

# Sophos Mobile Control



**Łukasz Naumowicz**

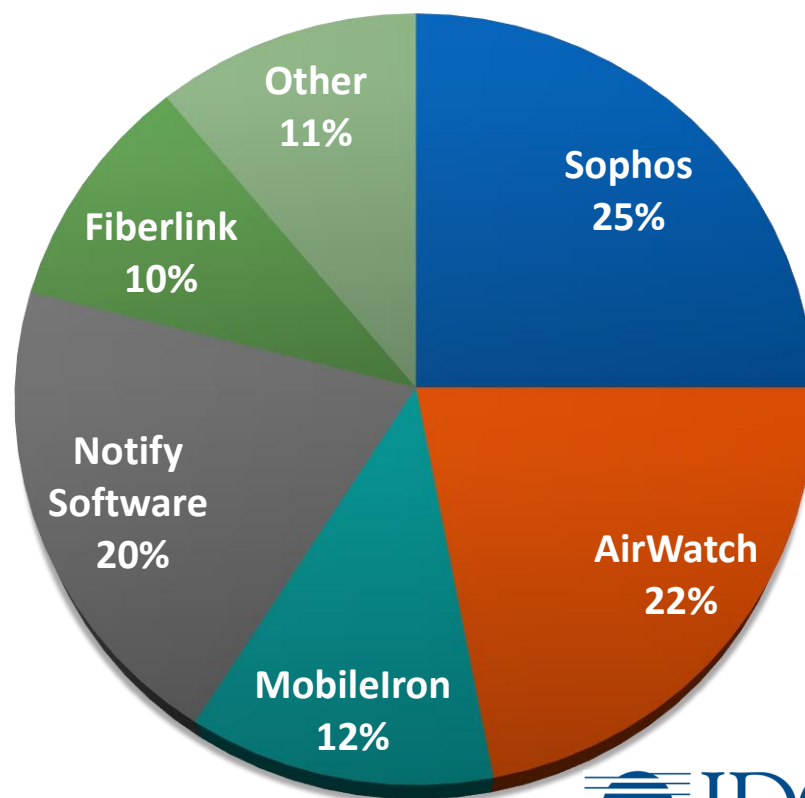
21.06.2016

**SOPHOS**

# Rozwiązanie MDM dla średnich przedsiębiorstw

- **24%** rynku SMB wykorzystuje rozwiązanie do zarządzania urządzeniami mobilnymi
- Edukacja pracowników i wprowadzenie polityk zarządzania urządzeniami mobilnymi to priorytety
- Wzrost ilości urządzeń powoduje problem z zarządzaniem nimi

Q. Z jakiego rozwiązania MDM korzystasz?



Source: 2013 SMB Mobility IT Decision-Maker Survey, Part 2 – Software Deep Dive (IDC #241784, July 2013)

# Klucz do sukcesu tkwi w prostocie

- 5 gwiazdek w kategorii „Ease of use“  
*SC Magazine June 2014*
- “Interfejs administracyjny jest atrakcyjny, prosty w obsłudze i gotowy na dodanie nowych funkcjonalności w kolejnych wersjach.”  
*InfoTech EMM Vendor Landscape 2015*
- Jedyny producent który otrzymał 5 na 5 gwiazdek za „Employee Experience“  
*Forrester WAVE – EMM Q3 2014*
- „Przedsiębiorstwa oraz małe i średnie firmy (SMB) poszukują rozwiązania prostego we wdrożeniu “  
*Gartner MQ for EMM Suites 06-2014*

## Enterprise Mobile Managment

# Enterprise Mobile Managment

Prekonfiguracja (poczta,  
wifi, vpn)

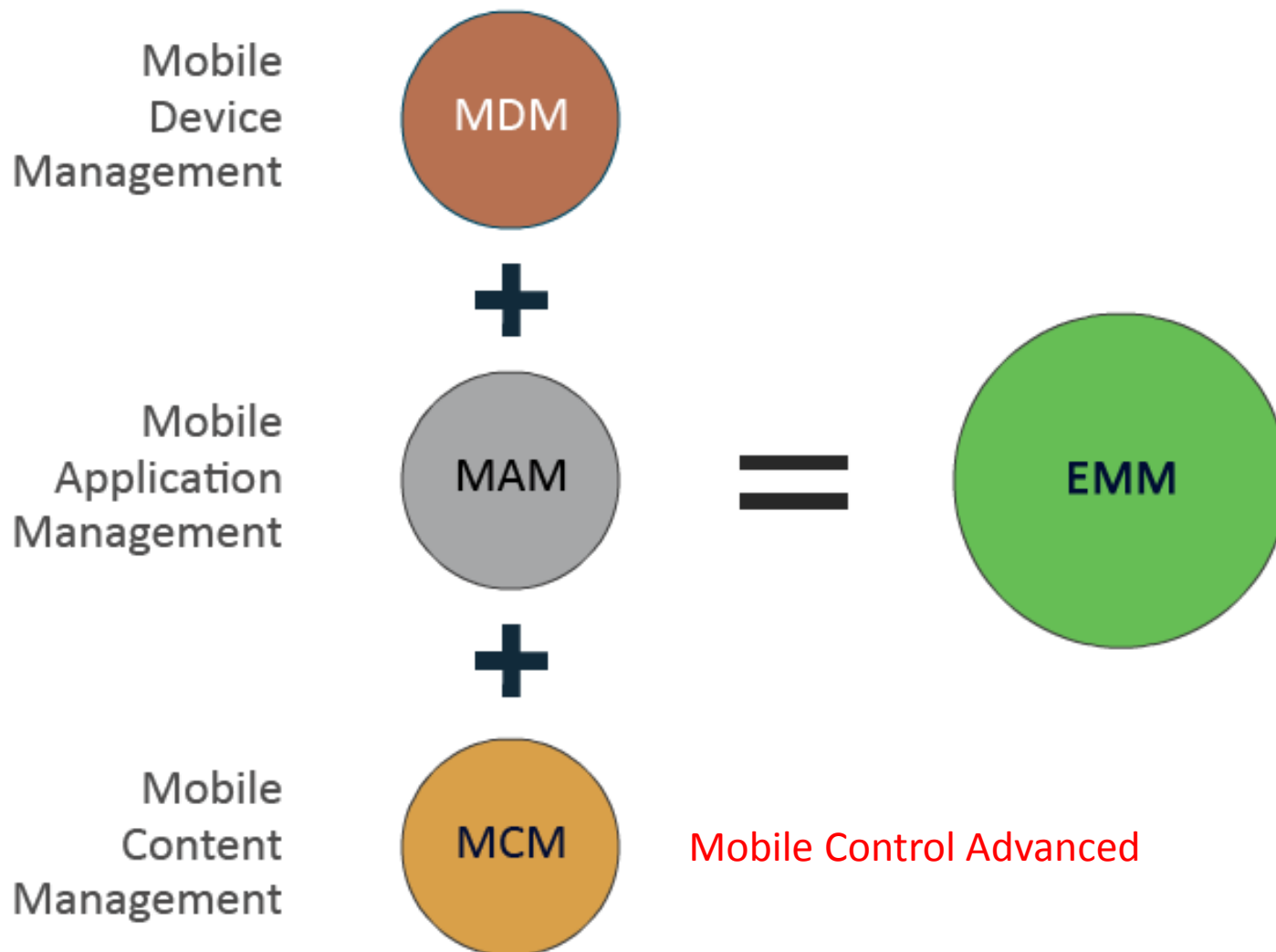
Lokalizacja/blokowanie/o  
dblokowanie urządzenia

Centralna instalacja  
aplikacji

Izolacja danych  
prywatnych i firmowych

Ograniczenia w dostępie  
do funkcji

# Z czego składa się EMM?



## Mobile Device Management Mobile Application Management

# Identyfikacja urządzeń

- Wszystkie urządzenia wykorzystujące sieci komórkowe
  - International Mobile Equipment Identity (IMEI)
  - Mobile Equipment Identifier (MEID)

- Urządzenia z kartą SIM
  - International mobile subscriber identity (IMSI)
  - Sieć/Operator karty/tryb roamingu

- W zależności od platformy
  - Nazwa modelu/Producent/Numer seryjny
  - Rodzina/Wersja

- Dodatkowe informacje w bazie danych Sophos Mobile Control
  - Nazwa/Opis (imię nazwisko jeśli przypisane do użytkownika)
  - Numer telefonu



|                          |                          |
|--------------------------|--------------------------|
| Model                    | Apple iPad 3 White 16 GB |
| Operating system         | iOS 9.1                  |
| Last MDM synchronization | Jun 20, 2016 11:01 AM    |
| Last SMC synchronization | Jun 20, 2016 11:01 AM    |
| Status                   | ✓ Managed                |
| Compliant                | ✓ Yes                    |
| Sophos container access  | ✓ Yes                    |
| Network access           | ✓ Yes                    |
| Open tasks               |                          |



