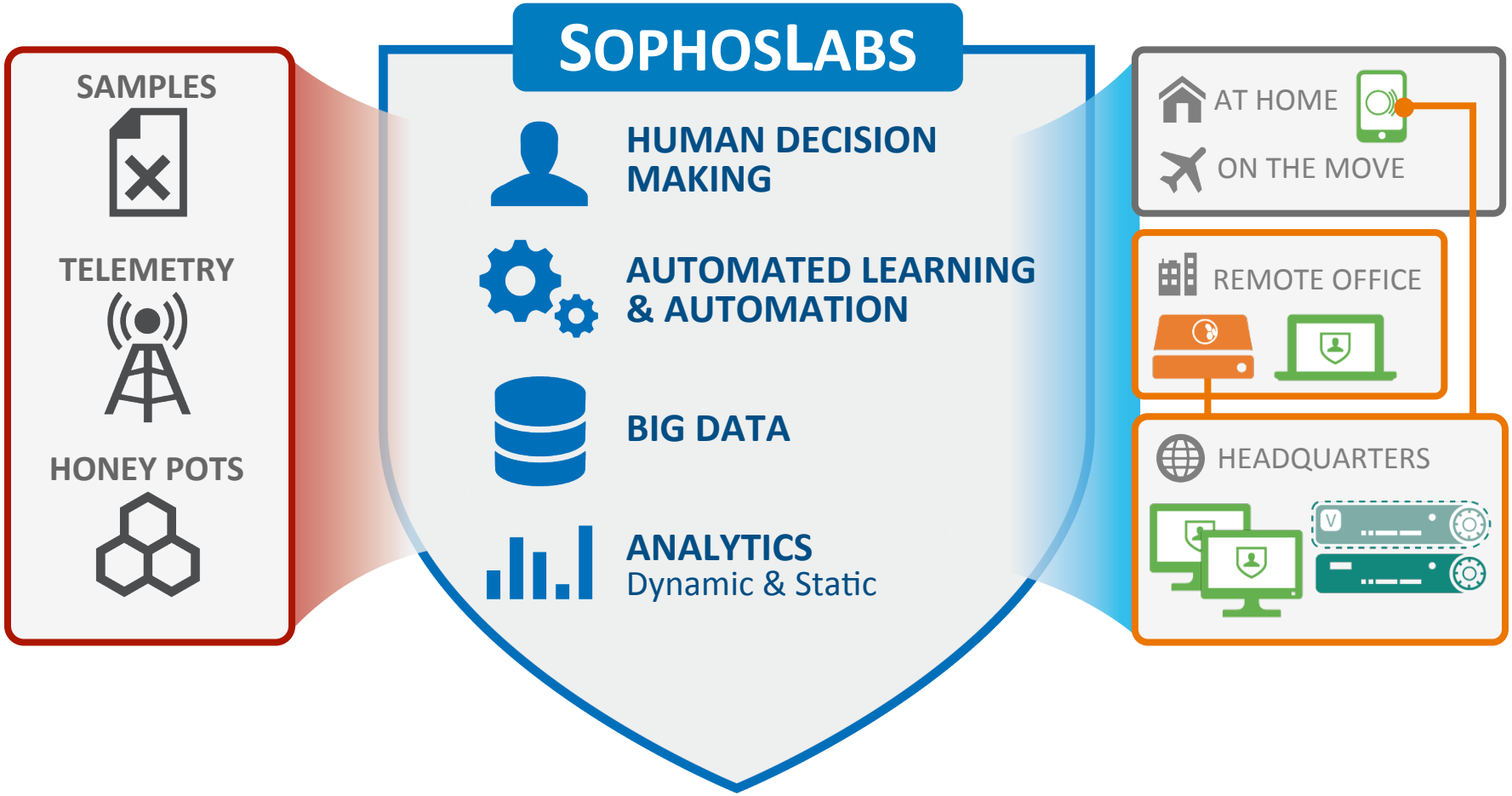
Sophos Email Protection

Łukasz Naumowicz

22.06.2016

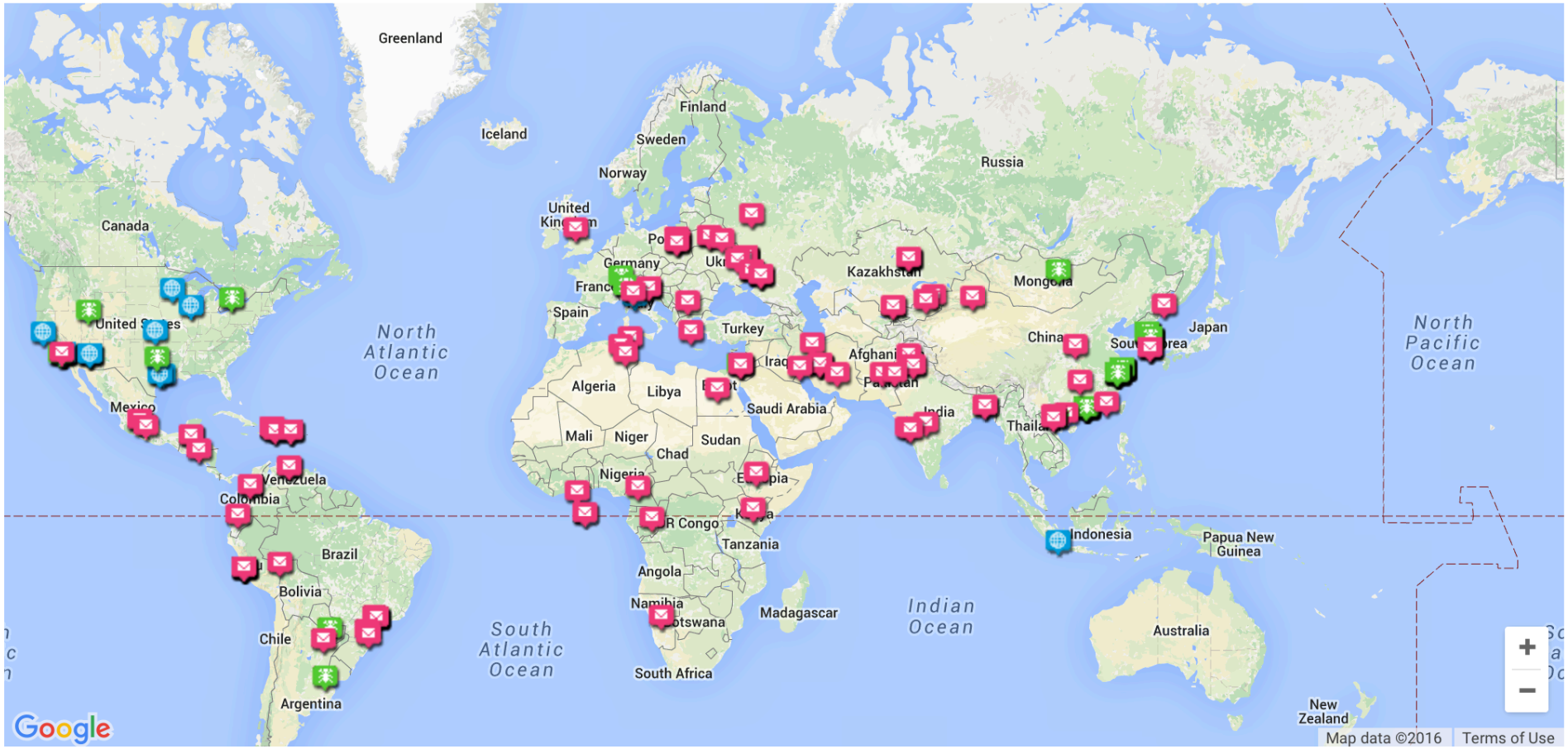
SOPHOS

Sophos Labs



https://www.sophos.com/en-us/threat-center/threat-monitoring/threatdashboard.aspx

Sophos Labs



https://www.sophos.com/en-us/threat-center/threat-monitoring/threatdashboard.aspx

Źródła informacji o spamie

- ~100 pułapek spam w 22 krajach
  >30 milionów wiadomości dziennie
- Dane Real-time, IP reputation
- Dane pochodzące z urządzeń
- Dane od klientów
  (spam, spear phishing, false positives)

Total countries: 22

Country Name	Traps
Canada	12
United States	11
Russian Federation	1
France	12
Japan	2
Germany	12
Taiwan, Province of China	2
China	2
Hong Kong	1
Italy	13
New Zealand	1
Australia	7
Thailand	1
United Kingdom	1
Spain	3
Croatia (local name: Hrvatska)	2
Singapore	2
Finland	1
Poland	2
Ireland	1
Philippines	1
Malaysia	1

Sophos Labs

Malware | Spam | Web

Today's Spam Threats

We monitor spam from all sources, every day. View our spam dashboard for real-time data.

More Spam Threat Stats

DrodZp	66.7%	▲
ZipMal	11.1%	▲
JSDldr	11.1%	▼
20151641	5.6%	▲
JavaBz	5.6%	▲

Mal/DrodZp-A

Category: Viruses and Spyware
Type: Malicious behavior
Prevalence:

Protection available since: 18 Jul 2012 20:57:09 (GMT)
Last Updated: 04 Oct 2012 23:12:17 (GMT)

Download our free Virus Removal Tool - Find and remove threats your antivirus missed

Summary | **More information**

Mal/DrodZp-A is an archive with malicious content. It often has a filename that uses social engineering to encourage receipients to open it, for example by pretending to be an invoice or order receipt.

Mal/DrodZp-A is typically seen as an attachment in spam email messages.

