EndUser Protection

Łukasz Naumowicz

9.06.2016

SOPHOS

Niebezpieczeństwa - Threatsaurus

https://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf?la=de-DE.pdf

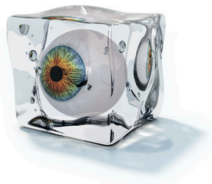
Adware

Potentially Unwanted Application (PUA)

Autorun worm

Internet Worm

Spyware



Data Leakage

Email Malware

Botnet

Fake Anti-virus Malware

Trojan

Phishing

Malware

C&C

Drive-by Download

Rootkit

Ransomware

Źródło: Sophos Threatsaurus

Ransomware


CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
10/9/2013
4:25 PM
Time left
95 : 56 : 35
Next >>

Zagrożenia których nie powstrzyma zwykły anty-wirus

1. Zero day-threat
2. Komputer poza organizacją
3. Nieautoryzowane aplikacje
4. Brak kontroli nad ruchem
5. WWW
   Zainfekowane urządzenia lub udziały sieciowe

Antywirus 1.0

- Sygnatury

Antywirus 2.0

- Sygnatury
- HIPS

Endpoint Protection 1.0

- Sygnatury
- HIPS
- Kontrola aplikacji
- Kontrola urządzeń
- Analiza podejrzanych plików i zachowań

Endpoint Protection 2.0

- Sygnatury
- Weryfikacja zagrożeń „na żywo” w chmurze
- HIPS
- Kontrola aplikacji
- Kontrola urządzeń
- Analiza podejrzanych plików i zachowań
- Jedna konsola

Na podstawie: Sophos Whitepaper – Eight Threats Your anty-virus won’t stop

Doświadczenie SophosLabs

- Malware
- Adware
- HIPS Rules
- Malicious URLs
- Spam Campaigns

- DLP (Sensitive data types)
- Application control
- Device control
- Web URL database
- Anonymizing proxies
- Application patches

Co analizujemy każdego dnia

1 milion	Podejrzanych adresów URL, analizowanych każdego dnia z 70 źródeł
350,000	Nie widzianych wcześniej plików, odbieranych codziennie przez SophosLabs, 3 na sekundę
3 miliony	Wiadomości spam każdego dnia, odnotowane w 80 miejscach 20 krajach
600 milionów	Plików sprawdzanych przez “Live Protection” każdego dnia
150,000	Plików malware dodawanych do bazy “Live Protection” w chmurze w wyniku detekcji
50%	Naszych wykryć bazuje na 19 tożsamościach malware.

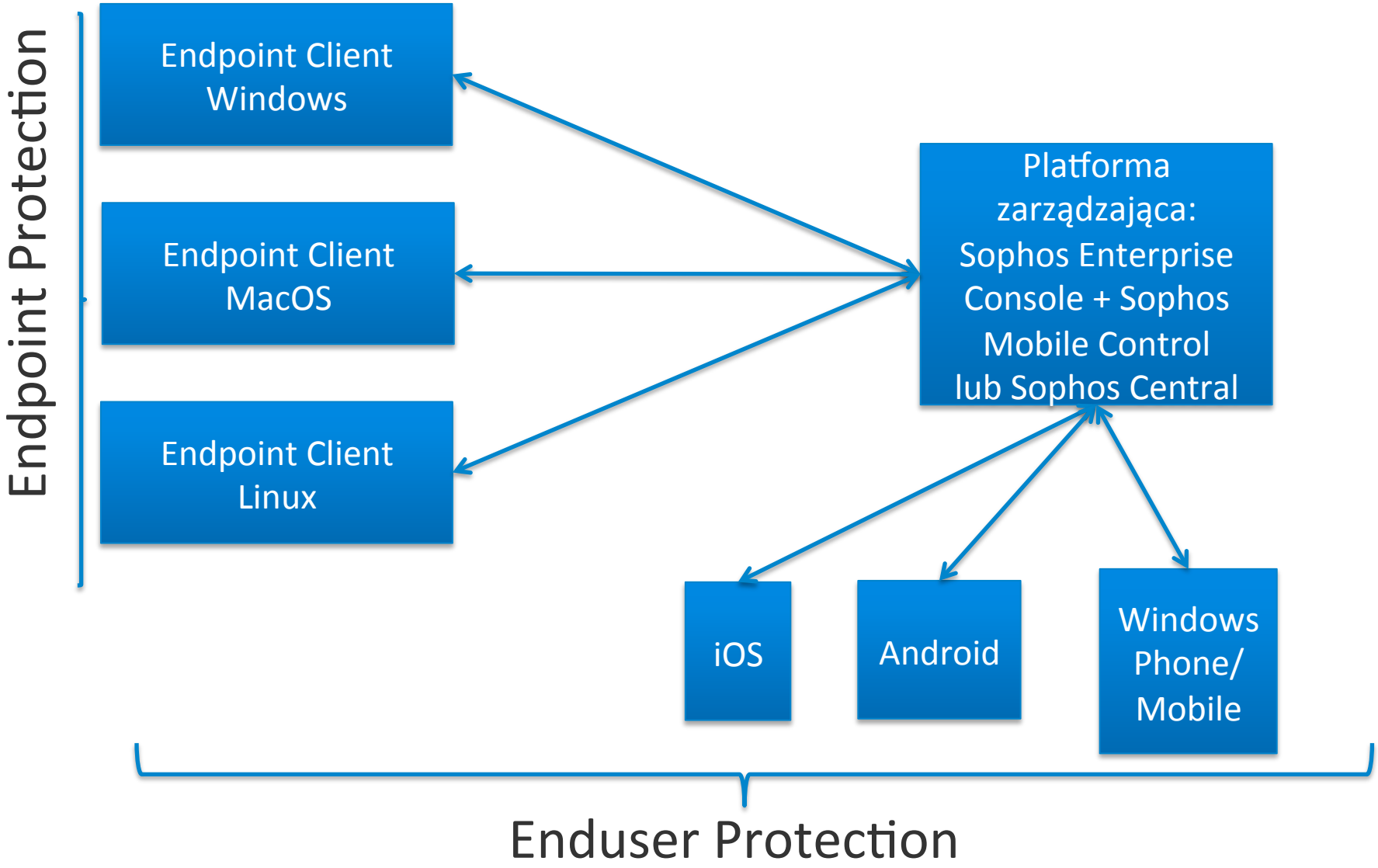
SOPHOS

Architektura

Sophos Central

On Premise

Podstawowe elementy



Sophos Central czy OnPremise

- Jeden panel zarządzania do wszystkich urządzeń
- Proste wdrożenie i zarządzanie
- Security Heartbeat (z platformą XG)
- Nie musisz utrzymywać serwera
- Dodatkowe funkcjonalności wkrótce

- Client Firewall
- Funkcjonalności DLP
- Patch Assesment
- Serwer do zarządzania pozostaje u Ciebie