# Ochrona urządzeń mobilnych

- Zdalne wymazanie
- Zdalna blokada
- Zdalny reset
- Polityki haseł
- Lokalizacja
- Przesyłanie wiadomości

 Refresh data

 Set network access

 Send message

 Duplicate this device

 Transfer task bundle

 Lock

 Reset password

 Reconfigure the SMC app

 Unenroll

 Wipe

# Zdalna konfiguracja urządzeń - profile

- Zależne od typu systemu operacyjnego, wersji, producenta(wtyczek/pluginów)
- Ograniczenie funkcjonalności platformy
- Zdalna konfiguracja poczty, wifi, vpn
- Blokowanie aplikacji
- Konfiguracja APN
- Wgrywanie certyfikatów

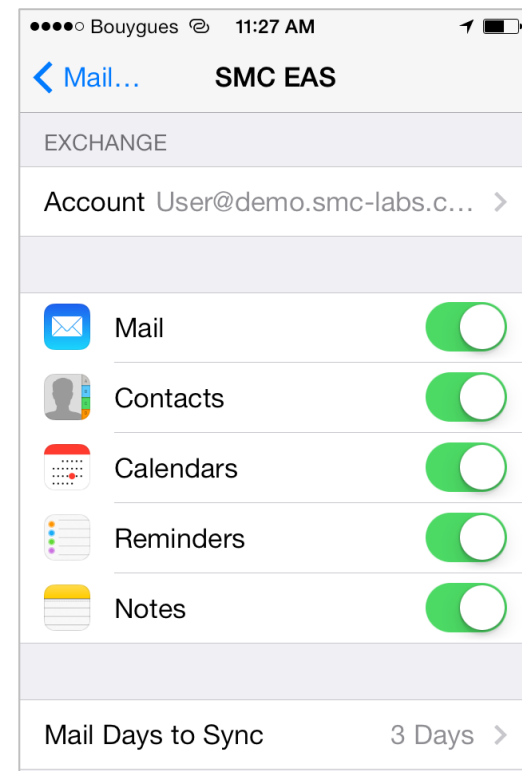
Configuration options for a device profile:

- ☒ Password policies
- ☐ Restrictions
- ☐ KNOX Premium restrictions KNOXv2+
- ☐ App protection
- ☐ App control
- ☐ Exchange ActiveSync SAFEv2+ LG GATEv1.0+ SONYv4+
- ☐ Wi-Fi
- ☐ VPN SAFEv2+ LG GATEv1.0+ SONYv4+
- ☐ Root certificate
- ☐ Client certificate
- ☐ SCEP
- ☐ Access Point Name SAFEv2+ LG GATEv1.0+ SONYv8+
- ☐ Kiosk mode SAFEv2+ LG GATEv2.0+ SONYv8+

Navigation: ← Back → Next

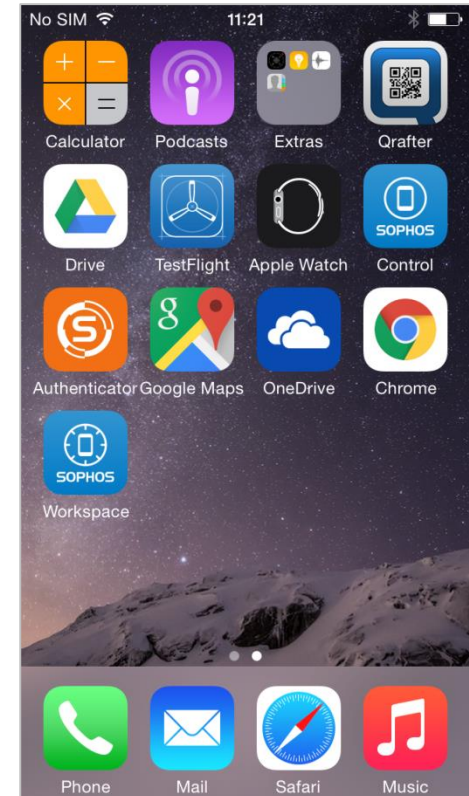
# Exchange ActiveSync (EAS)

- Bezpieczna synchronizacja...
  - Poczty
  - Kontaktów
  - Kalendarza
  - ...przez HTTPS
- Dla Microsoft Exchange, Lotus Traveler oraz Zimbra
- Usunięcie konta EAS usuwa dane EAS
- EAS proxy kontroluje dostęp do serwera pocztowego
- Android wymaga
  - Android 4.2 lub wyżej
  - Samsung SAFEv2
  - Nitrodesk Touchdown



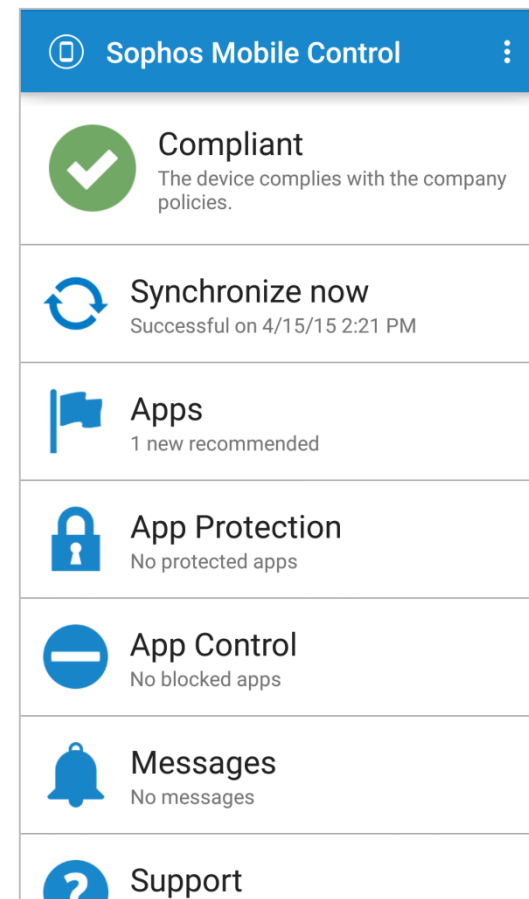
# Zarządzanie aplikacjami

- Inwentaryzacja aplikacji (oprócz Windows)
- Instalacja aplikacji
  - Przez użytkownika z wykorzystaniem SMC
  - Przez administratora instalacje push
  - Generowanie linków lub instalację aplikacji zainstalowanych na serwerze SMC jako paczek
- Blokowanie dostępu do Appstore
- (iOS, Windows Phone, Android z Samsung SAFE)
- Wsparcie Apple VPP (iOS)



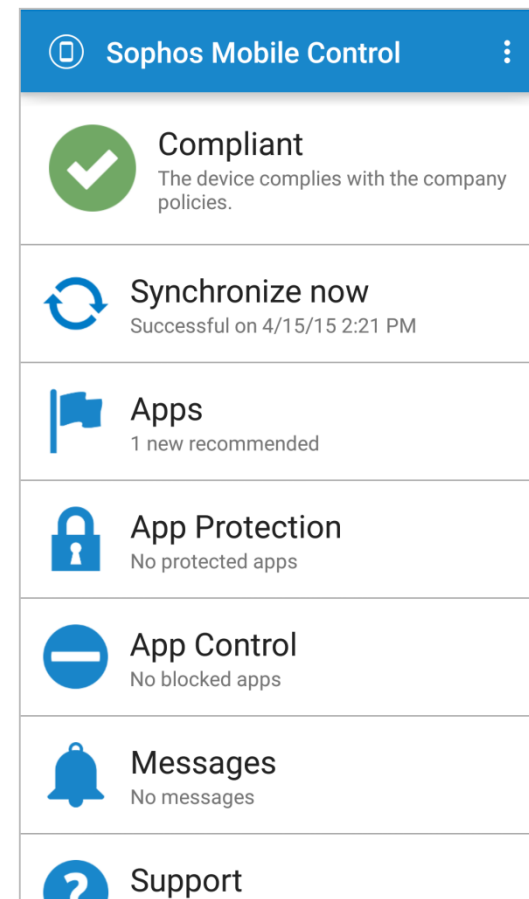
# Monitorowanie zgodności urządzeń

- Kontrola urządzenia
  - Wymagane w trybie zarządzania
  - Max odstęp synchronizacji
  - Min wersja klienta
  - “złamanie” Jailbreak (iOS), root rights (Android)
- Utrata/kradzież
  - Wymagane hasło (iOS, Windows 8)
  - Lokalizacja uruchomiona (iOS, Windows 8)
- Zarządzanie aplikacjami
  - Min/Max wersja OS
  - Listy aplikacji wymaganych i zabronionych
  - Pozwolenie na roaming danych
  - Pozwolenie na aplikacje spoza sklepu (Android)
- Aplikacje szkodliwe (Android z aplikacją SMSec)
  - Malware, Suspicious apps, PUA allowed
  - Interwał skanowania



