

Sophos Email Protection

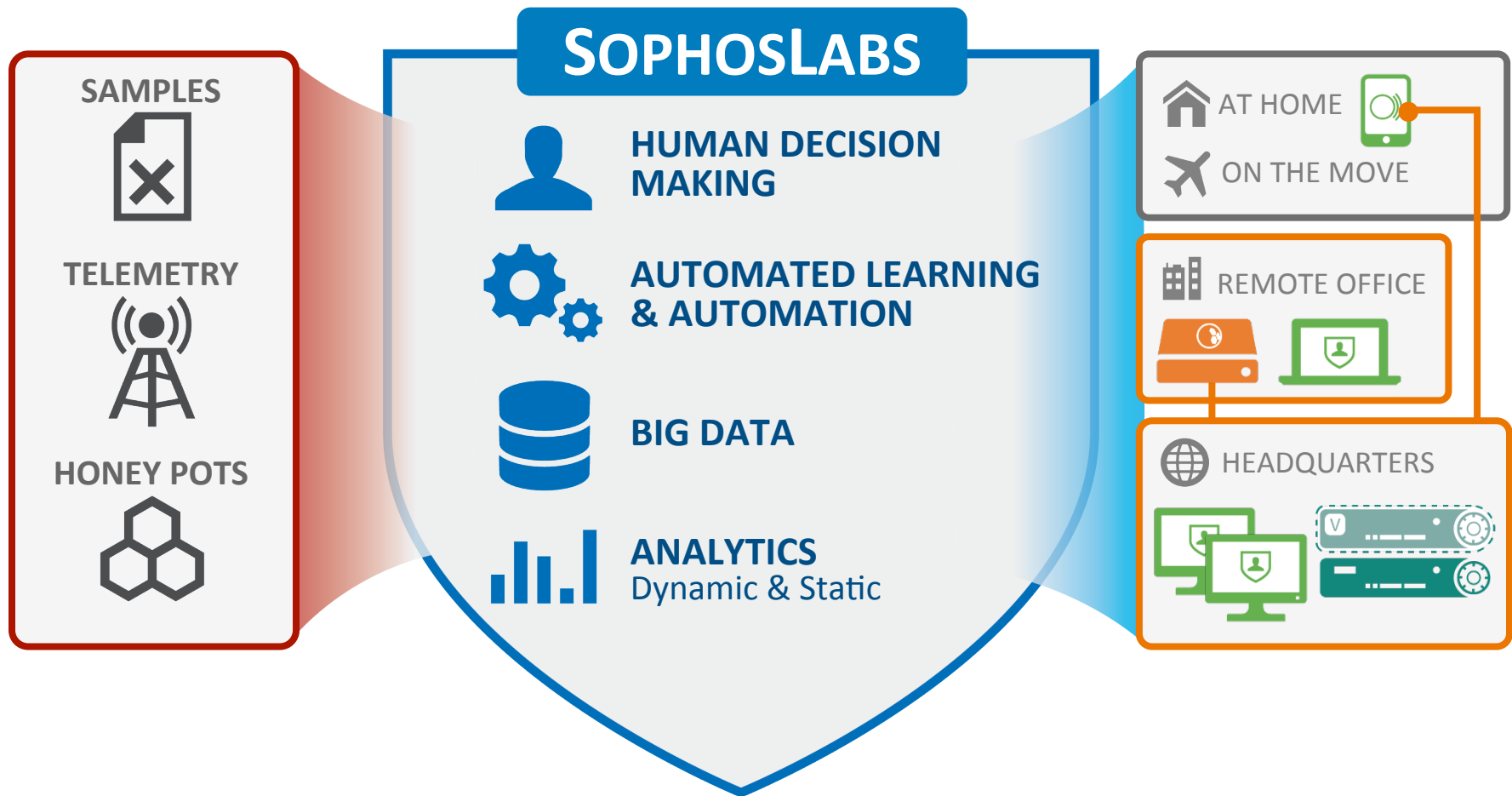


Łukasz Naumowicz

22.06.2016

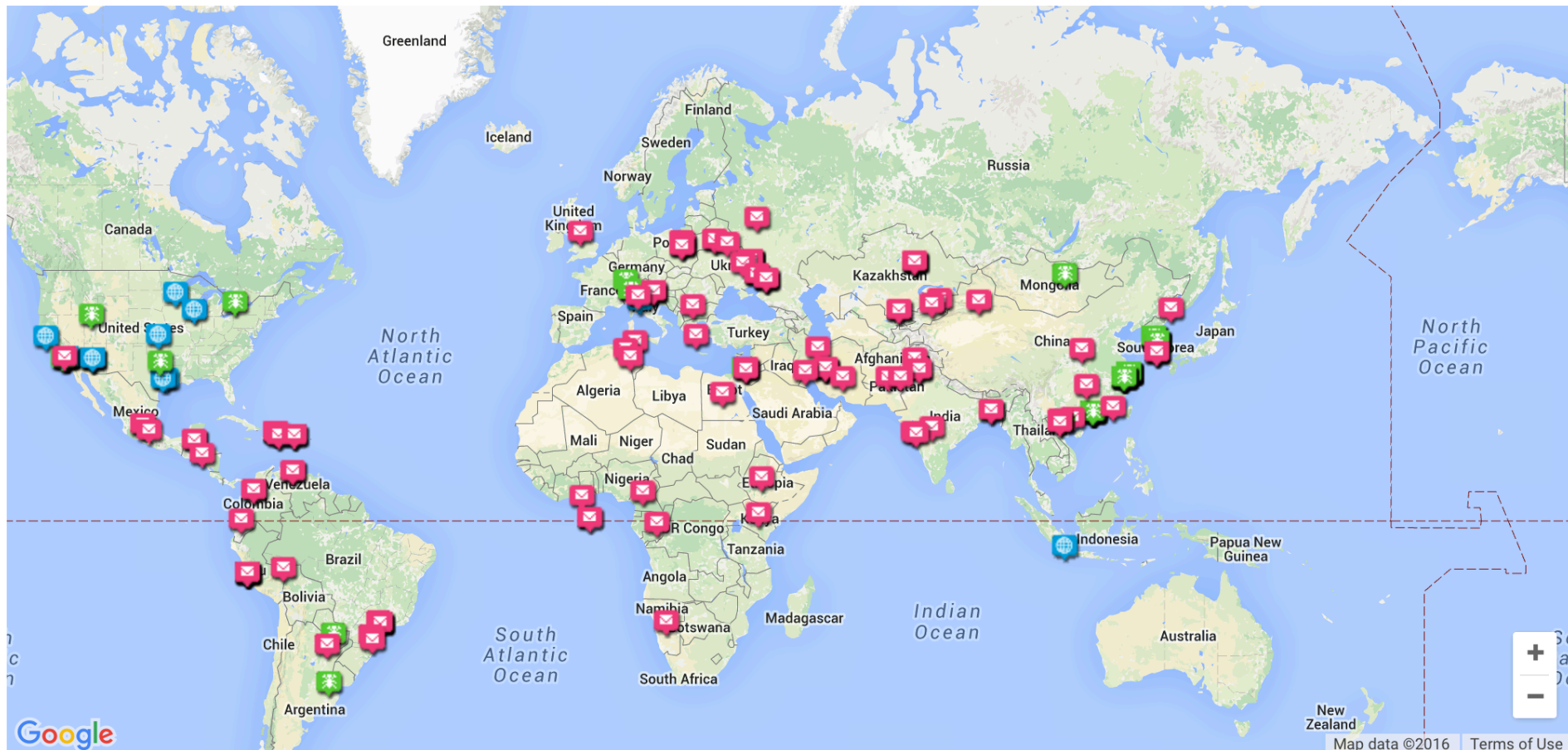
SOPHOS

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>

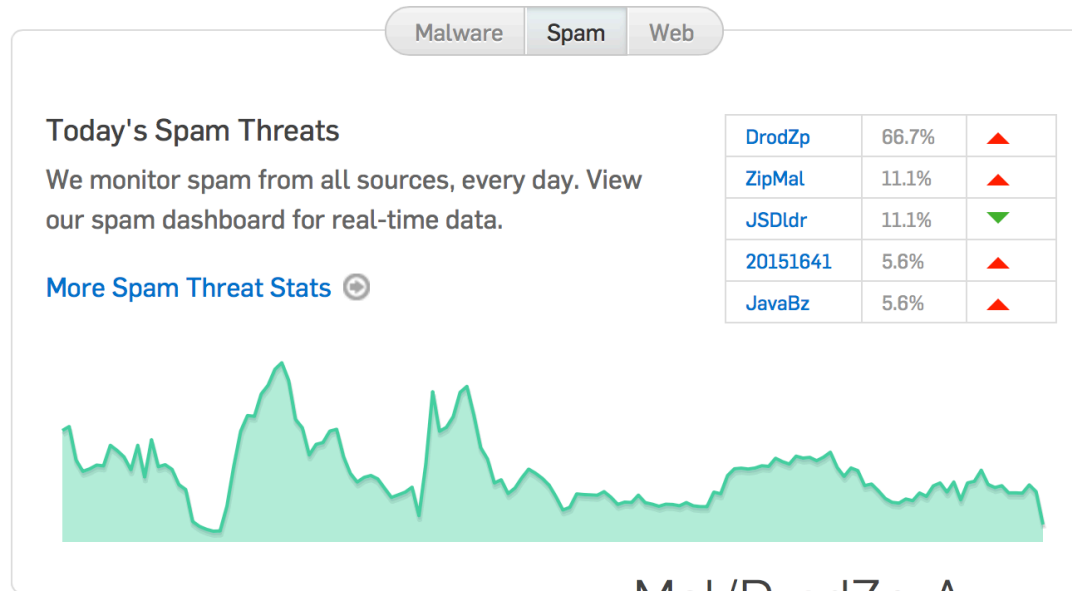
Źródła informacji o spamie

- ~100 pułapek spam w 22 krajach
>30 milionów wiadomości dziennie
- Dane Real-time, IP reputation
- Dane pochodzące z urzędzeń
- 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



Mal/DrodZp-A

Category: Viruses and Spyware
Type: Malicious behavior
Prevalence: 

Protection available since:
Last Updated:

18 Jul 2012 20:57:09 (GMT)
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 recipients 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...