SOPHOS

Moduły, opcje licencjonowania

	Sophos Cloud Enduser Protection	Sophos Cloud Endpoint Protection Advanced	Sophos Cloud Endpoint Protection Standard	Enduser Protection	Endpoint Protection Advanced	Endpoint Protection Standard
Management	**Web-based, hosted by Sophos in the cloud**			**Windows-based, deployed on premise**		
User-based policy	✓	✓	✓			
Anti-malware	✓	✓	✓	✓	✓	✓
HIPS	✓	✓	✓	✓	✓	✓
Web security	✓	✓	✓	✓	✓	✓
Web control (filtering)	Windows, Mac	Windows, Mac		Windows	Windows	Windows
Malicious traffic detection	✓	✓		✓	✓	
Download reputation detection	✓	✓	✓	✓	✓	✓
Patch assessment				✓	✓	
Application control	✓	✓		✓	✓	✓
Device control	✓	✓		✓	✓	✓
DLP				✓	✓	
Client firewall				✓	✓	✓
Active Directory sync	✓	✓		✓	✓	✓
Microsoft Exchange anti-spam and anti-malware				✓	✓	✓
Anti-malware for network storage (NetApp, EMC, Oracle)				✓	✓	
Mobile device management	✓			✓		
Integrated mobile encryption, Android security and web filtering				Optional		
OS support	Windows, Mac; iOS, Android Windows Server and Linux support available in Sophos Server Protection	Windows, Mac Windows Server and Linux support available in Sophos Server Protection	Windows, Mac Windows Server and Linux support available in Sophos Server Protection	Windows, Mac, Linux; iOS, Android, Windows Mobile, Windows Phone, BlackBerry	Windows, Mac, Linux	Windows, Mac

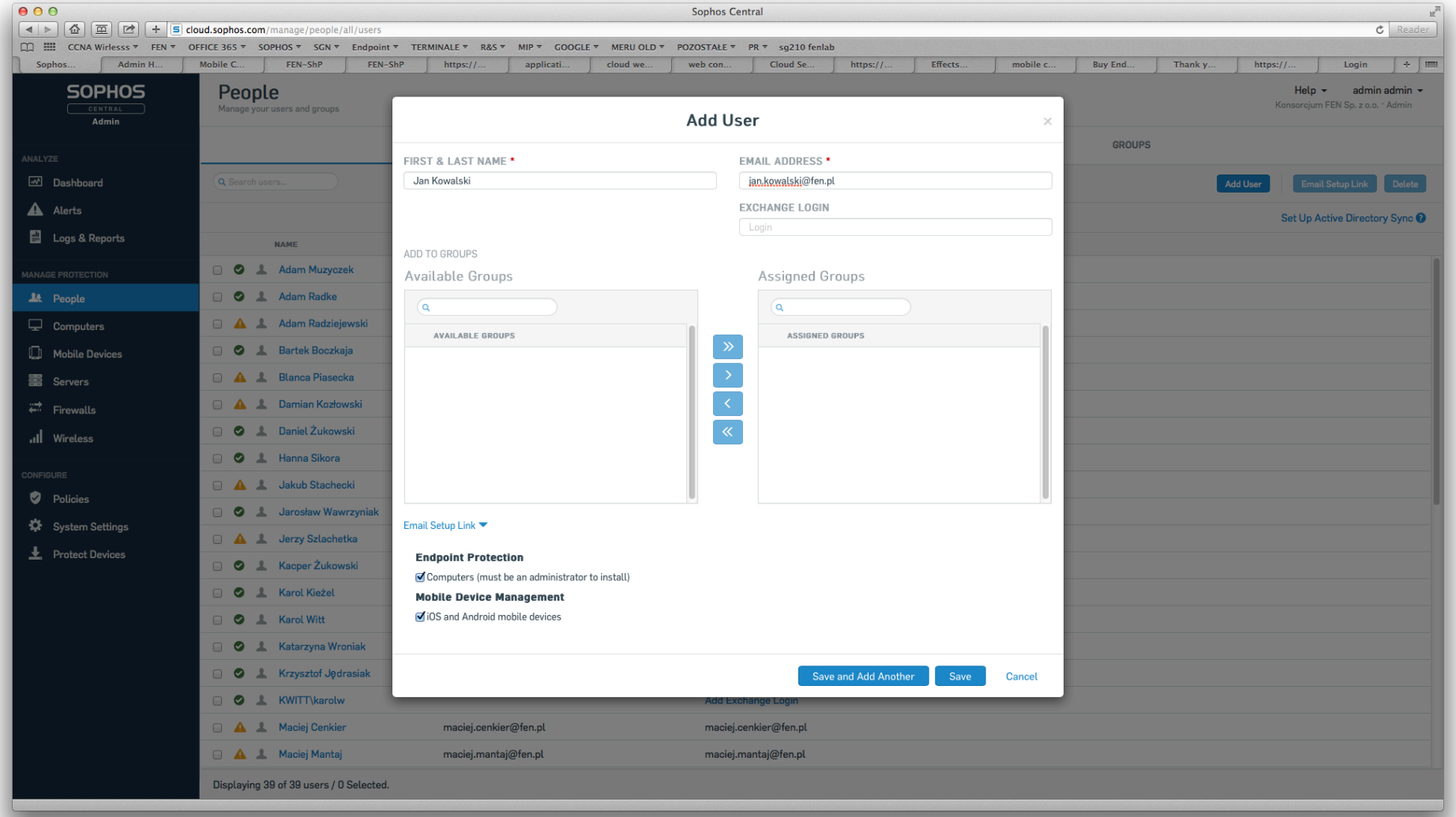
Moduł	Funkcjonalność
Anti-malware (anty-virus)	Wykrywanie i blokowanie oprogramowania skategoryzowanego jako szkodliwe OnAccess, OnDemand, Live Protection
HIPS (Host IPS)	Wykrywanie i analiza podejrzanie zachowujących się aplikacji i blokowanie ich dalszego wykonywania(np. zmiany w rejestrze, kopiowanie plików)
Web security/protection	Blokowanie dostępu do stron skategoryzowanych przez SophosLabs jako zawierające malware lub blokowanie dostępu na podstawie zawartości danej strony
Web control	Filtrowanie stron www po kategoriach lub adresach, filtrowanie po rodzajach plików
Malicious Traffic Detection	Monitorowanie ruchu HTTP pochodzącego z aplikacji innych niż przeglądarki, blokowanie kontaktu z C&C
Download Reputation Detection	Porównanie plików które użytkownik chce pobrać z bazą dostępną w SophosLabs, wyświetlanie monitów przy plikach o niskiej reputacji
Application Control	Kontrola i możliwość blokowania aplikacji
Device Control	Kontrola i możliwość blokowania urządzeń peryferyjnych (pamięci USB, zewnętrzne dyski twarde, nośniki optyczne, interfejsy sieciowe(wifi, modemy USB, Bluetooth, irDA, protokoły MTP, PTP)
Security Heartbeat	Współpraca Endpointa i XG Firewall(wymagany Network Protection lub Enterprise Guard lub FullGuard)
Patch Assesment	Analiza pod kątem aktualności łat systemowych i łat w aplikacjach
DLP	Monitorowanie i filtrowanie informacji wysyłanych za pośrednictwem określonych klientów pocztowych, przeglądarek, przenoszonych na pamięci USB, po typach plików i określonych wzorcach danych w plikach jak numery kart kredytowych
Client Firewall	Monitorowanie ruchu sieciowego, możliwości dopuszczenia ruchu tylko z wybranych aplikacji, ochrona przed wykradaniem danych przez aplikacje nieautoryzowane
Tamper Protection	Ochrona przed wprowadzaniem zmian w oprogramowaniu przez użytkownika

Ochrona serwerów

Nazwa	Przeznaczenie	Korzyści
Sophos Anty-virus for vShield	Ochrona maszyn wirtualnych z vmware i vshield	• ochrona wszystkich maszyn • scentralizowane zarządzanie • sumaryczne aktualizacje • lepsza wydajność*
Pure Message for Microsoft Exchange	Ochrona serwerów pocztowych przed spamem, wirusami i innymi zagrożeniami	• eliminacja spamu do 99% • dostęp dla użytkowników do portalu kwarantanny • plugin Outlook do oznaczania spamu • dostępna wersja na UNIX
Sophos for Microsoft Sharepoint	Ochrona serwerów Sharepoint**	• ochrona stron w czasie rzeczywistym(sygnatury, analiza zachowań) • kontrola zawartości na stronach(słowa kluczowe, rodzaje plików) • intuicyjny panel zarządzania przez webUI
Sophos for Network Storage	Ochrona macierzy NetApp, EMC, Oracle/Sun	• Wykrywanie i blokowanie malwaru zanim rozprzestrzeni się • Ochrona w czasie rzeczywistym, • Integracja z mechanizmami ochrony macierzy
Server Lockdown	Ochrona serwerów przed nieznanymi aplikacjami	• Pełna kontrola nad aplikacjami pracującymi na serwerz • „Zamrożenie” serwera w danym momencie

*w porównaniu do TrendMicro Deep Security, McAfee MOVE Agentless

Sophos Central



Sophos Central – Endpoint Client

This mail was generated by Sophos Cloud. In case of issues, you can contact your Sophos Cloud administrator by replying to this mail.

