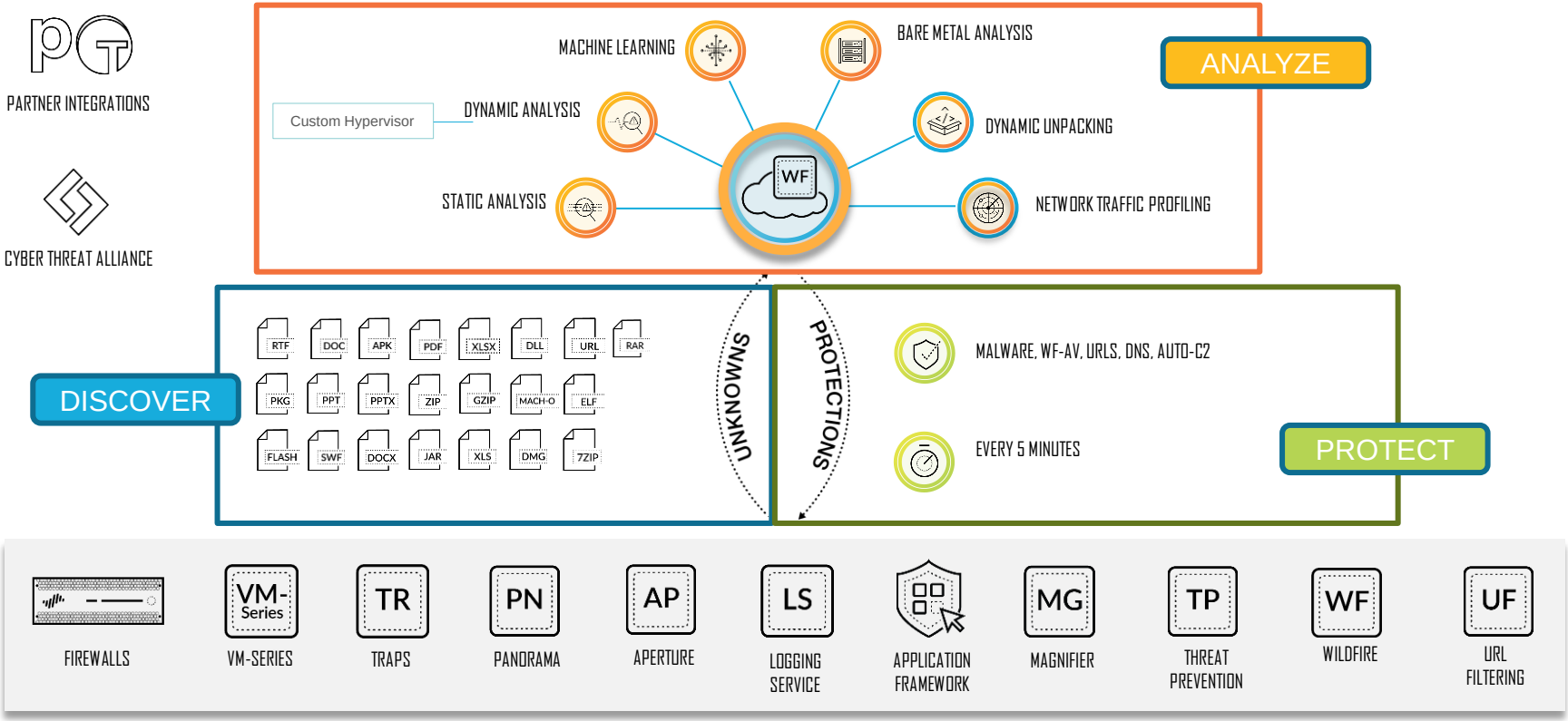
Next Generation Firewall

Marcin Szewczuk

Channel Engineer, Poland

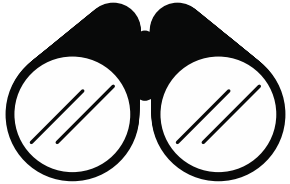
marcin.szewczuk@clico.pl

Pełna ochrona od Palo Alto Networks



Ochrona sieciowa

Co zyskujemy dzięki firewall'om Palo Alto Networks



COMPLETE VISIBILITY

- Wszystkie aplikacje
- Wszyscy użytkownicy
- Wszystkie treści
- Ruch zaszyfrowany

- SaaS
- IaaS, PaaS
- Chmura

- Urządzenia mobilne

REDUCE ATTACK SURFACE

- Blokujemy wszystko poza tym, co dozwolone
- Dopuszczamy aplikacje biznesowe
- Blokujemy groźne aplikacje
- Ograniczamy typy plików
- Kontrolujemy URL'e

PREVENT KNOWN THREATS

- Blokujemy:
  - Exploity
  - Malware
  - Ruch C&C
  - Groźne strony
  - Groźne domeny
- Zapobiegamy kradzieży danych do logowania

PREVENT UNKNOWN THREATS

- Analiza dynamiczna
- Analiza statyczna
- Wykrywanie anomalii
- Machine Learning
- Analiza w środowisku zwirtualizowanym oraz fizycznym
- Analityka i raportowanie

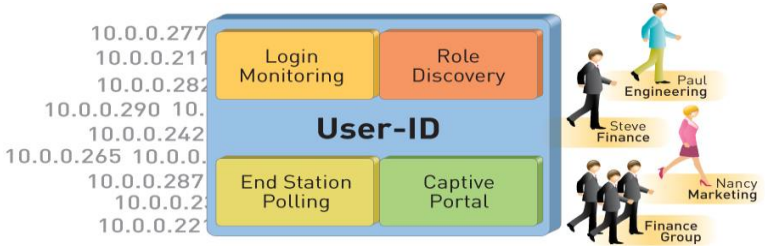
Kluczowe cechy firewall'i Palo Alto Networks