Examples of Mal/DrodZp-A include:

Download Sophos Home

Free business-grade security for the home.

https://www.sophos.com/en-us/threat-center/threat-monitoring/threatdashboard.aspx

Prywatność a poczta email…

Prywatność a poczta email…

SOPHOS

Rozwiązania do ochrony poczty

Portfolio rozwiązań do ochrony poczty

Sophos Email Appliances

Szyfrowanie danych

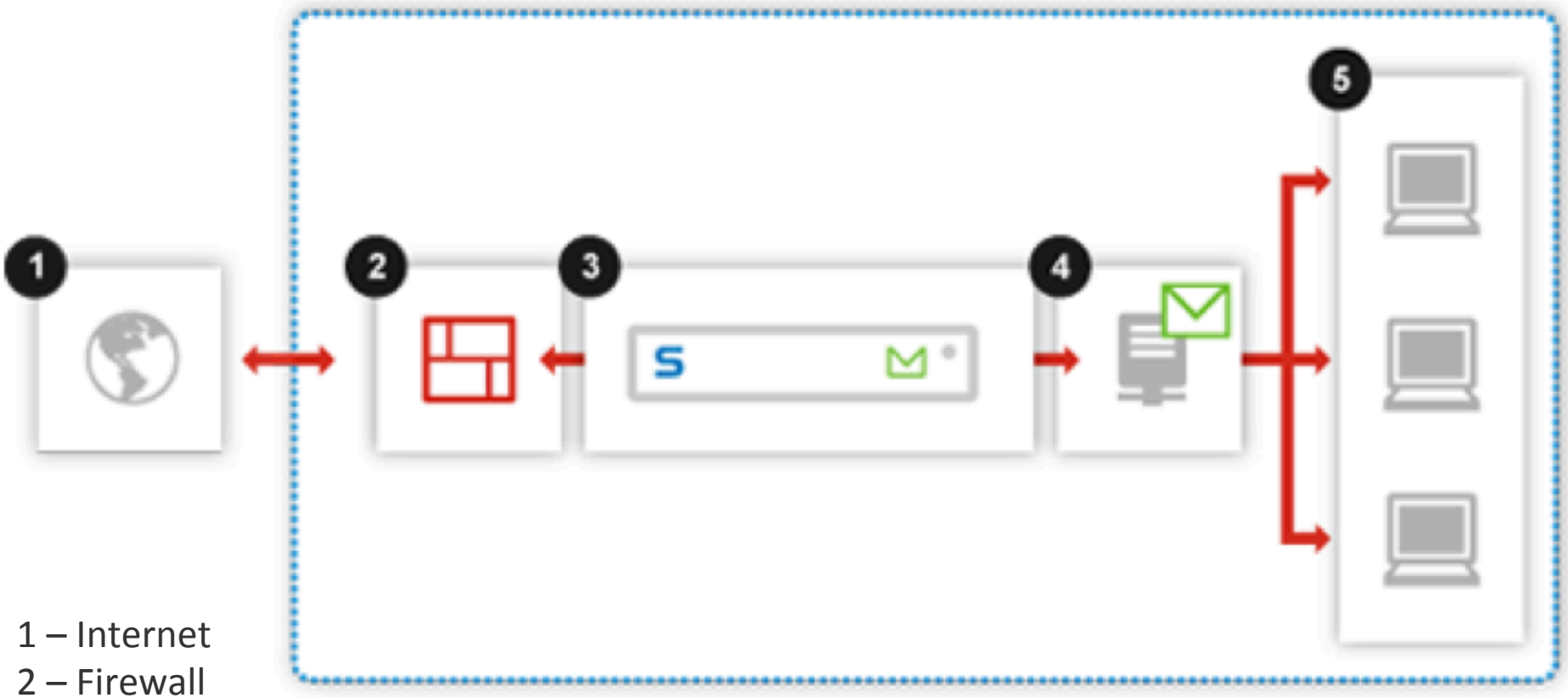
Ochrona DLP

SOPHOS
Virtual Appliance

Anty-Spam

Anty-Malware

SEA – przykład instalacji



1 – Internet
2 – Firewall
3 - Sophos Email Appliance
4 – Serwer pocztowy
5 – klienci poczty

SEA sprzęt

	ES100	ES1100	ES5000
Message Capacity	Up to 95,000/hour	Up to 200,000/ hour	Up to 550,000/ hour
Hardware			
Processor	ULV Dual core	Dual core	Quad core
Hard drive	250 GB SATA	250 GB SATA	2 hot-swap 160 GB SAS (RAID 1)
Power supply	200W 100-240V AC	260W 100-240V AC	2 hot-swap 920W 100-240V AC
Mounting	1U rack-mountable	1U rack-mountable	1U rack-mountable
Dimensions	17.2 x 1.7 x 9.8 in (427 x 43 x 249 mm)	16.8 x 1.7 x 14.0 in (427 x 43 x 356 mm)	17.0 x 1.7 x 25.6 in (432 x 43 x 650 mm)
Weight	10 lbs/4.5 kg	26 lbs/11.8 kg	45 lbs/20.5 kg
Regulatory/safety certifications	UL 60950, CE, FCC PART 15, VCCI, C-TICK, TUV-GS, SABS, RoHS, WEEE		
Support	Up to 3-year advance-replacement hardware warranty (subject to valid software licensing)		

Virtual Email Appliance

Pre-defined profiles	Small	Small-Medium	Medium	Large
Capacity (approximate number of users)	300	1,000	5,000	10,000
Capacity (messages per hour)	60,000	200,000	400,000	600,000
Recommended CPU	1	2	2	4
Recommended RAM	1 GB	2 GB	3 GB	4 GB
Recommended disk storage	20 GB	30 GB	40 GB	50 GB

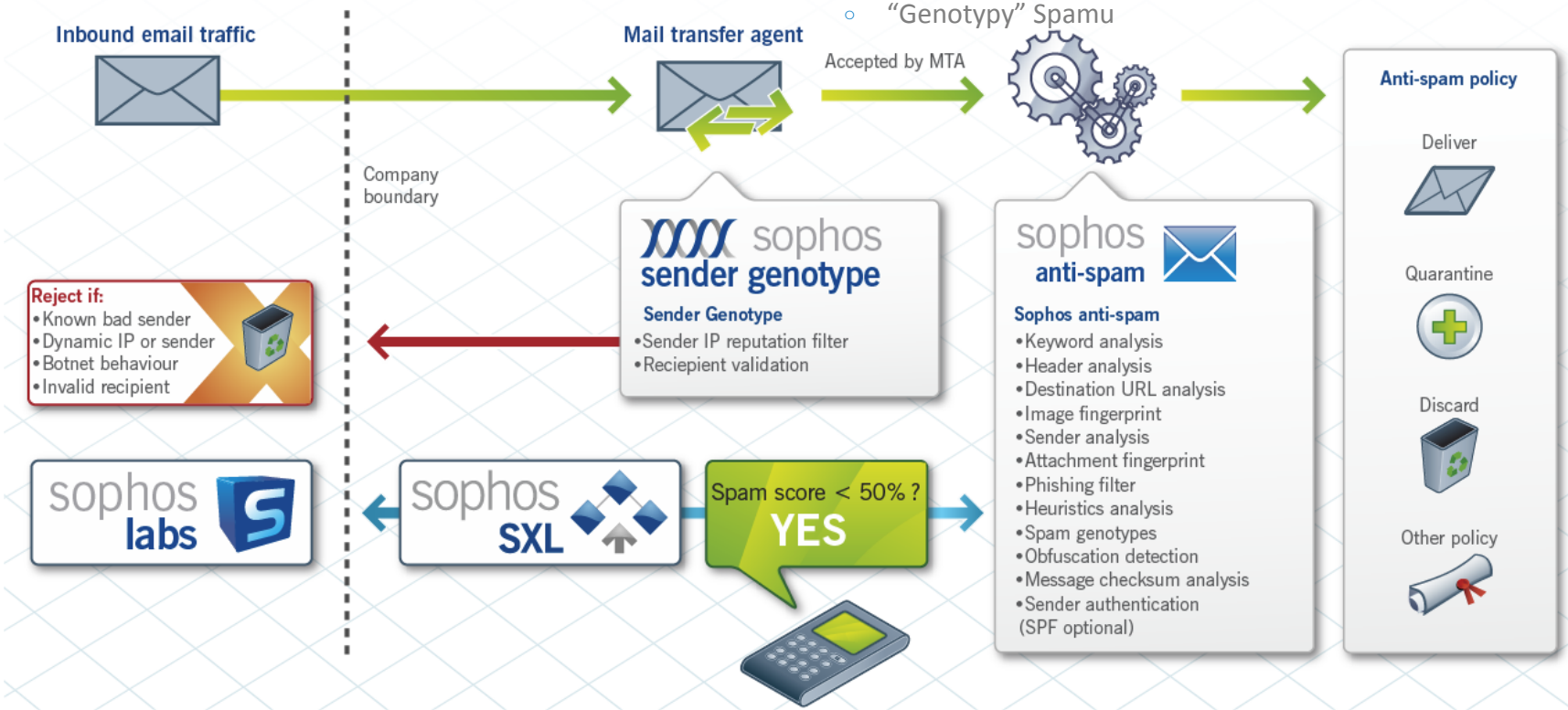
Jak lepiej radzimy sobie ze spamem

Skąd pochodzi ten email?

- Weryfikacja reputacji adresu IP I klasyfikacja
- Identyfikacja domen DNS, uchodzących za rozsyłające spam – blokowanie wszystkich domen
- "Genotypy" Spamu

Co zawiera ten email?