This is an automated message initiated by your security software administrator.

Please visit the links below for the Sophos agent and operating system you need to download and install on your computer:

For Sophos Endpoint Protection:

- Mac OS X
- Windows

If the link does not work in your browser you can copy and paste the link below in your browser's address bar.

For Sophos Endpoint Protection:

- Mac OS X: https://dzr-api-amzn-eu-west-1-9af7.api-upe.p.hmr.sophos.com/api/download/53810c059c4af2ec3a0adb899fcfd671/SophosInstall.zip
- Windows: https://dzr-api-amzn-eu-west-1-9af7.api-upe.p.hmr.sophos.com/api/download/3cb476a4f17c4d137a3a19e8d15bae42/SophosInstall.exe

If you have more than one computer, for instance a desktop and a laptop, please visit the links above for each device you want to protect and complete the installation as instructed.

If you have any questions or concerns about the authenticity of this message, or if you are encountering difficulty with the software installation, please contact your IT administrator directly.

Thank you!

Mail Attachment.png (2 KB)

Sophos Central – Mobile Device Management

This is an automated message initiated by your security software administrator (The links and QR code in this email contain personal information. Do not forward to other people)

Install the Sophos Mobile App

Reading this on your mobile?

1. Install the app.
2. Configure the app so that Sophos Cloud can manage it.
3. If an empty screen is displayed, restart the app to synchronize with Sophos Cloud.
4. Repeat for all your mobile devices.

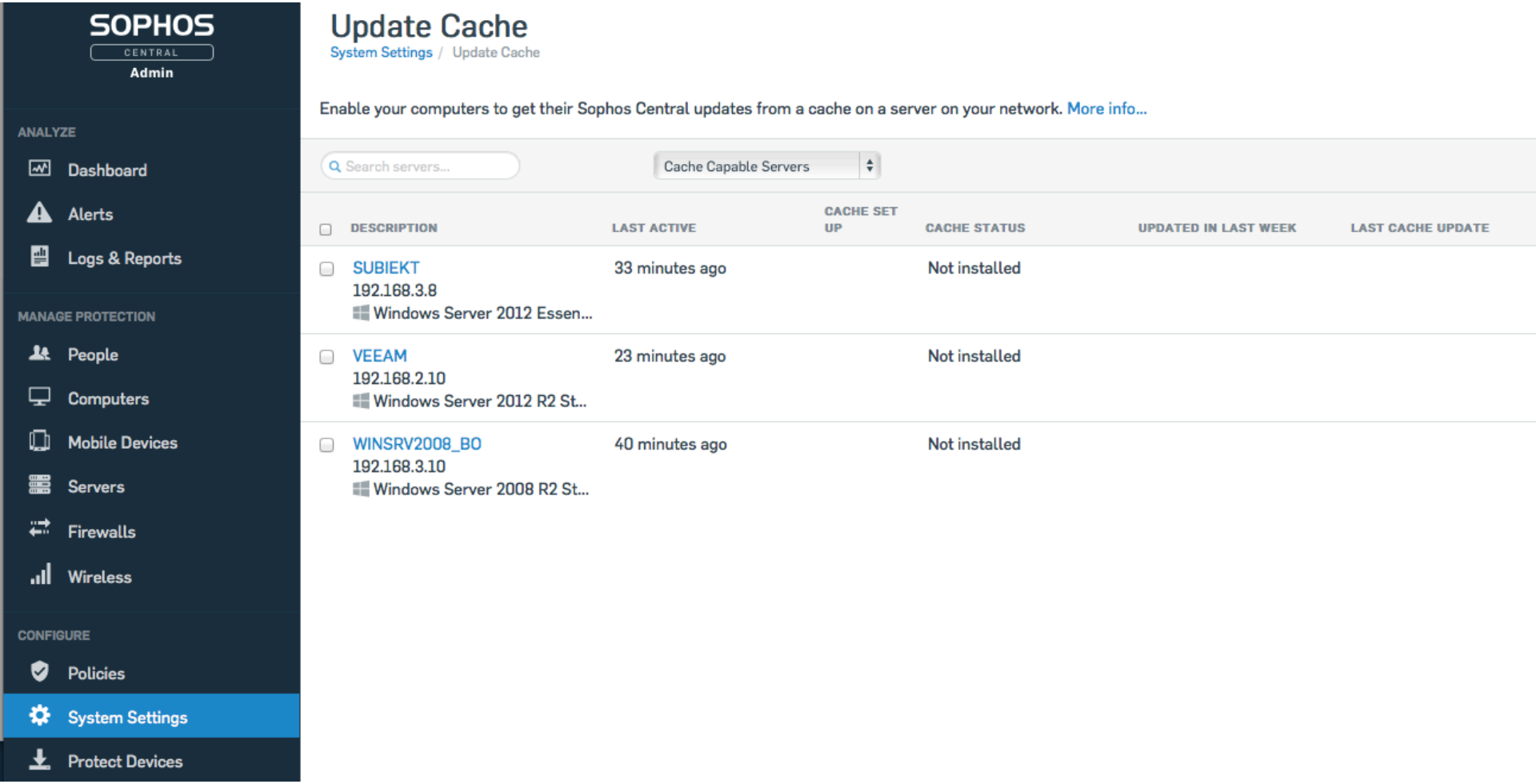
Note: If the links above does not work, do a manual setup If your administrator needs you to install more than one app, the second install will start automatically

Reading this on your computer?