Rozwiązania do ochrony poczty

Portfolio rozwiązań do ochrony poczty



Dedykowany Email Appliance



Wirtualny Email Appliance



UTM



PureMessage UNIX



Cloud (Przyszłość)*

SMB

Średnie firmy

Korporacje

Operatorzy

Sophos Email Appliances

Szyfrowanie
danych

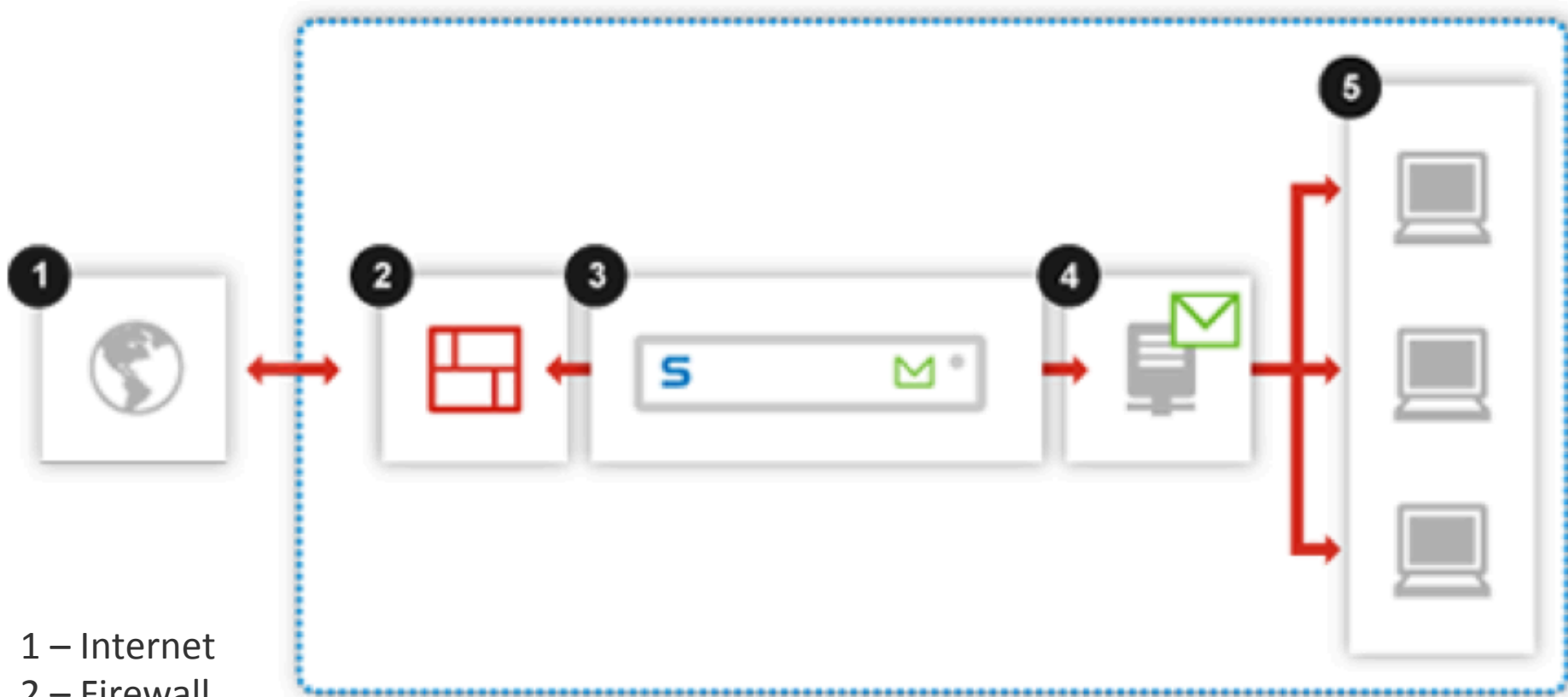
Ochrona DLP



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

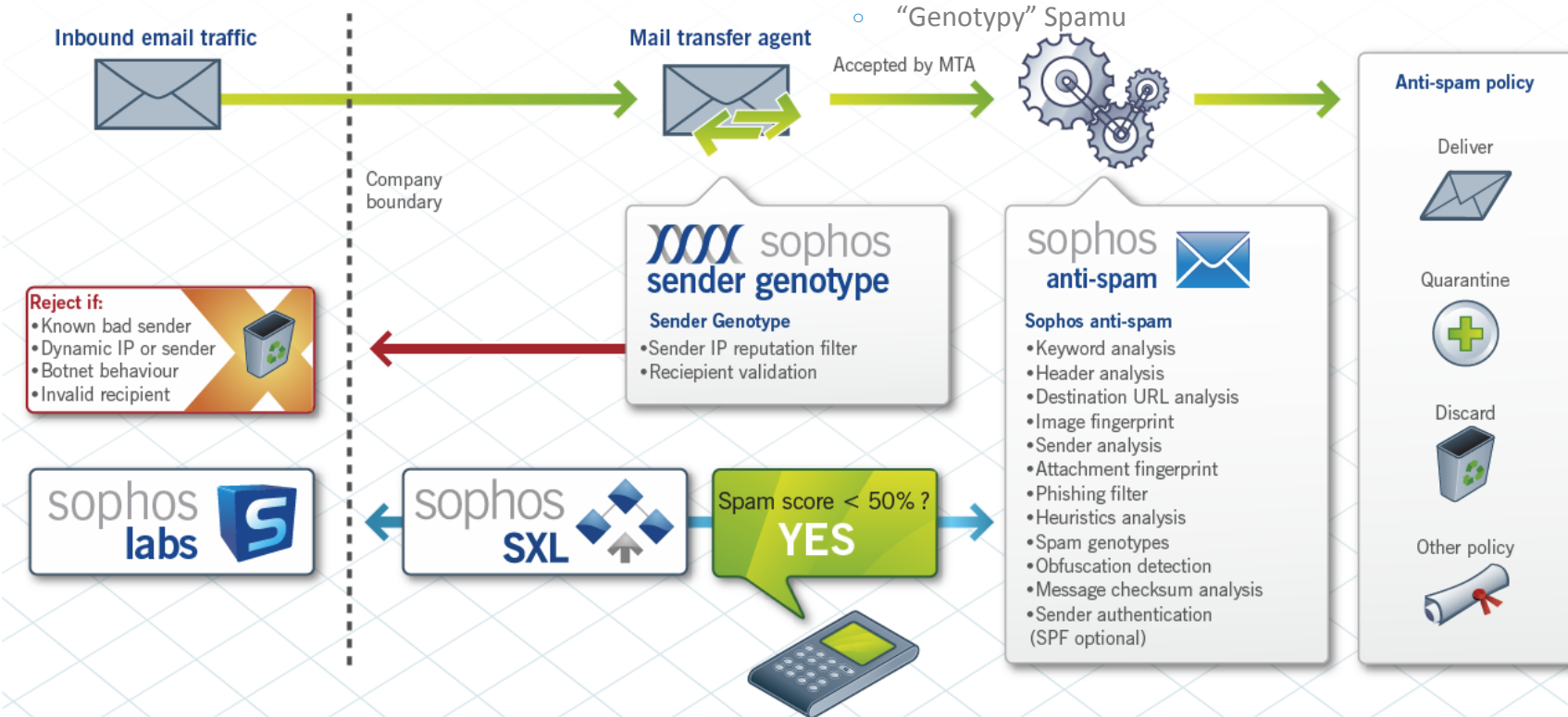
Jak lepiej radzimy sobie ze spamem

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 heurystyczne (frazy, struktura wiadomości)
- "Genotypy" Spamów

Skąd pochodzi ten email?

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



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

Add Policy Rule

 Rule Type

 Rule Config

 Message Attributes

 Select Users

 Main Action

i Choose what type of data control policy rule to create.

Select rule type

☒ Messages containing financial information.

☐ Messages containing personally-identifiable information (PII).

☐ Messages with attachments containing confidential document markers.

☐ Messages matching specific Sophos Content Control Lists (CCLs).

☐ Messages matching specific words or phrases.

☐ Messages containing certain types of attachments.

☐ Enable advanced policy options

Description

Detect and take action on messages containing credit or debit card information. This rule is used to meet compliance requirements.

This rule uses Sophos Content Control Lists (CCLs), which you can configure further in the wizard, if 'Enable advanced policy options' is selected.

For instructions on how to configure, test and use data control policies, see the [Data Control Policies](#) page.

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

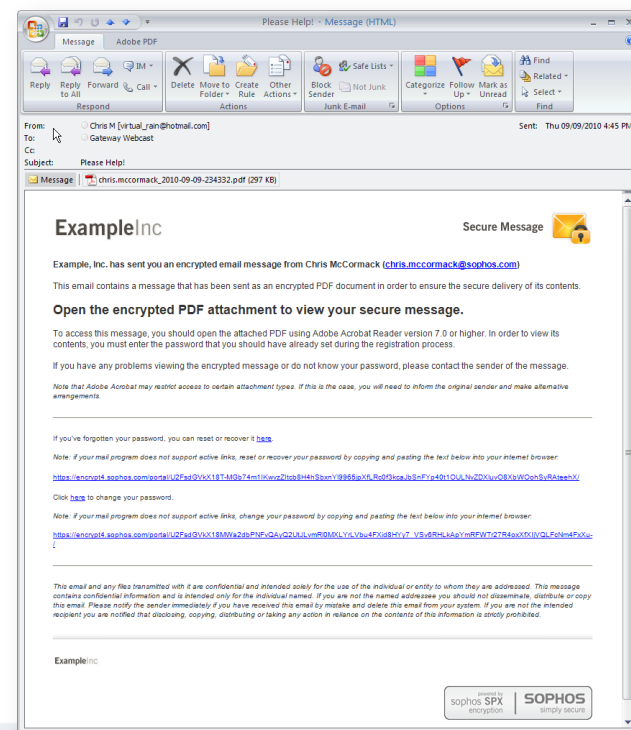
- Dla administratorów IT

- 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



Funkcje szyfrowania Secure Pdf eXchange

- Moduł dostępny w Email Protection Advanced
- Automatyczne 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
 - Wysła 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)



Sender



SPX
Encryption



Recipient



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:

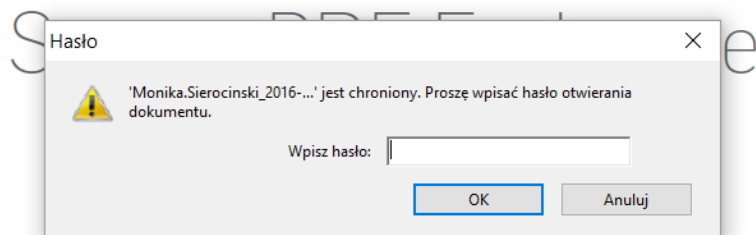
<https://encrypt4.sophos.com/portal/U2FsdGVkX18WJZba1-ZxSdIEG6HG2kxYzUi0mVFozzhPCK8q006cXDRTNPzDnYLEulLeyIFh31JF-yDKvsmDpQ/>

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

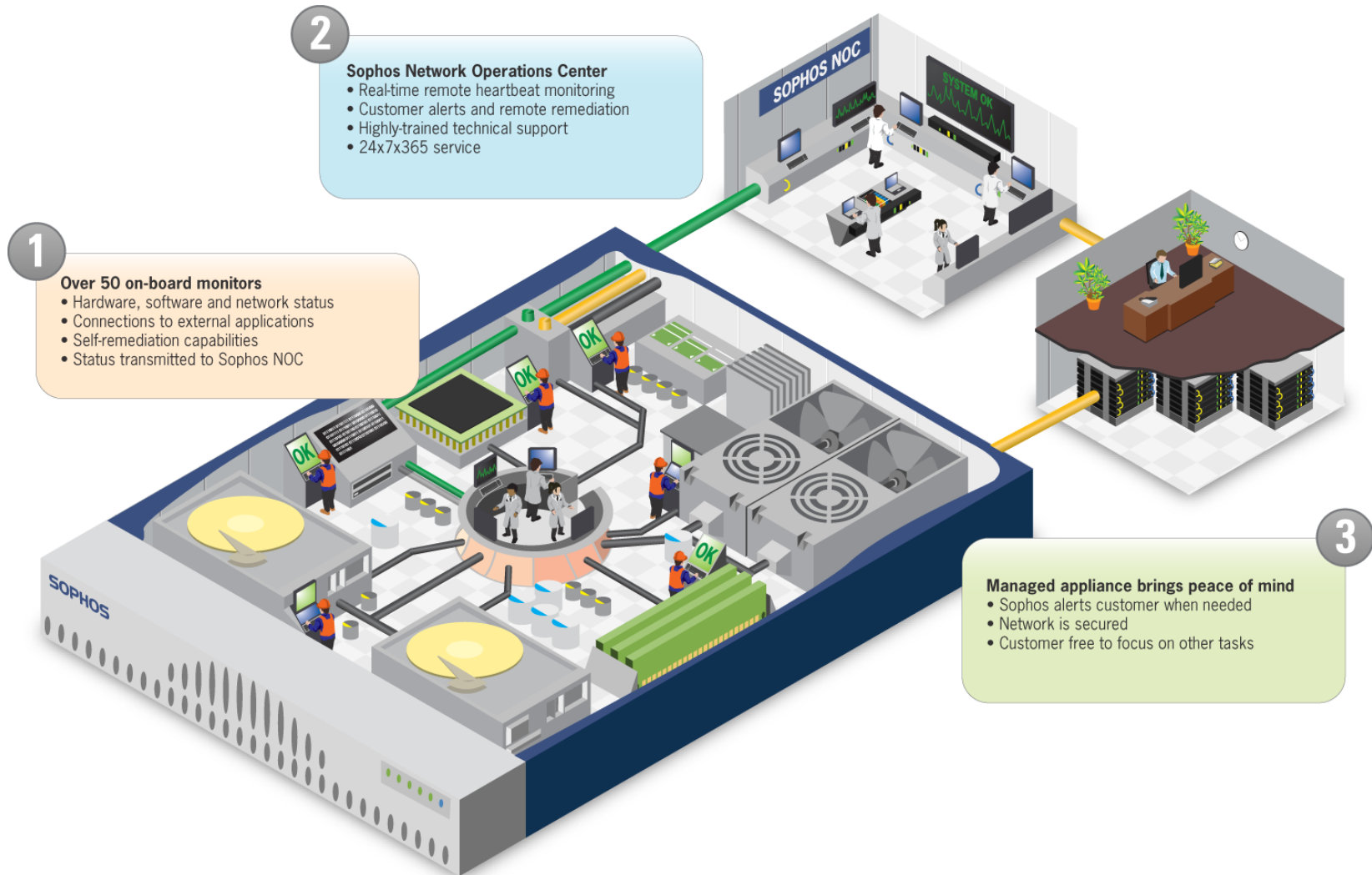
Note: if your mail program does not support active links, reset or recover your password by copying and pasting the text below into your internet browser:

<https://encrvot4.sophos.com/portal/U2FsdGVkX18WJZba1-ZxSdIEG6HG2kxYzUi0mVFozzhPCK8a006cXDRTNPzDnYLEulLeyIFh31JF->

Sophos SPX



Monitorowanie SEA



Monitorowanie SEA

☆ lukasz@fen.pl

To: lukasz@fen.pl

16 czerwca 2016 16:40

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

The screenshot displays the PureMessage Server Group Manager web interface. The top navigation bar includes links for Dashboard, Policy (active), Quarantine, Reports, Local Services, and Server Groups. The main heading is "Policy : Rules".

On the left, there are three sections:

- Manage**: Policy Rules, Anti-Spam Options, Anti-Spam Rules, Anti-Virus Options, Test Current Policy, Test List/Map, Policy Repository.
- Backups**: (no backups), with a "Create" button.
- Lists**: Anti-spam opt-outs, Blacklisted hosts, Blacklisted senders, End Users, Internal hosts, IP Blocking Exception list, IP Blocking Inclusions list, Offensive words, Quarantine digest users, RPC Hosts, Suspect attachment names, Suspect attachment types, Trusted Relay IPs, Whitelisted hosts, Whitelisted senders, Log Reasons, manage... (with a "New" button).

The main area shows a configuration for a rule. It starts with "This configuration is shared: 0 subscriber(s)". The rule logic is as follows:

- Mail from internal hosts
  - Check for mail containing viruses
    - Allow unscannable messages to pass through
    - Reject mail containing viruses
- or
- Mail from external hosts
  - Quarantine blocked IP addresses (Sophos Blocklist)
  - Check for mail containing viruses
    - Allow unscannable messages to pass through
- or
- Quarantine mail containing viruses

The "Quarantine mail containing viruses" section is expanded, showing:

- No tests in this rule, always match. [add test](#)
- Execute actions and rules: [add action](#) [add rule](#)
- Log the message with key/value pair [pmx\\_reason](#)
- Quarantine the message [Virus](#)
- Stop processing

At the bottom, there are buttons for Save, Cancel, Copy, Cut, and Delete.

