

Sophos bez tajemnic Safe Guard Enterprise

Łukasz Naumowicz

16.06.2016

SOPHOS

Kilka faktów i liczb

- **86%** organizacji straciło laptopa, kradzież lub zagubienie¹
- **\$49,246** średnia wartość jednego utraconego laptopa²
- **7.1%** laptopów w trakcie cyklu swojego życia zostanie zagubionych²
- **>8,000** laptopów zostawionych na lotniskach w US każdego tygodnia³
- **81%** średnich organizacji (100-1,000) nie szyfruje laptopów⁴
- **64%** dużych organizacji (1,000+) nie szyfruje laptopów⁴
- **87%** doświadczonych pracowników wysyłało/wysyła dane firmowe korzystając z prywatnych skrzynek email lub prywatnych kont w serwisach chmurowych⁵
- **58%** doświadczonym pracownikom zdarzyło się przesłać poufne informacje przez przypadek do niewłaściwej osoby⁵

1. Ponemon Institute, 2010,

2. Ponemon Institute, 2013

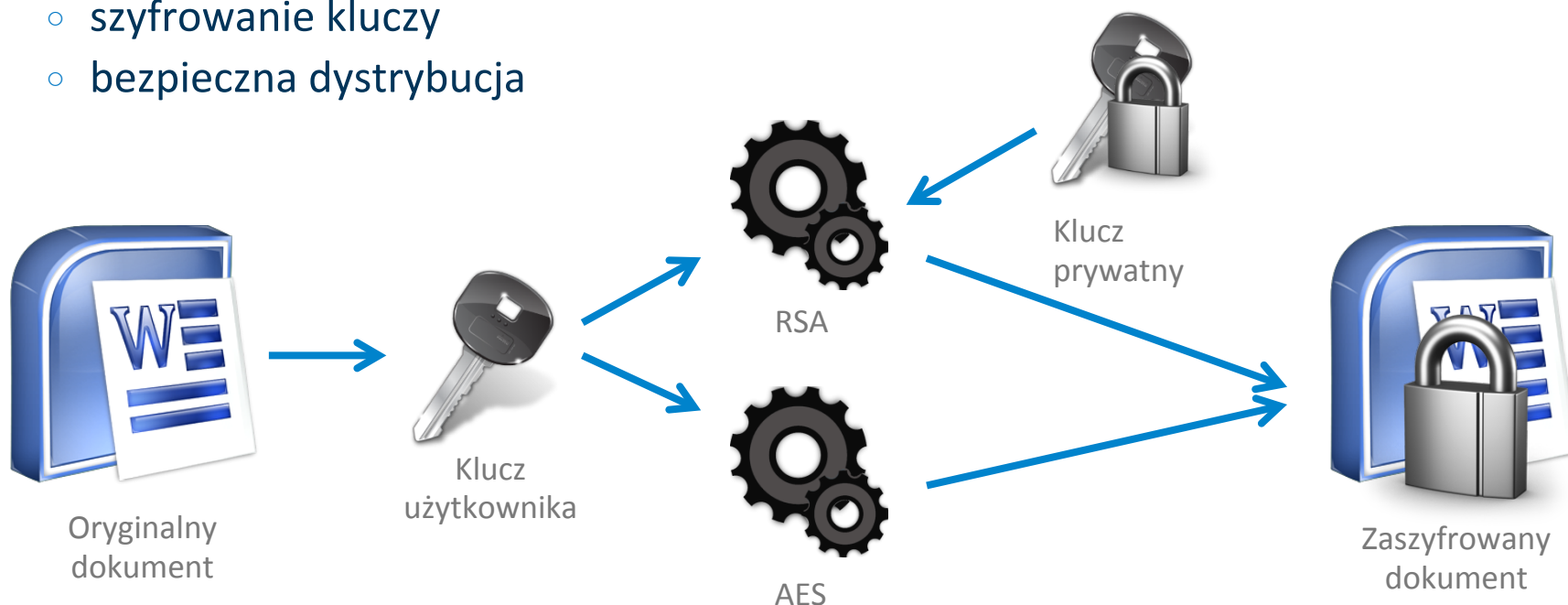
3. Ponemon Institute, 2008 (67% of 12,000)