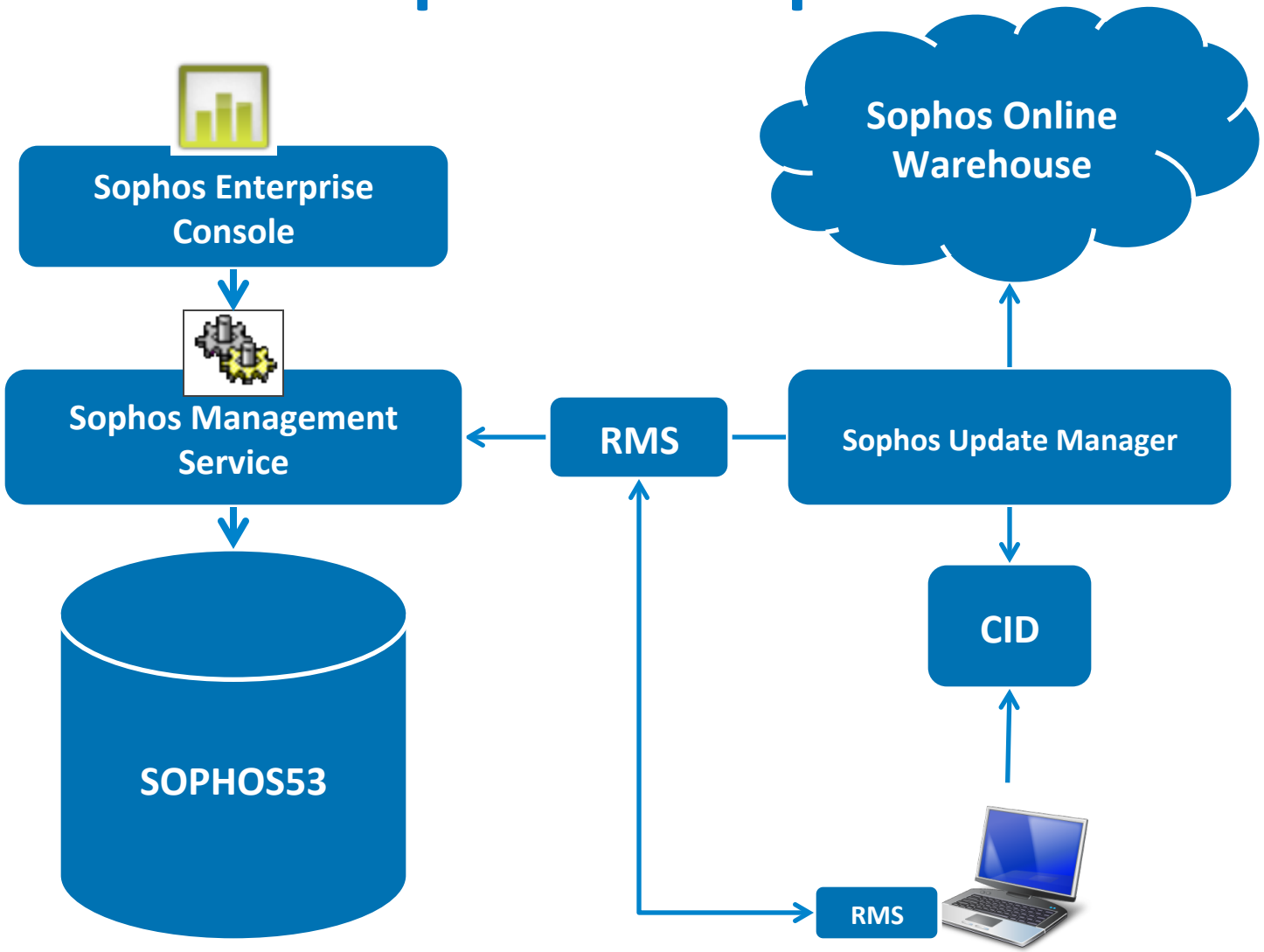
1. To install the app, use your mobile device to scan the QR code below:
   Note: You need an app installed that lets your mobile device read QR codes.

2. To configure the app so that Sophos Cloud can manage it, start the app and scan the QR code again.
3. Repeat for all your mobile devices.
   Note: If your administrator needs you to install more than one app, the second install will start automatically

Sophos Central – Update Cache

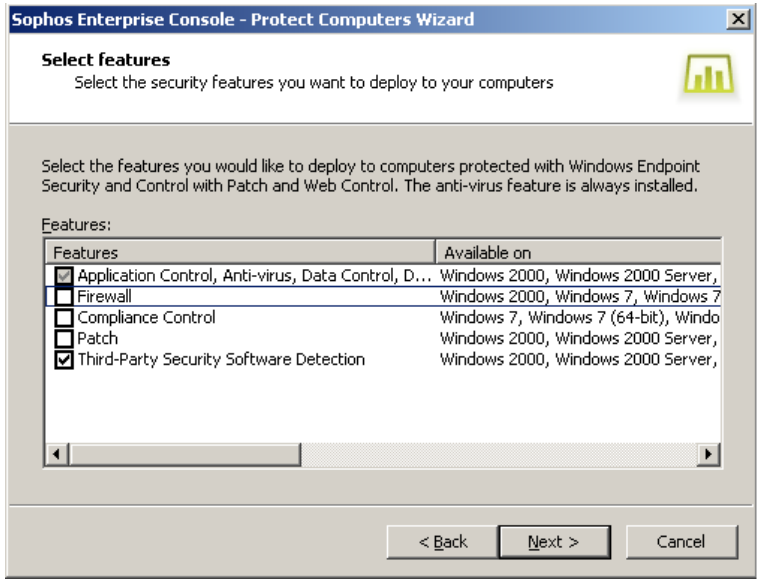


On Premise – Sophos Enterprise Console



Kreator konfiguracji

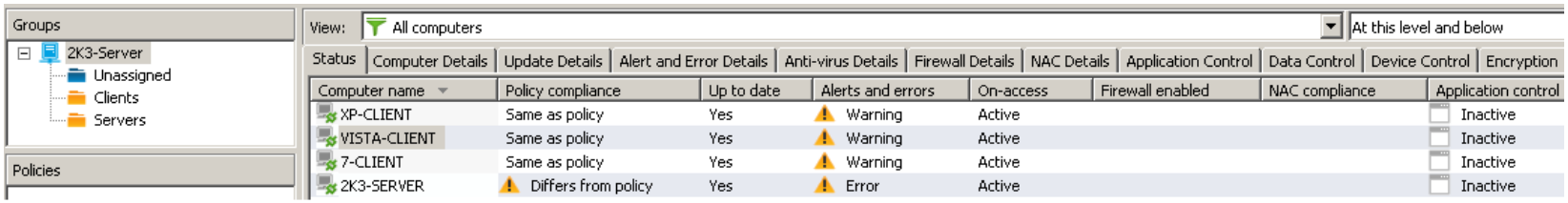
- Centralne wdrożenie I administracja wybranymi komponentami

