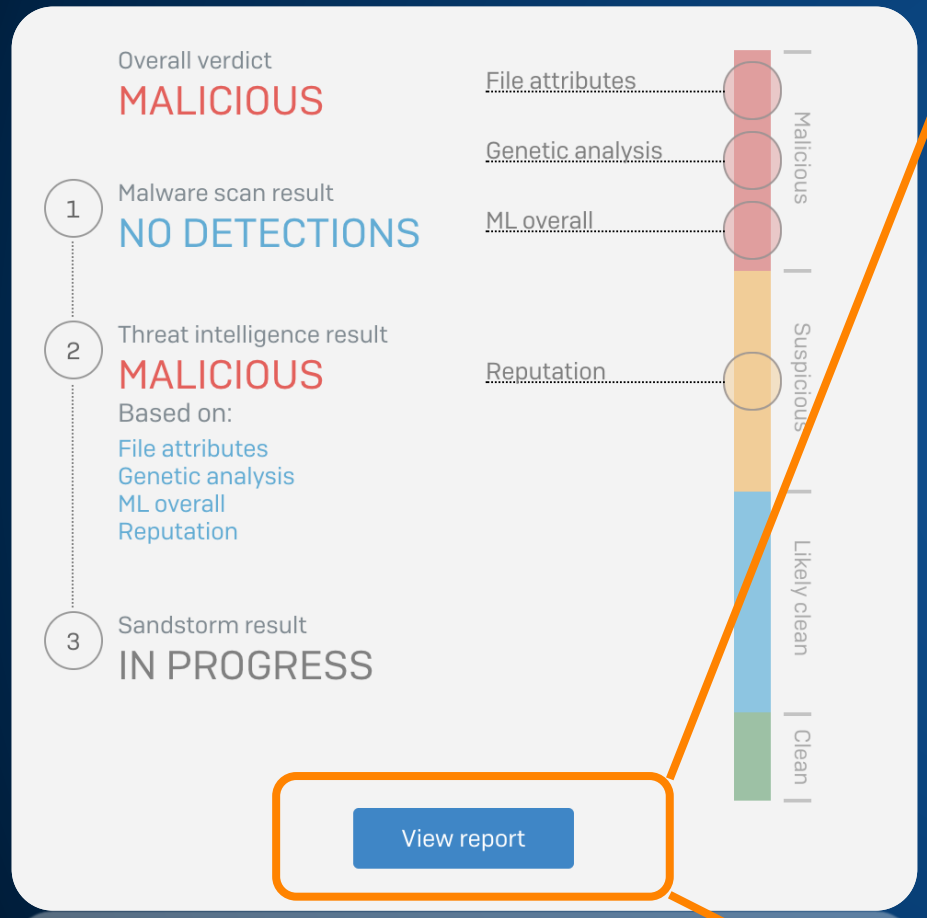
- Analiza plików AV

How it Works

Works in parallel with Sophos Sandstorm – Part of the same license



Threat Intelligence



Investigation and actions

[drive]\[redacted]\file.exe

Blocked 5 times for 3 users. Source details

Time of analysis

Static: 2019-07-26 21:09:08
Sandstorm: 2019-04-16 17:40:58

Overall verdict

MALICIOUS

Analysis summary

MALICIOUS	MALICIOUS	MALICIOUS	SUSPICIOUS	NOT DETECTED	9/71	None
Machine learning Overall analysis	Machine learning File features	Machine learning File structure	File reputation	Sandstorm	VirusTotal detections	XG malware scan

Information about your file

File name	[drive]\[redacted]\file.exe
File type	application/x-dosexec
SHA1	41b68b777b6fd365e72f1344ae29fcdaf2f2e9af
SHA256	6f14a34560d2076523e95ae66b126d363d5552730459399a9cb3d9a4f2172086
File size	10,096,640 bytes

All details

Machine learning

MALICIOUS Overall verdict based on the Sophos deep learning model

Our model identifies many attributes of the file and compares their occurrence, individually and in different combinations, with millions of known good and known malware samples.
The reports below show probabilities based on key components of the overall score. Each component isn't a strong indicator on its own but, in combination, they provide a critical insight.This model identifies many different characteristics of your file and compares the occurence of those characteristics, individually and in combinations, across millions of known good and known malware samples.

Feature analysis

- Identifies specific features of the file.
- Randomly selects one million (out of 2,906,531) known good and one million (out of 20,045,125) known bad files.
- Counts the number of good and bad sample files that have the same features. These simple counts are shown in the graph below.
- The verdict may also take into account more complex combinations of features
- This test rates **file.exe** as MALICIOUS.