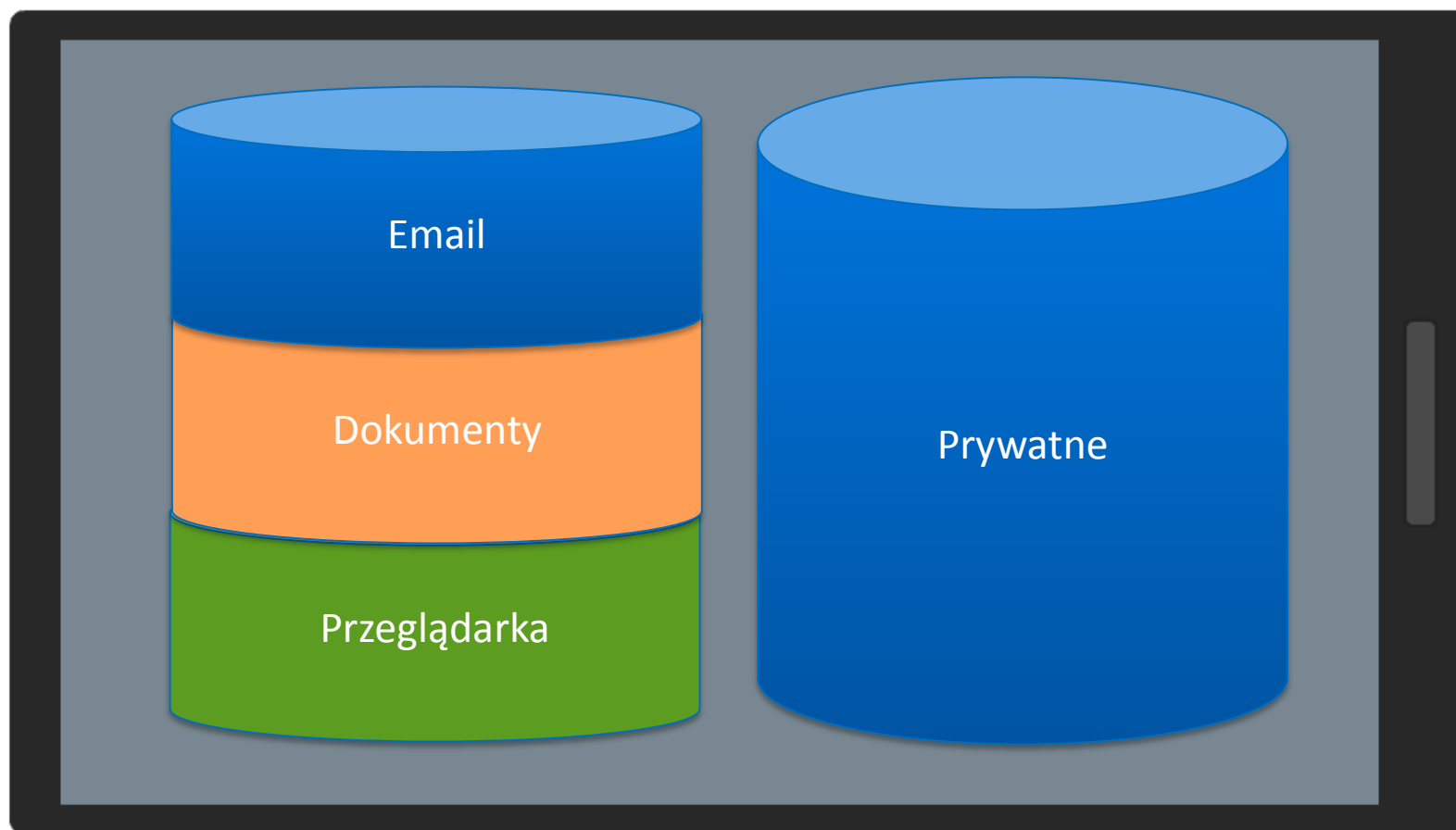
# Monitorowanie zgodności urządzeń

- A jeżeli nie zgodne:
  - Zablokuj ActiveSync
  - Zablokuj dostęp do dokumentów (Android, iOS)
  - Zablokuj dostęp do sieci (Android, iOS, Windows Phone)
  - Powiadom administratora
  - Wykonaj zadanie zbiorcze (Android, iOS)



## Mobile Content Management

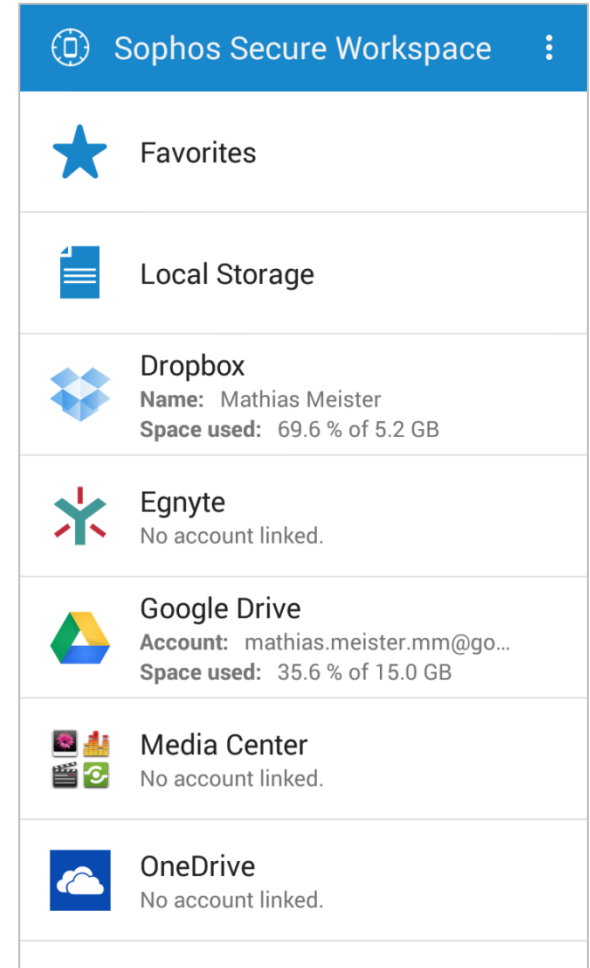
# Kontenery Sophos





# Sophos Secure Workspace

- Dostępna na Android i iOS
  - Zarządzanie przez Mobile Control z licencją Advanced
- Odczyt plików zaszyfrowanych SafeGuard (klucz lokalny)
- Szyfrowanie plików lokalnie lub do serwisów chmurowych
- Dostęp do dokumentów korporacyjnych
- Przegladarka internetowa



# Zarządzanie dokumentami

## Documents

Listed documents can be shared

[+ Add document](#)

| Name                                    |
|-----------------------------------------|
| <a href="#">filter action 2.png</a>     |
| <a href="#">Installation Guide.pdf</a>  |
| <a href="#">spaced-practice-web.pdf</a> |
| <a href="#">Startup Guide.pdf</a>       |
| <a href="#">User Guide Android.pdf</a>  |
| <a href="#">User Guide iOS.pdf</a>      |

[1](#)

## Edit document

Name: Sophos Mobile Control Installation Guide (English).pdf Created by admin a few minutes ago

Category: Mobile

☒ Copy to clipboard

☒ Share document

☒ Use document offline

Assigned groups: [Show](#) All groups selected

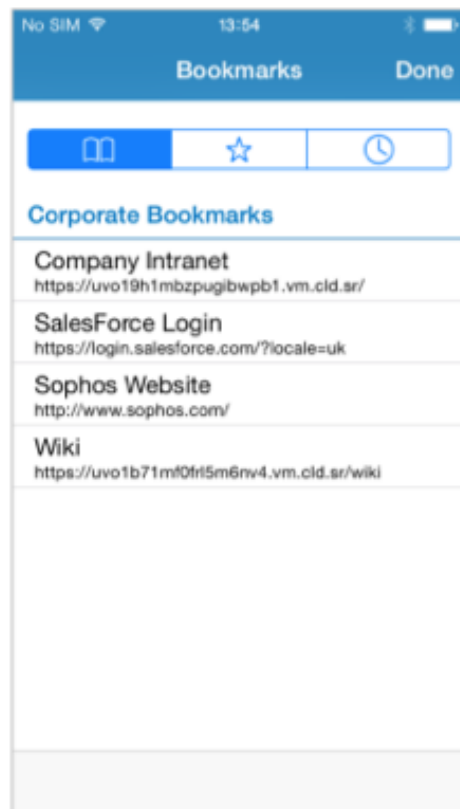
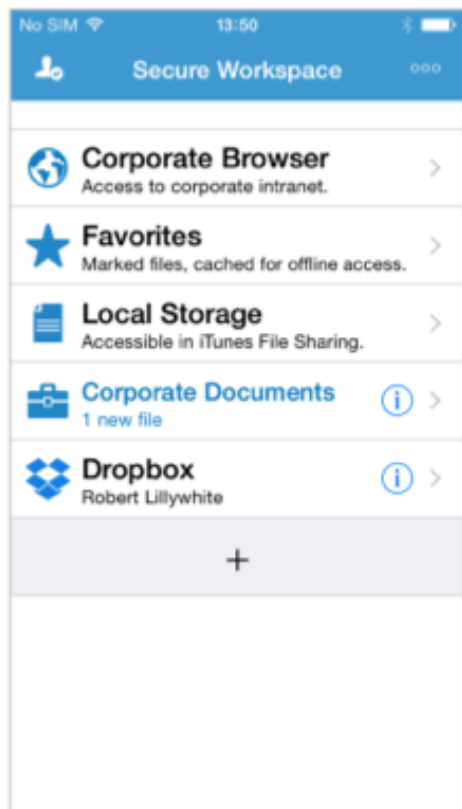
Description: Installation guide for Sophos Mobile Control in English