- Reputacja adresu URL/Domenowego
- Weryfikacja checksum (body, fuzzy, paragraphs, images, attachments)
- Numery tel., IM, znaki specjalne
- Deterministyczne oznaki spamu (fałszerstwa, mistyfikacje)
- Reguły heurystyczme (frazy, struktura wiadomości)
- "Genotypy" Spamu



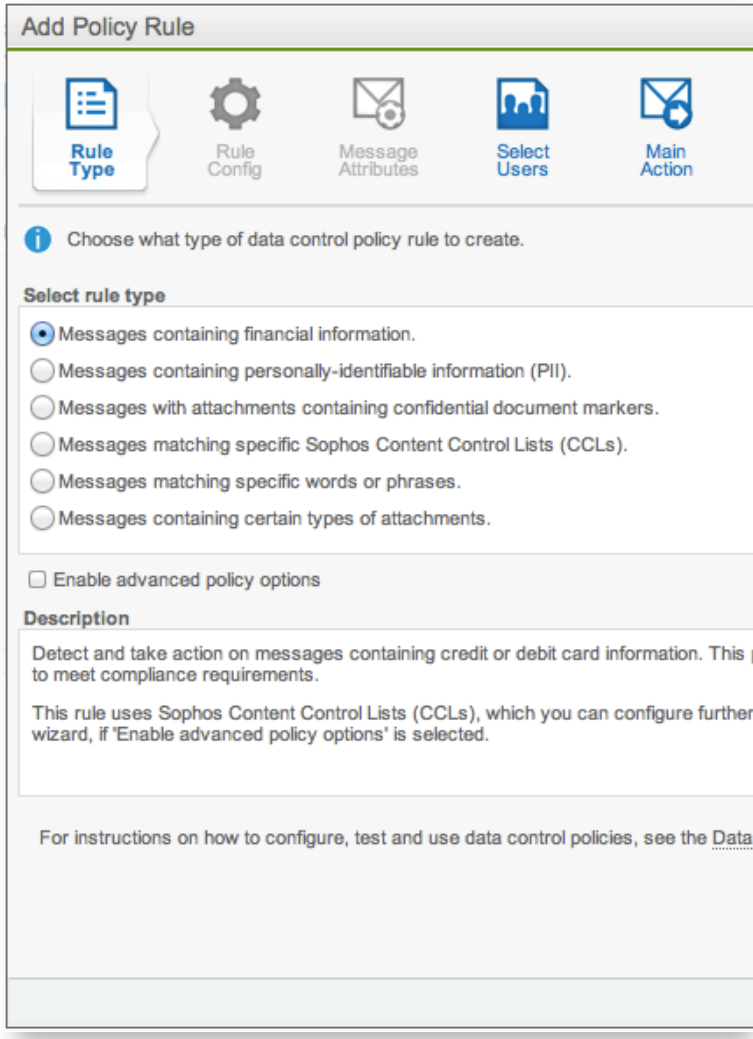
Anty-spam skuteczność

- Wysoka pozycja w Virus Bulletin!
- Jeden z 5 produktów z zerową ilością fałszywych pozytywów

Complete solutions sorted by final score	
OnlyMyEmail	99.999
Libra Esva	99.98
ZEROSPAM	99.91
Bitdefender	99.90
Sophos	99.81
Netmail Secure	99.67
SpamTitan	99.66
ESET	99.65
GFI	99.64
Kaspersky LMS	99.63
FortiMail	99.61
IBM	99.46
McAfee Email Gateway	99.39
McAfee SaaS	99.13
Scrollout	99.00
Axway	97.55
Halon Security	97.55
Net At Work NoSpamProxy	96.92

Funkcje DLP

- Dołączone do wszystkich Email Appliance
- Zawartość sprawdzana na bramie
- Unikalna kontrola proaktywna
  - Predefiniowane rodzaje danych wrażliwych
  - Zarządzane I aktualizowane przez Sophos Labs
  - Aktualizacje cykliczne
- Elastyczna konfiguracja polityk
  - Skanowanie szerokich wzorców lub określonych typów
  - Skanowanie zawartości email i załączników
  - Kontrola per użytkownik, grupy lub odbiorcy
- Ten sam system klasyfikacji w Email/Endpoint
  - Spójne polityki
  - Kopiowanie wzorców między systemami



Szyfrowanie wiadomości Email

Dlaczego firmy nie korzystają z szyfrowania email?

- Powoduje zamieszanie lub zakłóca pracę użytkowników
- Trudne do wdrożenia i zarządzania
- Duży koszt i/lub brak budżetu na szyfrowanie i DLP

Jak lepiej radzimy sobie z ochroną danych

- Dla użytkowników
  - Wysyłaj/odbieraj zaszyfrowane wiadomości tak jak robiłeś to przed tem
  - Brak konieczności tworzenia złożonych procedur
  - Wszystko dzieje się automatycznie

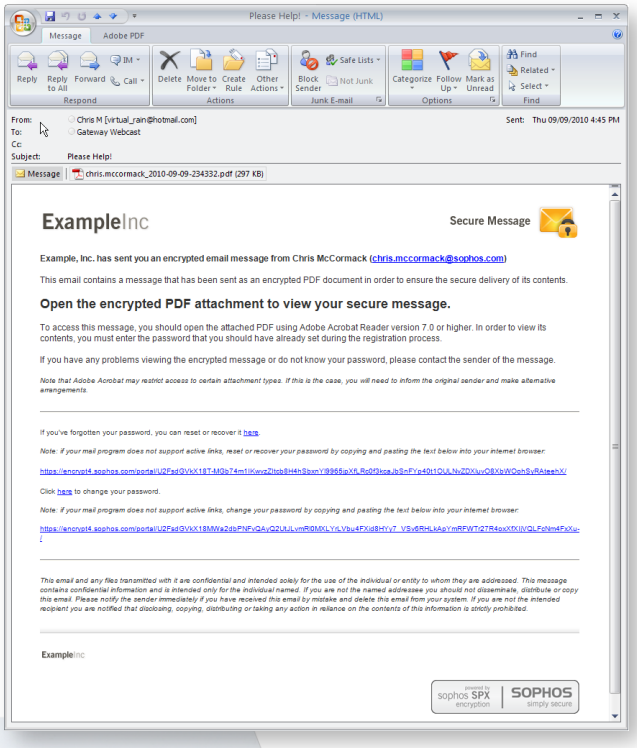
- Dla administratorów IT
  - Wdrożenie i wymuszenie polityk w kilka minut
  - Setki predefiniowanych wzorców danych wrażliwych
  - Wrażliwe dane nie wyciekają
  - Bez instalacji oprogramowania klienckiego
  - Bez konieczności przechowywania osobnej infrastruktury do przechowywania kluczy

HIPAA Health Insurance Portability & Accountability Act

PCI DSS COMPLIANT

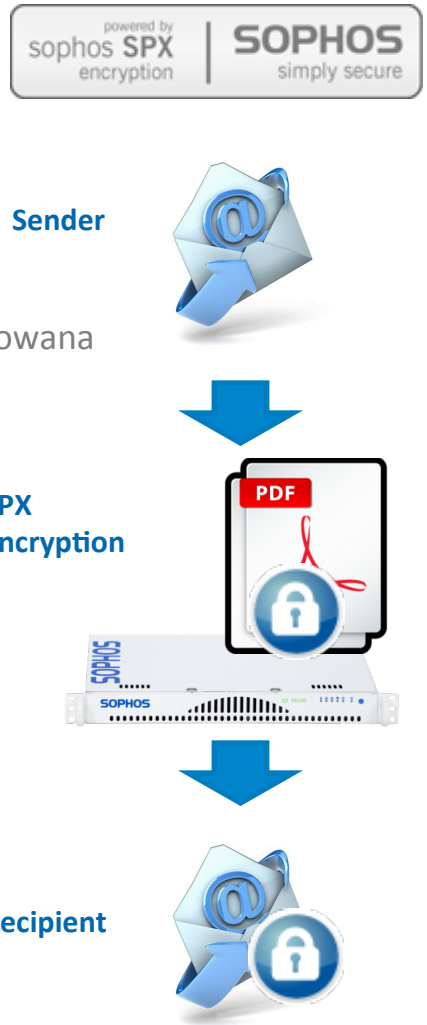
Funkcje szyfrowania Secure Pdf eXchange

- Moduł dostępny w Email Protection Advanced
- Autmatyczne szyfrowanie oparte na politykach na poziomie bramy
- Unikalna technologia
  - Nikt nie robi tego tak jak my
  - Wykorzystujemy zwykłe PDFy
  - Szyfrowanie algorytmem 128-bit brak możliwości złamania
- Pozytywny odbiór użytkowników
  - Bez specjalnych procedur – dostraczane do Twojej skrzynki
  - Dostęp na każdej platformie (również urządzenia mobilne)
  - Przeczytaj online, albo offline, nie ma znaczenia
- Elastyczna konfiguracja polityk
- Wsparcie brandingu



Szyfrowanie SPX – jak działa:

- Nadawca
  - Wysyła wiadomość przez swojego ulubionego klienta poczty
- Sophos Email Appliance z szyfrowaniem SPX
  - Polityka automatycznie decyduje czy wiadomość powinna być zaszyfrowana
  - Wiadomość szyfrowana do kontenera PDF
  - Opcje hasła:
    - Ustalane przez odbiorcę jednokrotnie
    - Generowane automatycznie
    - Zintegrowane z systemem uwierzytelniania
- Odbiorca
  - Odbiera wiadomość jak zwykle(z zaszyfrowanym załącznikiem)
  - Otwiera/wyświetla przez wpisanie hasła
  - Odpowiada szyfrowaną wiadomością(przycisk do portalu)



http://esa.sophos.com/sea_docs/en/ESA/concepts/ConfigPolEncryptSPXMain.html

Szyfrowanie SPX – jak działa:

Encrypted Email Message

Encrypted email notification from Sophos
Encrypted email message from "Monika Sierocinski"

This email contains a message that has been sent as an encrypted PDF document in order to ensure the secure delivery of its contents.

To access this message, you should open the attached PDF using Adobe Acrobat Reader version 7.0 or higher. In order to view its contents, you must enter the password that you should have already set during the registration process.

If you have any problems viewing the encrypted message or do not know your password, please contact the sender of the message.

Note that Adobe Acrobat may restrict access to certain attachment types. If this is the case, you will need to inform the original sender and make alternative arrangements.

If you've forgotten your password, you can reset or recover it here.

Note: if your mail program does not support active links, reset or recover your password by copying and pasting the text below into your internet browser:

https://encrypt4.sophos.com/portal/U2FsdGVkX18WJZba1-ZxSdlEG6HG2kxYzUi0mVFozzhPCK8q006cXDRTNPzDnYLEulLeylFh31JF-yDKvsmDpQ/

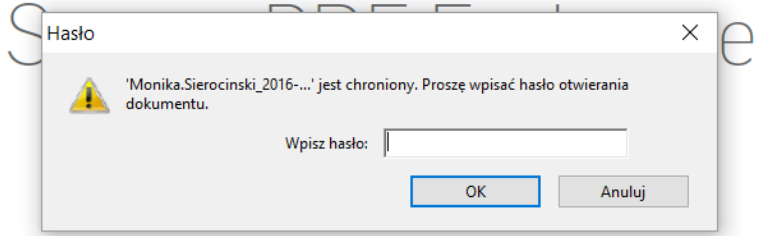
New feature: We now support password recovery. To be able to recover you password, you need to set your security questions. If you haven't set your question yet, click here.