More likely in bad files >>>	<<< More likely in good files	File feature
6,747	5,292	Can access the registry: "RegDeleteKeyW"
30,962	31,332	[!] The program may be hiding some of its imports: "GetProcAddress"
23,868	22,093	[!] The program may be hiding some of its imports: "LoadLibraryA"
48,199	49,165	Stack Canary: "disabled"
122	30	Packer: "Unusual section name found: .vmp0"
108	24	Packer: "Unusual section name found: .vmp1"

Feature combinations

Ulepszone raportowanie aktywności w Sanbox'ie

Zawarte w raportach analizy zagrożeń

Sandstorm detonation

MALICIOUS

Submitted at	2019-11-06 00:34:41
Detonated at	2019-11-06 00:35:53
Analysis duration	181 seconds
Sandbox version	4.1.1.283
File type	PDF document, version 1.3
File executed as	pdf
SHA1	f2927bb7ec0395d3f50b7c183504a36353ff0e87
SHA256	fcc862d1f79cda12b78fd1dee8fcf443ed1dd4886b921e49d4488b477cb460e1

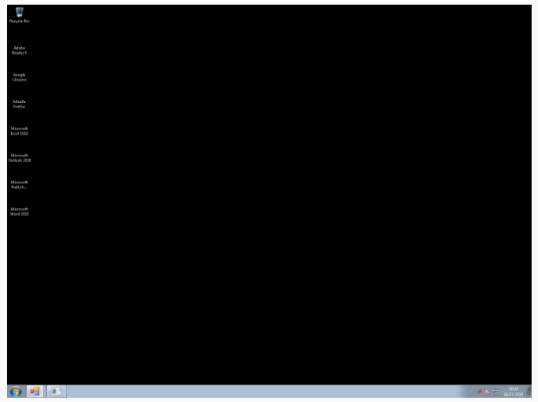
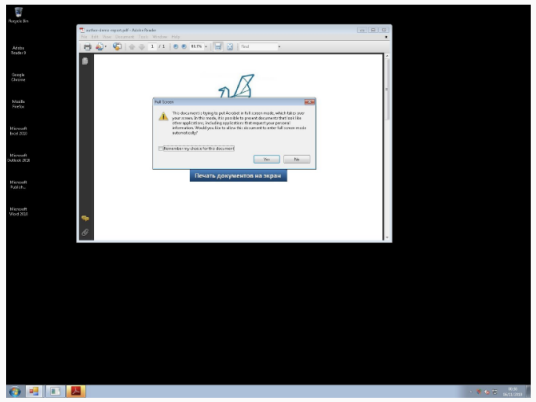
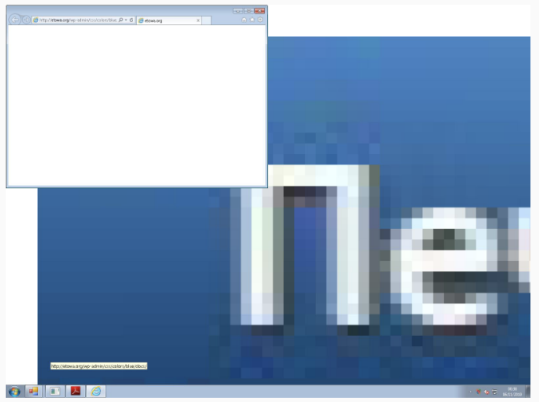
Malicious activity

Network	Connects to remote server classified as high-risk
Signature	Triggers malware detections by Sophos Anti-Virus

Malicious detections: 4

#	Classification	Found in	Classification type
1	Mal/DrodZp-A	%localappdata%\microsoft\windows\temporary internet files\content.ie5\k2uasb86\doc[2].zip (file)	SAV detection
2	Mal/DrodZp-A	%localappdata%\microsoft\windows\temporary internet files\content.ie5\k2uasb86\doc[1].zip (file)	SAV detection
3	Mal/DrodZp-A	%localappdata%\microsoft\windows\temporary internet files\content.ie5\k2uasb86\doc.zip (file)	SAV detection
4	HIGH (MALWARE_REPOSITORY)	hxxp://etowa.org/wp-admin/css/colors/blue/docs/ (URL)	Web reputation