4. IDC, 2012

5. Stroz Friedberg, 2014

Metody szyfrowania

- Szyfrowanie powoduje że dane bez klucza szyfrującego są nieczytelne
- Enkrypcja na poziomie 128-bit jest odporna na ataki brute-force
- Szyfrowanie symetryczne (np. AES)
- Szyfrowanie asymetryczne (np. RSA):
 - szyfrowanie kluczy
 - bezpieczna dystrybucja



Szyfrowanie jest najlepszym rozwiązaniem, ale...

- ...może ograniczyć “wolność” użytkowników / i zmniejszyć ich produktywność
- ...może spowolnić proces uruchamiania komputera i drażnić użytkowników
- ...czasami nie działa na każdym sprzęcie
- ...może sprawić, że dane będą bezużyteczne jeśli zawiedzie
- ...może ograniczyć metody współdzielenia i dystrybucji informacji w organizacji
- *Będzie wymagało czasu od działu IT*

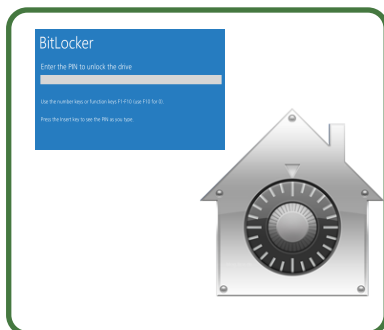


Strategia Ochrony Danych Sophos

Zapewnić jak najlepszą Ochronę przy maksymalnej Wydajności

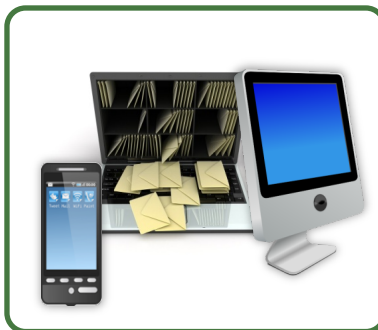
Wydajność

Wykorzystać
możliwości
systemu
operacyjnego



Wiele platformowe zarządzanie

Windows, Mac,
Mobilne



Dane zabezpieczone wszędzie