Note: if your mail program does not support active links, reset or recover your password by copying and pasting the text below into your internet browser:

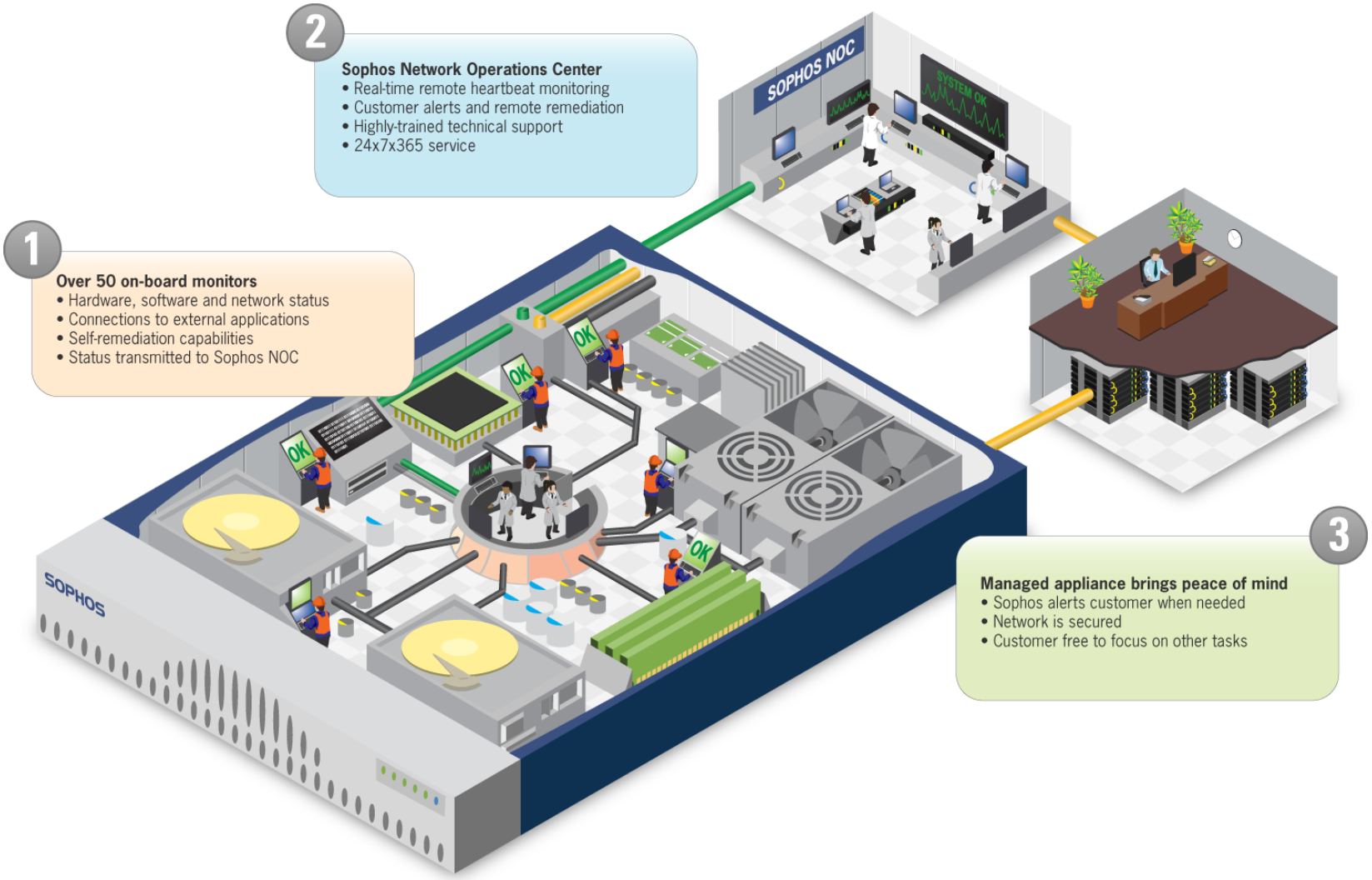
https://encrypt4.sophos.com/portal/U2FsdGVkX18WJZba1-ZxSdlEG6HG2kxYzUi0mVFozzhPCK8q006cXDRTNPzDnYLEulLeylFh31JF-

ENCRYPTED MESSAGE

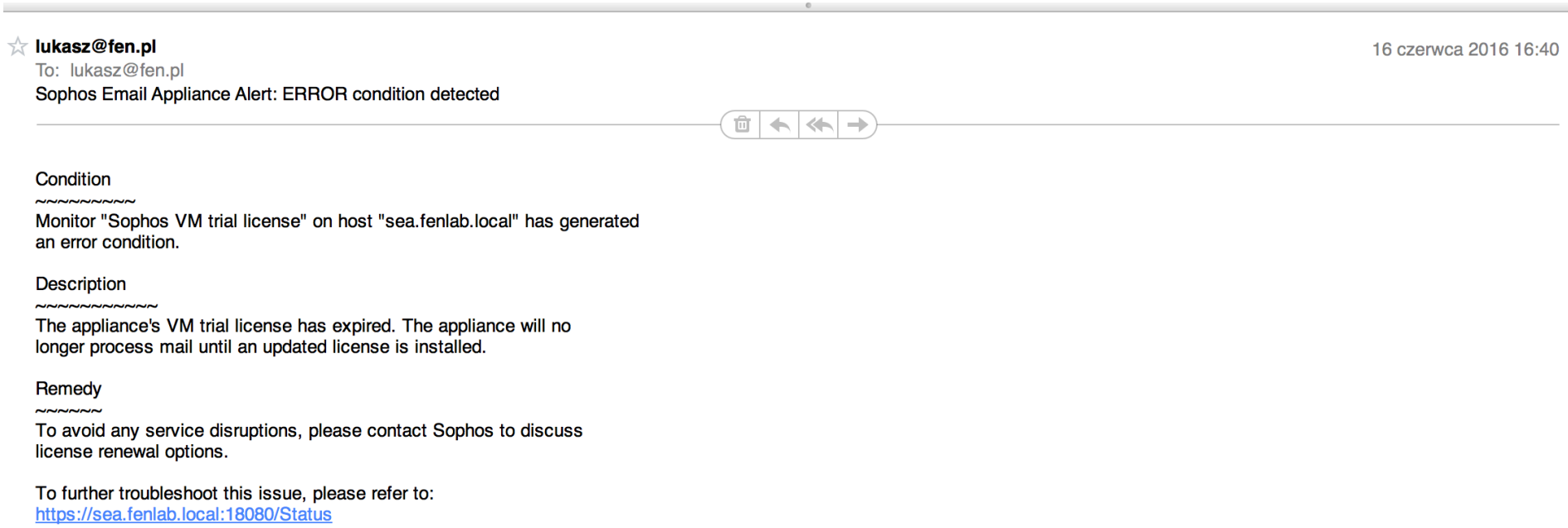
Sophos SPX



Monitorowanie SEA



Monitorowanie SEA



lukasz@fen.pl 16 czerwca 2016 16:40
To: lukasz@fen.pl
Sophos Email Appliance Alert: ERROR condition detected

Condition
~~~~~~~~~~
Monitor "Sophos VM trial license" on host "sea.fenlab.local" has generated an error condition.

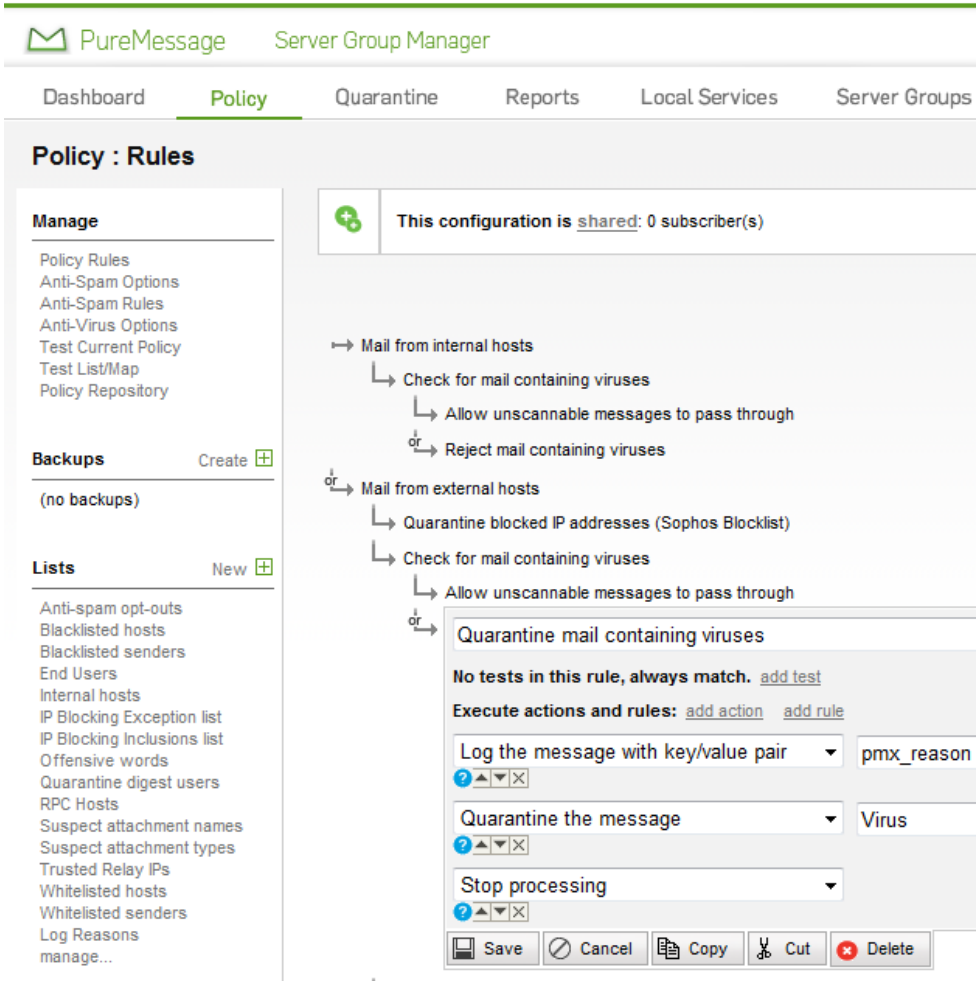
Description
~~~~~~~~~~~~
The appliance's VM trial license has expired. The appliance will no longer process mail until an updated license is installed.