[Upload a file](#)

| Name                                                                                                                                       | Size    | MIME type       |
|--------------------------------------------------------------------------------------------------------------------------------------------|---------|-----------------|
|  Sophos Mobile Control Installation Guide (English).pdf | 1024597 | application/pdf |

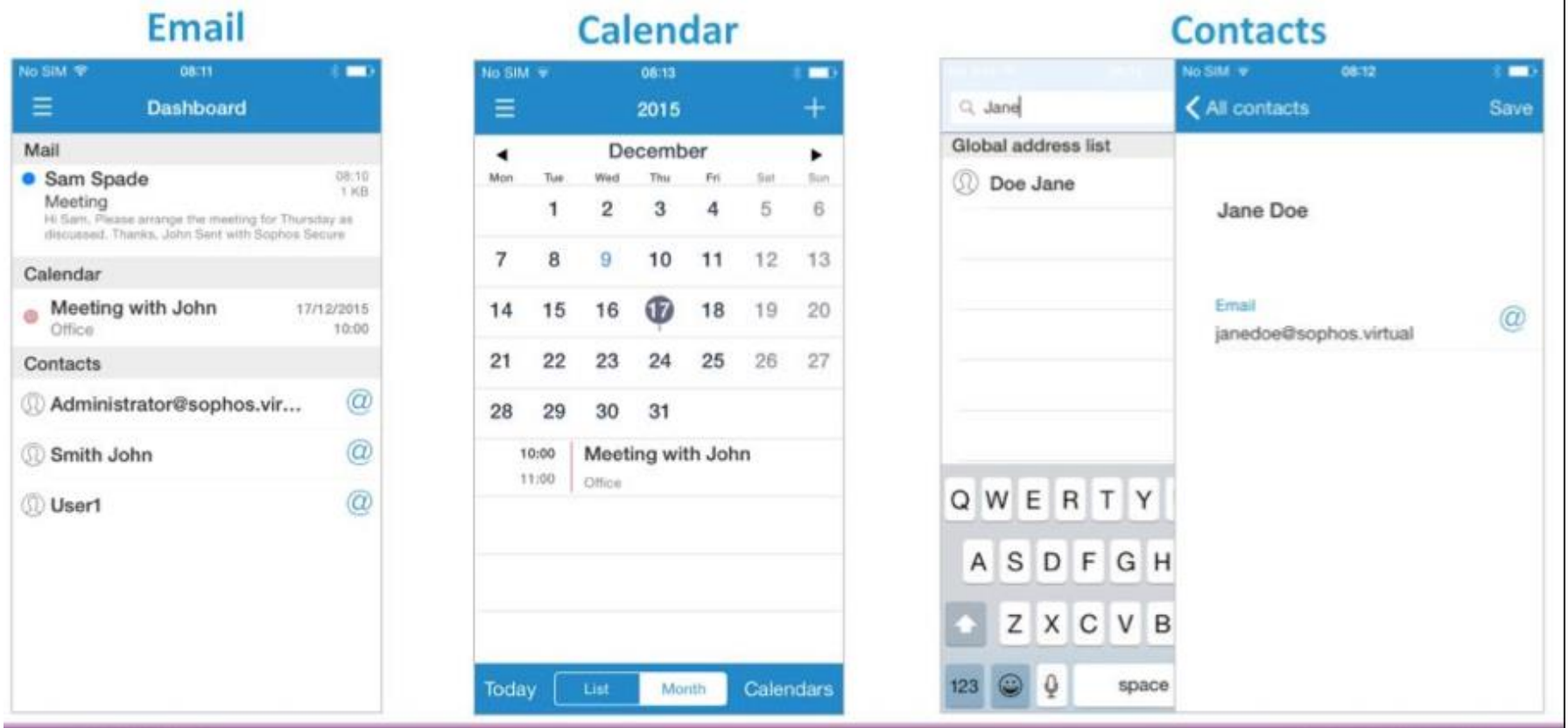
# Bezpieczna przeglądarka Internetowa

- Element Sophos Secure Workspace
- Dostęp do stron i witryn zdefiniowanych przez administratora



# Sophos Secure Email

- Połączenie z serwerami poprzez EAS Proxy
- Skrzynka pocztowa, kalendarz, kontakty
- Możliwość zablokowania dostępu do danych



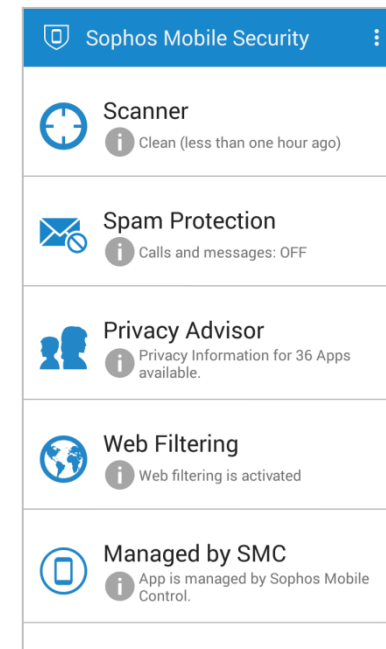
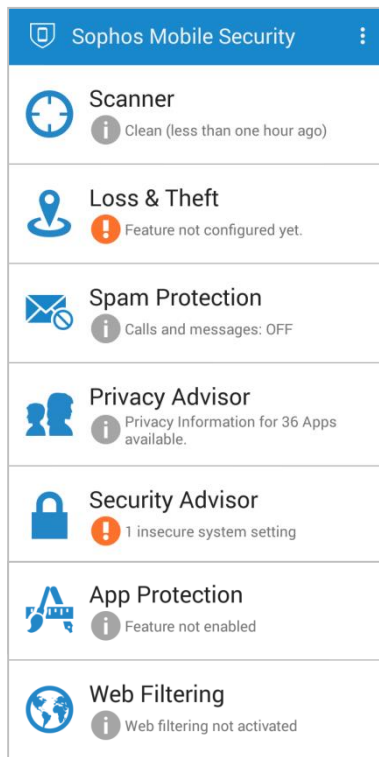
# Kontener Samsung Knox (licencja Samsung)