Urządzenia przenośne,
Udziały sieciowe,
Mobilne, Chmura



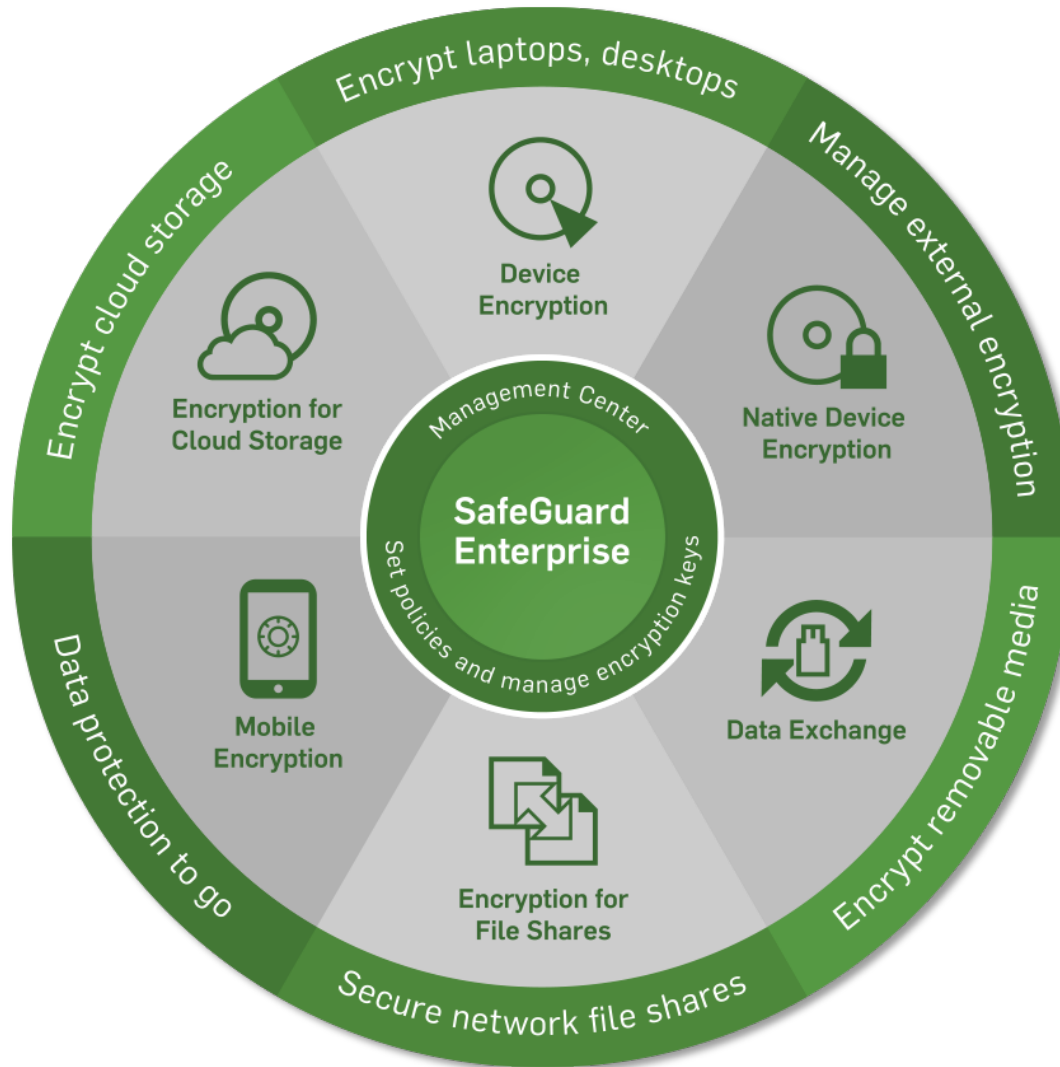


SafeGuard Enterprise Przegląd modułów

Szyfrowanie wolumenów vs plików

Funkcjonalność	Szyfrowanie Volume-based	Szyfrowanie File-based
Szybkie szyfrowanie symetryczne(e.g. AES128)	Y	Y
Transparentne dla użytkownika	Y	Y
Możliwość odzyskania danych	Y	Y
Ochrona WSZYSTKICH danych lokalnych i nośników	Y	
Ochrona plików systemowych, plików hibernacji	Y	
Szybkość (mały wpływ na wydajność stacji)	Y	
Szyfrowanie wybranych plików i folderów		Y
Pozwala sprawdzić które pliki są zaszyfrowane		Y

Sophos SafeGuard Enterprise



SafeGuard Management Center

Serce systemu Safe Guard



- Jeden panel zarządzania
- Centralne zarządzanie kluczami, politykami bezpieczeństwa danych oraz chronionymi urządzeniami
- Obsługa wielu platform z jednego panelu FileVault 2, BitLocker oraz sprzętowych
- Integracja z AD
- Predefiniowane i konfigurowalne role dla administratorów
- Konta serwisowe dla administratorów
- Gromadzenie zdarzeń, generowanie raportów, audyt urządzeń i dostępuów