Remedy
~~~~~~~
To avoid any service disruptions, please contact Sophos to discuss license renewal options.

To further troubleshoot this issue, please refer to:
https://sea.fenlab.local:18080/Status
~~~~~~~

PureMessage UNIX

- Lepsza ochrona przed spamem
  - Mniej spamu, mniej fałszywych alarmów
- Kompletna ochrona
  - Otwarta architektura
  - Personalizacja
  - Granularne polityki
  - Administracja oparta na profilach
  - Wsparcie trybu Multi-tenant
- Elastyczne skalowane wdrożenie
  - Wsparcie wielu platform
  - Klastrowanie serwerów
  - Zgodne z dowolnym rozwiązaniem SMTP
  - Integracja z LDAP
  - Wsparcie IPv6



Features & Capabilities

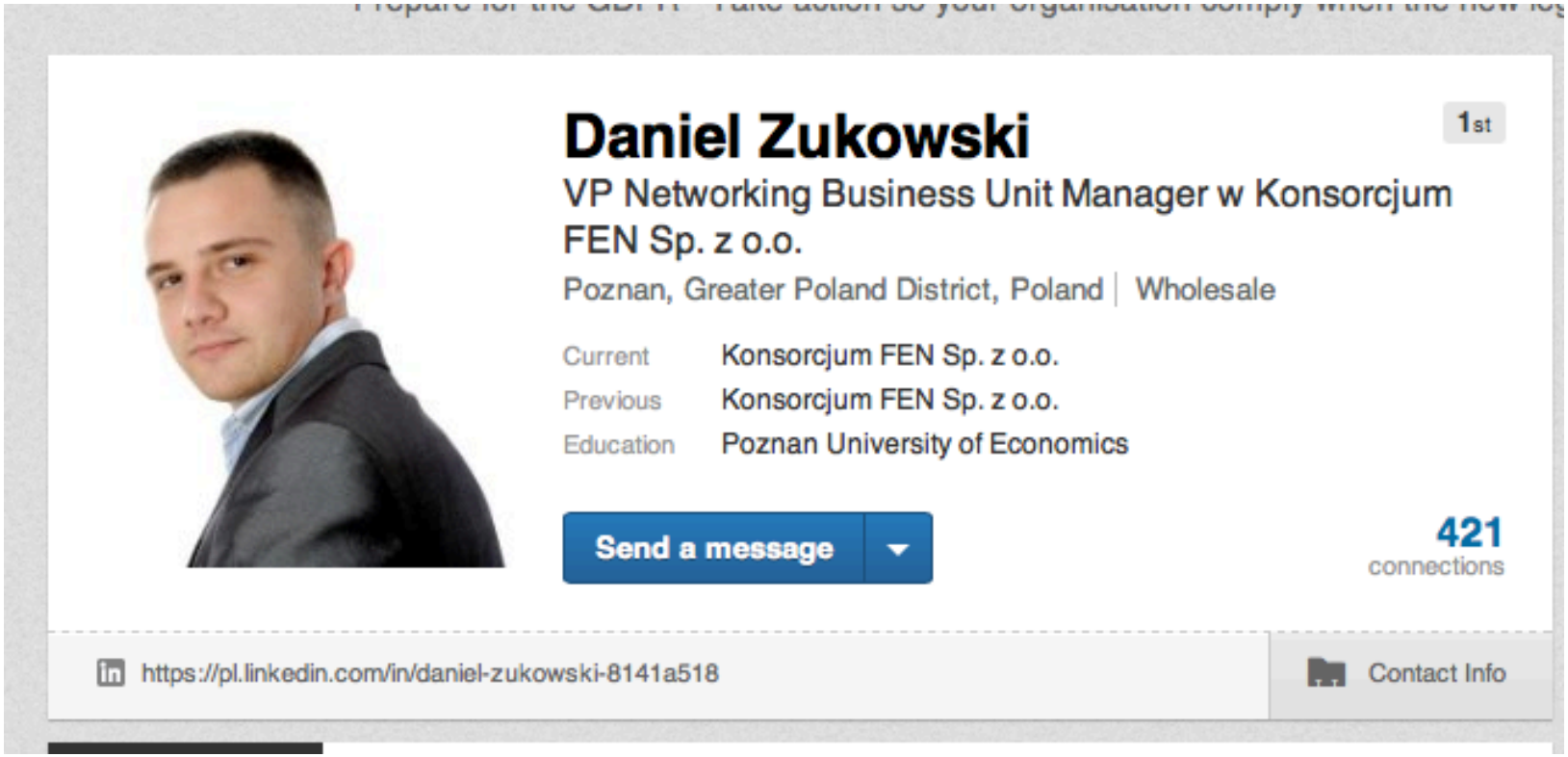
	Email Appliances (Hardware/Virtual)	PureMessage for UNIX	PureMessage for Exchange	PureMessage for Domino
Deployment				
Network Gateway or Mail Server	Network Gateway	Network Gateway	Exchange Server/Cluster	Domino Server/Cluster
Threat protection				
Sophos Anti-virus	●	●	●	●
Zero-day protection	●	●	●	●
Malicious URL blocking	●	●	●	●
Spam protection				
Sender Genotype Reputation Filtering	●	●	●	●
Live Anti-spam	●	●	●	●
Data protection				
Integrated policy-based SPX Encryption	●			
Integrated TLS encryption	●	●	●	●
Content filtering rules	●	●	●	●
Offensive content blocking	●	●	●	●
Content aware DLP	●			
SophosLabs managed DLP dictionaries	●			
Management				
Real-time dashboard	●	●	●	
Policy based reporting	●	●	●	●
Support				
Managed appliance service	●			
24/7/365 Support	●	●	●	●
Free updates/upgrades	●	●	●	●
Advance replacement warranty	3 years	N/A	N/A	N/A