# Sophos Mobile Security



- Bezpłatna aplikacja na Androida

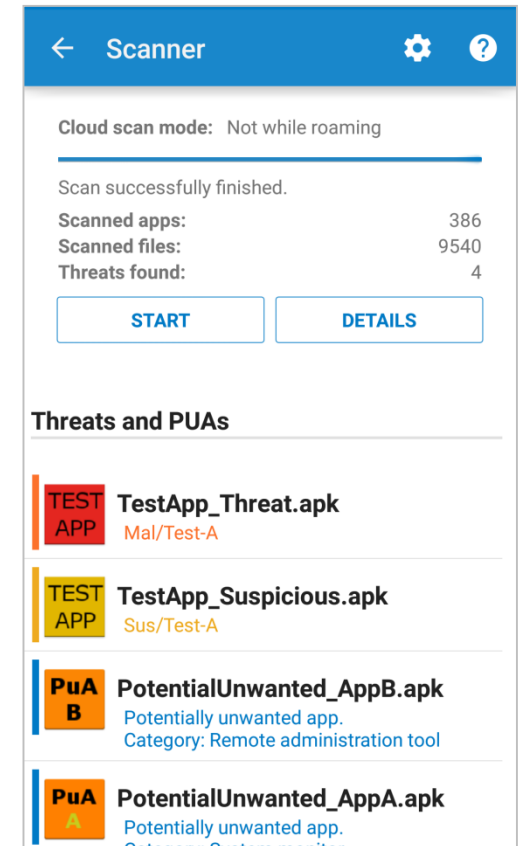


**Standard (niezarządzana)**

**Enterprise (zarządzana przez SMC)**

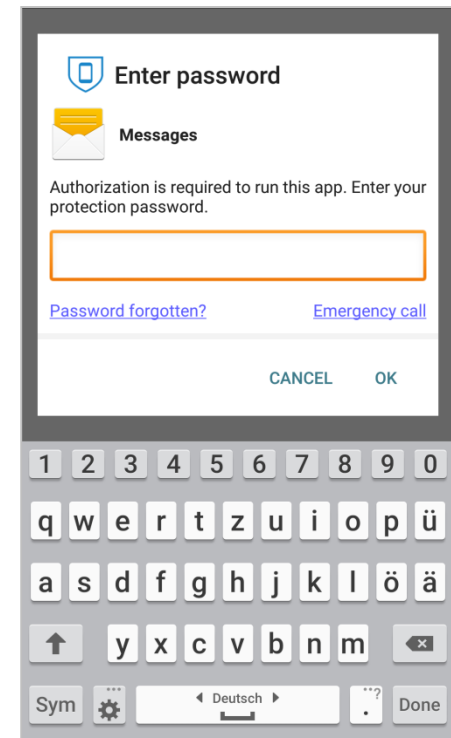
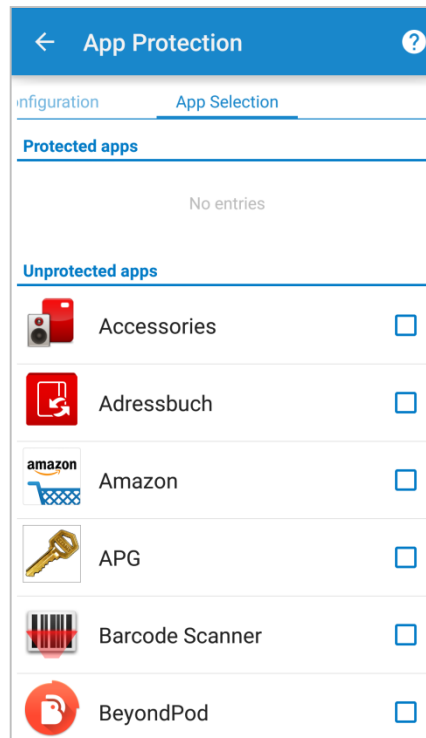
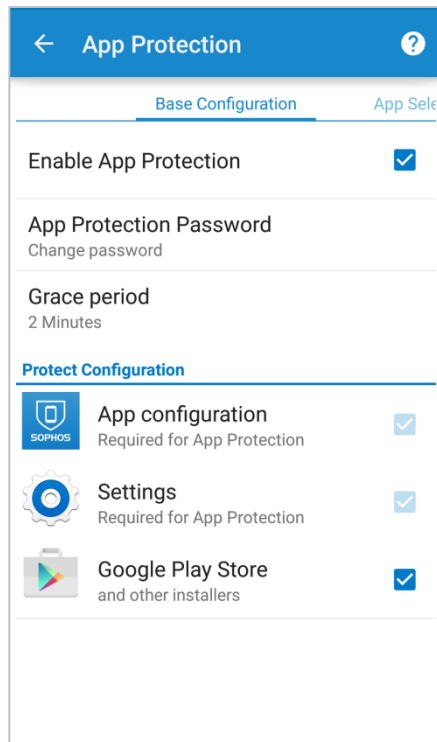
# Skaner

- Skanowanie pod kątem aplikacji szkodliwych:
  - Przy instalacji
  - Na żądanie
  - Wg harmonogramu
- Może dotyczyć:
  - Kart SD oraz pamięci USB
  - Aplikacji Systemowych
  - Potentially unwanted applications (PUAs)
- Cloud lookup
  - Sprawdzanie sygnatur w chmurze lub lokalnie



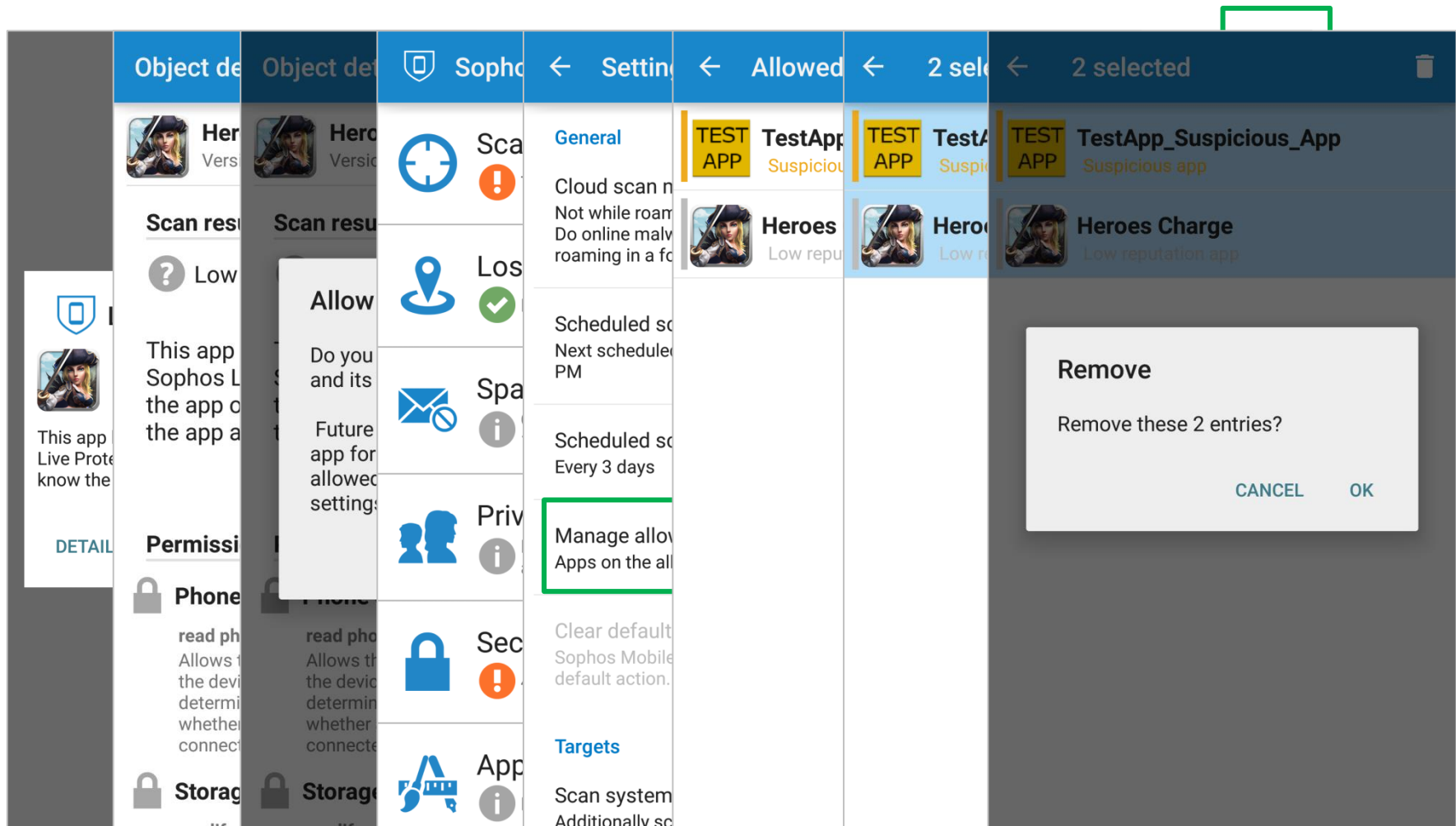
# Ochrona Aplikacji

- Zabezpiecza przed uruchomieniem aplikacji
- Ochrona ustawień urządzenia oraz danych w aplikacjach
- Wymaga podania hasła przy dostępie





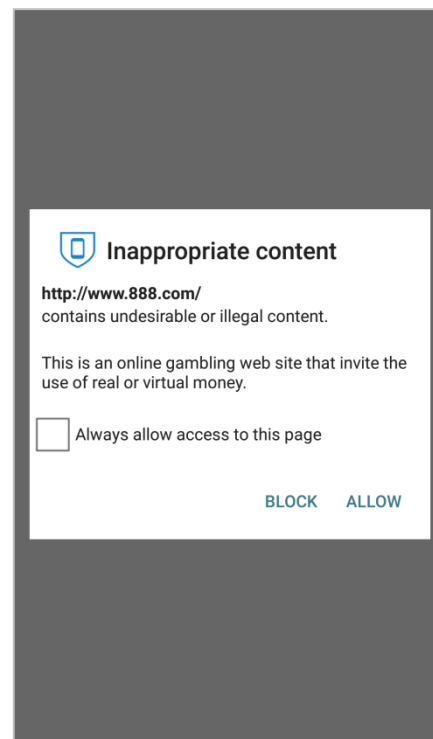
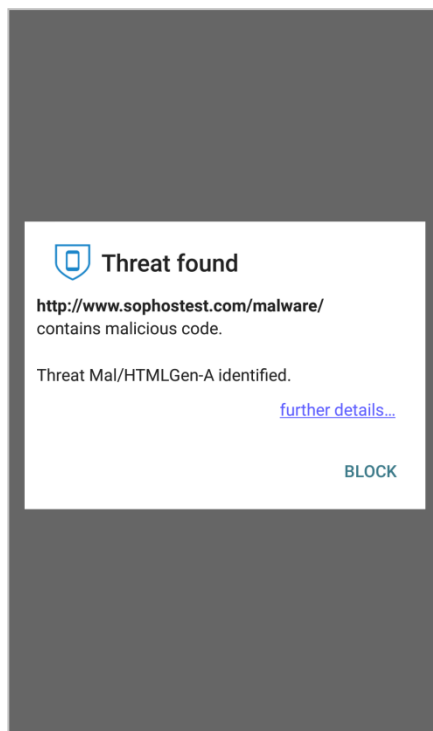
# Weryfikacja reputacji aplikacji