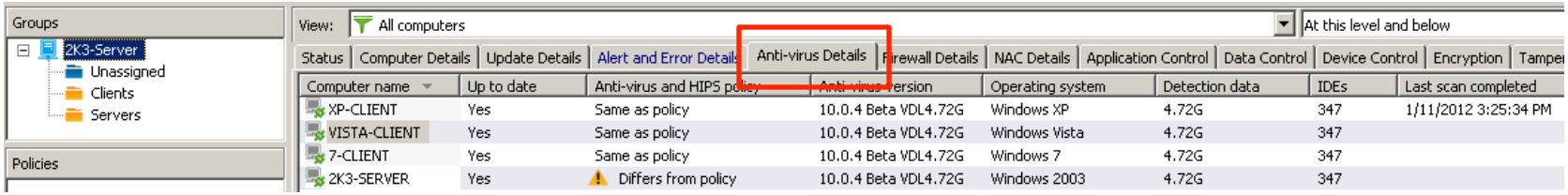


Ochrona stacji

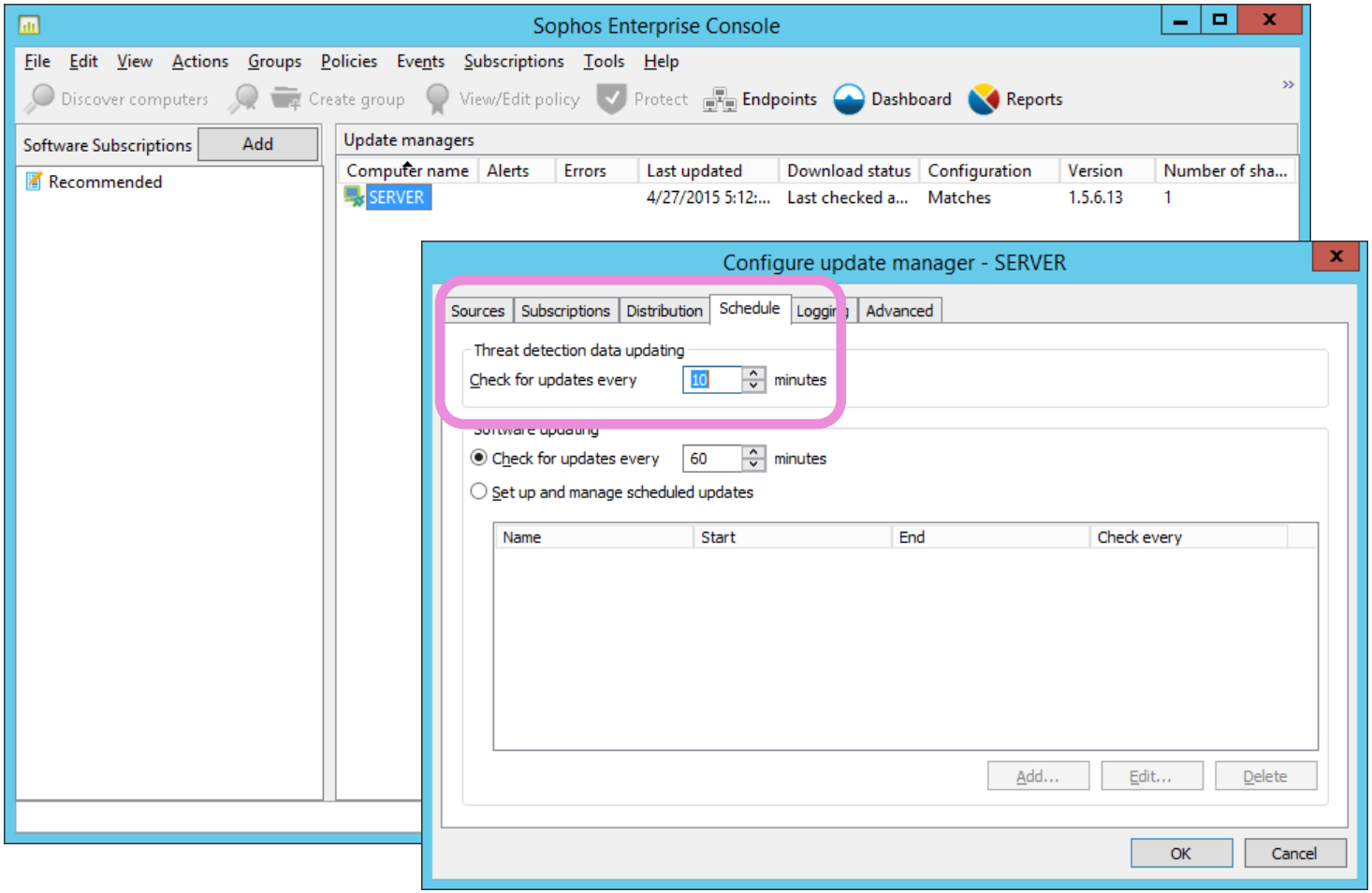
- Po zakończeniu instalacji Endpoint pojawia się w panelu SEC

- RMS instalowany razem z SEC, odpowiada za komunikację z Endpointami i raportuje aktualne dane do SEC





Update Manager



SOPHOS

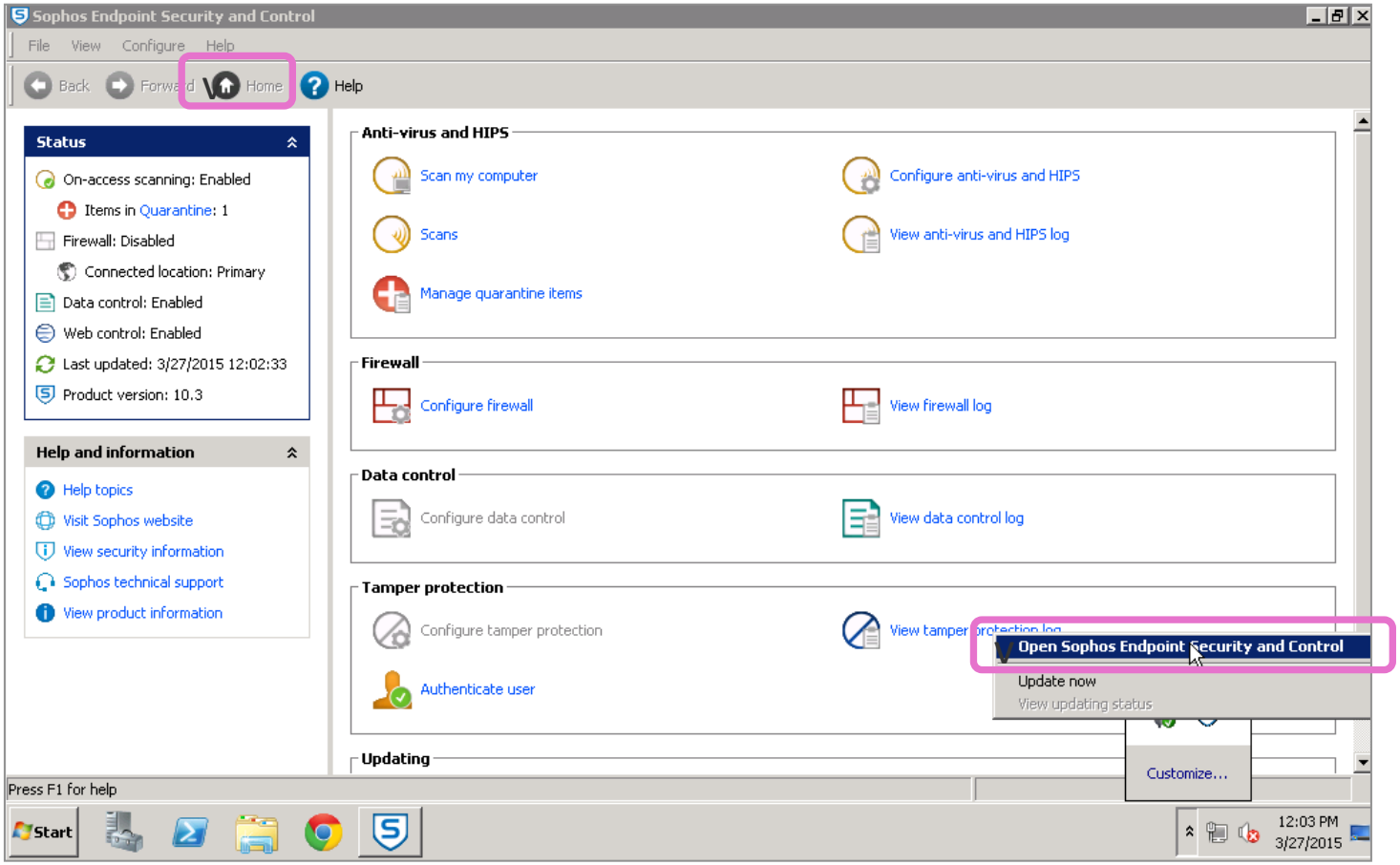
Endpoint Client z perspektywy użytkownika