SOPHOS

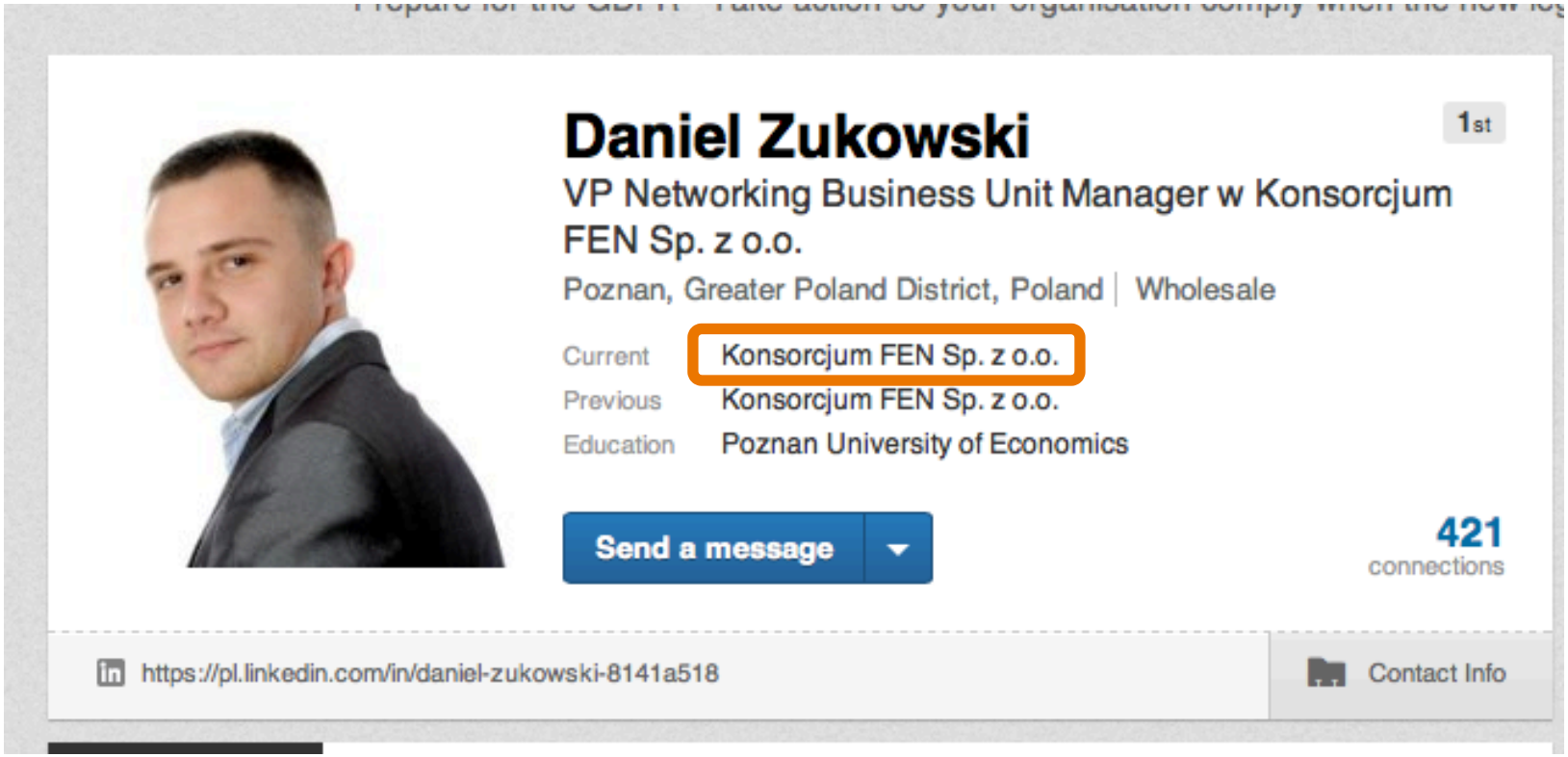
Nowe zagrożenia

Cel ataku

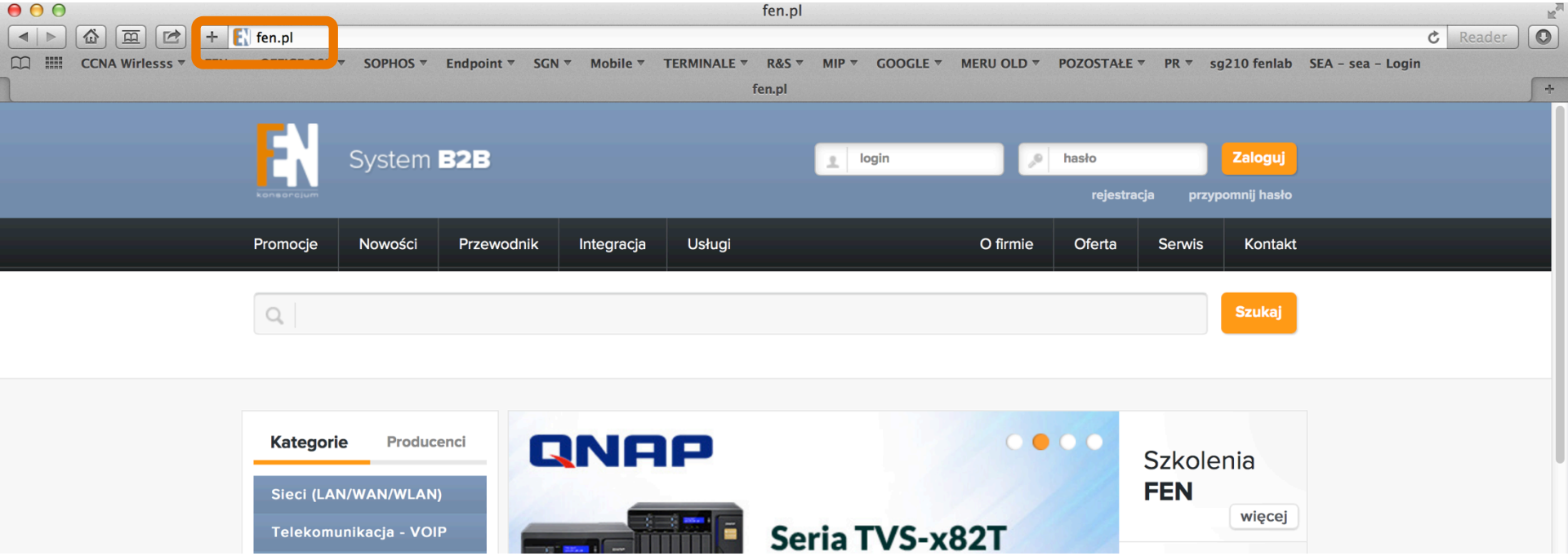
Cel ataku


Daniel Zukowski
1st
VP Networking Business Unit Manager w Konsorcjum FEN Sp. z o.o.
Poznan, Greater Poland District, Poland | Wholesale
Current Konsorcjum FEN Sp. z o.o.
Previous Konsorcjum FEN Sp. z o.o.
Education Poznan University of Economics
Send a message
421
connections
https://pl.linkedin.com/in/daniel-zukowski-8141a518
Contact Info

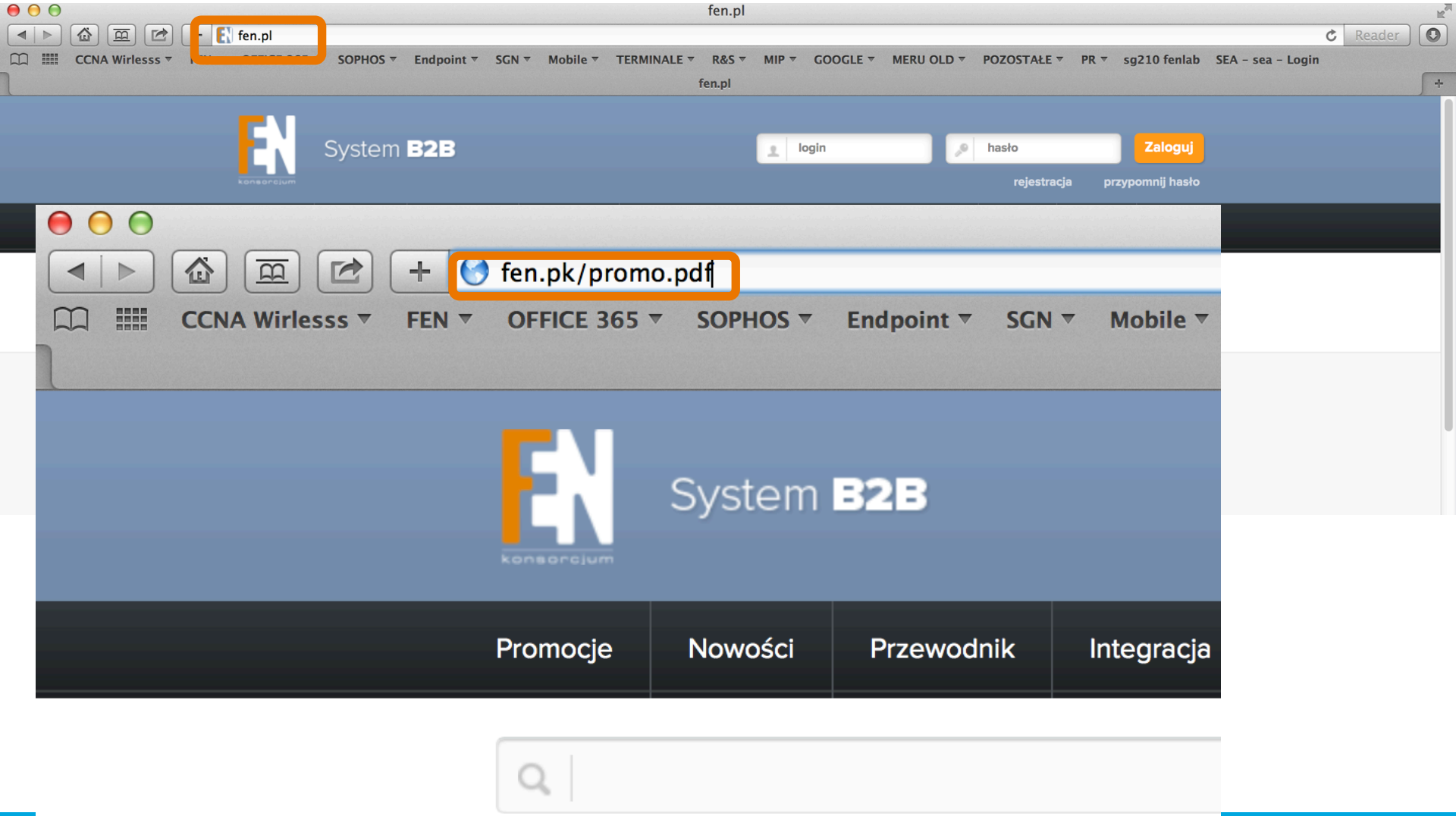
Cel ataku


Daniel Zukowski
1st
VP Networking Business Unit Manager w Konsorcjum FEN Sp. z o.o.
Poznan, Greater Poland District, Poland | Wholesale
Current Konsorcjum FEN Sp. z o.o.
Previous Konsorcjum FEN Sp. z o.o.
Education Poznan University of Economics
Send a message
421
connections
https://pl.linkedin.com/in/daniel-zukowski-8141a518
Contact Info

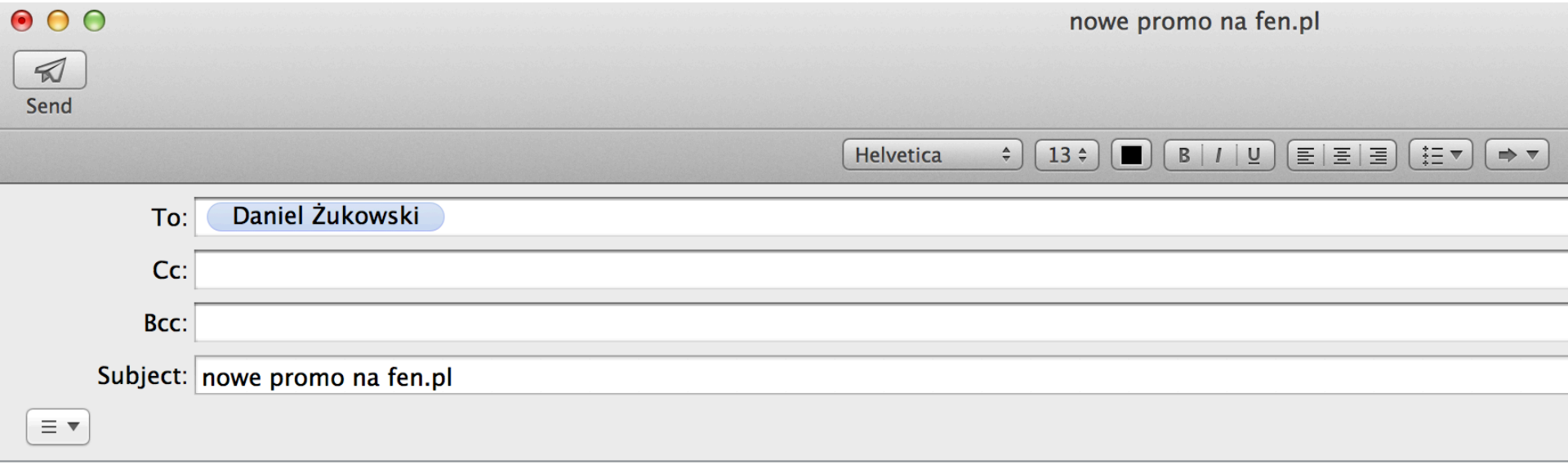
Przygotowanie pułapki



Przygotowanie pułapki



Dostarczenie przynęty



Hej,

Widziales tego PDFa z lista nowych promocji?
Link

Pzdr,

Łukasz Naumowicz
Technical Support Manager

Tel. +48 61 66 90 724
GSM +48 510 044 724

Konsorcjum FEN Sp. z o.o.
ul. Dąbrowskiego 273a, 60-406 Poznań

NIP 778-12-13-207
Numer KRS 0000196881, SR w Poznaniu,
VIII Wydział Gospodarczy KRS
Kapitał zakładowy: 200.000 zł

Uzbrojenie strony

Oczekiwanie na “cel”

Wykorzystanie danych

Co nowego w Sophos Email Appliance?