App-ID™

Identyfikacja aplikacji

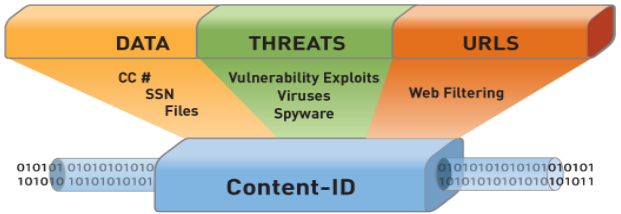
User-ID™

Identyfikacja użytkowników

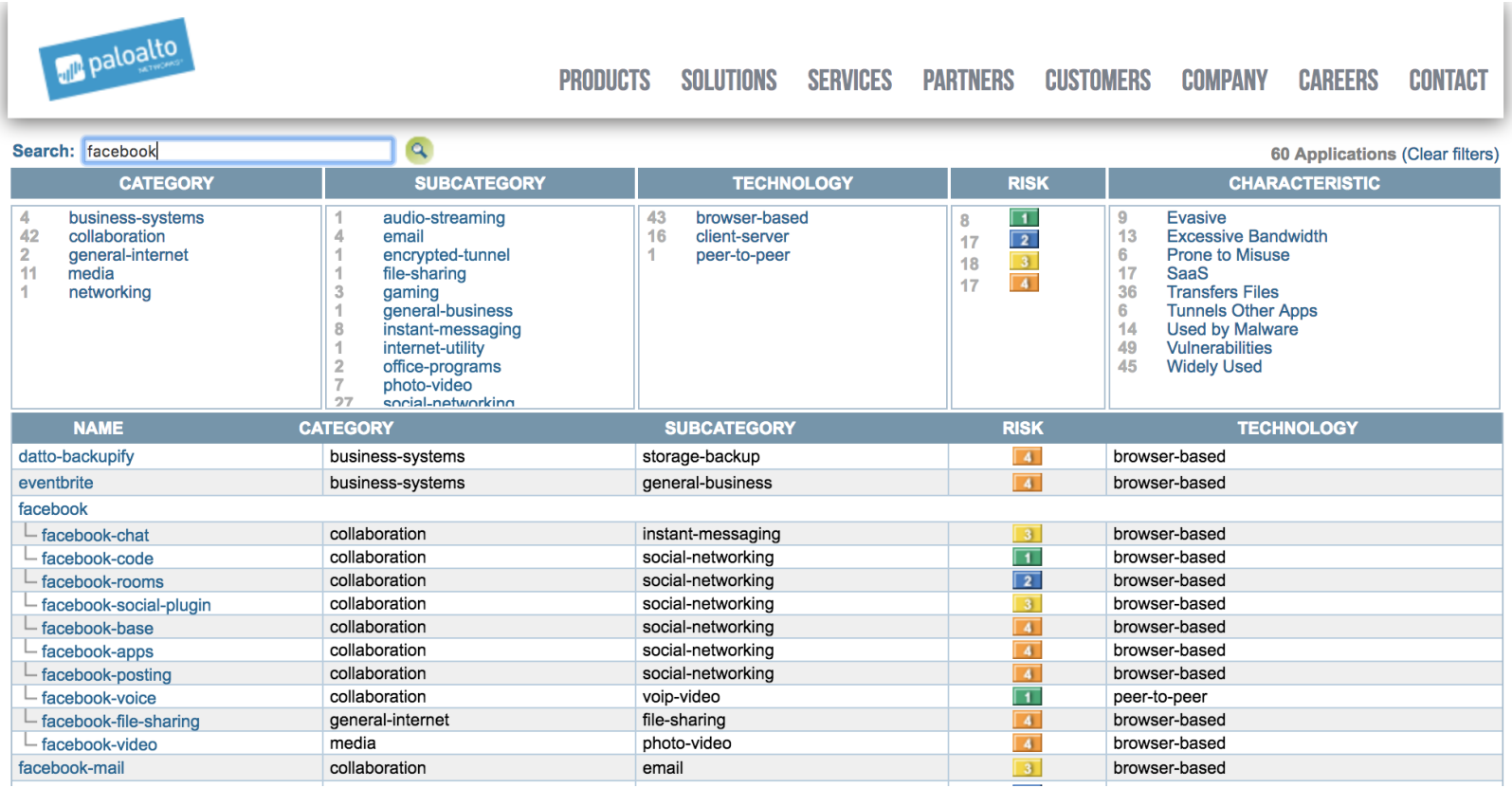


Content-ID™

Inspekcja zawartości

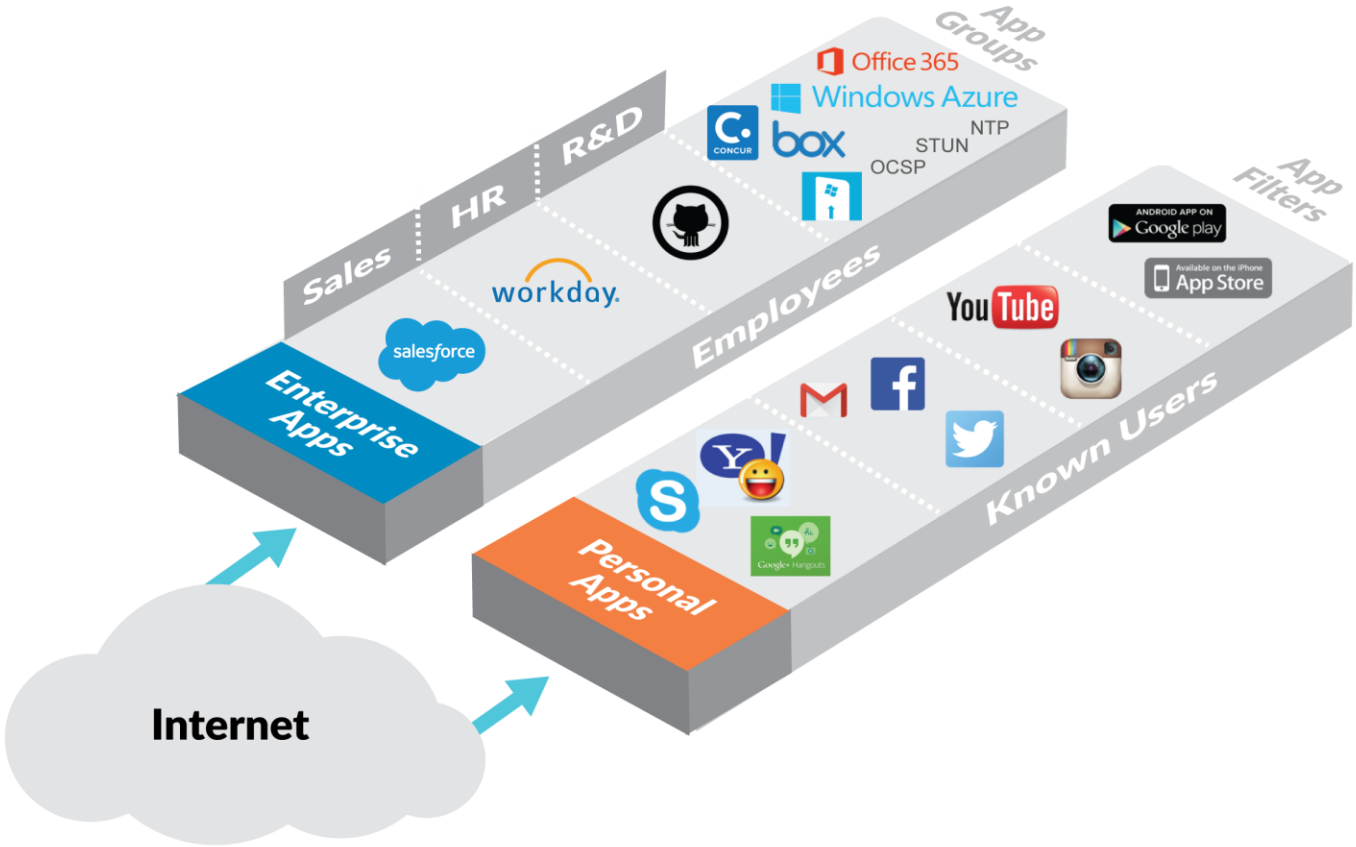


App-ID – wspierane aplikacje



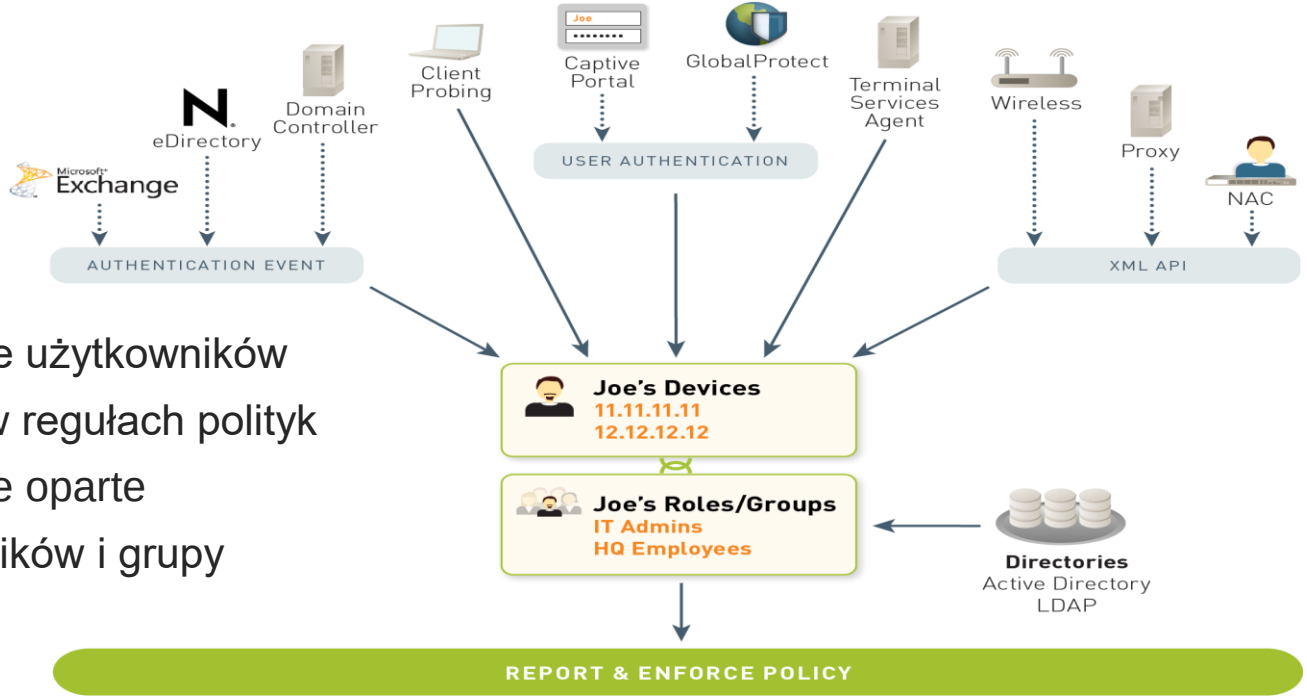
https://applipedia.paloaltonetworks.com/

App-ID – bezpieczne udostępnianie aplikacji



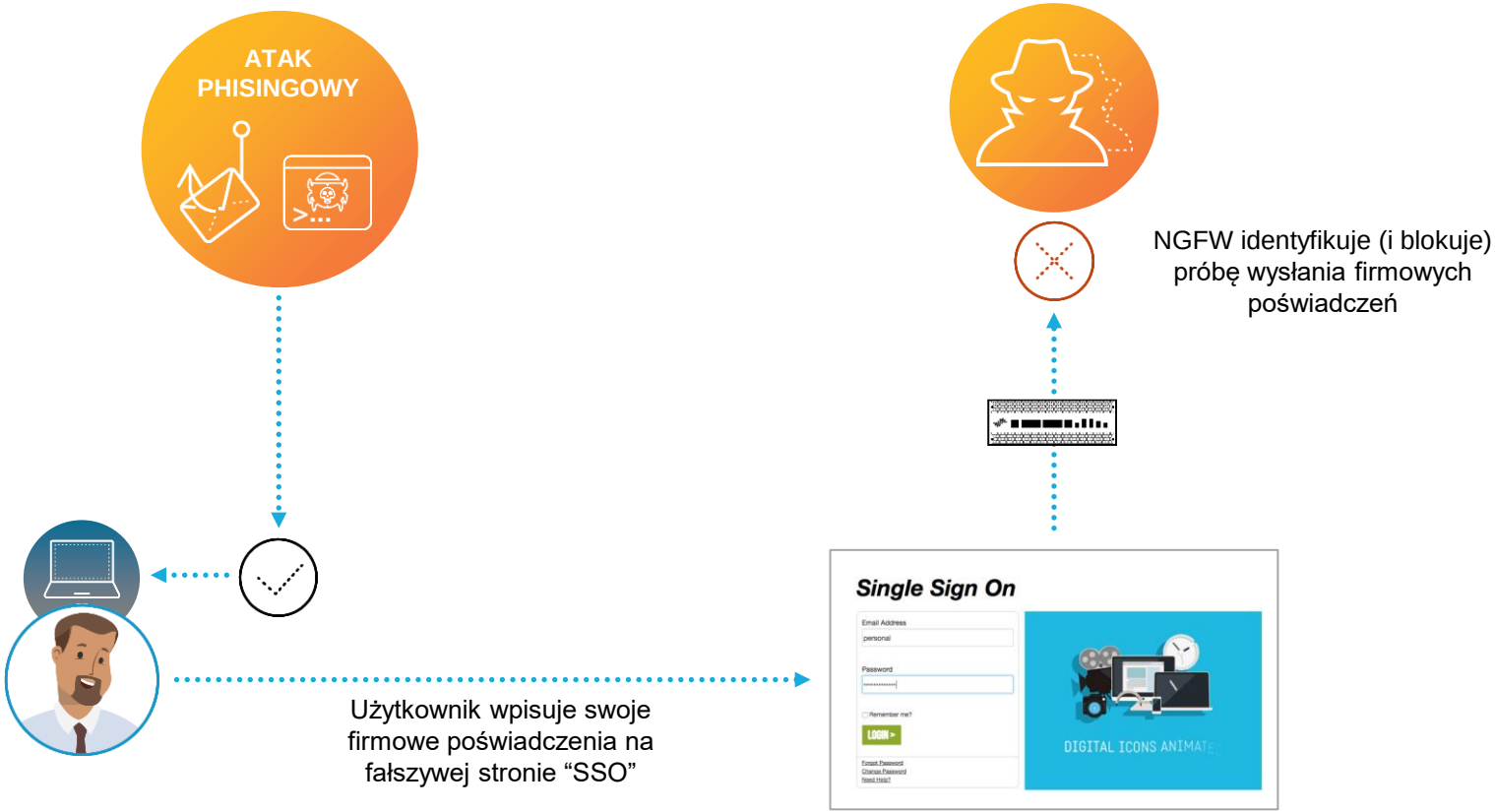
User-ID – źródła informacji o użytkownikach

- Dopasowanie użytkowników do ich adresów IP

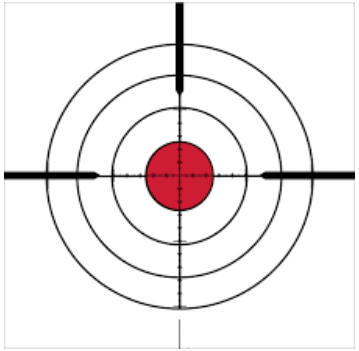


- Zastosowanie użytkowników oraz grup w regułach polityk
- Raportowanie oparte o użytkowników i grupy

User-ID – ochrona przed kradzieżą poświadczeń



Content-ID – inspekcje bezpieczeństwa



AV

IPS

URL

AS

Filtrowanie treści

Filtrowanie plików

WildFire

Content-ID – skuteczność sygnatur

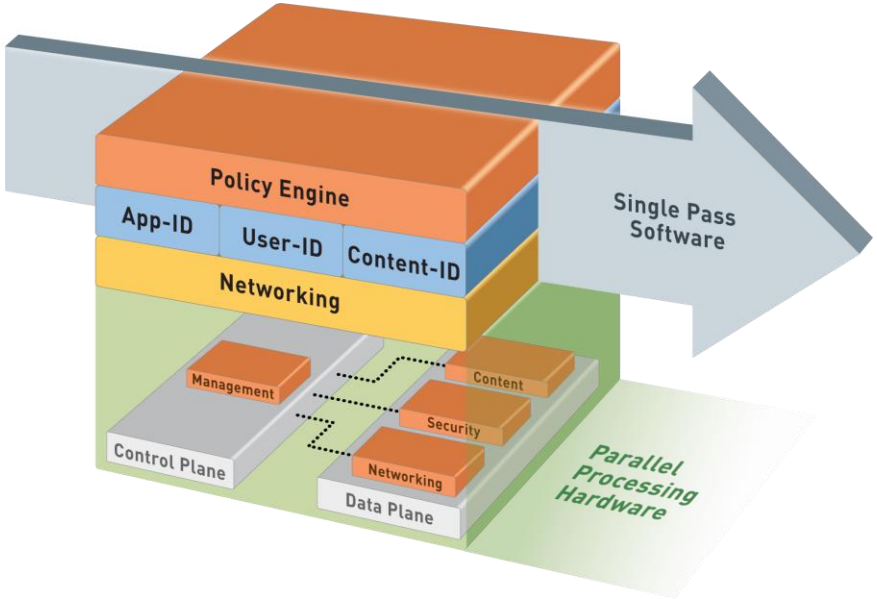
(Grudzień 2018)

NAME	SAMPLES
Virus/Win32.parite.etuo	1,255,688
Virus/Win32.madang.ojo	920,707
Virus/Win32.Ipamor.b	897,322
Trojan/Win32.zbot.xuob	560,581
Virus/Win32.madang.ojx	532,480
Trojan-Spy/Win32.qukart.xi	347,321
Trojan/Win32.upatre.gpg	343,292
TrojanDropper/Win32.dinwod.adi	318,605
Virus/Win32.dropper.ut	318,357
Trojan/Win32.vilsel.ajugl	302,745

NAME	SAMPLES
Virus/Win32.parite.xqfd	296,604
Virus/Win32.sillydl.e	214,261
Worm/Win32.vb.ckvyk	191,785
Trojan/Win32.Scar.ylz	183,040
TrojanDownloader/Win32.upatre.bukc	156,082
Trojan/Win32.cosmu.dggw	154,468
Worm/Win32.mira.cbve	150,387
Virus/Win32.Mepaow.bi	149,298
Malware/Win32.virut.egqq	147,745
Trojan/Win32.upatre.gqr	146,453