# Filtrowanie WWW

- Skanowanie pod kątem złośliwego kodu
- Filtrowanie w oparciu o kategorie
  - Zezwól, Zablokuj, Ostrzeż

| Web Filtering                                              |       |
|------------------------------------------------------------|-------|
| Filter malicious websites                                  |       |
| Malicious content<br>Containing potential malicious code   | BLOCK |
| Filter categorized websites                                |       |
| Adult<br>Features explicit sexual and pornographic content | WARN  |
| Alcohol & tobacco<br>Promotes alcohol & tobacco products   | WARN  |
| Anonymizers<br>Includes sites for anonymous surfing        | ALLOW |
| Criminal activity<br>Invites to criminal activities        | WARN  |
| Gambling<br>Contains online gambles                        | WARN  |
| Hacking<br>Contains hacking tools and instructions         | WARN  |
| Illegal drugs<br>Propagates illegal drugs                  | WARN  |



# Integracja z NAC (np. Sophos UTM)

License

iOS APNS

EAS proxy

Network Access Control

SMTP

HTTP proxy

Access whitelist

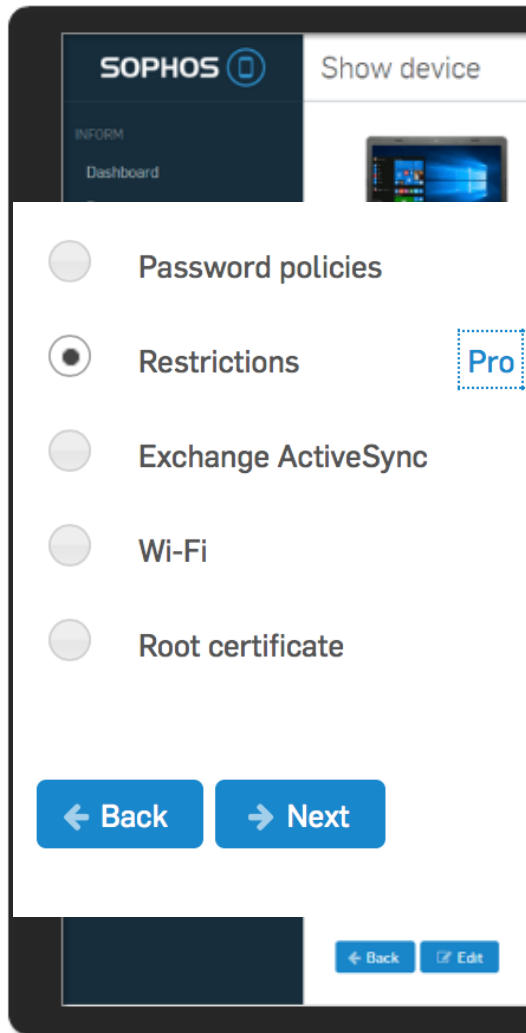
Sophos UTM ▾

This setting enables Sophos UTM integration (version 9.2 and higher). The integration requires you to set the SMC server URL and admin user credentials in the UTM WebAdmin under Management - Sophos Mobile Control, as described in the UTM online help.

Save



# Wsparcie Wi



## Device

- ☐ Forbid SD card
- ☐ Forbid manual addition of non-Microsoft email accounts
- ☐ Forbid developer mode
- ☐ Forbid camera
- ☐ Disable Edge Autofill
- ☐ Disable Edge F12 Developer Tools
- ☐ Disable Edge pop-up blocker
- ☐ Disable AutoPlay settings
- ☐ Disable Date & Time settings
- ☐ Disable Language settings
- ☐ Disable Power & Sleep settings
- ☐ Disable Region settings
- ☐ Disable Sign-in settings
- ☐ Disable VPN settings
- ☐ Disable Workplace settings
- ☐ Disable Account settings

Telemetry

Allowed

## Architektura i instalacja

# Wybór należy do Ciebie

- **On premise**

- Prosty instalator Windows dla platform serwerowych
- Łatwa integracja z infrastrukturą IT
- Kreator przygotowania wymaganych certyfikatów

- **Software as a Service**

- Można korzystać już w kilka minut po rejestracji
- Funkcjonalności prawie identyczne z instalacją On-premise (część funkcji opcjonalna)
- Nie wymagana ingerencja w lokalną infrastrukturę IT

# On-premise vs SaaS

- Serwer zarządzany przez Sophos
- Jeden klient per SMCaaS

| Funkcjonalności                  | On-premise | SMCaaS     |
|----------------------------------|------------|------------|
| Aktualizacje Sophos              | ✗          | ✓          |
| EAS proxy                        | ✓          | ✓          |
| LDAP                             | ✓          | ✓          |
| Network Access Control           | ✓          | ✓          |
| Lokalizacja przez administratora | ✓          | opcjonalna |
| SCEP                             | ✓          | ✗          |

# Formularz przedwdrozeniowy

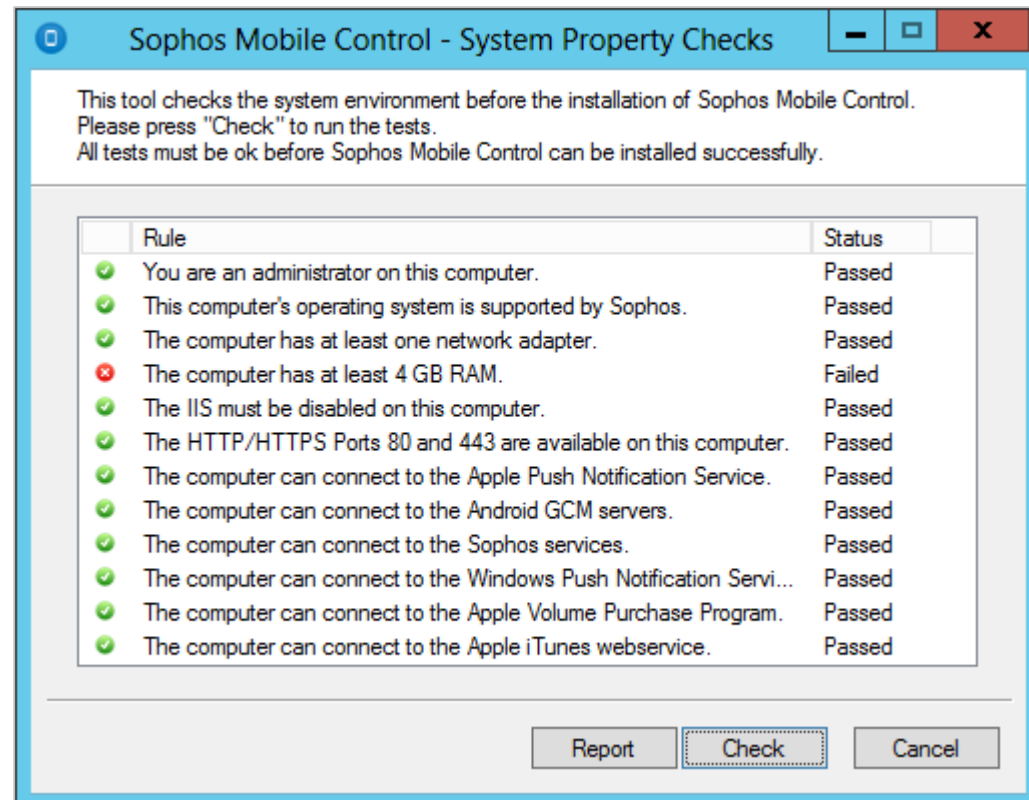
- Sophos Mobile Control wymagania
  - <http://www.sophos.com/en-us/support/documentation/mobile-control.aspx>
  - Kompletny formularz do wypełnienia przed wdrożeniem