Screenshots: 9

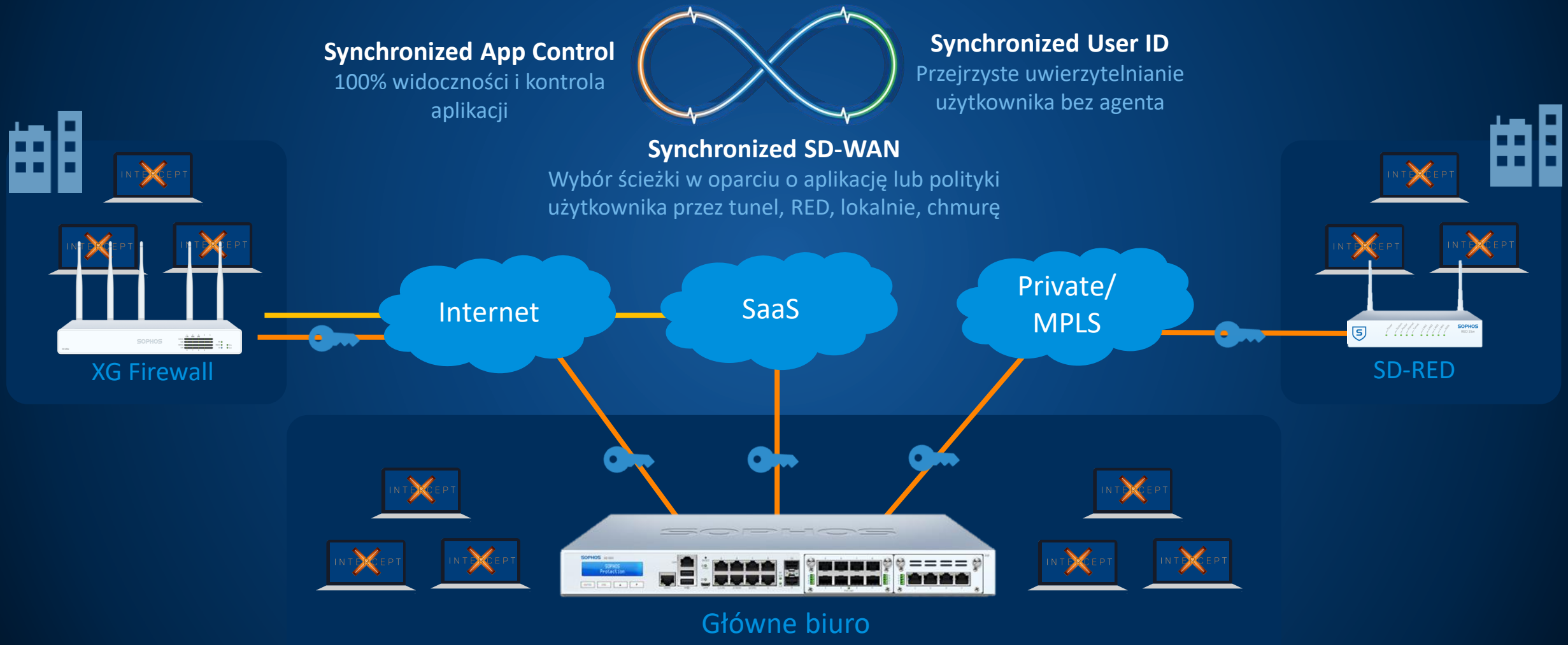
Synchronized SD-WAN

Doskonała widoczność, kontrola i wybór ścieżki

Synchronized App Control
100% widoczności i kontrola aplikacji

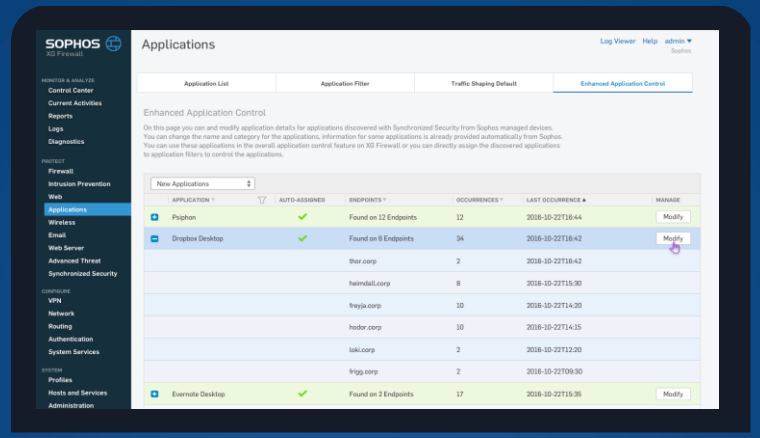
Synchronized User ID
Przejrzyste uwierzytelnianie użytkownika bez agenta

Synchronized SD-WAN
Wybór ścieżki w oparciu o aplikację lub polityki użytkownika przez tunel, RED, lokalnie, chmurę