## Features & Capabilities

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



## Nowe zagrożenia

# Cel ataku

# Cel ataku

Prepare for the GDPR. Take action so your organisation complies with the new reg.



## Daniel Zukowski

1<sup>st</sup>

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

Prepare for the GDPR. Take action so your organisation complies with the new reg.



## Daniel Zukowski

1<sup>st</sup>

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 |

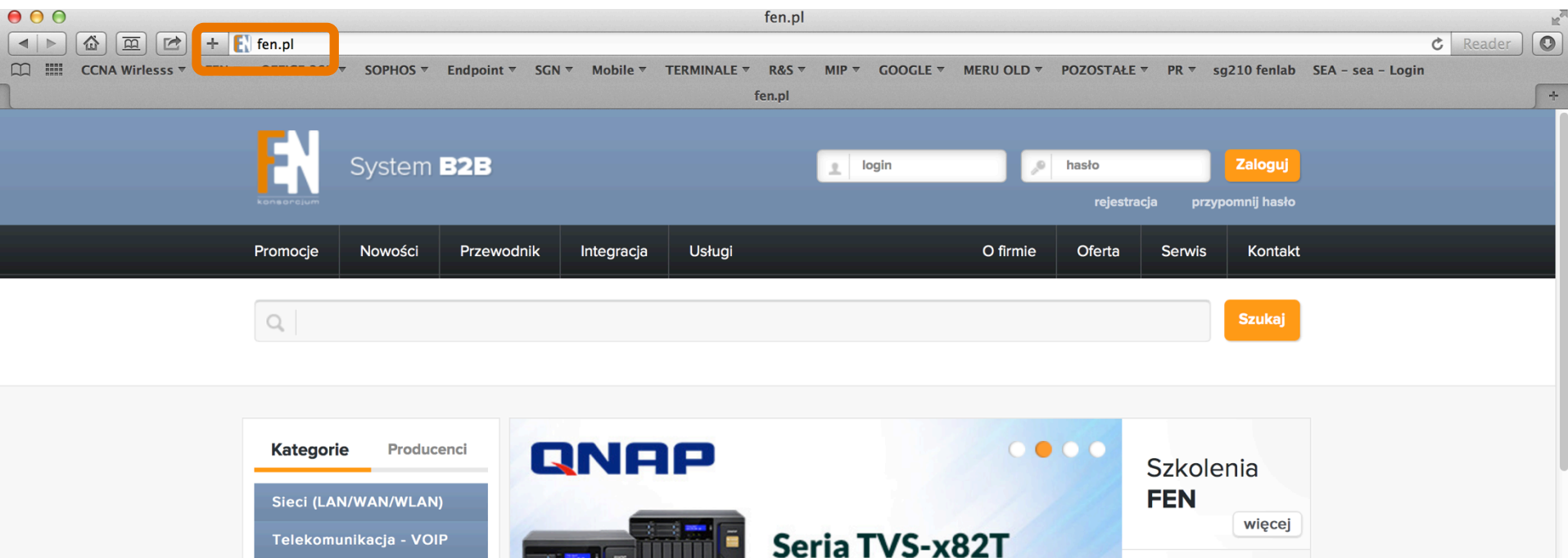
[Send a message](#) ▼

**421**  
connections

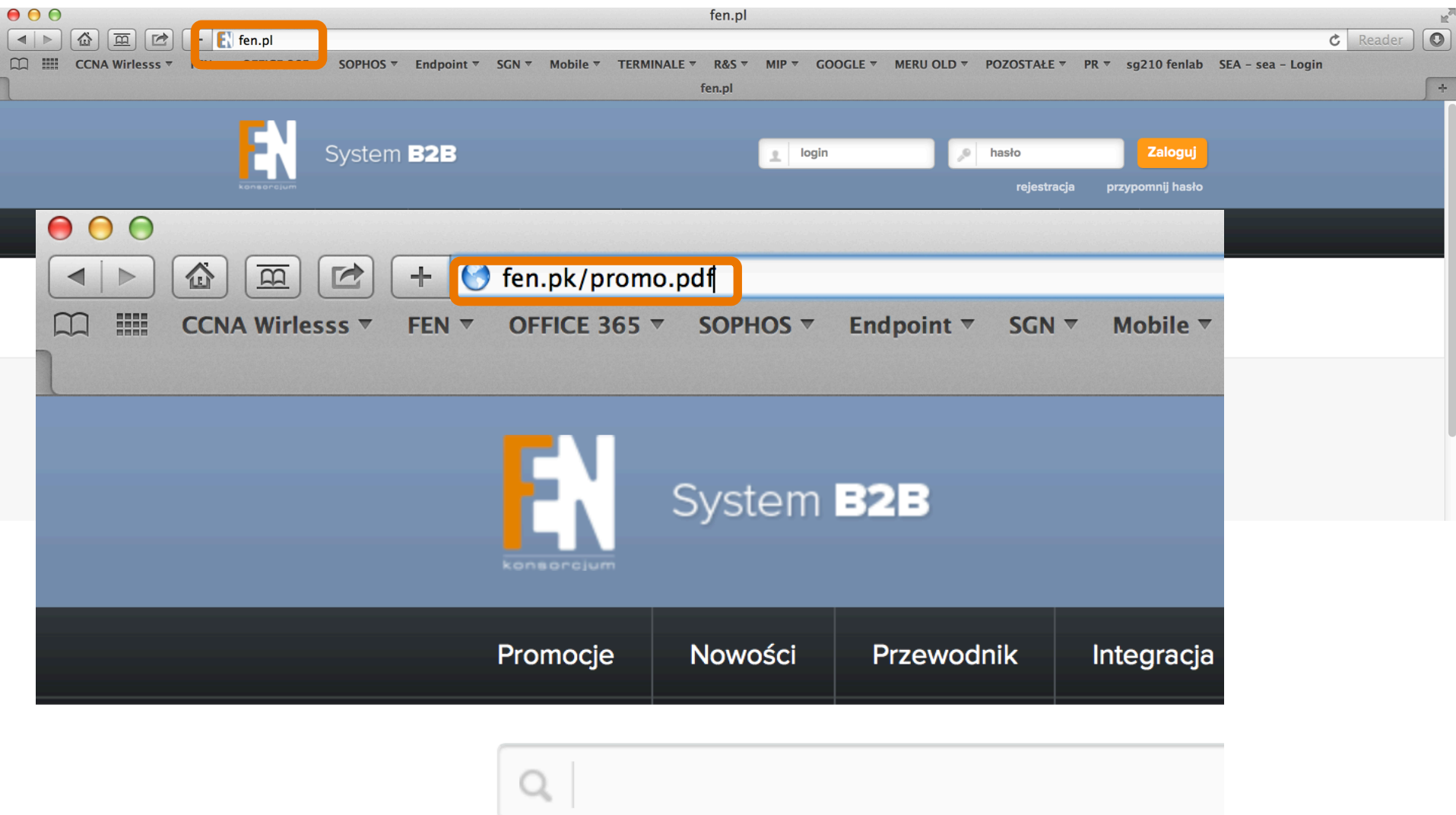
<https://pl.linkedin.com/in/daniel-zukowski-8141a518>