Aplikacja na Windows

Klient zainstalowany

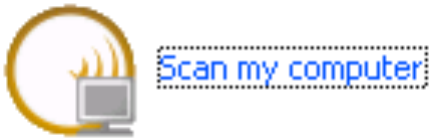
Wiadomość dla użytkownika

Błąd aktualizacji



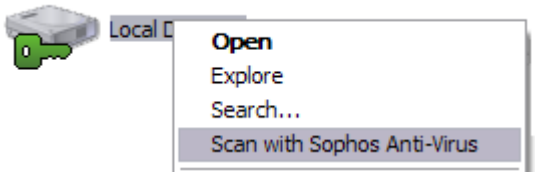
Skanowanie OnDemand

Przeskanuj komputer

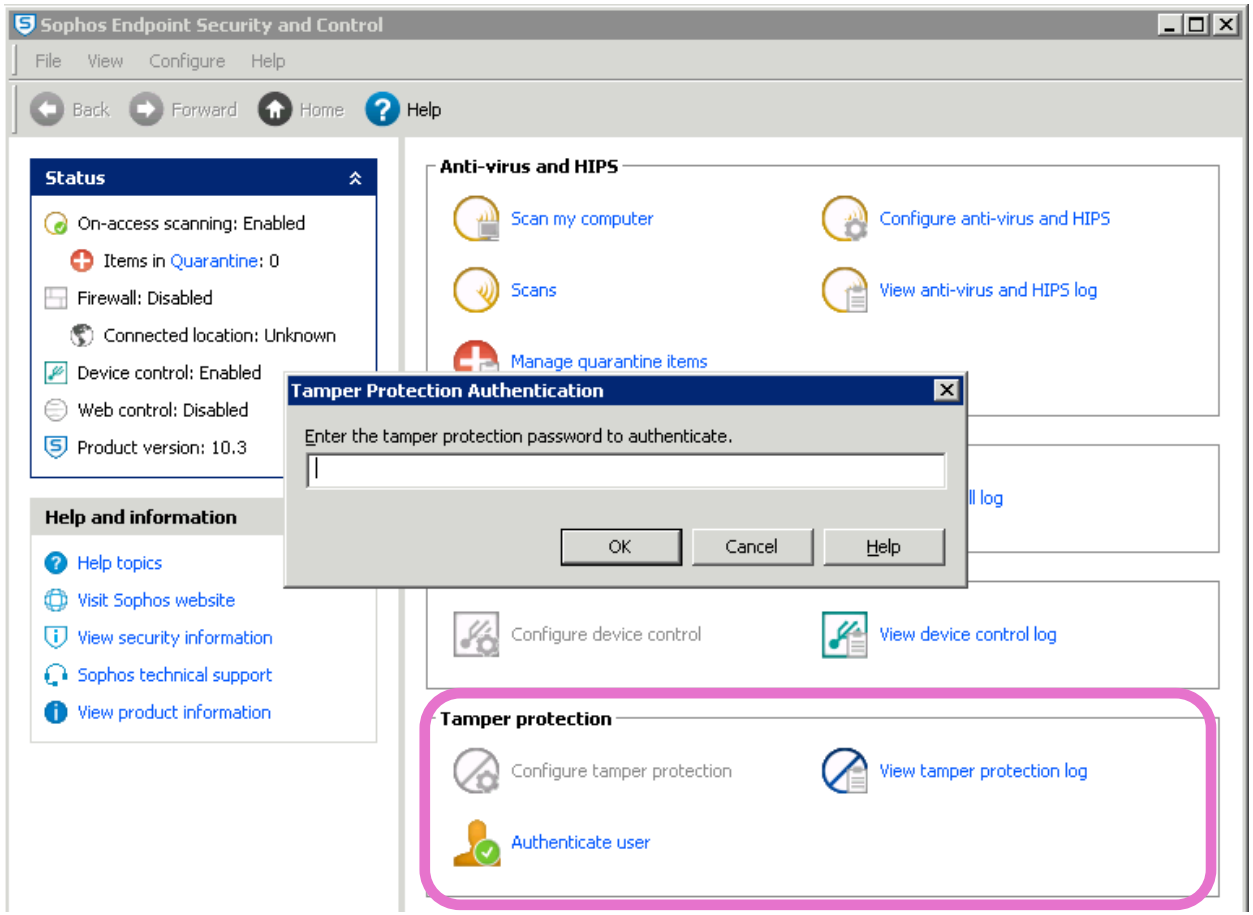


Uruchom skan wybranych elementów lub utwórz harmonogram

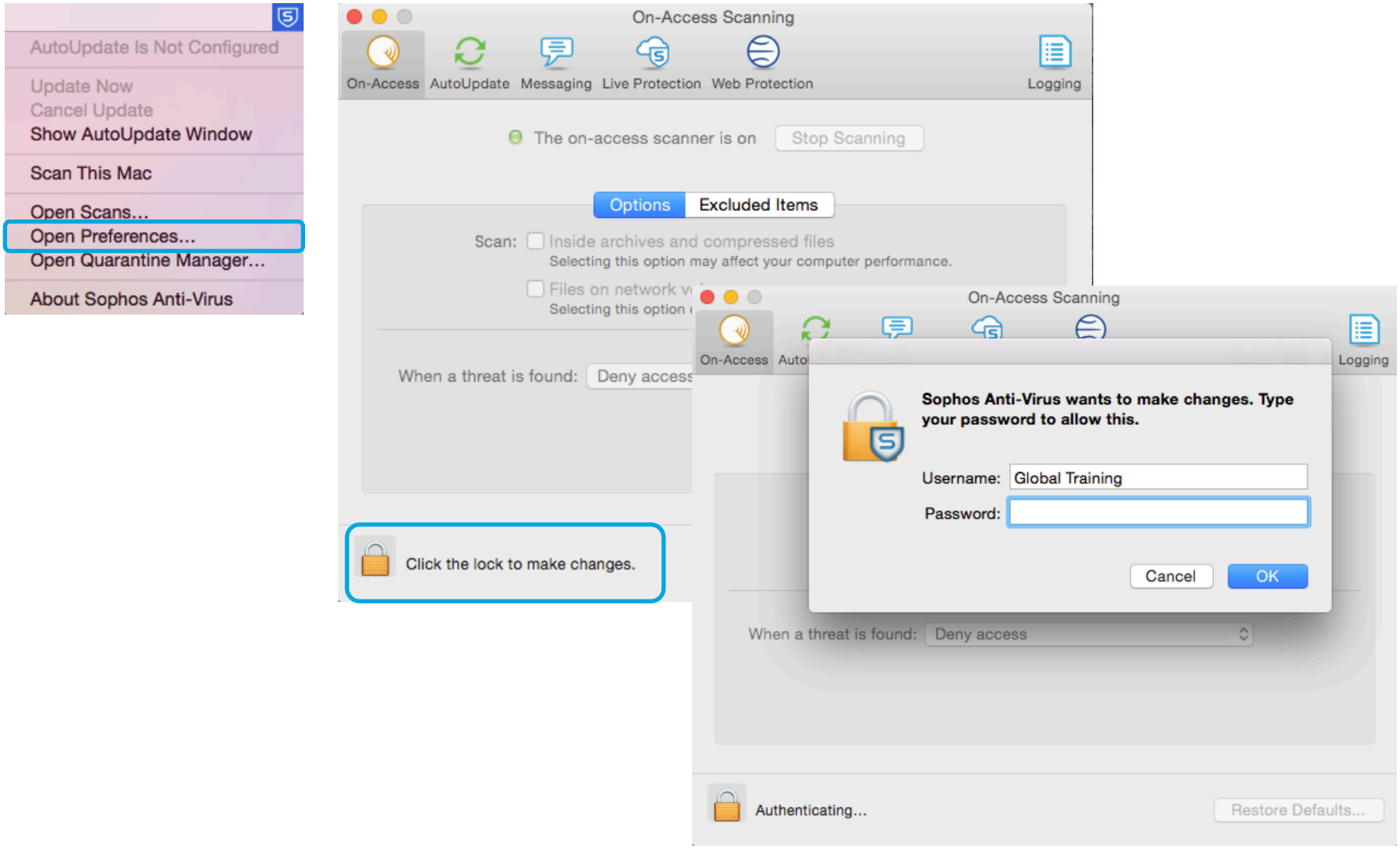
Skanowanie prawym przyciskiem



Ochrona przed wprowadzeniem zmian



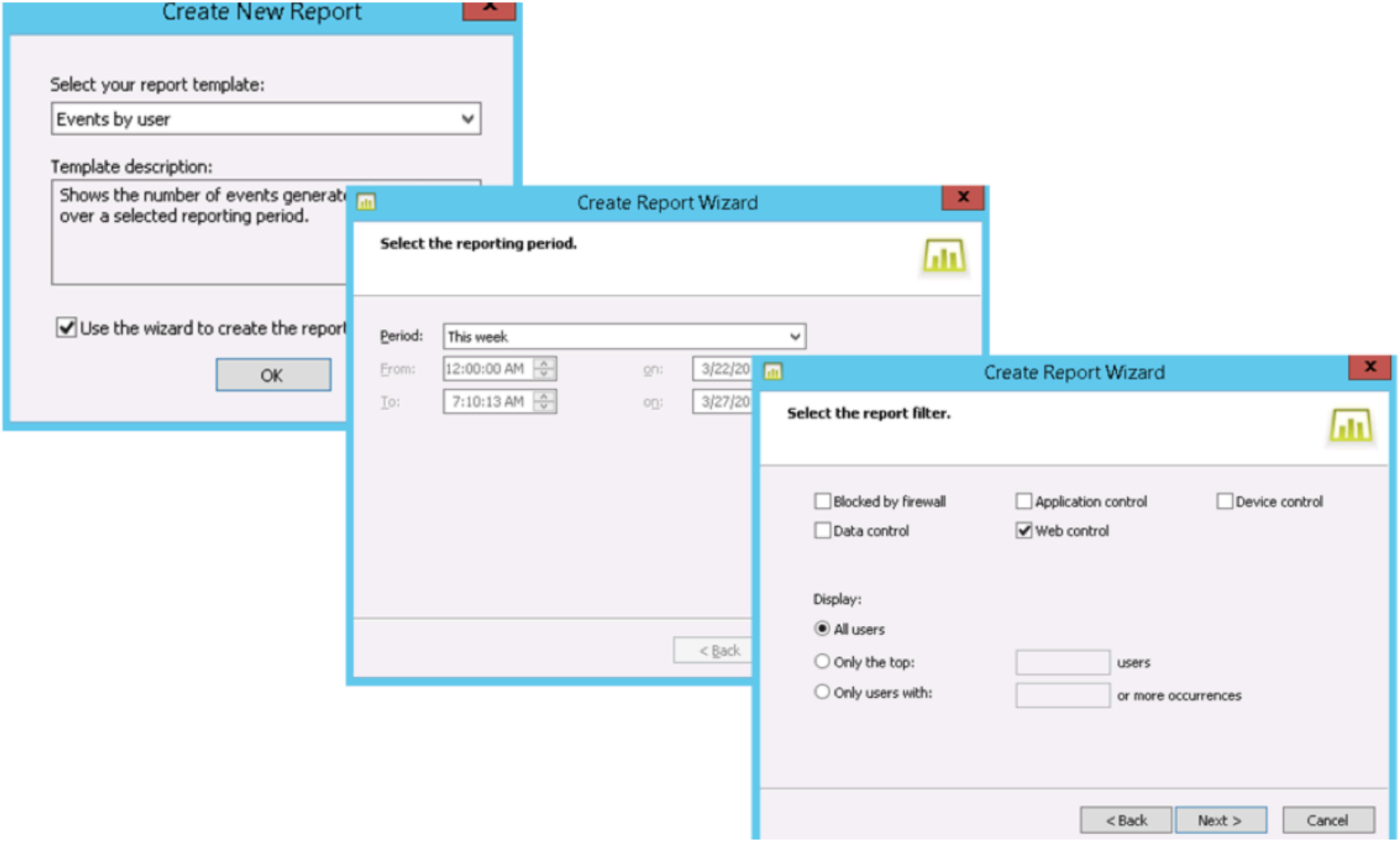
Aplikacja na MacOS



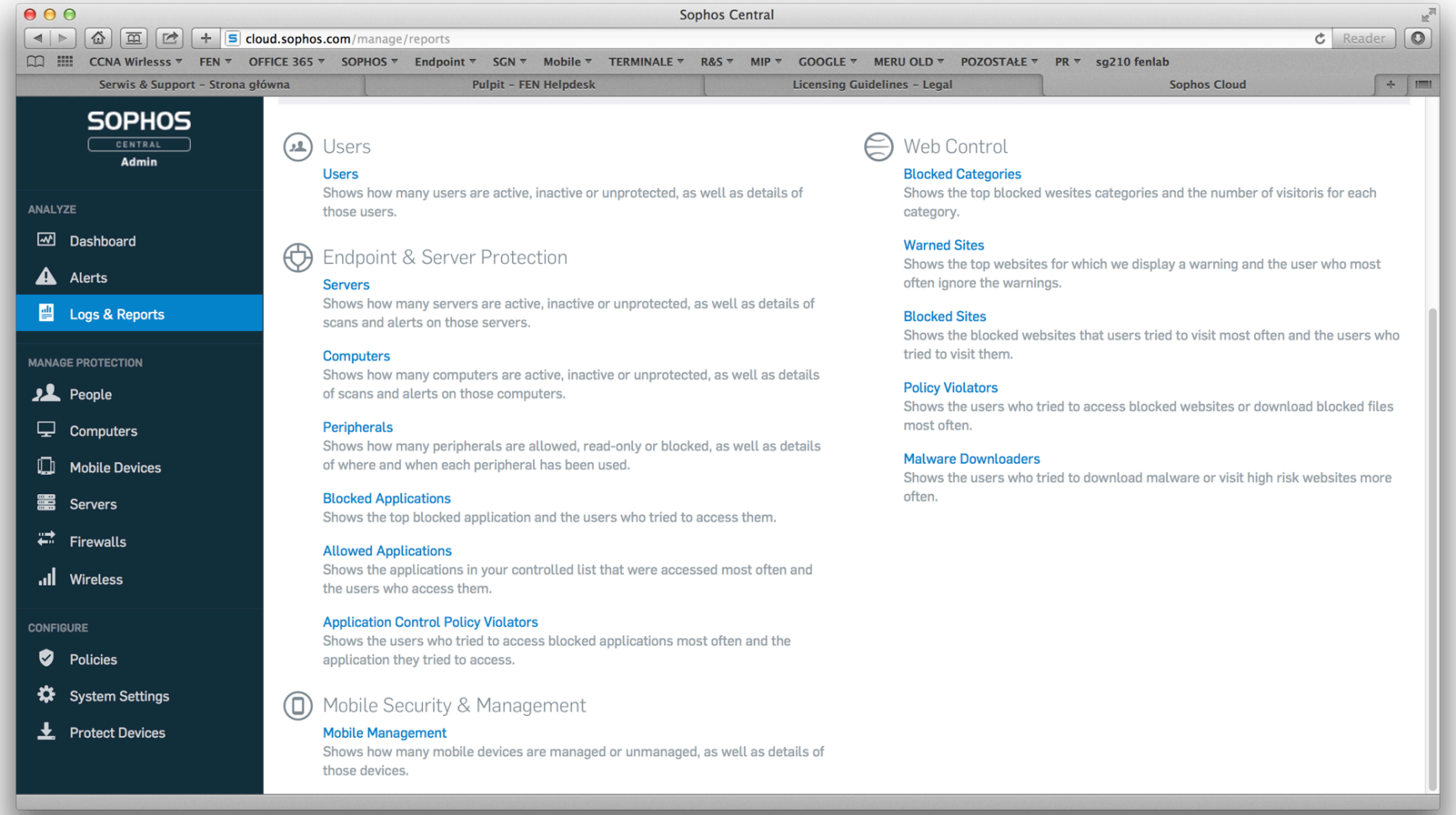
SOPHOS

Raportowanie i audyt

OnPremise


Create New Report
Select your report template:
Events by user
Template description:
Shows the number of events generate