* 20 aktywnych sygnatur AV wykrywa i blokuje 7.6 miliona próbek

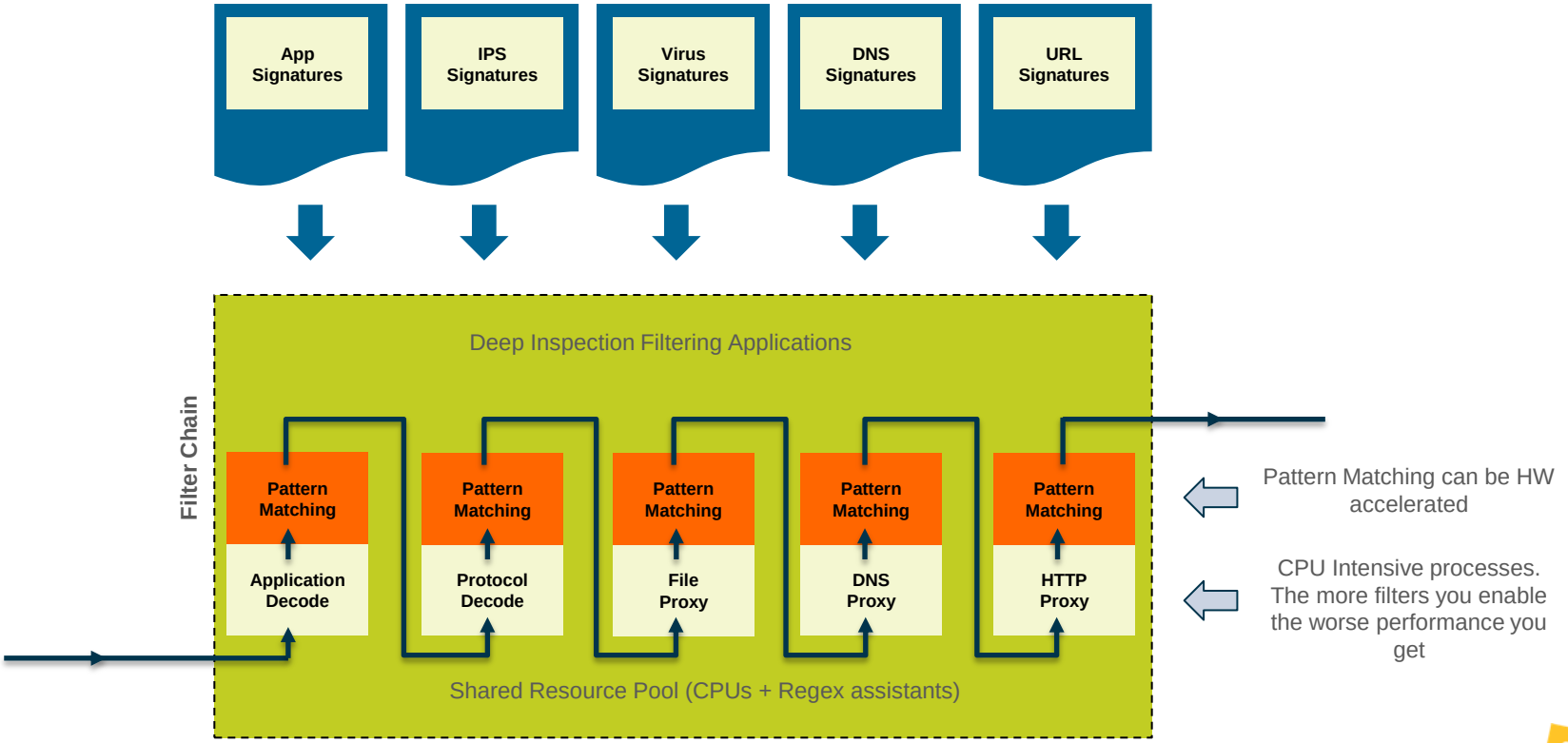
Single Pass Parallel Processing (SP3)



- Wydzielony Control Plane
- Wydzielony Data Plane
- Jednokrotne przejście pakietów
- Operacje wykonywane raz dla pakietu
  - Klasyfikacja ruchu (per aplikacja)
  - Mapowanie użytkownika do grupy
  - Skanowanie ruchu – zagrożenia, URLe, dane poufne
- Jedna polityka
- Równoległe przetwarzanie
- Silniki sprzętowe zapewniające równoczesną realizacje funkcji

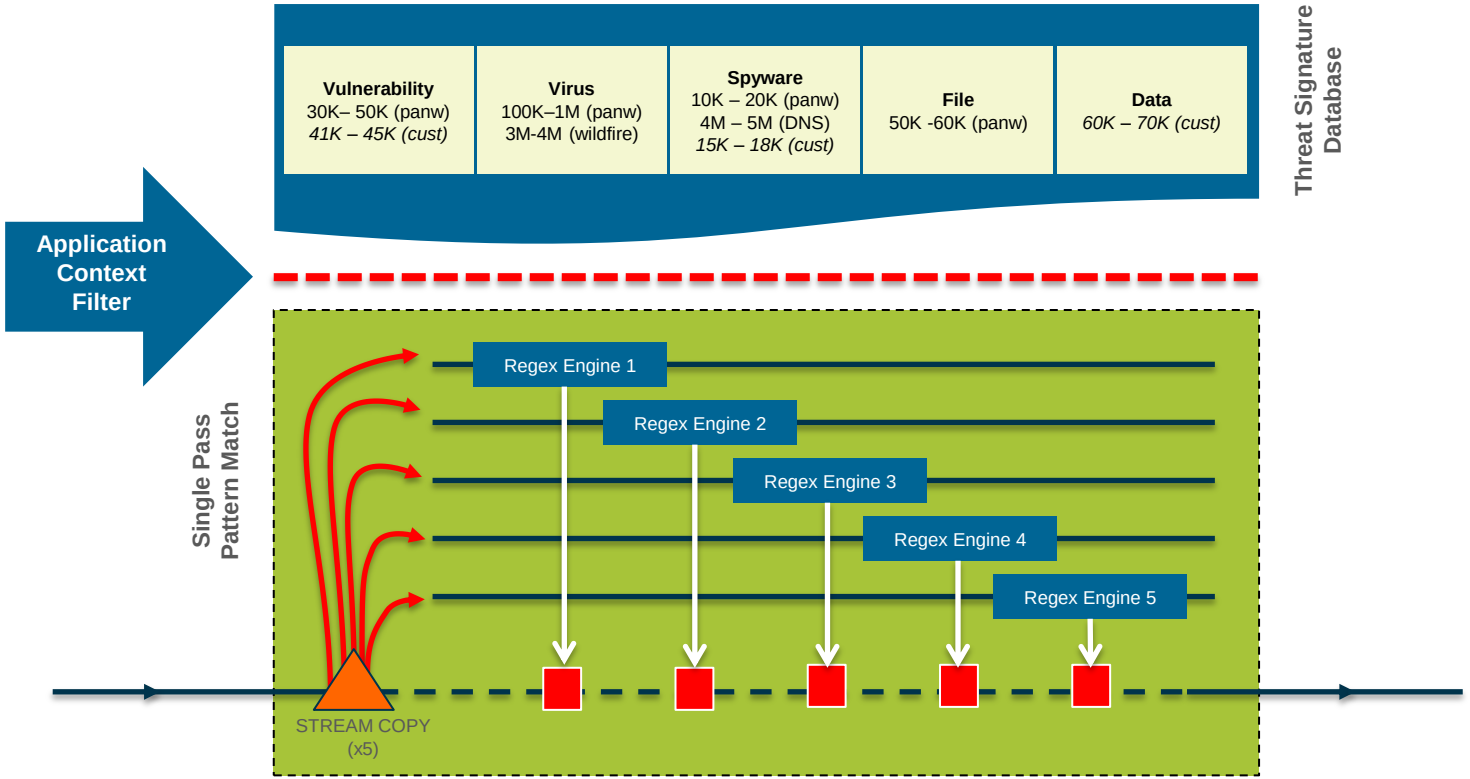
Przetwarzanie szeregowe

Moduły konkurują o wspólne zasoby sprzętowe

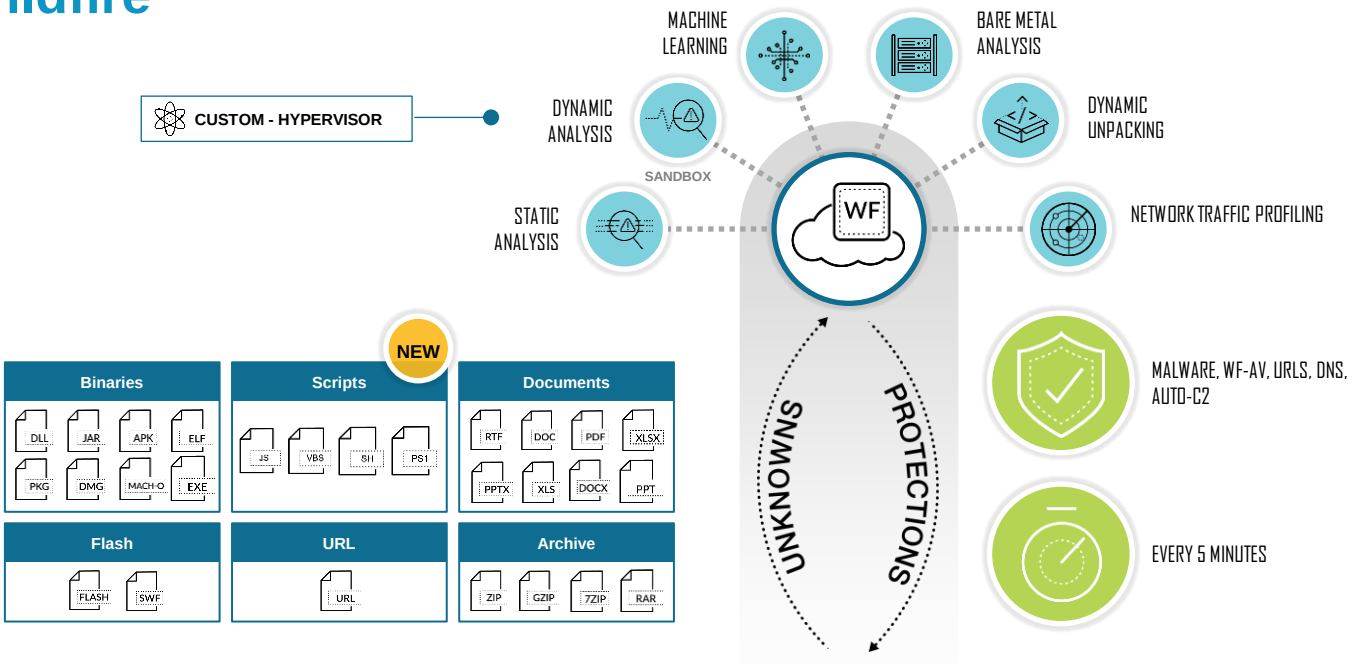


Single Pass Parallel Processing

Równoległa głęboka inspekcja pakietów z minimalnym opóźnieniem



Wildfire



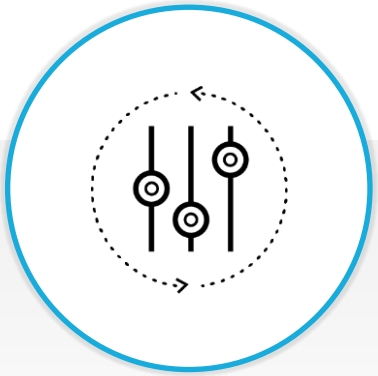
Sensors and Enforcement points

Policy optimizer

New!

WIĘKSZE BEZPIECZEŃSTWO
Wykorzystanie App-ID aby zmniejszyć wektor ataku

MNIEJSZA LICZBA BŁĘDÓW
Główna przyczyna naruszeń bezpieczeństwa



OSZCZĘDNOŚĆ CZASU
dzięki intuicyjnym regułom

Tradycyjne reguły widoczne w policy optimizer

Policies

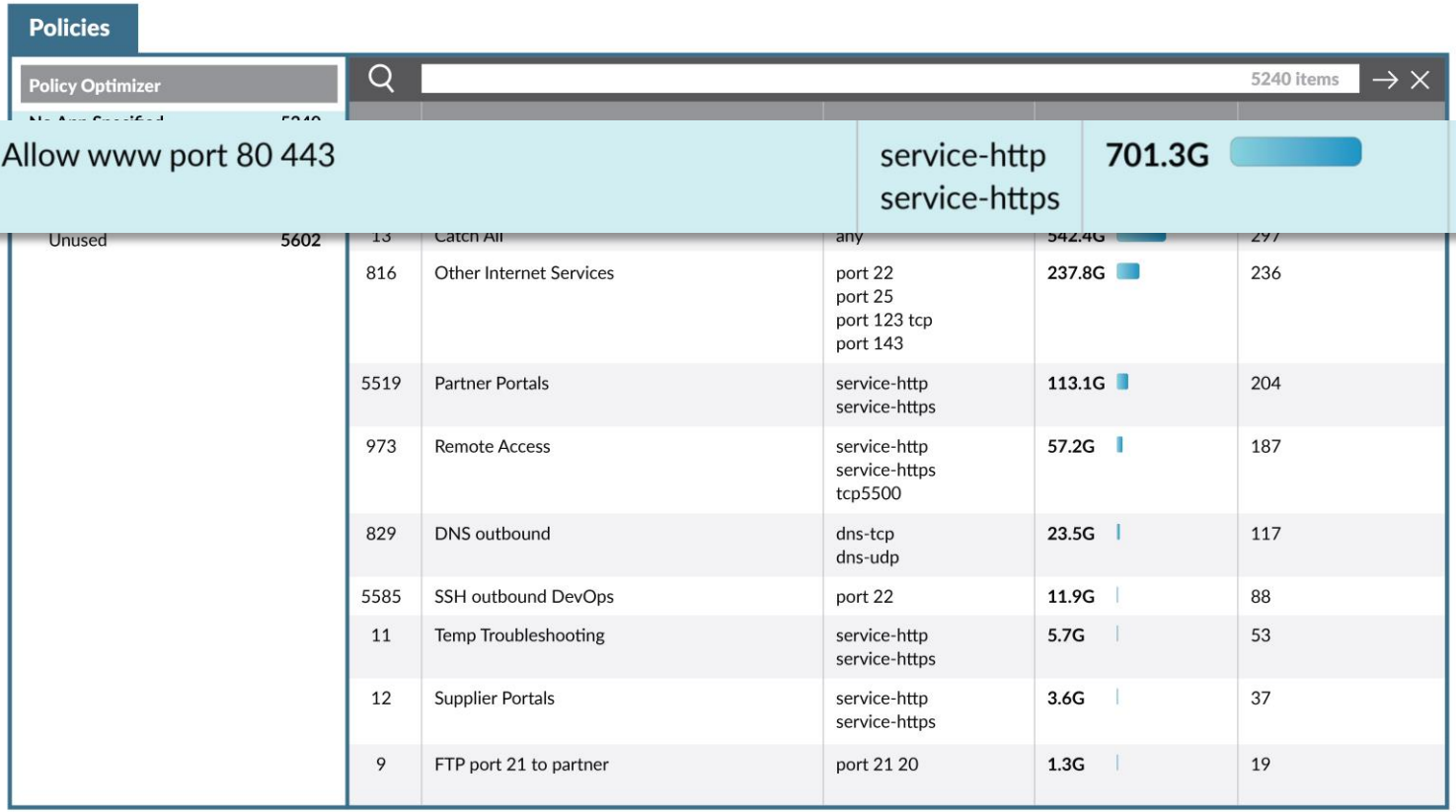
Policy Optimizer

No App Specified	**5240**
Unused Apps	**0**
Rule Usage	
Unused in 30 Days	**5604**
Unused in 90 Days	**5602**
Unused	**5602**