Synchronized Application Control

Przełom w widoczności i kontroli sieci



Co firewalle widzą dzisiaj

Co widzi zapora sieciowa Sophos XG

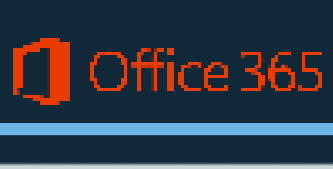
Przyspieszenie Aplikacji

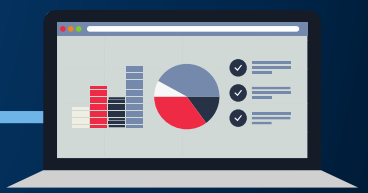
Akceleracja zaufanego ruchu FastPath

Firewall Stack
(Normalna ścieżka)

Silnik DPI
IPS, Web, AV, App, SSL

Network Flow FastPath





Sophos Central

Sophos Central

Uproszczenie dzień po dniu...

Zarządzanie

Jedna konsola do zarządzania

Z łatwością zarządzaj wszystkimi zaporami XG i innymi produktami Sophos razem

Raportowanie

Analiza na wyciągnięcie ręki

Gotowe narzędzia do raportowania i wizualizacji

Wdrożenie

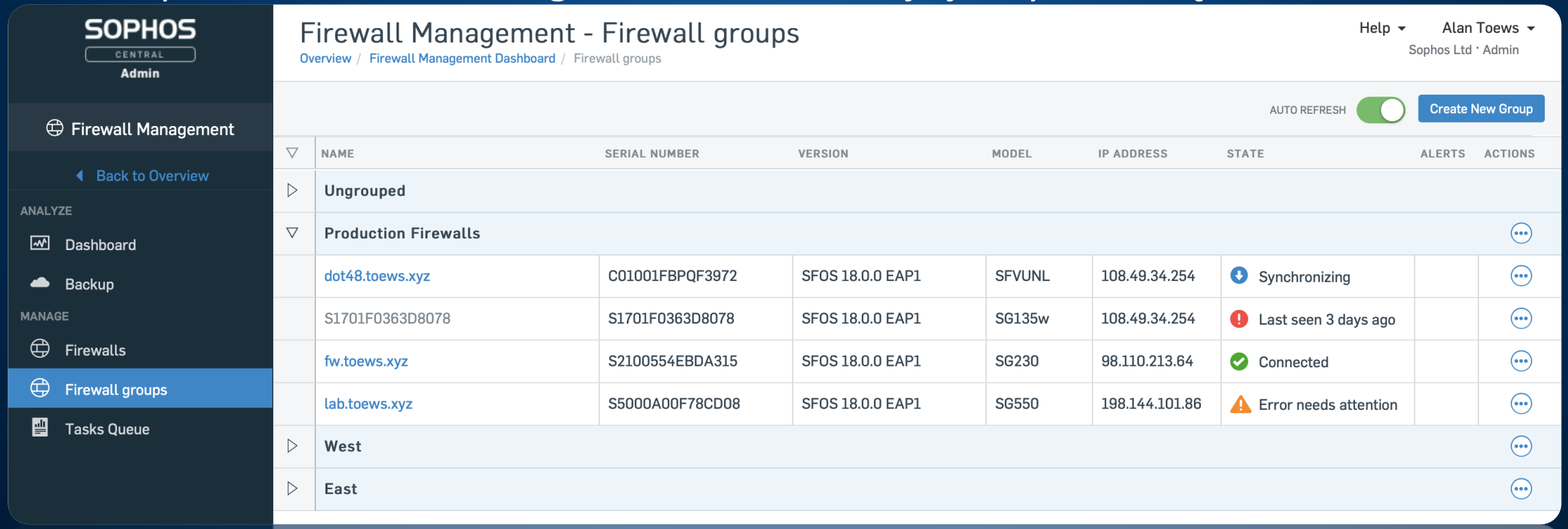
Zero-Touch* Deployment

Wdrożenie i konfiguracja XG z Sophos Central

Firewall Group Management in Sophos Central

Zbudowany z myślą o MSP

- Firewall Group Management – Dokonaj zmiany raz, a zostanie ona automatycznie zsynchronizowana
- Backup and Firmware management – Aktualizacje jednym kliknięciem