over a selected reporting period.
Use the wizard to create the report
OK
Create Report Wizard
Select the reporting period.
Period:
This week
From:
12:00:00 AM
on:
3/22/20
To:
7:10:13 AM
on:
3/27/20
< Back
Create Report Wizard
Select the report filter.
Blocked by firewall
Application control
Device control
Data control
Web control
Display:
All users
Only the top:
users
Only users with:
or more occurrences
< Back
Next >
Cancel

Sophos Central



SOPHOS

Dlaczego warto wybrać rozwiązanie Sophos EndUser Protection?

Gartner

Source: Gartner (February 2016)

Tolly Group

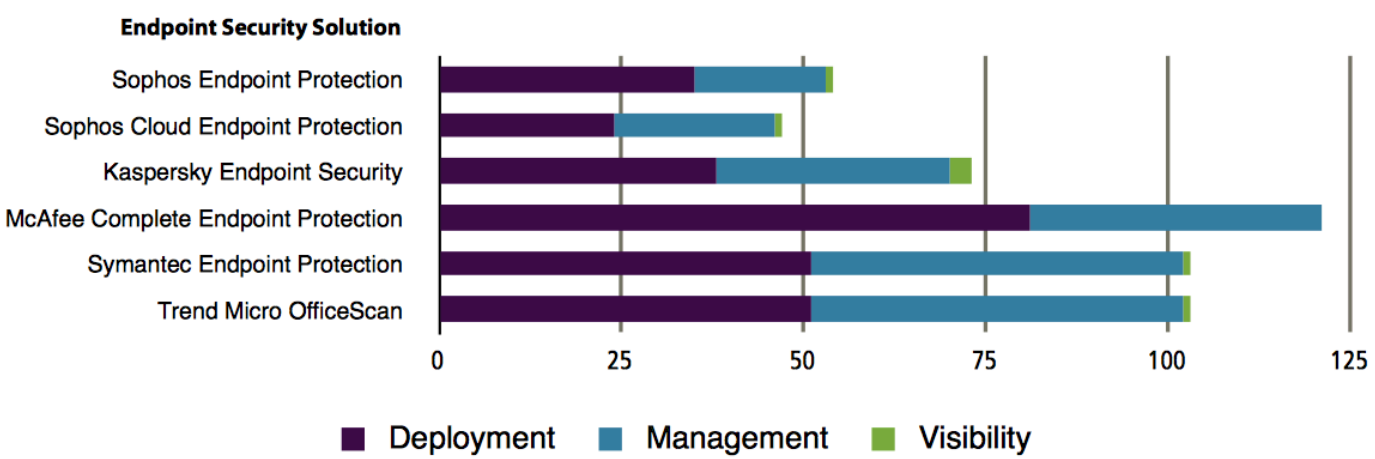
THE BOTTOM LINE

Sophos endpoint security solutions are:

1. Easy to configure and deploy "out of the box"