Contact Info

# Przygotowanie pułapki



# Przygotowanie pułapki



# Dostarczenie przynęty

nowe promo na fen.pl

Send

Helvetica 13 B I U

To: Daniel Żukowski

Cc:

Bcc:

Subject: nowe promo na fen.pl

▼

Hej,

Widziałes 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

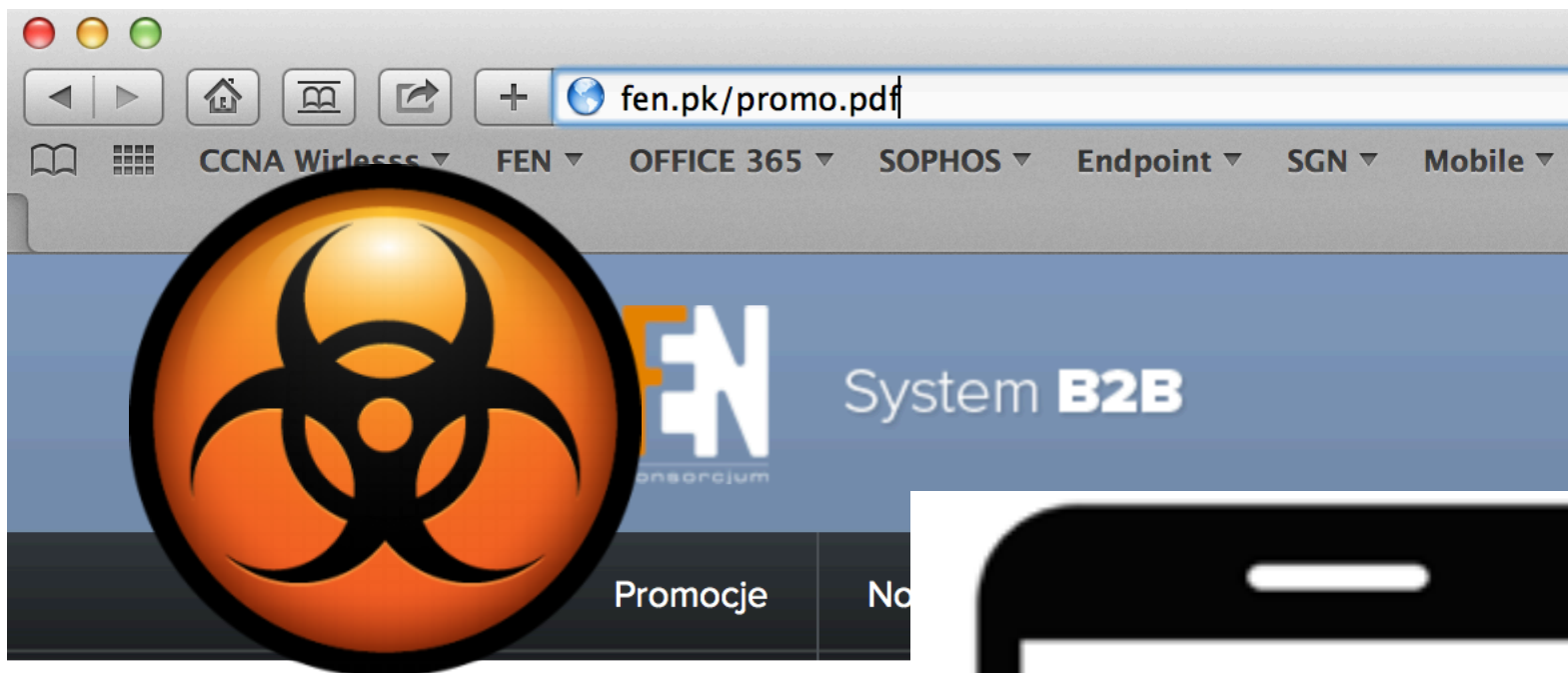


**Kategorie**

**Producenci**

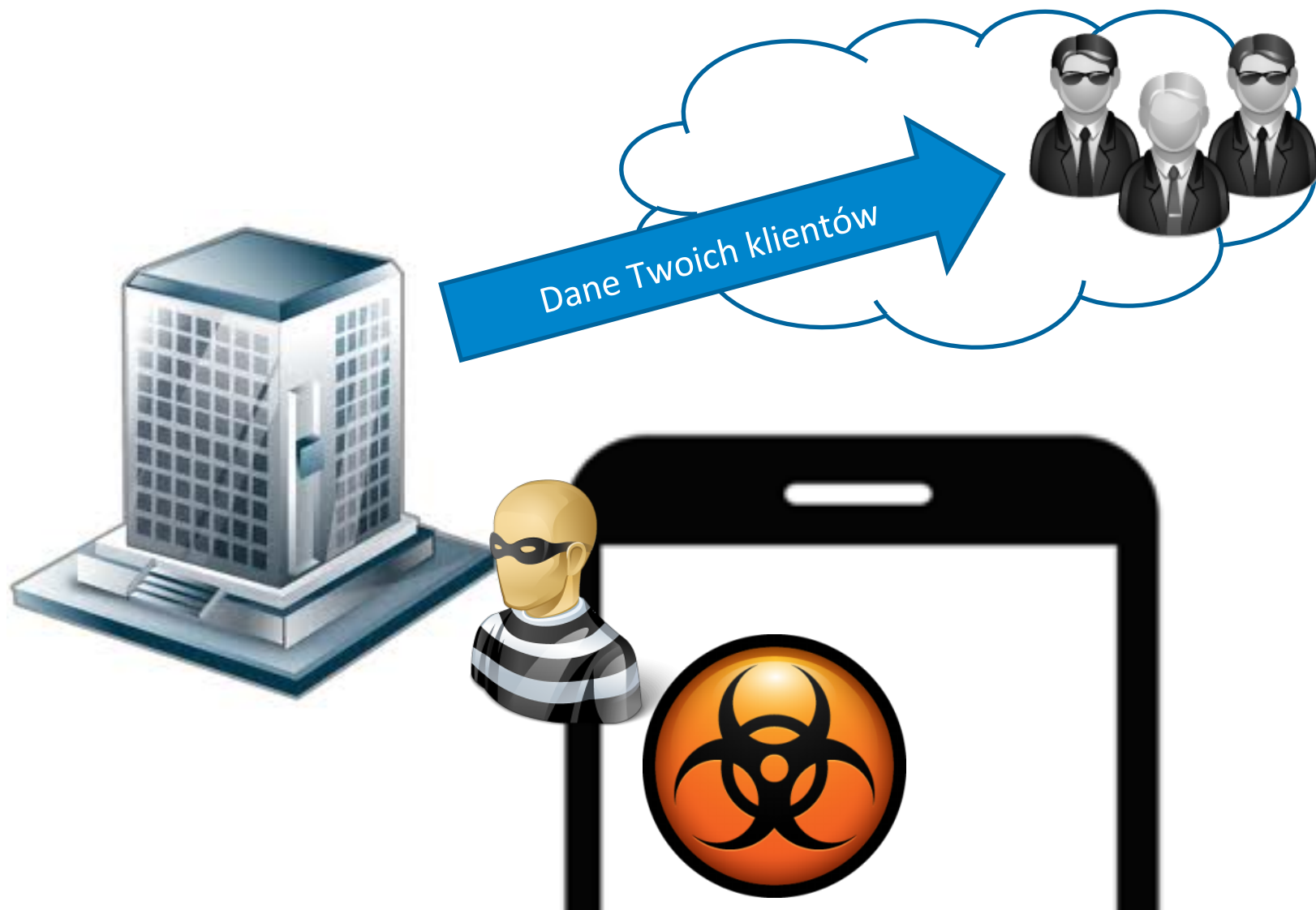


# Oczekiwanie na “cel”



Kategorie

# Wykorzystanie danych



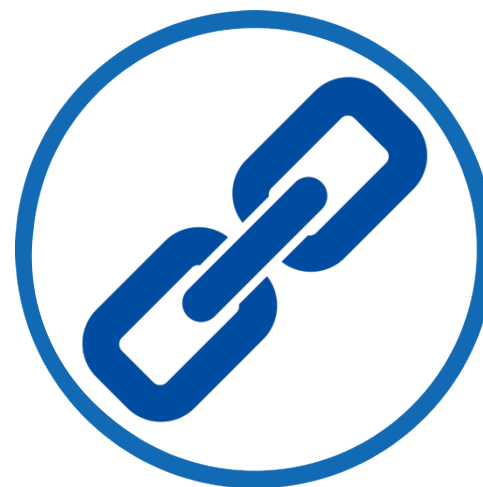
# Co nowego w Sophos Email Appliance?

Sophos Sandstorm