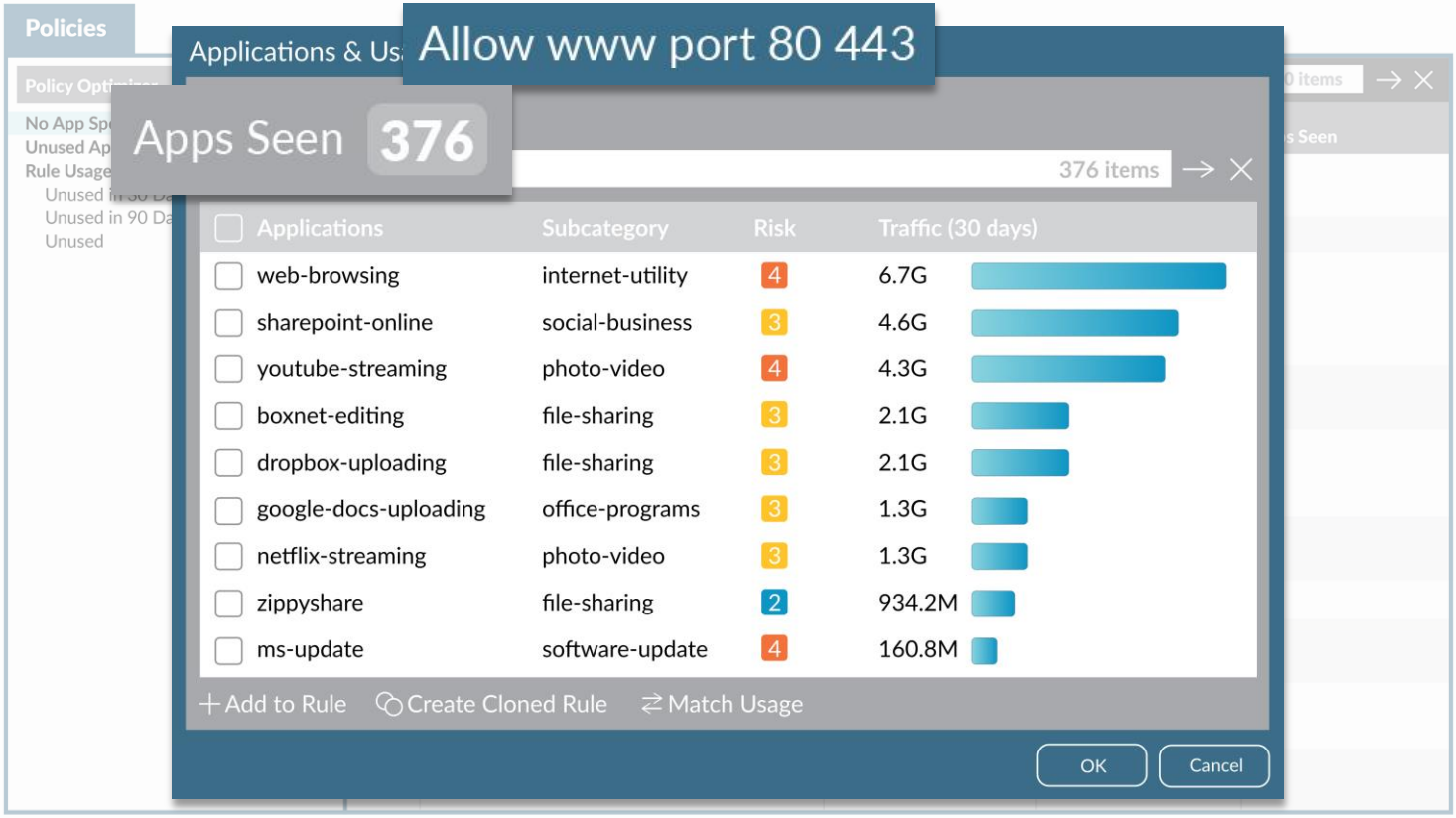
5240 items

	Name	Service	Traffic (Bytes, 30 days)	Apps Seen
4	Allow www port 80 443	service-http service-https	**701.3G**	376
13	Catch All	any	**542.4G**	297
816	Other Internet Services	port 22 port 25 port 123 tcp port 143	**237.8G**	236
5519	Partner Portals	service-http service-https	**113.1G**	204
973	Remote Access	service-http service-https tcp5500	**57.2G**	187
829	DNS outbound	dns-tcp dns-udp	**23.5G**	117
5585	SSH outbound DevOps	port 22	**11.9G**	88
11	Temp Troubleshooting	service-http service-https	**5.7G**	53
12	Supplier Portals	service-http service-https	**3.6G**	37
9	FTP port 21 to partner	port 21 20	**1.3G**	19

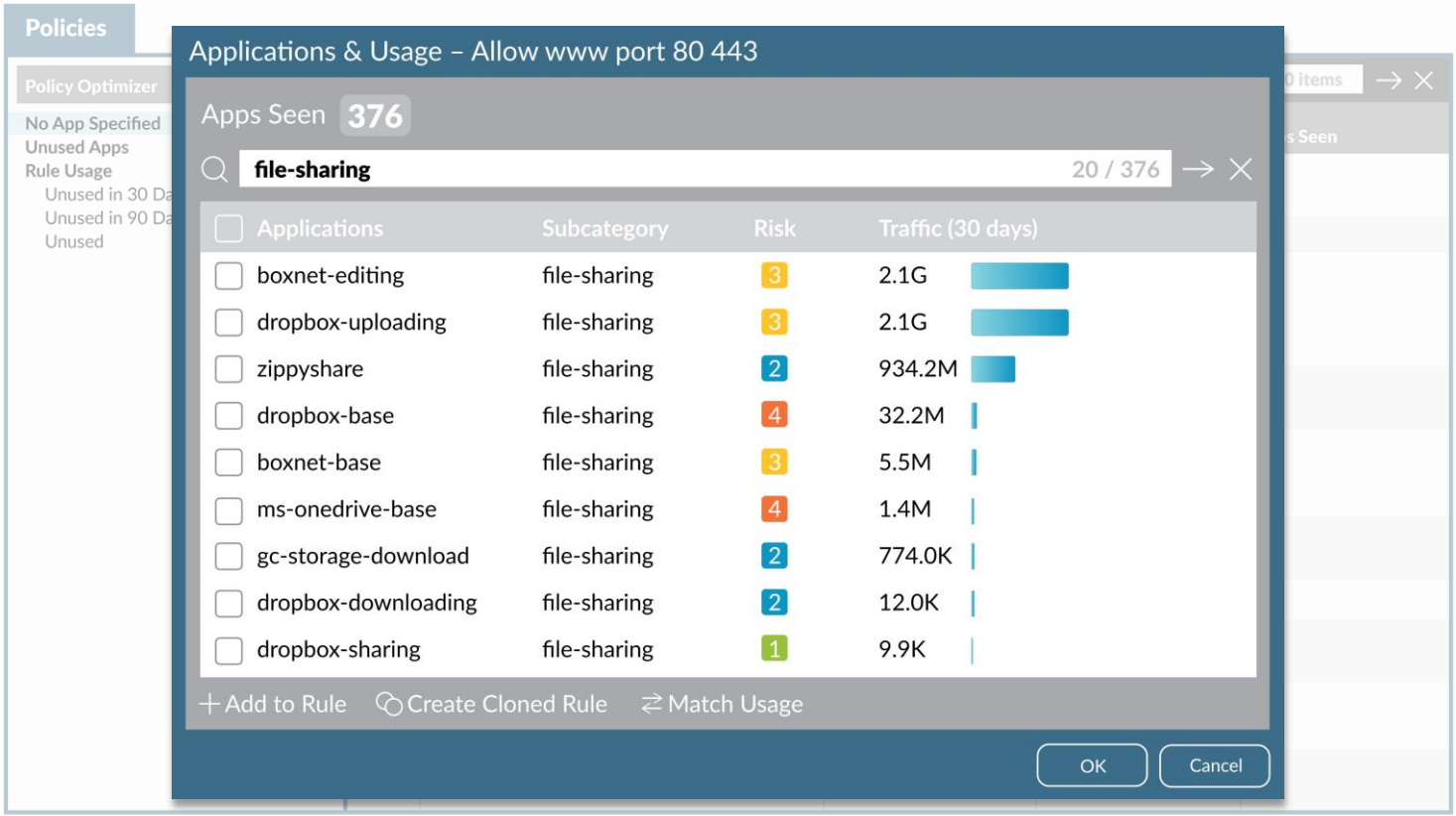
Krok 1: Wybór reguły do optymalizacji



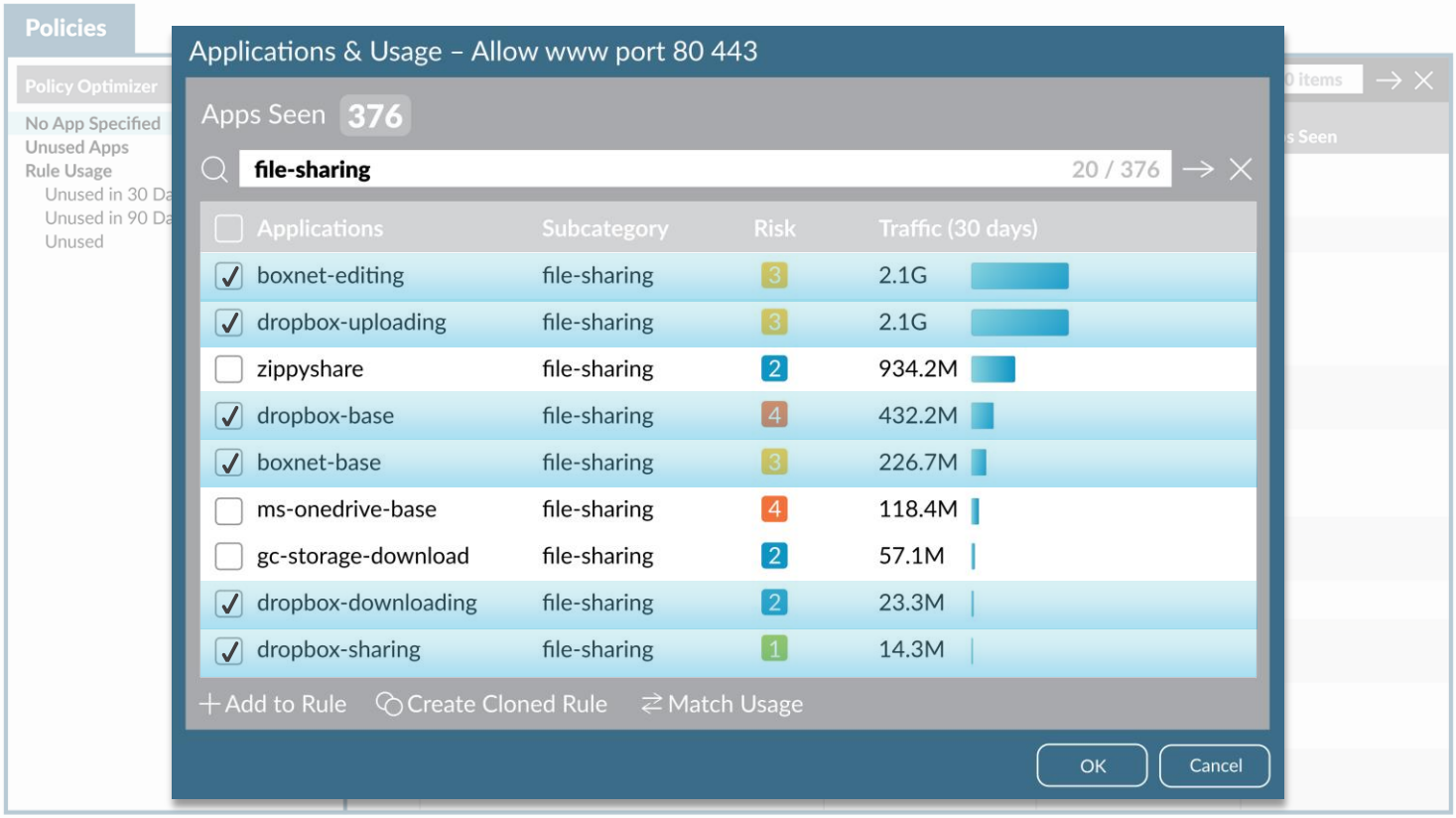
Krok 2: Podgląd aplikacji „wpadających” w regułę