Central Firewall Raportowanie

elastyczny, wizualny

Dashboard

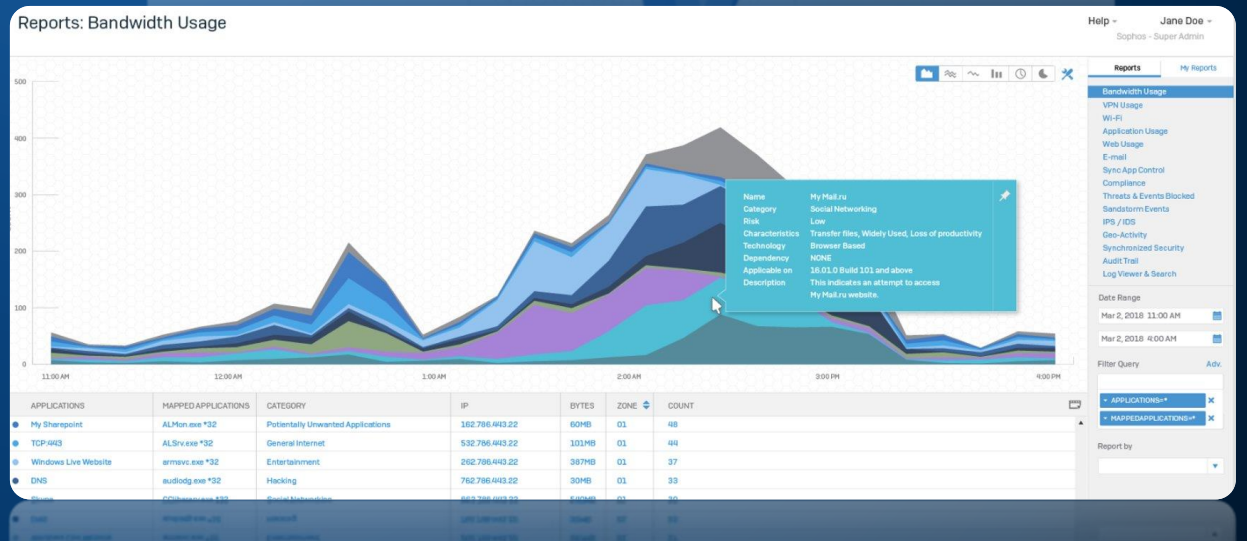
- Najważniejsze wskaźniki i zagrożenia w skrócie: stan sieci, incydenty, zdarzenia związane z bezpieczeństwem i najwyższym ryzykiem
- Uzyskaj dostęp do szczegółowych danych

Reportowanie

- Wydajne i elastyczne wielowymiarowe raportowanie
- Łatwe tworzenie niestandardowych raportów za pomocą zapytań, filtrów, wykresów i narzędzi do wyboru kolumn
- Intuicyjne opcje wizualizacji danych
- Pobierz i zaplanuj raporty pocztą e-mail

Logowanie

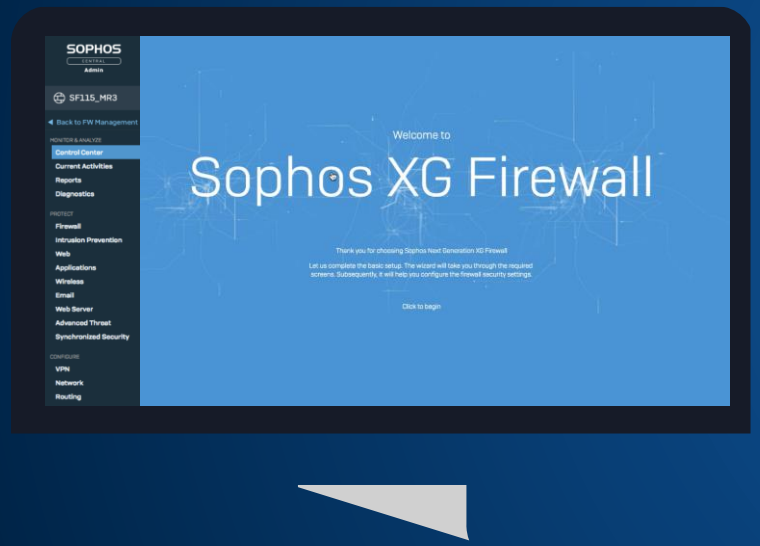
- Pełny widok dziennika i narzędzia wyszukiwania



Central Firewall – proste wdrożenie

Zero-touch wdrożenie urządzenia bez inżyniera na miejscu

1. Użyj Kreatora instalacji w Sophos Central



2. (Opcjonalnie) Wyślij plik konfiguracyjny pocztą e-mail do zdalnej lokalizacji

3. Przenieś plik konfiguracyjny na pamięć USB

4. Uruchom urządzenie z podłączoną pamięcią USB

Najlepsza na świecie widoczność, ochrona i reakcja