Ochrona przed szkodliwą zawartością  
w załącznikach

Sophos Time-Of-Click  
Protection



Ochrona użytkowników przed atakami  
Spear-Phishing

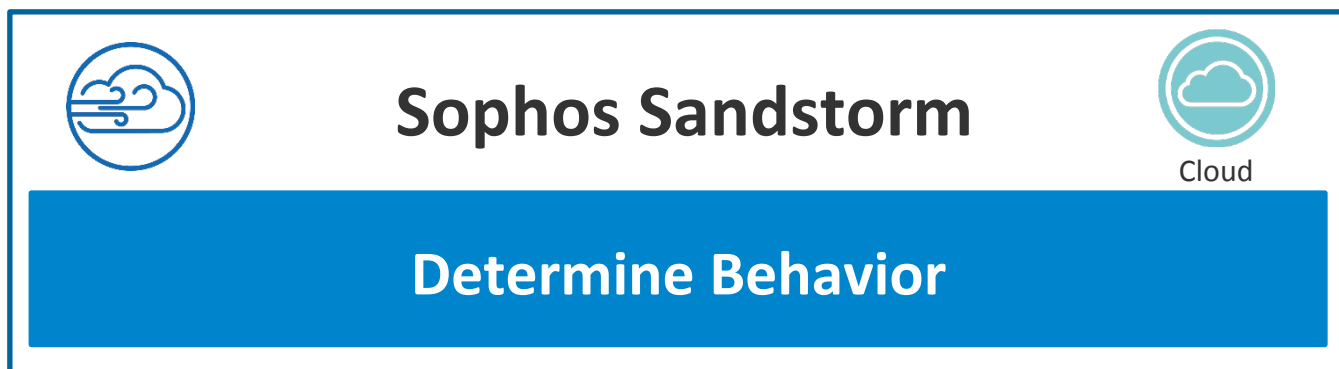
# Czym jest Sophos Sandstorm?

Ochrona użytkowników przed szkodliwymi załącznikami email

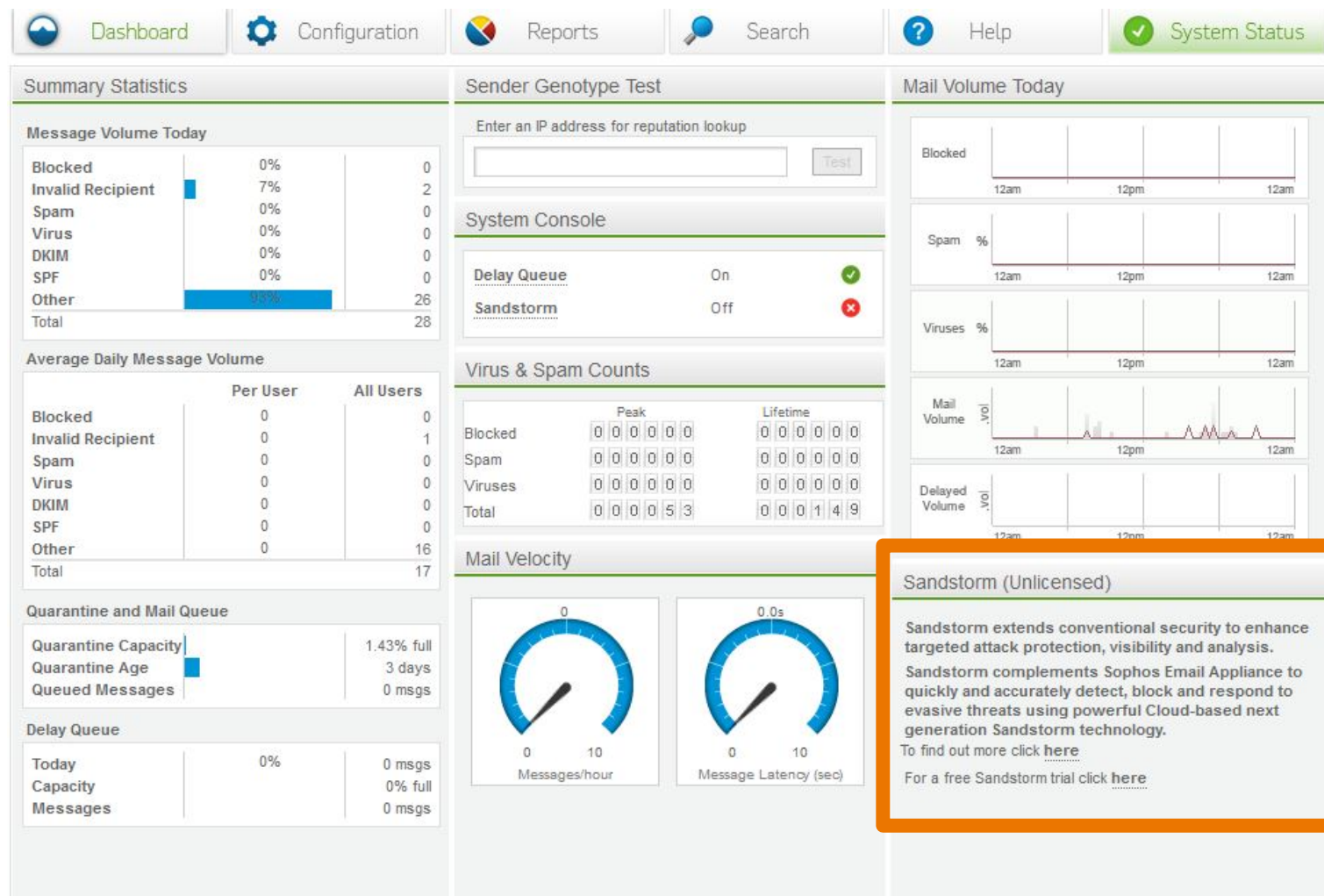
- Zupełnie nowy mechanizm detekcji w portfolio Sophos
- System sandbox oparty na środowisku chmurowym
- Ochrona przed atakami kierowanymi
- Wykrywa, powstrzymuje i odpowiada na nieznane zagrożenia
- Wymaga dodatkowej licencji