Krok 3: Wybór interesującej nas kategorii (np. „file-sharing”)



Krok 4: Wybór interesujących nas aplikacji



Krok 5: Powstaje reguła bazująca na aplikacjach

	Name	Source User	[illegible]	Service	[illegible]	[illegible]
1	Sanctioned SaaS Apps	corp-users	boxnet concur confluence dropbox jira ms-office365 slack	application-default		Allow

Policies

Policy Optimizer	
No App Specified	**5240**
Unused Apps	**0**
Rule Usage	
Unused in 30 Days	**5604**
Unused in 90 Days	**5602**
Unused	**5602**

	Name	Service	Traffic (Bytes, 30 days)	Hit Count
4	Allow www port 80 443	service-http service-https	0	0

Wynik działania Policy Optimizer

70 items

	Name	Source User	[illegible]	Service	[illegible]	[illegible]
1	Sanctioned SaaS Apps	corp-users	boxnet concur confluence dropbox jira ms-office365 slack	application-default		Allow
2	Tolerated SaaS Apps	corp-users contractors	docusign evernote google-base google-cloud-storage google-docs	application-default		Allow
3	Approved Social Media	marketing	facebook glassdoor linkedin twitter	application-default		Allow
4	Approved Web Email	corp-users	gmail icloud yahoo-mail	application-default		Allow
5	Software Updates	corp-users marketing contractors	apple-update google-update java-update ms-update paloalto-updates	application-default		Allow
6	Other Web Traffic URL Filtering	corp-users contractors	ssl web-browsing	application-default		Allow

Zbiór narzędzi redukujących ryzyko ataku

NARZĘDZIA

- Security Lifecycle Review
- Expedition Migration Tool
- Best Practice Assessment
- Prevention Posture Assessment

FUNKCJE NGFW

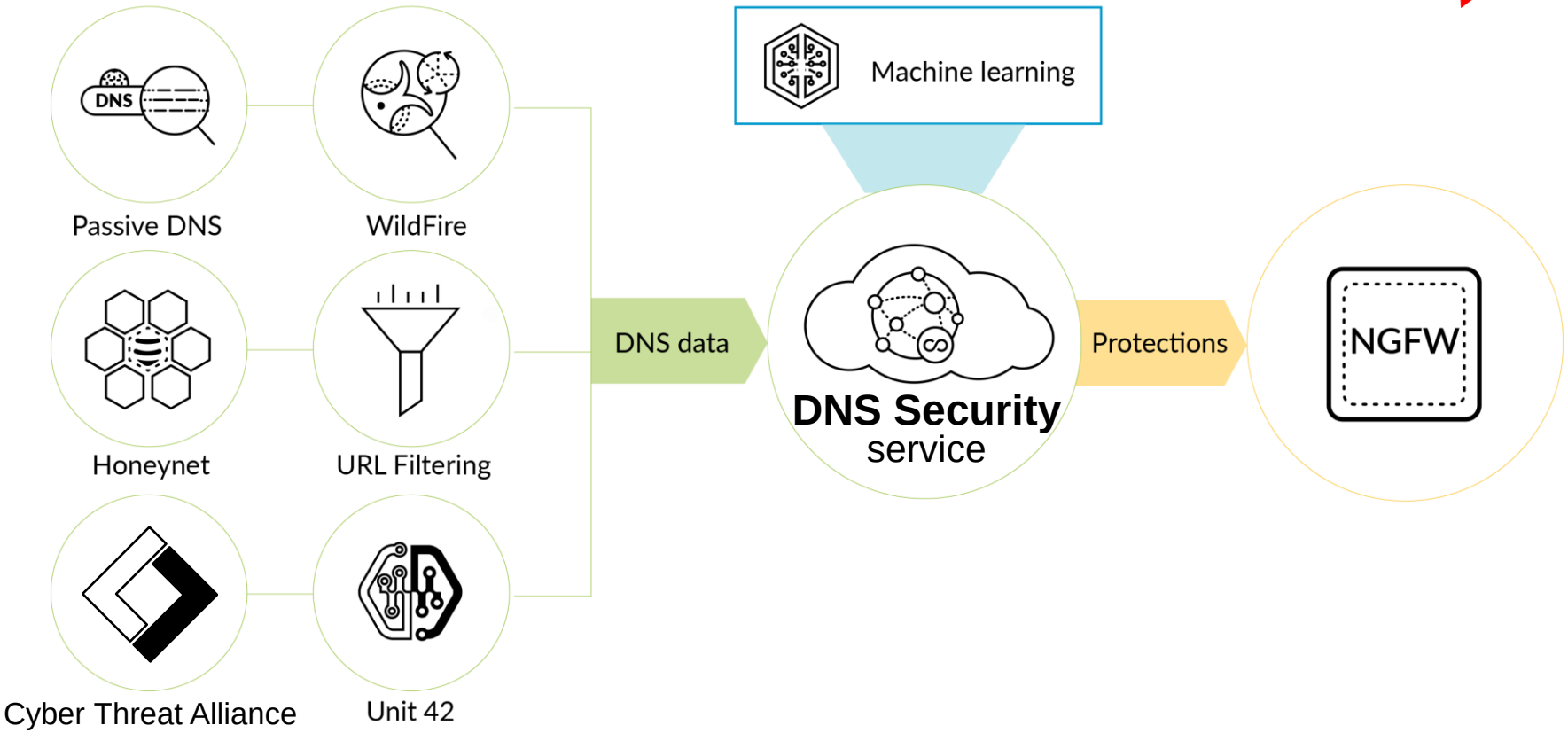
- Plain language security policies
- Rule usage tracker
- New Policy Optimizer

ZASOBY

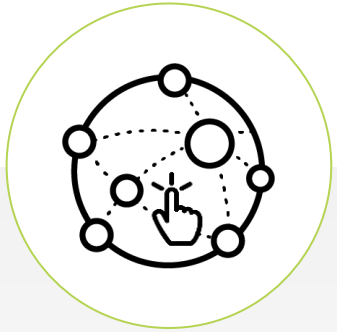
- Best practices documentation
  https://docs.paloaltonetworks.com/best-practices
- Live community
- Professional services
- Iron Skillet
  https://github.com/PaloAltoNetworks/iron-skillet

DNS Security

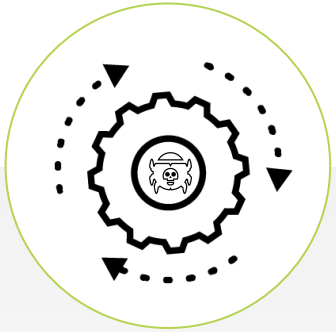
New!



Ataki wykorzystujące DNS są często niewykrywane



DNS wymagany jest do prawidłowego działania infrastruktury/biznesu



DNS jest powszechnie wykorzystywany przy próbach ataków

Klienci mają trudności z odpowiednio szybką aktualizacją informacji na temat złośliwych domen

Dlaczego ochrona DNS jest tak ważna?

90% złośliwego oprogramowania

Wykorzystuje DNS do komunikacji C2

18% złośliwego oprogramowania

Wykorzystuje DGA (domain generation algorithms) aby uniknąć wykrycia

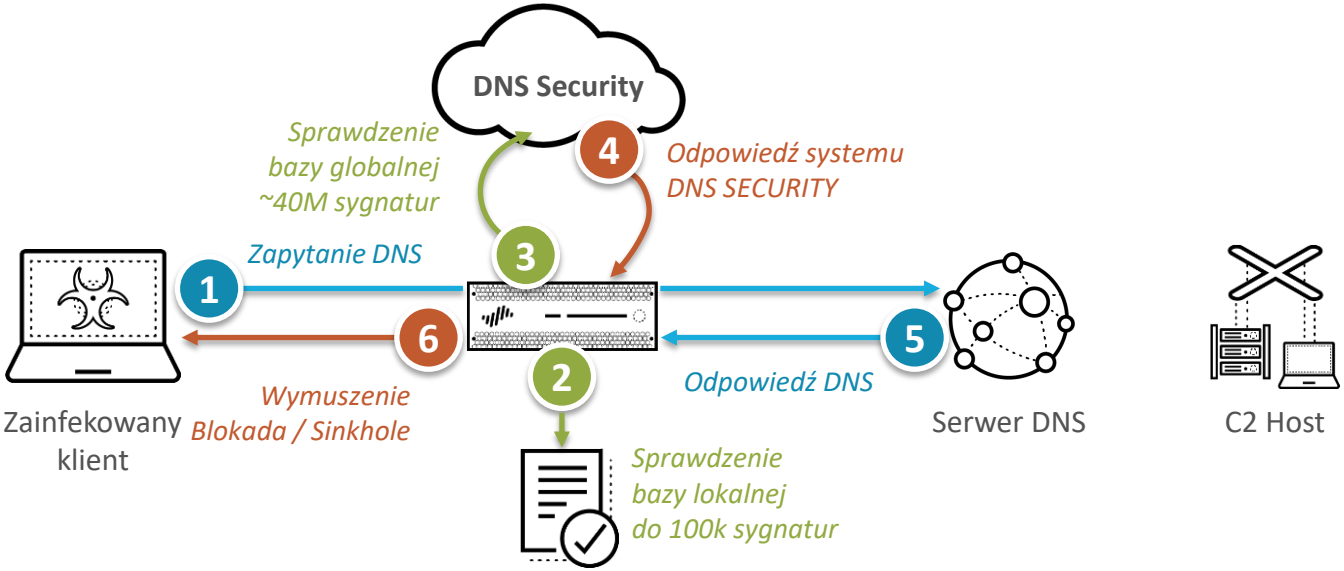
OilRig

Tunelowanie DNS
Szybka zmiana adresów IP

UNIT 42
RESEARCH

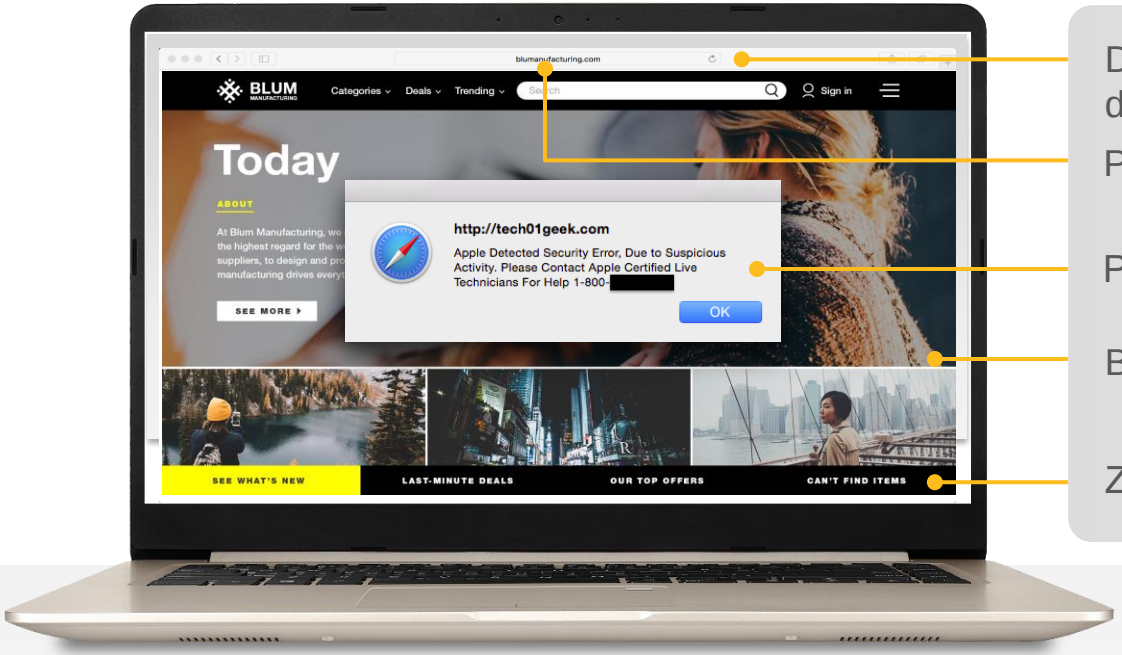
paloalto NETWORKS

Jak działa DNS Security



Granularna kategoryzacja URL'i

New!