Sophos Sandstorm

Ochrona przed szkodliwą zawartością w załącznikach

Sophos Time-Of-Click Protection

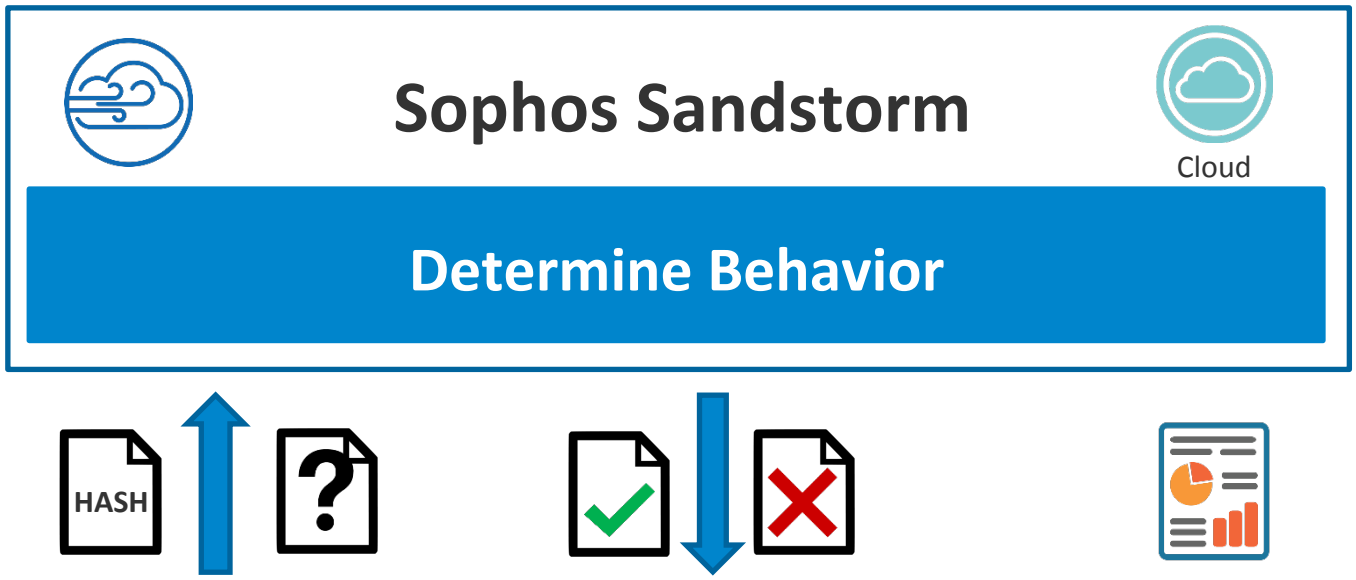
Ochrona użytkowników przed atakami Spear-Phishing

Czym jest Sophos Sandstorm?

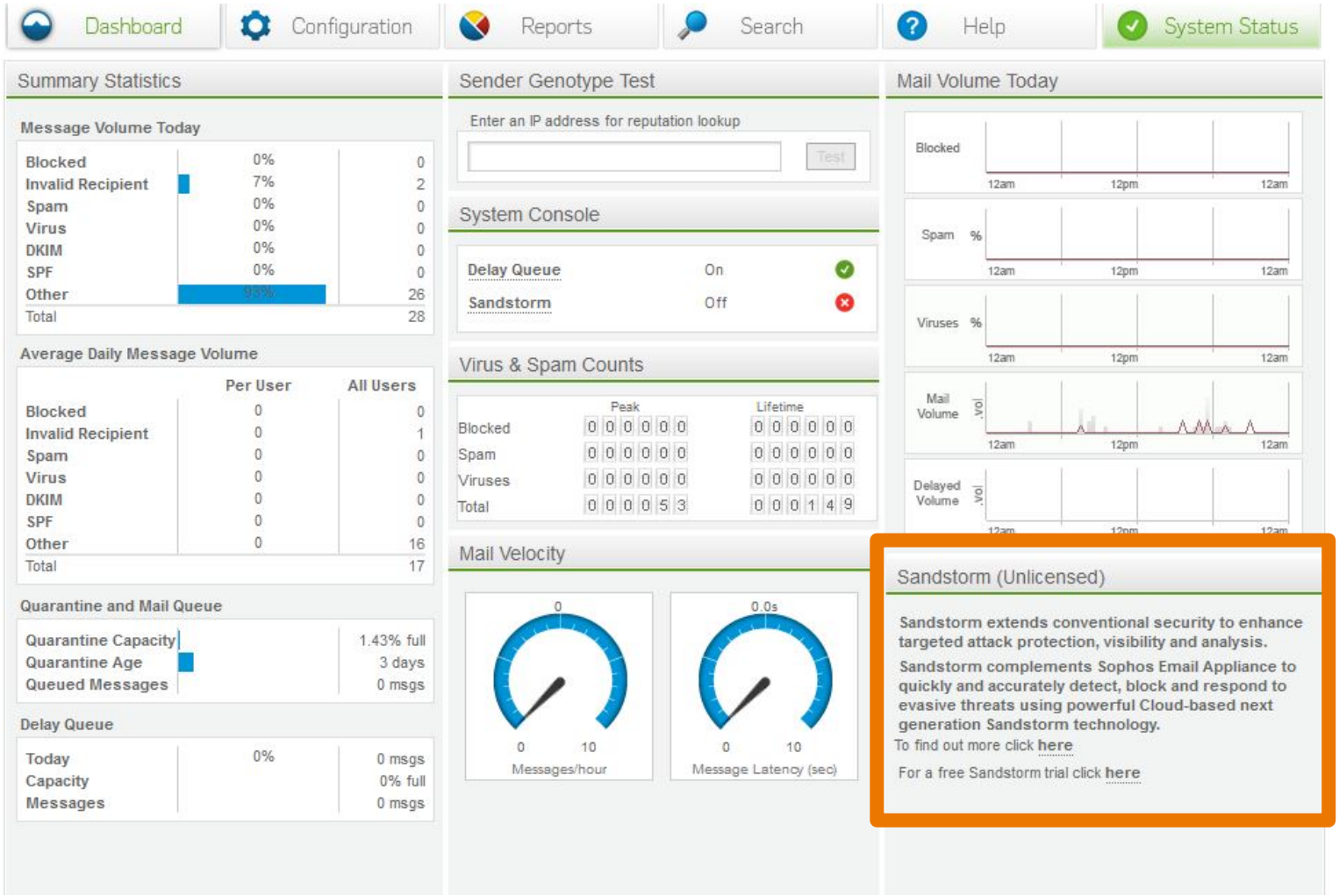
Ochrona użytkowników przed szkodliwymi załącznikami email

- Zupełnie nowy mechanizm detekcji w portfolio Sophos
- System sanbox oparty na środowisku chmurowym
- Ochrona przed atakami kierowanymi
- Wykrywa, powstrzymuje I odpowiada na nieznane zagrożenia
- Wymaga dodatkowej licencji

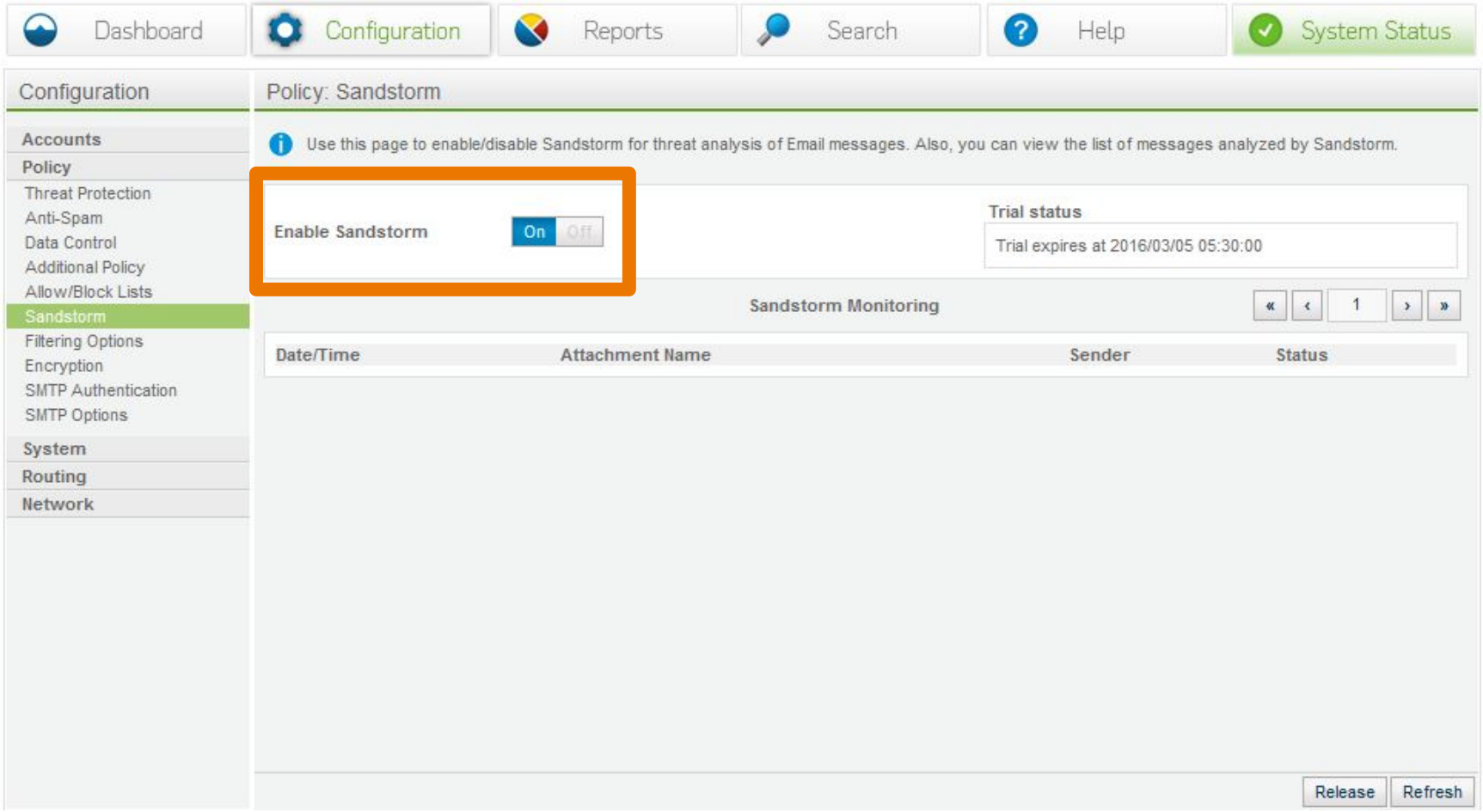
Jak działa Sophos Sandstorm?