# Jak działa Sophos Sandstorm?



# Łatwo dostępne demo



# Proste wdrożenie

Dashboard

Configuration

Reports

Search

Help

System Status

Configuration

Accounts

Policy

Threat Protection

Anti-Spam

Data Control

Additional Policy

Allow/Block Lists

Sandstorm

Filtering Options

Encryption

SMTP Authentication

SMTP Options

System

Routing

Network

Policy: Sandstorm

Enable Sandstorm

On Off

Trial status

Trial expires at 2016/03/05 05:30:00

Sandstorm Monitoring

«

◀

1

▶

»

| Date/Time | Attachment Name | Sender | Status |
|-----------|-----------------|--------|--------|
|-----------|-----------------|--------|--------|

Release

Refresh

# Proste zarządzanie

Dashboard

Configuration

Reports

Search

Help

System Status

Reports

Mail Trends: Sandstorm Volume

Parameters

Mail Trends

Volume

Delayed Volume

Message Actions

Sandstorm Volume

Performance

Senders

Recipients

Policy Analysis

Files

25

20

15

10

5

0

00:00

04:00

08:00

12:00

16:00

20:00

Status

00:00

04:00

08:00

12:00

clean

0

0

0

0

convicted

0

0

0

0

Total

0

0

0

0

Configuration

Policy: Sandstorm

Accounts

Policy

Threat Protection

Anti-Spam

Data Control

Additional Policy

Allow/Block Lists

Sandstorm

Filtering Options

Encryption

SMTP Authentication

SMTP Options

System

Routing

Network

Use this page to enable/disable Sandstorm for threat analysis of Email messages. Also, you can view the list of messages analyzed by Sandstorm.

Enable Sandstorm

On

Off

Trial status

Trial expires at 2016/03/05 05:30:00

Sandstorm Monitoring

«

«

1

»

»

Date/Time

Attachment Name

Sender

Status

2016-02-04/20:02:29

Convicted\_100\_seconds\_wait.exe

vivek.yagnik@outlook.com

Convicted

Release

Refresh



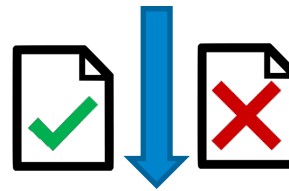
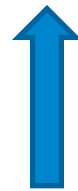
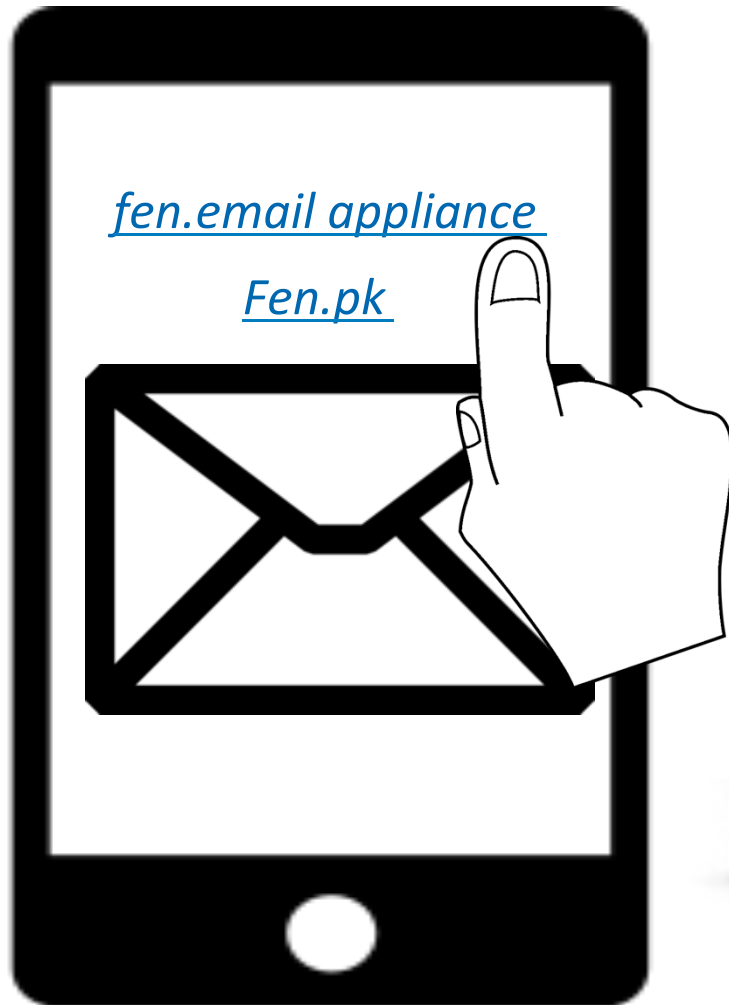
# Czym jest Sophos Time-of-Click Protection?

## 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 subskrypcji Sandstorm



# Jak działa Time-of-Click Protection?



## Licencjonowanie

# Licencjonowanie



Email Protection Advanced  
(subskrypcja na ilość użytkowników)



Sophos Sandstorm  
(subskrypcja na taką samą ilość użytkowników)



## 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, attachments so everything runs sandboxed if suspicious.

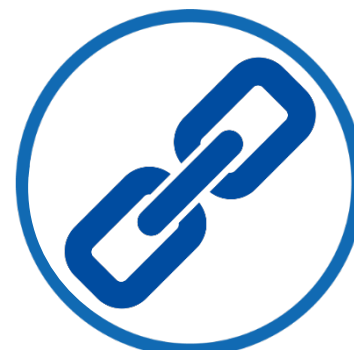


**Anonymous** shared this idea · April 12, 2015 · [Flag idea as inappropriate...](#)

# Sophos Email Appliances

Szyfrowanie  
danych

Ochrona DLP



Anty-Spam

Anty-Malware

# SOPHOS