Domena zarejestrowana 5 dni temu

Podejrzany URL

Podejrzana zawartość

Business & Economy

Zawartość marketingowa

NOWE KATEGORIE W ZALEŻNOŚCI OD RYZYKA

Poziom ryzyka | Ostatnio zarejestrowane | Dynamic-DNS

WŁASNE FILTRY KATEGORII

Możliwość łączenia kilku kategorii

Klasyfikacja ryzyka na bazie skorelowanych danych

Niskie Ryzyko

Domena lub host niezwiązany ze złośliwymi działaniami przez okres co najmniej 90 dni.

Średnie Ryzyko

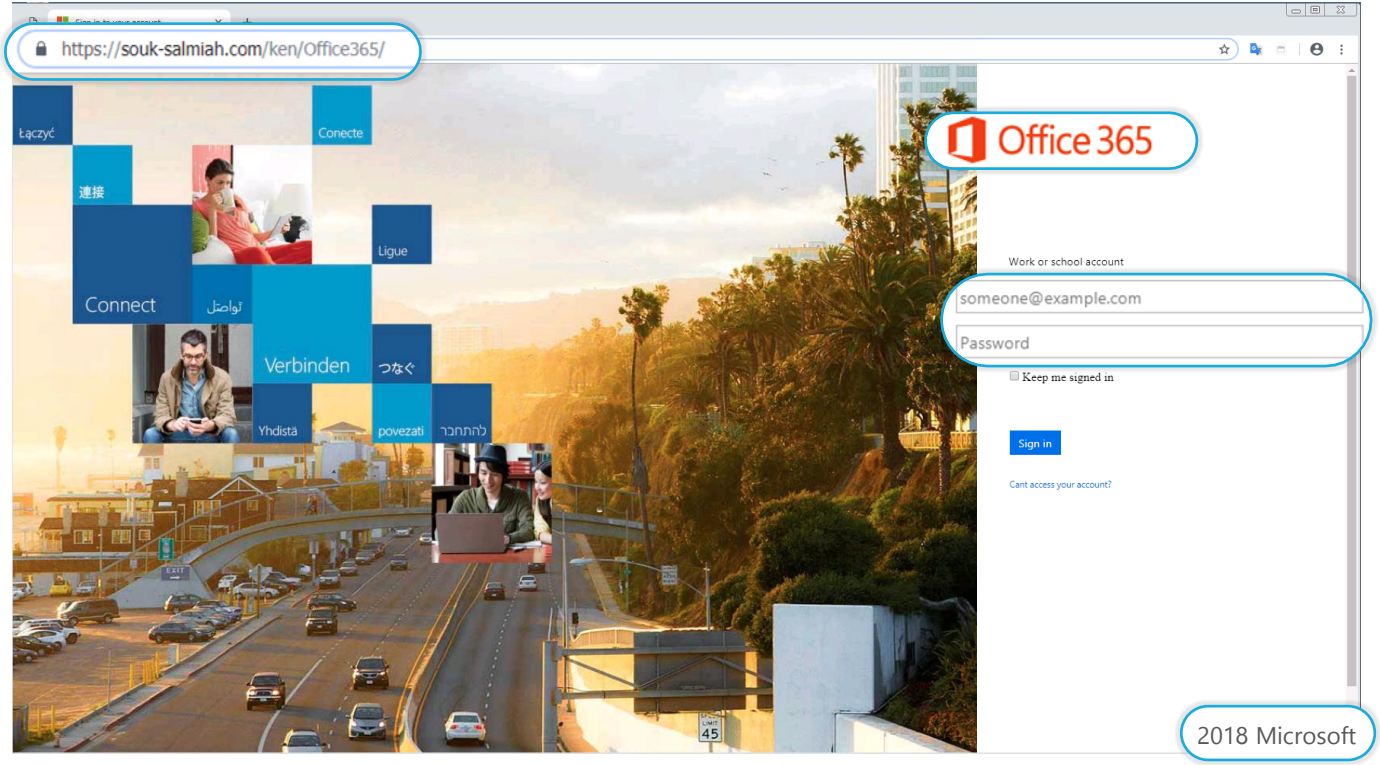
Domena lub host związany w ciągu ostatnich 90 dni ze złośliwymi działaniami lub podatna na nadużycia, ale nie wykazująca tych cech obecnie.

Wysokie Ryzyko

Domena lub host obecnie związany ze złośliwym działaniem lub powszechnie wykorzystywana do złośliwego działania ze względu na swoją naturę.

Analiza zawartości stron phishing'owych

New!



Rozpoznawanie obrazków

Blokowanie zaawansowanych ataków phisingowych z wykorzystaniem ML

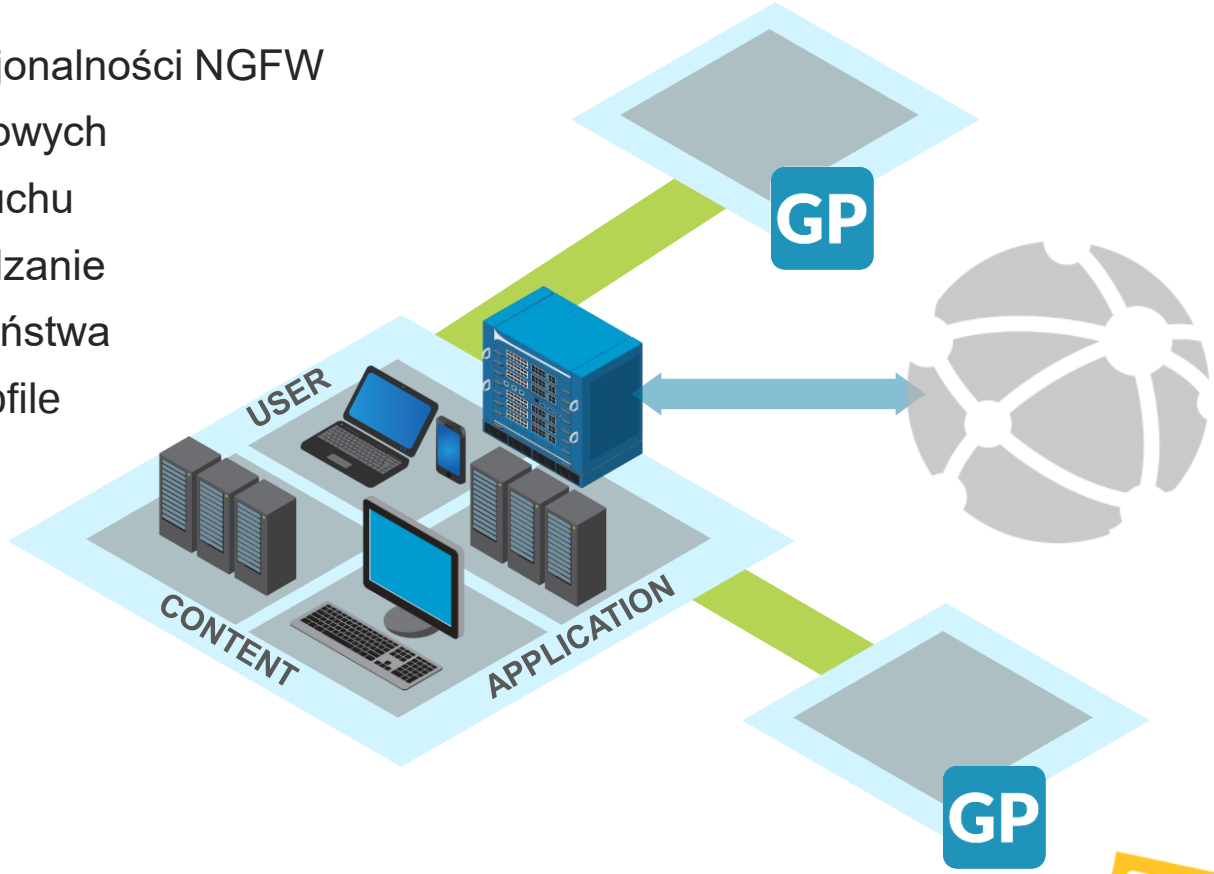
Skoordynowana analiza

Identyfikacja nowych typów stron phisingowych z wysoką dokładnością

paloalto NETWORKS

Podłączanie użytkowników zdalnych poprzez Global Protect

- Rozciągnięcie funkcjonalności NGFW do urządzeń końcowych
- Pełna widoczność ruchu
- Uproszczone zarządzanie polityką bezpieczeństwa
- Host Information Profile
- Clientless (SSL)
- IPSec/SSL
- Wsparcie dla MFA
- Integracja z MDM



Platformy wspierane przez Global Protect

techDOCS paloalto

Products | Recently Updated | Best Practices | Resources

Home | Compatibility Matrix

Compatibility Matrix

DOWNLOAD PDF

LAST UPDATED: Thu Jan 10 08:18:52 PST 2019

Table of Contents

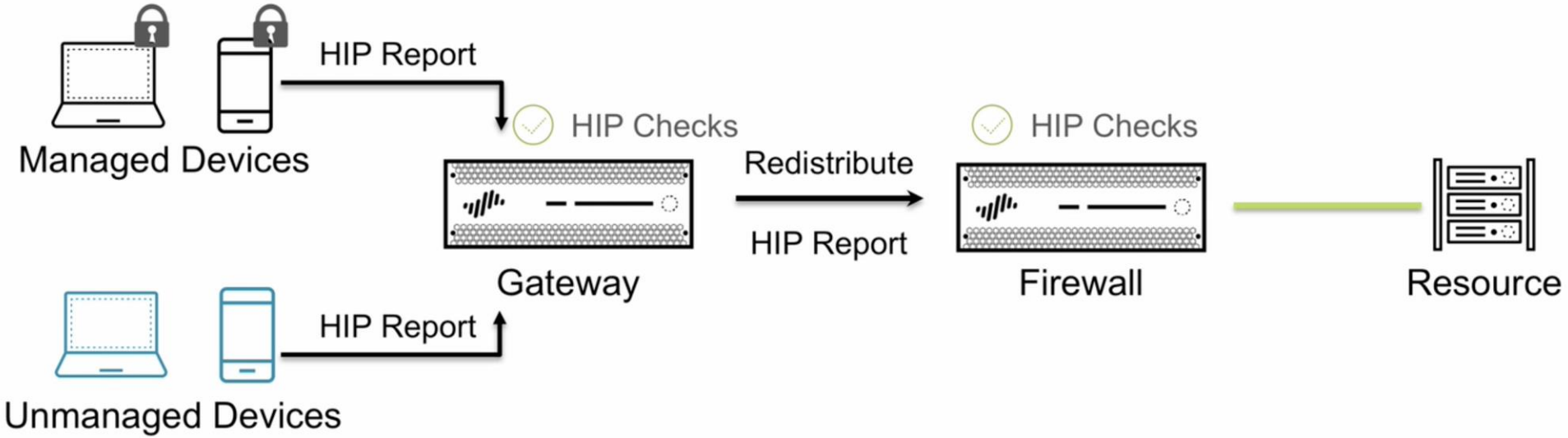
https://docs.paloaltonetworks.com/compatibility-matrix