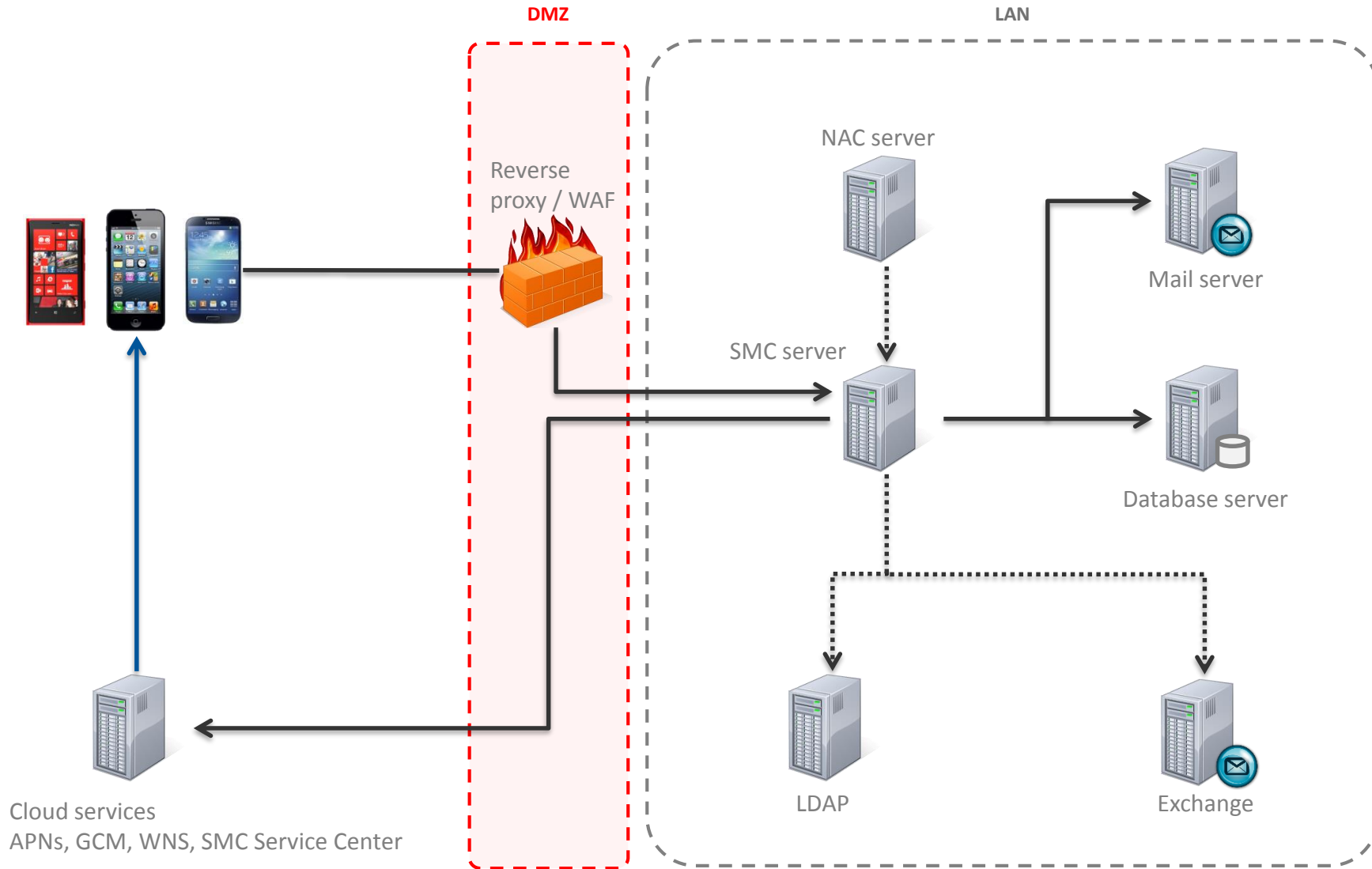
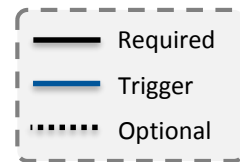


# Instalacja – Weryfikacja zgodności systemu

- Sprawdza czy system spełnia wymagania
- Nie pozwala na kontynuację instalacji jeśli serwer nie spełnia wymagań
- Brak możliwości obejścia weryfikacji instalatora



# Architektura



# Komunikacja

- Połączenie sieciowe:



- Protokoły:

- HTTPS
- APNs (Apple Push Notification service)
- GCM (Google Cloud Messaging)
- MPNS (Microsoft Push Notification Service)
- WNS (Windows Notification Service)



# Wspierane urządzenia

| Platforma     | Wersja                                                                                                                                |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Apple iOS     | 6.0 lub wyższe<br>7.0 lub wyższe<br>8.0 lub wyższe<br>9.0                                                                             |
| Android       | 2.3.3 lub wyższe (telefony)<br>3.0 lub wyższe (tablety)<br>4.0 lub wyższe (tablety I telefony)<br>5.0 lub wyższe (tablety I telefony) |
| Windows Phone | 8.0 lub wyższe<br>8.1<br>Windows Mobile 10                                                                                            |

# Wymagania serwera

- Fizyczny lub wirtualny
- Wymagania sprzętowe

|                          | Do 200 urządzeń | Do 1000 urządzeń | Do 2000 urządzeń |
|--------------------------|-----------------|------------------|------------------|
| <b>CPU<br/>(rdzenie)</b> | 1               | 2                | 4                |
| <b>RAM</b>               | 4GB             | 4GB              | 8GB              |

- Ilość wspieranych urządzeń
  - Do 20,000 urządzeń per serwer SMC

# Wymagania serwera

| Systemy operacyjne            | Wersje                        |
|-------------------------------|-------------------------------|
| Windows Server 2008 64 bit    | SP 2                          |
| Windows Server 2008 R2 64 bit | SP 2                          |
| Windows Server 2012 64 bit    | SP 1                          |
| Windows Server 2012 R2 64 bit | SP 1                          |
|                               |                               |
| Bazy użytkowników             | Wersje                        |
| Microsoft Active Directory    | Zgodnie z wersjami powyżej    |
| Novell eDirectory             | 8.8 SP 8                      |
| Lotus Domino                  | 8.5.3                         |
| OpenLDAP                      | Zgodnie z wersją w Zimbra 8.0 |

# Wymagania serwera – Baza danych

| Baza danych                       | Wersje          |
|-----------------------------------|-----------------|
| Microsoft SQL Server 2008         | SP3 (32/64 bit) |
| Microsoft SQL Server 2008 R2      | SP3 (64 bit)    |
| Microsoft SQL Server 2012         | SP2 (64 bit)    |
| Microsoft SQL Server 2012 Express | SP2 (32/64 bit) |
| Microsoft SQL Server 2014         | (64 bit)        |
| Microsoft SQL Server 2014 Express | (64 bit)        |
| MySQL                             | 5.6+            |

- Instalator zawiera Microsoft SQL 2014 Express

# Wymagania serwera – serwer poczty

| Serwer poczty         | Wersje |
|-----------------------|--------|
| Exchange 2003         | SP2    |
| Exchange 2007         | SP3    |
| Exchange 2010         | SP2    |
| Exchange 2013         | SP1    |
| Lotus Domino Traveler | 8.5    |
| Zimbra                | 8.0    |



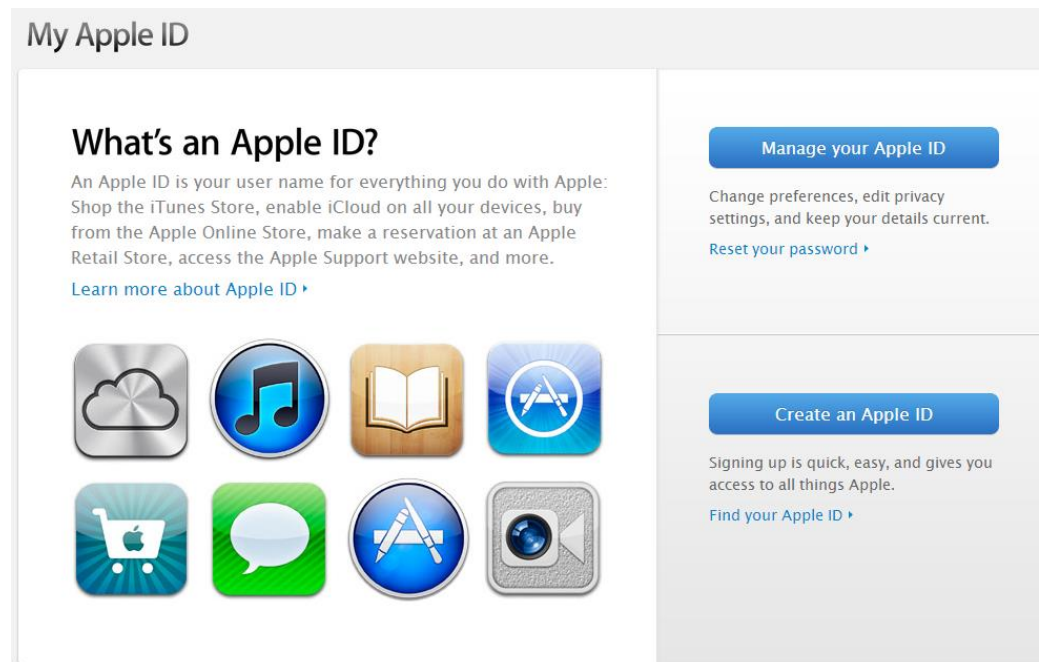
# Wymagania serwera – certyfikat SSL

- Z zaufanego Certificate Authority (CA)
  - Rekomendowany dla instalacji produkcyjnych
  - Najlepsze efekty na wszystkich platformach
- Self-signed lub z “nie zaufanego” Certificate Authority (CA)
  - Brak możliwości instalacji aplikacji bezpośrednio z serwera SMC do urządzeń Android
  - Użytkownicy Windows Phone 8 muszą importować certyfikaty self-signed
  - Przydatny dla celów testowych i PoC
- Format certyfikatu
  - Komponenty pojedyncze – klucz prywatny i hasło, certyfikat serwera, certyfikat pośredni CA (jeśli wymagany) certyfikat root CA
  - PKCS#12 – zawierający wszystkie komponenty