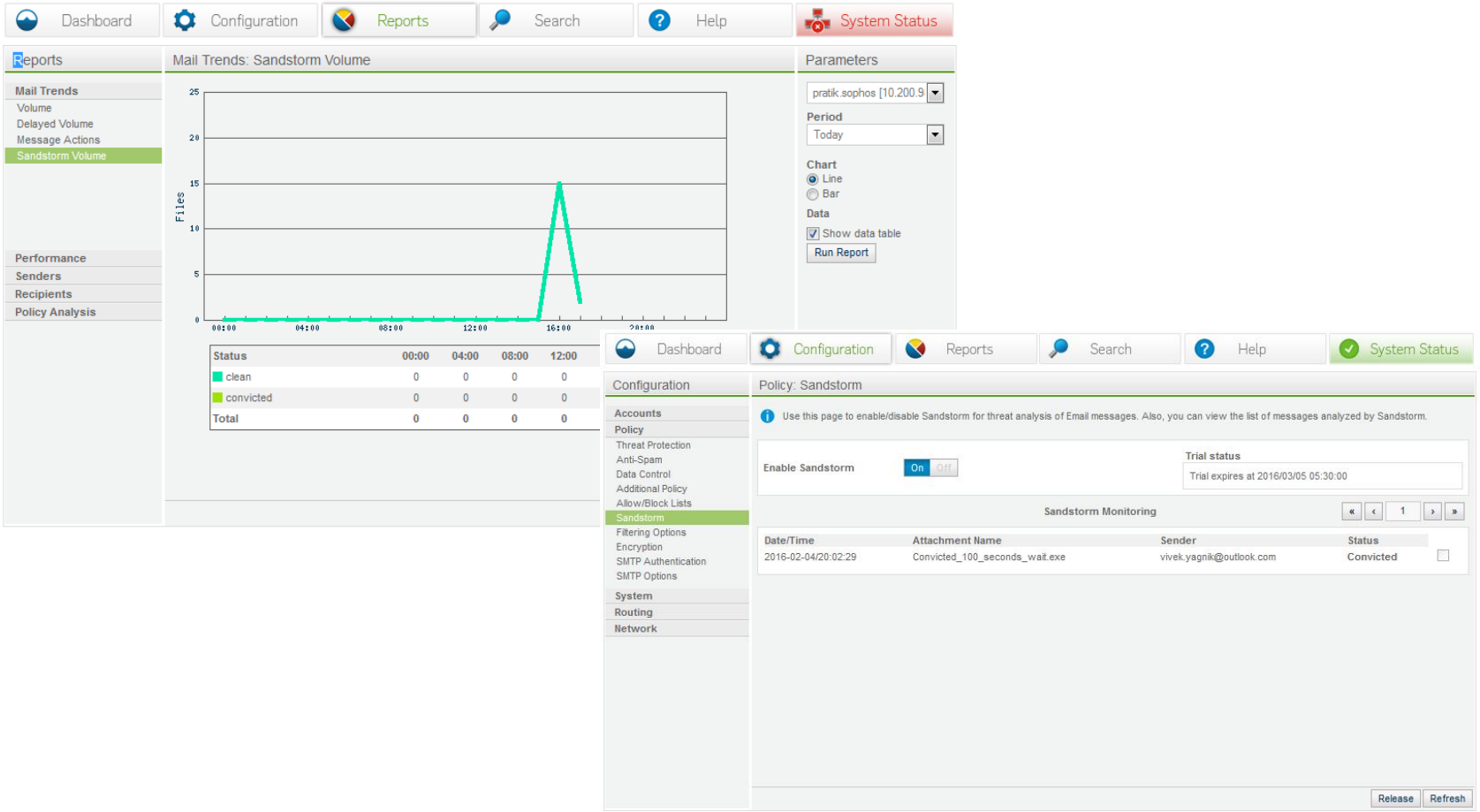
Łatwo dostępne demo



Proste wdrożenie



Proste zarządzanie

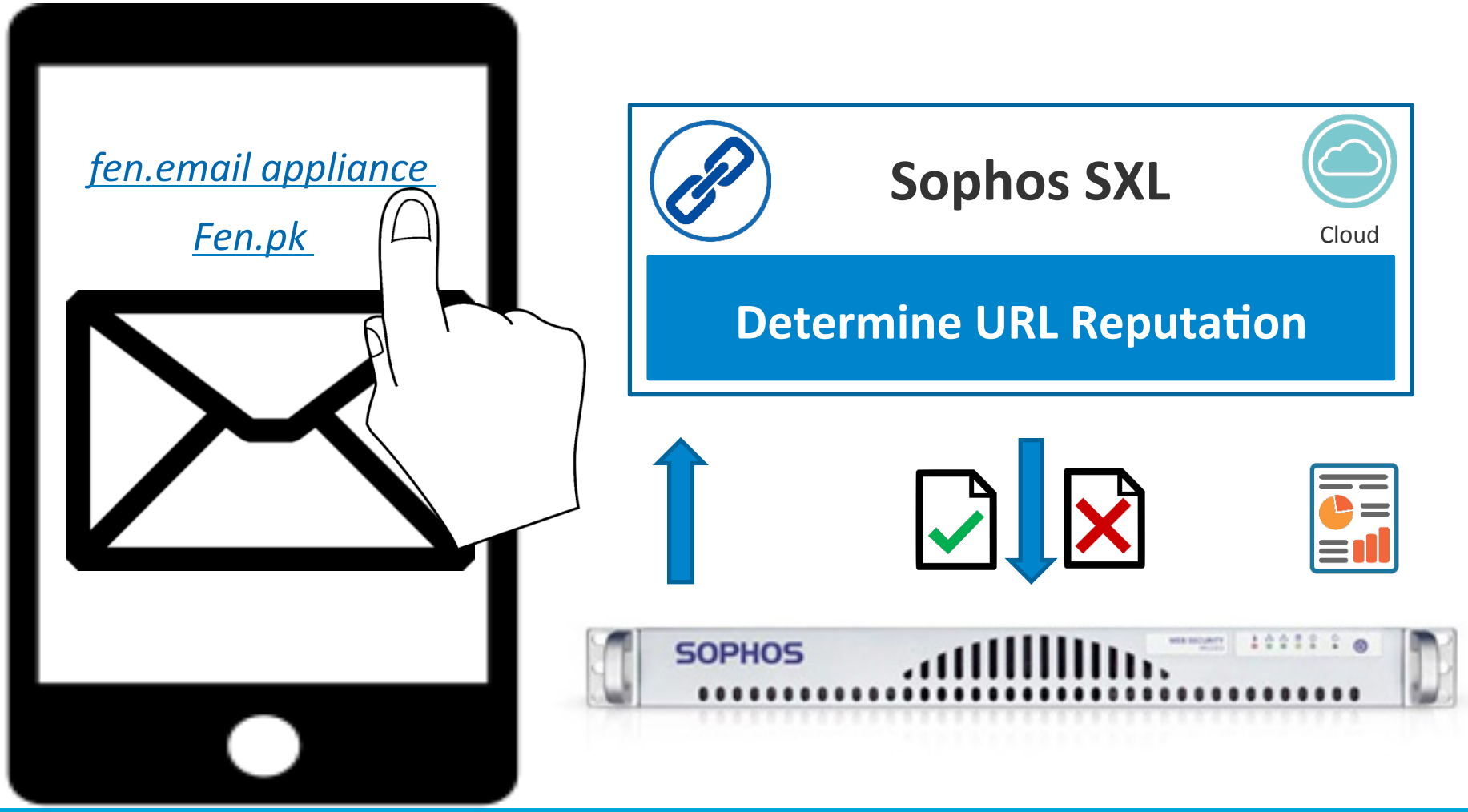


Czym jest Sophos Time-of-Click Protection?

Ochrona użytkowników przed atakami spear-phishing

- Sprawdzamy każdy klik, za każdym razem, w czasie rzeczywistym
- Ochrona przed ukrytymi, opóźnionymi atakami
- Natychmiastowa ochrona na wszystkich urządzeniach, wewnątrz i poza siecią firmową
- Bez zakłócania pracy użytkowników
- Szczegółowe raportowanie
- w ramach subskrycpcji Sandstorm

Jak działa Time-of-Click Protection?



SOPHOS

Licencjonowanie

Licencjonowanie

SOPHOS
Virtual Appliance

Email Protection Advanced
(subskrypcja na ilość użytkowników)

Sophos Sandstorm
(subskrypcja na taką samą ilość użytkowników)

SOPHOS

Dlaczego Sophos?

How would you change it?

I suggest you ...

← UTM (Formerly ASG) Feature Requests

5
votes

Vote

time-of-click protection for email spear-phishing attack

Many of today's threats, begin with a spear-phishing attack: a single, carefully crafted email that tricks a recipient into clicking a link to download malware or open a malicious attachments.

Handling this type of emails like proofpoint would be really nice to have in UTM as email protection appliance. Handling is to actually replace links, attachements so everything runs sandboxed if suspicious.

Anonymous shared this idea · April 12, 2015 · Flag idea as inappropriate…

Sophos Email Appliances

Szyfrowanie danych

Ochrona DLP

Anty-Spam

Anty-Malware

SOPHOS