- iOS, Mac OS, Android, Chrome OS, Linux, Windows

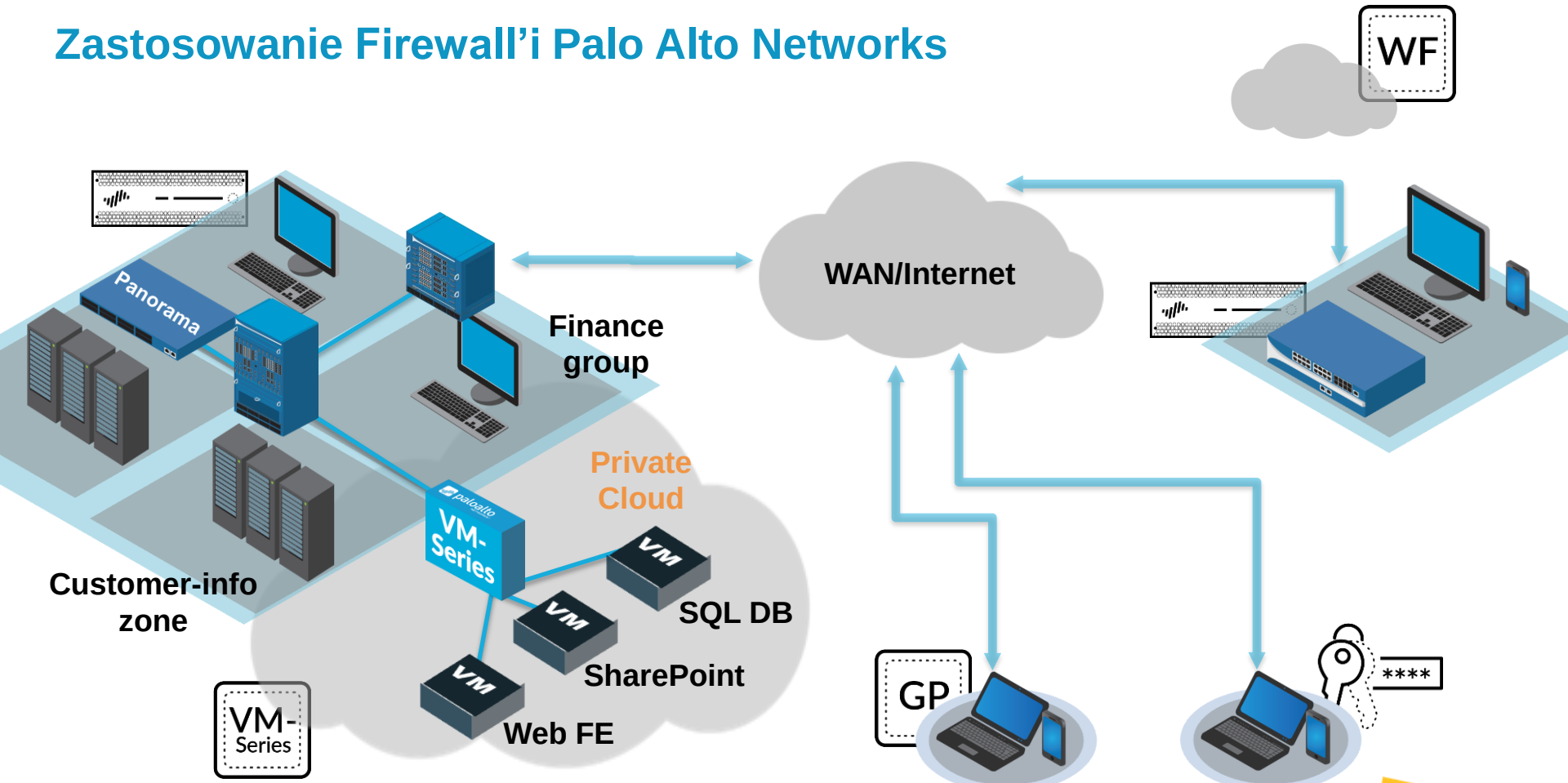
OPERATING SYSTEM	RELEASE 4.0	RELEASE 4.1	RELEASE 5.0
Apple iOS			
iOS 8	–	–	–
iOS 9	–	–	–
iOS 10	✓ (64-bit devices only)	✓ (64-bit devices only)	✓ (64-bit devices only)
iOS 11	–	✓ (64-bit devices only)	✓ (64-bit devices only)
iOS 12	–	–	✓ (64-bit devices only)
Apple Mac			
Mac OS X 10.5 (64-bit only)	–	–	–
Mac OS X 10.6	–	–	–

Global Protect i redystrybucja HIP

New!



Zastosowanie Firewall'i Palo Alto Networks



Ochrona końcówek

Różnica między Exploit a Malware

Exploits

Zmodyfikowane treści lub pliki danych

Omijają normalne działanie aplikacji

≠

Malware

Programy wykonywalne

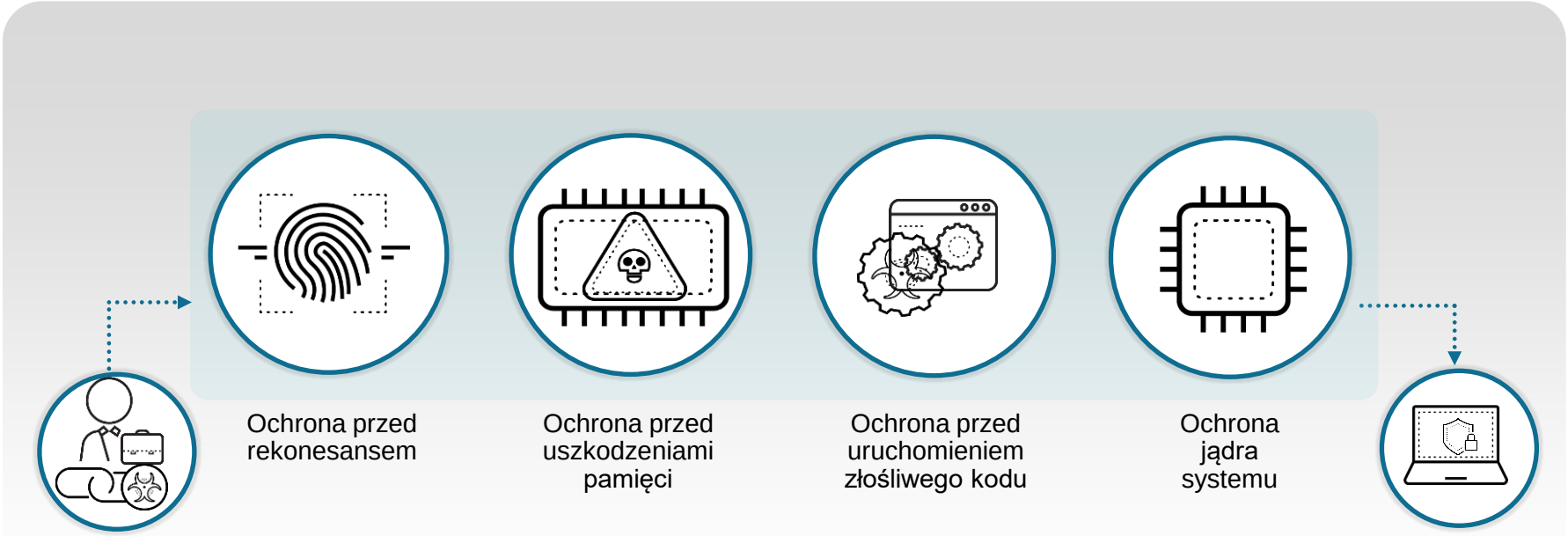
Wykonują złośliwe działanie

Traps, czyli Advanced Enpoint Protection

- Ochrona stacji końcowej przed złośliwym oprogramowaniem:
  - Restrykcje uruchamiania (foldery, hash-e)
  - Integracja z Wildfire
  - Lokalna analiza statyczna
  - Silnik anty-ransomware
  - Silnik behawioralny od wersji 6.0

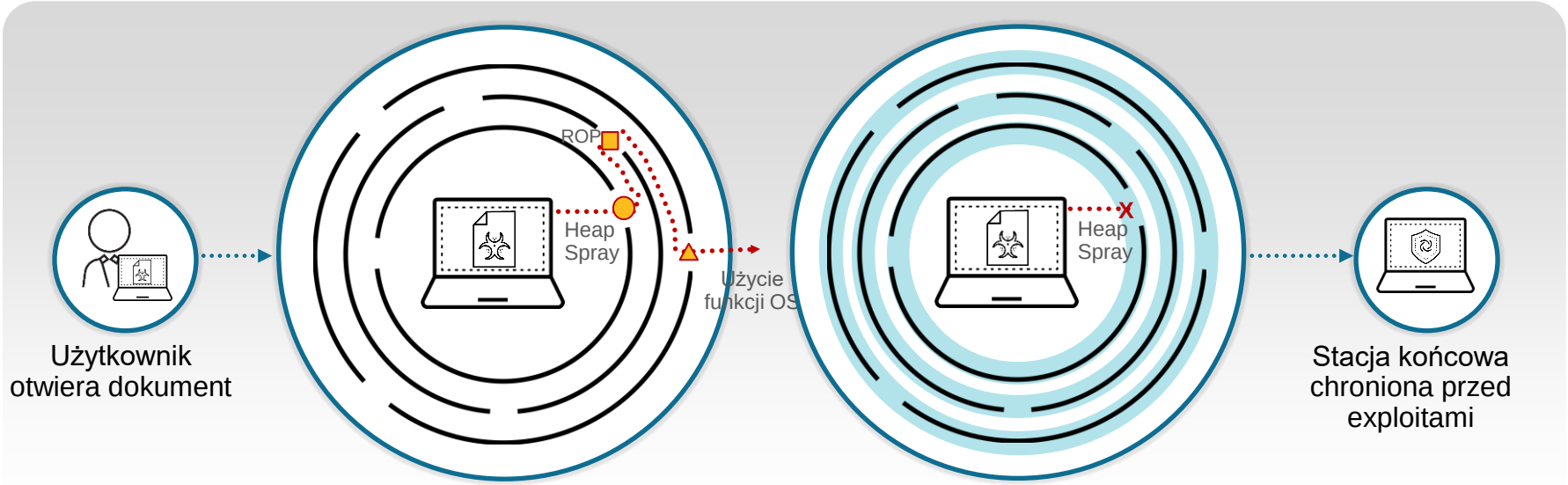
- Ochrona stacji końcowej przed próbami exploitacji:
  - dla Microsoft Windows od XP SP3
  - dla Mac OS od 10.10 (Yosemite)
  - dla Linuxa od RedHat 6.x, CentOS 6.x, Ubuntu Server 12.x, SUSE 12.1

Ochrona przed metodami exploitacji



Wiele metod ochrony które zatrzymują ataki „zero day”

Ochrona przed metodami exploitacji



Traps skupiają się na metodach exploitacji *a nie na konkretnych exploitach*

BLOKUJ ZNANE I NOWE ZŁOŚLIWE OPROGRAMOWANIE

Wiele metod prewencji poprawiające skuteczność i zasięg ochrony

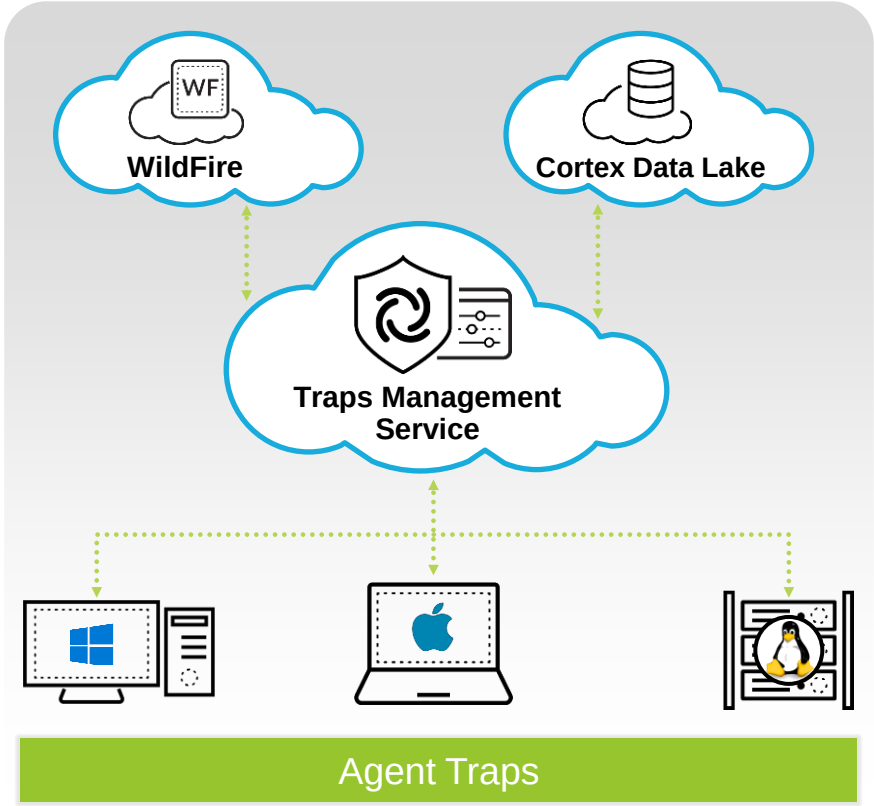
Traps Management Service

System dostępny z chmury

- System zarządzania przeniesiony do chmury
- Brak konieczności instalowania lokalnych serwerów
- Nowy, bardziej intuicyjny interfejs admin

Integracja z Cortex

- Szczegółowe logowanie zdarzeń do Cortex Data Lake
- Umożliwia korelowanie zdarzeń pochodzących z końcówek, sieci i chmury
- Pozwala na łatwiejszą integracje nowych funkcji (np. Cortex XDR)