# Wymagania serwera - APNs



- Certyfikat Apple Push Notification Service (APNs) tworzony przez kreator dla Windows do pobrania z konsoli SMC
- Wymaga posiadania Apple ID  
<https://appleid.apple.com/choose-your-country>



# Konfiguracja nowych urządzeń

This is an automated message generated by your administrator.



## Account created

You have been added to the Self Service Portal. Follow the link below to activate your account.

<https://smcdemo.sophos.com/changePassword.xhtml?c=1&u=131&t=4HZmMX9ZBORR52iQ&ut=s>

Your login credentials are:

Customer: demo

User: lukasz

Note: If you did not expect to be added to the Self Service Portal, please contact your administrator.



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

### Want to do a manual setup?

1. Search the device's App store for the Sophos app you need, download and install the app  
**Apps:** Sophos Mobile Control  
**Note:** If your administrator needs you to install more than one app, the second install will start automatically
2. Start the app and enter the following to configure it:  
**Token:** fuhapplepret  
**Server URL:** dzt-mob-amzn-eu-west-1-9af7.upe.p.hmr.sophos.com  
**Email:** admin@fen.pl
3. Repeat for all your mobile devices.

### Need help?

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

## Licencjonowanie

# Jakie mamy opcje?

|                          | MOBILE CONTROL STANDARD | MOBILE CONTROL ADVANCED | ENDUSER PROTECTION           |
|--------------------------|-------------------------|-------------------------|------------------------------|
| Mobile Device Management | ✓                       | ✓                       | ✓                            |
| Mobile Security          |                         | ✓                       | Optional                     |
| Secure Workspace         |                         | ✓                       | Optional                     |
| Deployment options       | SaaS or on-premise      | SaaS or on-premise      | On-premise                   |
| Also included            | n/a                     | n/a                     | Endpoint Protection Advanced |

|                         |   |                                                        |
|-------------------------|---|--------------------------------------------------------|
| Mobile Control Standard | = | MDM + MAM                                              |
| Mobile Control Advanced | = | EMM (MDM, MAM, MCM)                                    |
| Enduser Protection      | = | Endpoint Protection Advanced + Mobile Control Standard |

# Lista funkcjonalności a licencja



## Sophos Mobile Control 6.0

Feature Matrix 01/2016

Apple iOS

Android

Windows10 Mobile

|                                                                                                    |   |                |   |
|----------------------------------------------------------------------------------------------------|---|----------------|---|
| <b>Server</b>                                                                                      |   |                |   |
| <b>Admin User Interface</b>                                                                        |   |                |   |
| Easy-to-use web interface                                                                          | X | X              | X |
| Flexible Dashboard with 18 different widgets                                                       | X | X              | X |
| Flexible filter mechanism                                                                          | X | X              | X |
| Role-based access                                                                                  | X | X              | X |
| Multitenancy                                                                                       | X | X              | X |
| Communication from superadmin to all tenants (administration and SSP UI)                           | X | X              | X |
| Sophos technical notifications                                                                     | X | X              | X |
| Sending of text messages (via APNS, GCM, Baidu, MPNS)                                              | X | X              | X |
| <b>Self Service Portal</b>                                                                         |   |                |   |
| Register new device                                                                                | X | X              | X |
| Device wipe                                                                                        | X | X              | X |
| Device lock                                                                                        | X | X              | X |
| Device locate                                                                                      | X | X              | X |
| Passcode reset for Device, App Protection (Android), Sophos Container (iOS, Android)               | X | X              | X |
| Trigger device checkin                                                                             | X | X              | X |
| Decommission device from management (incl. corporate wipe on iOS, Samsung SAFE, Windows 10 Mobile) | X | X <sup>5</sup> | X |
| Delete decommissioned device from inventory                                                        | X | X              | X |
| Monitor device status and compliance information                                                   | X | X              | X |

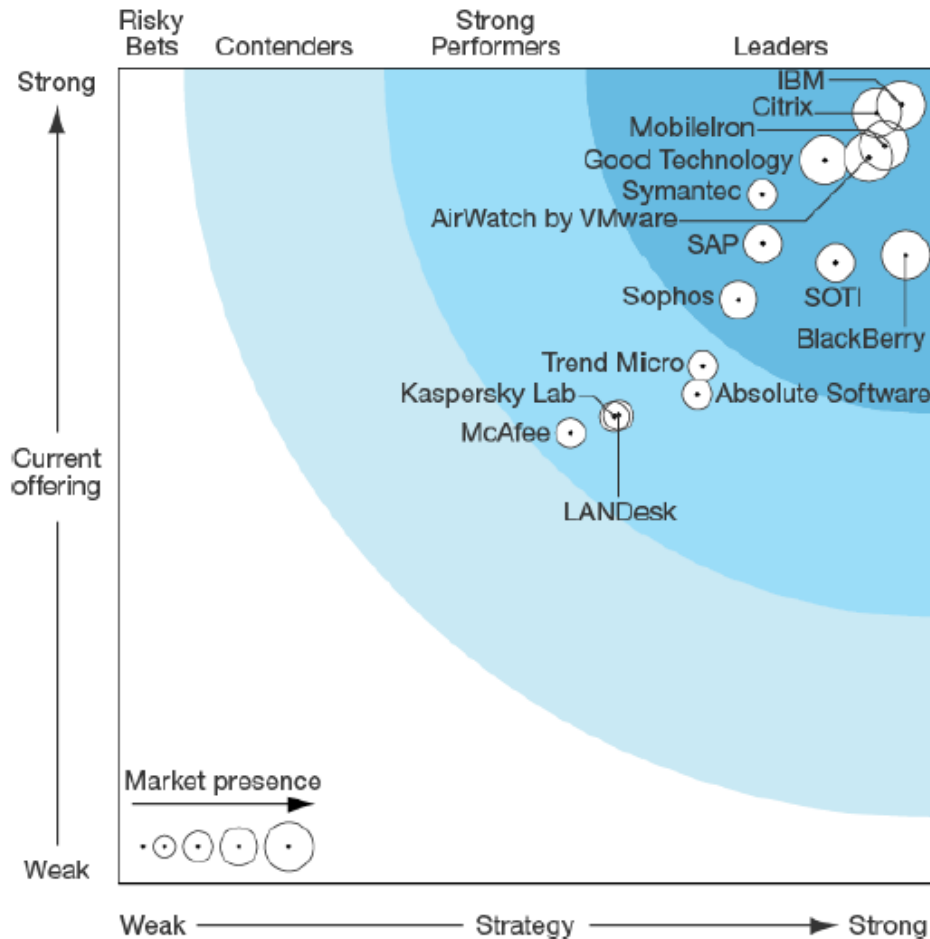
<https://partnerportal.sophos.com/en-us/medialibrary/PartnerPortal/Files/Tools/SalesGuidance/smc-6-feature-matrix.pdf?la=en>

## Dlaczego Sophos?



# Pozycjonowanie

**Figure 2** Forrester Wave™: Enterprise Mobile Management, Q3 '14



# Zalety Sophos Mobile Control



Rozwiązanie do zarządzania urządzeniami mobilnymi nie musi być skierowane tylko do dużych firm



Zarządzanie urządzeniami nie musi być trudne, możesz zacząć w kilka minut, nie musisz się martwić o serwery, aktualizacje oprogramowania czy wsparcie



Kontenery Sophos oferują zaawansowane możliwości przeznaczone również dla dużych firm



To wszystko bez dużych nakładów finansowych na zasadzie subskrypcji per użytkownik



SMC może integrować się z innymi produktami oferując jednocześnie nie tylko zarządzanie urządzeniami ale również ochronę urządzeń mobilnych lub stanowić część kompletnego systemu

# SOPHOS