2. Designed for rapid access to common management & visibility tasks
3. Better able to deliver pre-configured, ready to use security functionality than other tested solutions

Endpoint Security: Summary of Steps Required for Various Tasks

Lower numbers are better

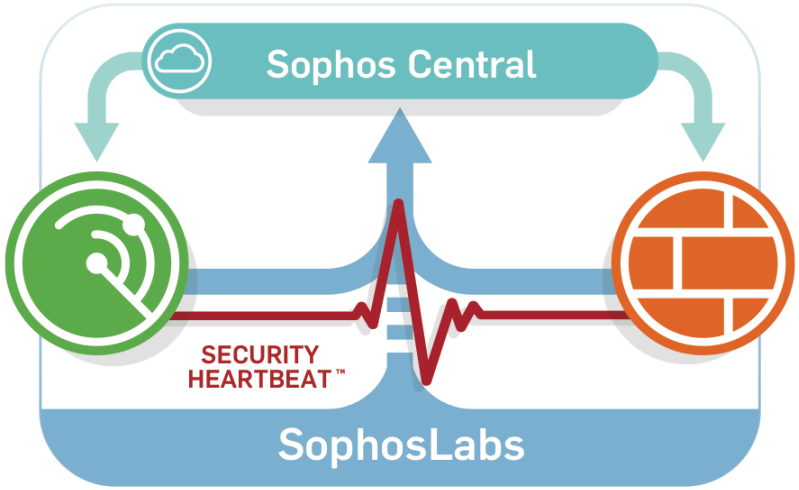


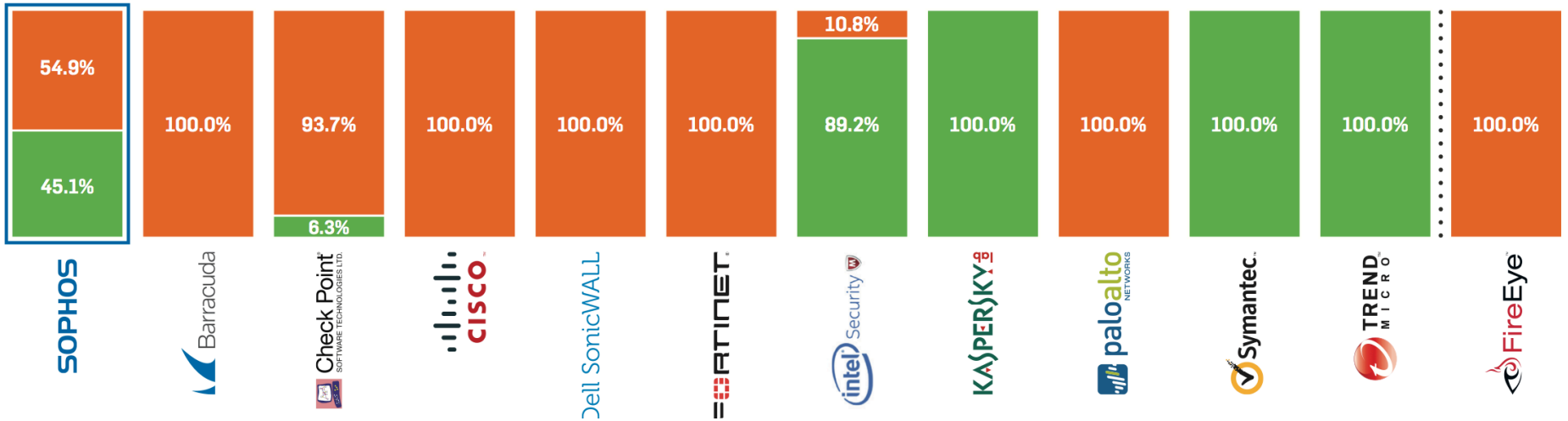
Notes: 1. The figure summarizes the number of steps required to perform various tasks that are detailed in the feature tables of this report. Tasks measured in time, such as installation, are not included. McAfee does not offer the single visibility task.

Source: Tolly, March 2015

Figure 1

Security Heartbeat





SOPHOS