Lepsze „doznania” administracyjne

Intuicyjny interfejs webowy

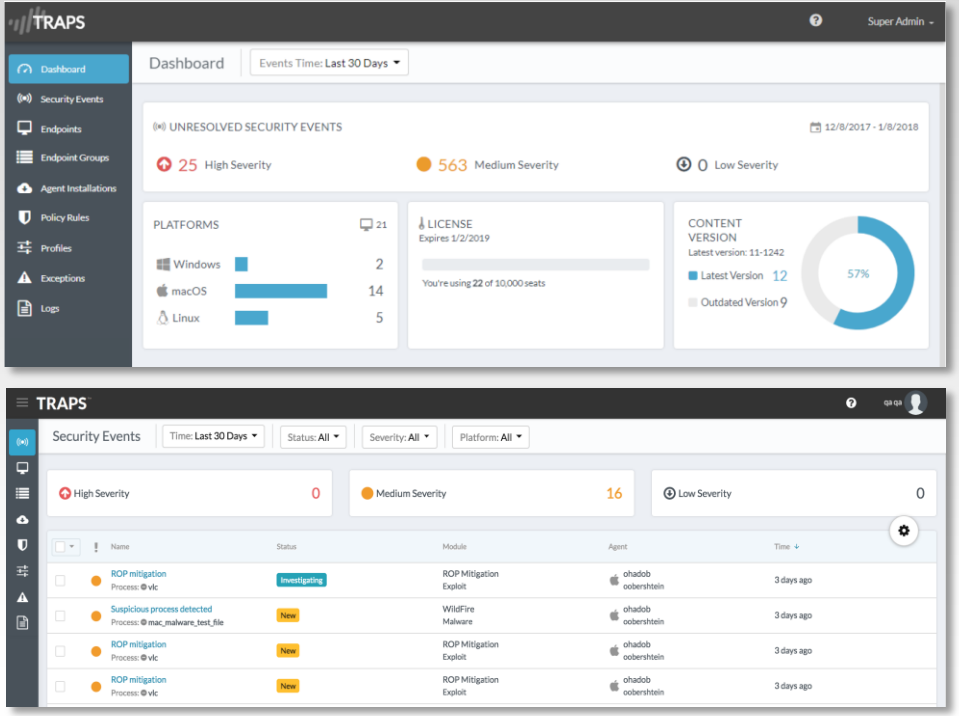
- Minimalizujący wyzwania administracyjne
- Pozwalający na konsekwentne zarządzanie politykami
- Pozwalający na dynamiczne grupowanie stacji końcowych

Uproszczone zarządzanie zdarzeniami

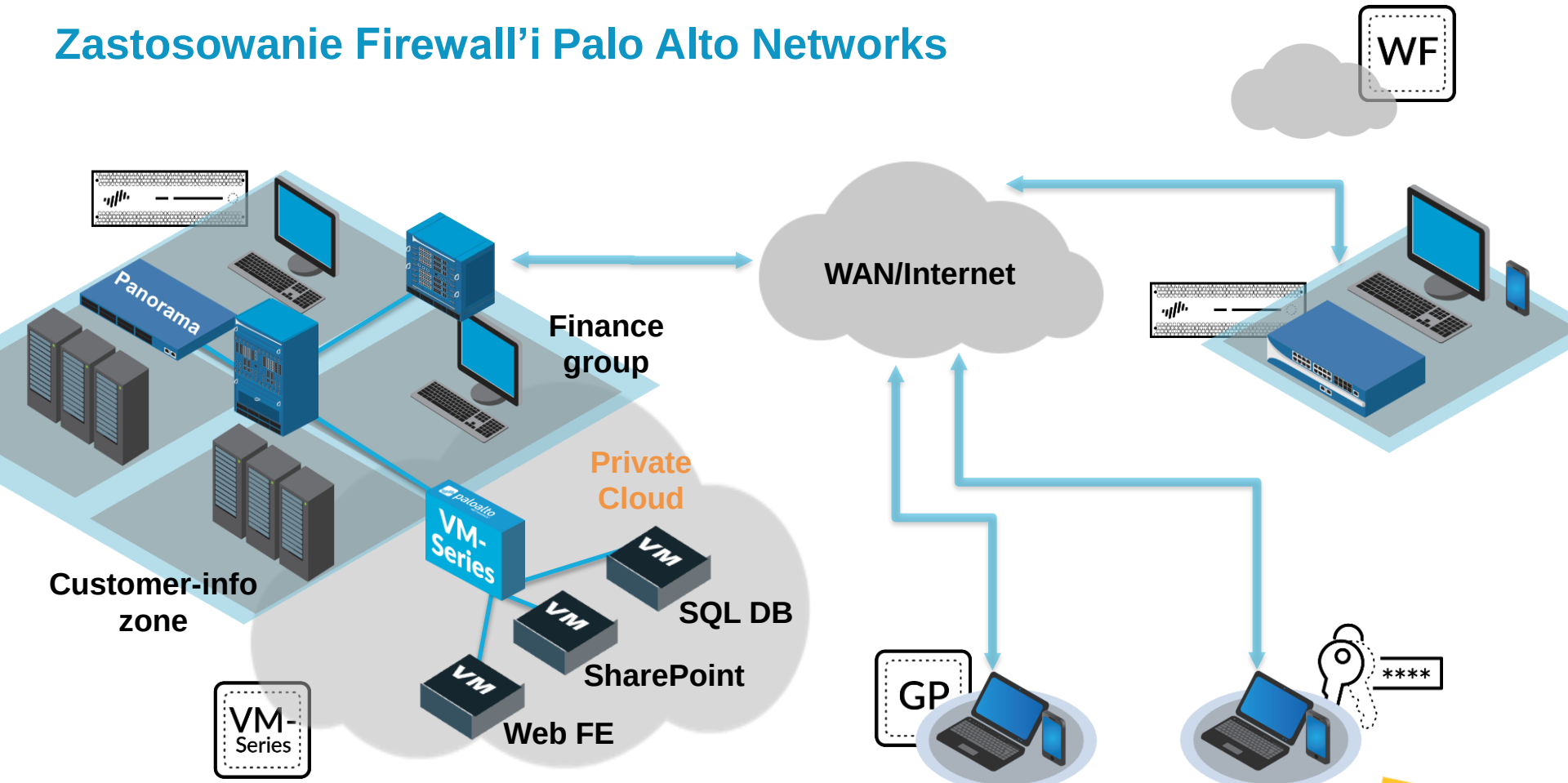
- Panel kontrolny zdarzeń
- Ocena stanu zagrożeń
- Śledzenie statusu zdarzeń

Zintegrowane raporty WildFire

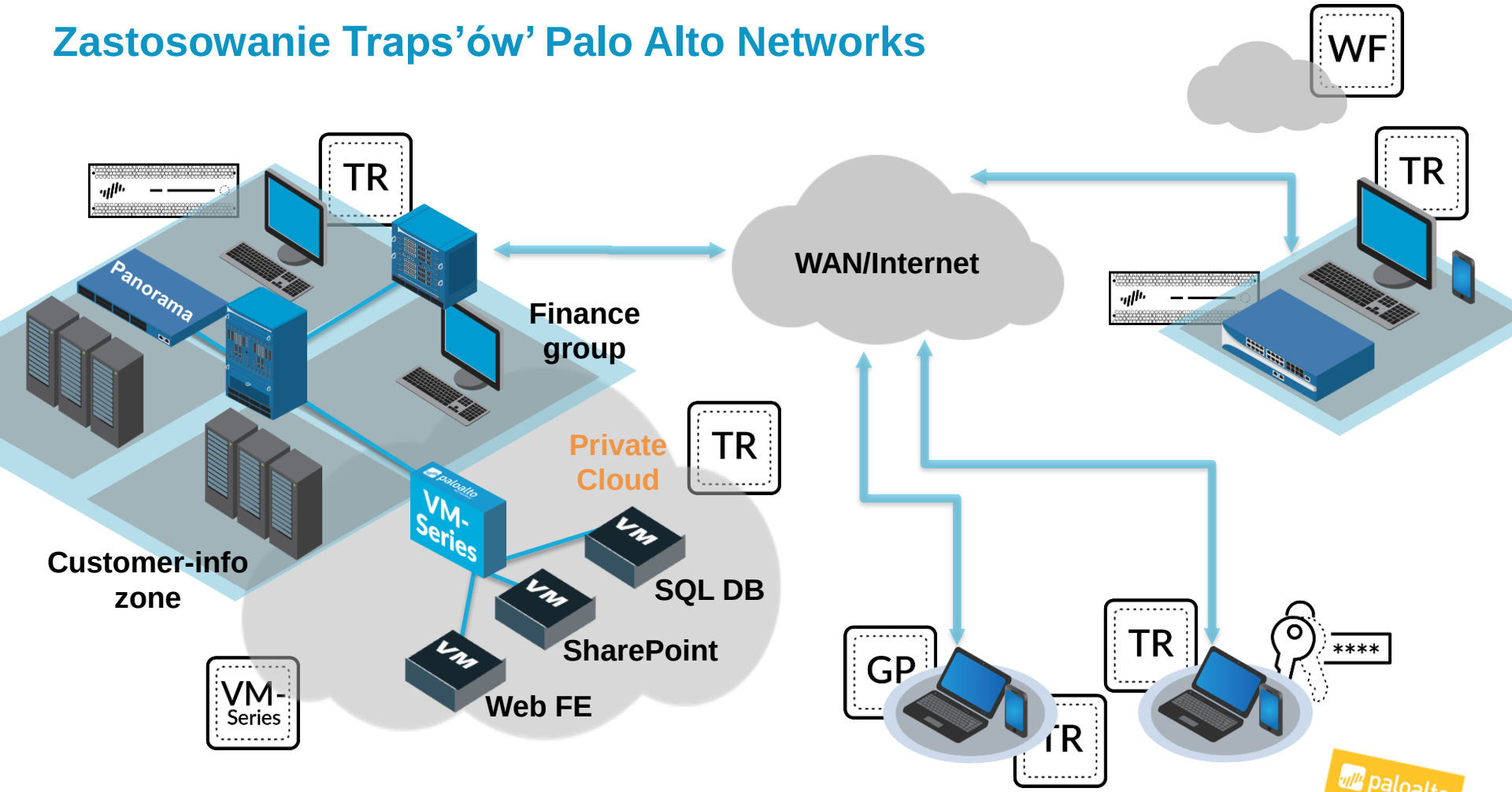
- Szybki wgląd w zagrożenia
- Wyświetlenie informacji o:
  - Zaatakowanych użytkownikach
  - Aplikacjach użytych przez zagrożenia
  - URL-ach użytych przez zagrożenia
- Zaobserwowanych zachowaniach



Zastosowanie Firewall'i Palo Alto Networks



Zastosowanie Traps'ów' Palo Alto Networks



Podsumowanie

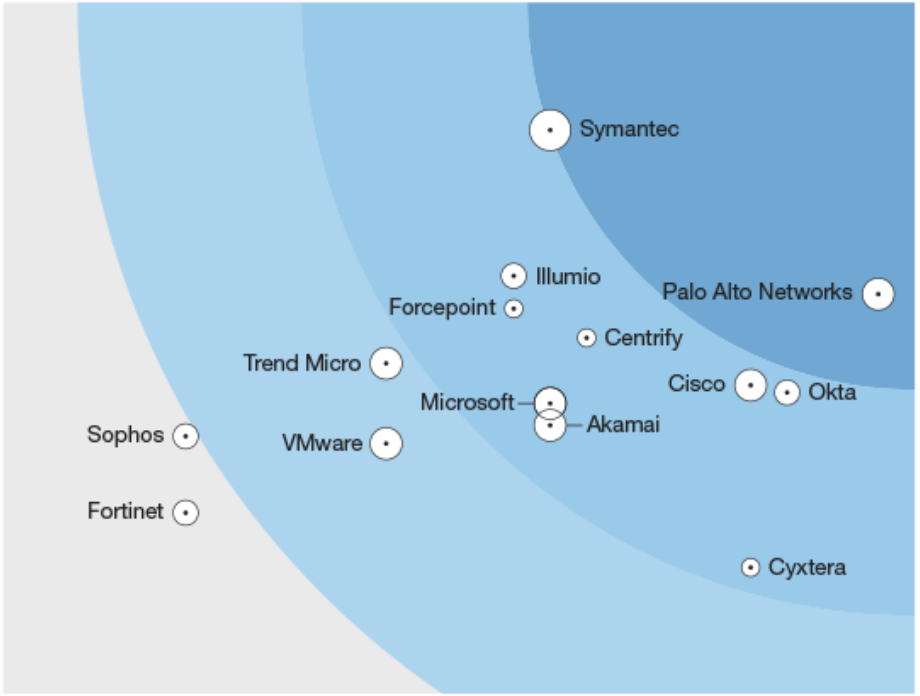
Palo Alto Networks Security Operating Platform

Lider nie tylko w Gartnerze:

THE FORRESTER WAVE™

Zero Trust eXtended (ZTX) Ecosystem Providers

Q4 2018



Dziękuję!