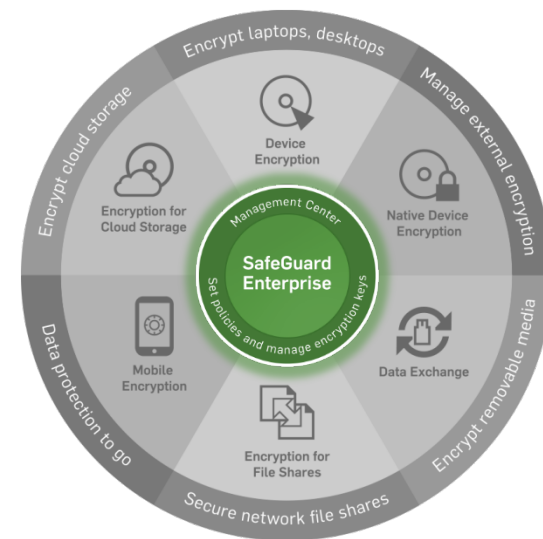
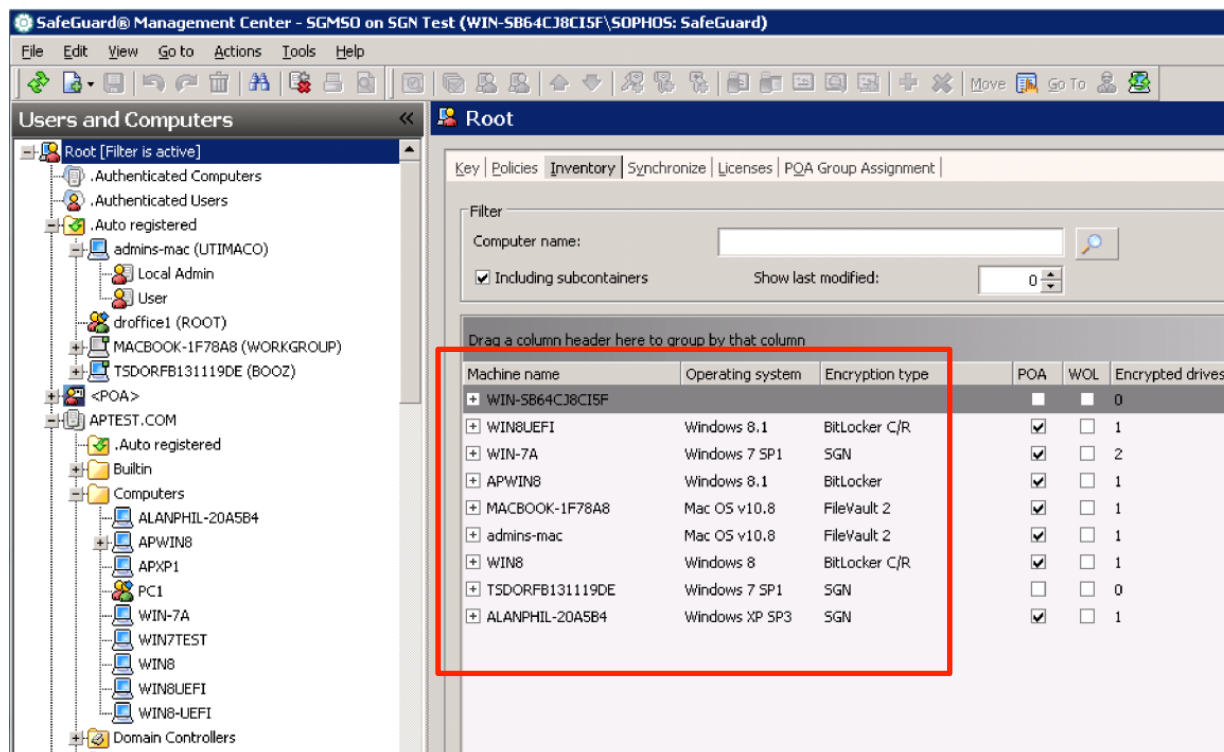
OPAL 1 i 2



SafeGuard Management Center



- Wszystkie urządzenia i platformy dostępne z jednej konsoli:



SafeGuard Device Encryption

Szyfrowanie dysków



- Full-disk encryption to moduł wykorzystujący technikę szyfrowania opracowaną przez Sophos
- Bezpieczna i certyfikowana
 - FIPS 140-2, CC EAL 4, VS-NfD* etc.
- Ochrona wszystkich danych na dyskach przez zagubieniem lub kradzieżą
- Szybkie szyfrowanie wstępne i niewielki wpływ na wydajność
- Licencja zawiera moduł Native Device Encryption
- Obejmuje również Disk Encryption for Mac (OS X 10.5/10.6/10.7)



*) VS-NfD certification for version 5.60.2, others to follow

SafeGuard Native Device Encryption



Natywne szyfrowanie dysków

- Moduł Full-disk encryption jednak wykorzystujący możliwości wbudowane w system operacyjny
- Zarządzanie oprogramowaniem BitLocker dla Windows oraz FileVault 2 dla Mac za pomocą jednej konsoli
- Szybsze, prostsze, pewniejsze
 - Szybsze uruchamianie systemu, krótszy czas szyfrowania wstępnego, lepsza kompatybilność sprzętowa



SafeGuard Native Device Encryption



Natywne szyfrowanie dysków

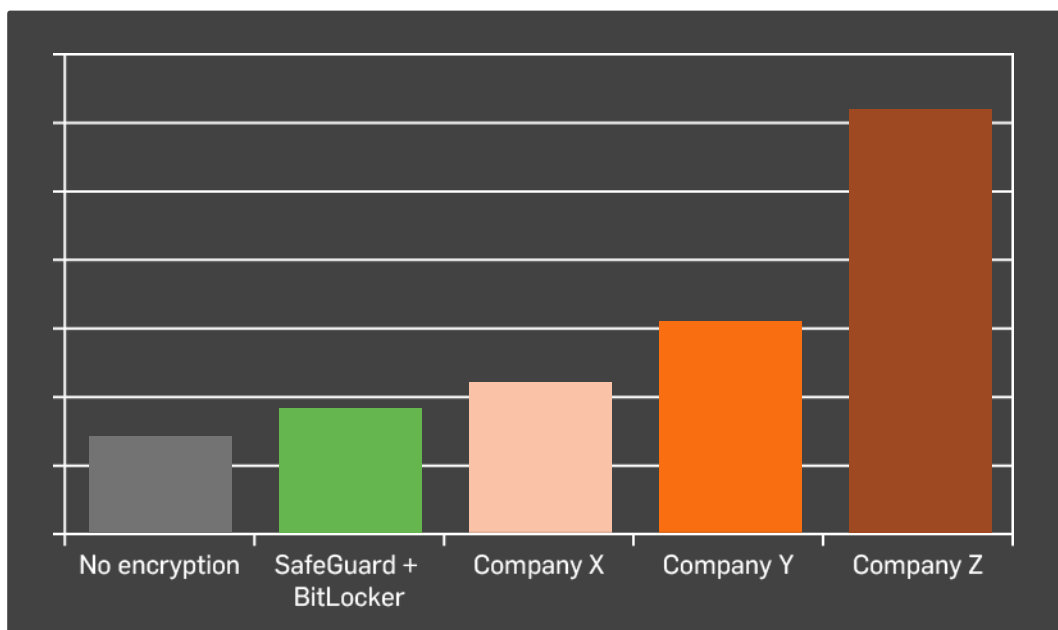
- Dziedziczny certyfikaty i kompatybilność z mechanizmu szyfrowania na poziomie systemu operacyjnego
- Zapewnia mechanizmy odzyskiwania danych i centralne repozytorium kluczy szyfrujących
- Scentralizowane raportowanie, weryfikacja zgodności oraz logowanie zdarzeń
- Dostępny w bundlu SafeGuard Device Encryption lub jako osobna licencja



SafeGuard Native Device Encryption

Natywne szyfrowanie dysków

- Mały wpływ na czas uruchamiania



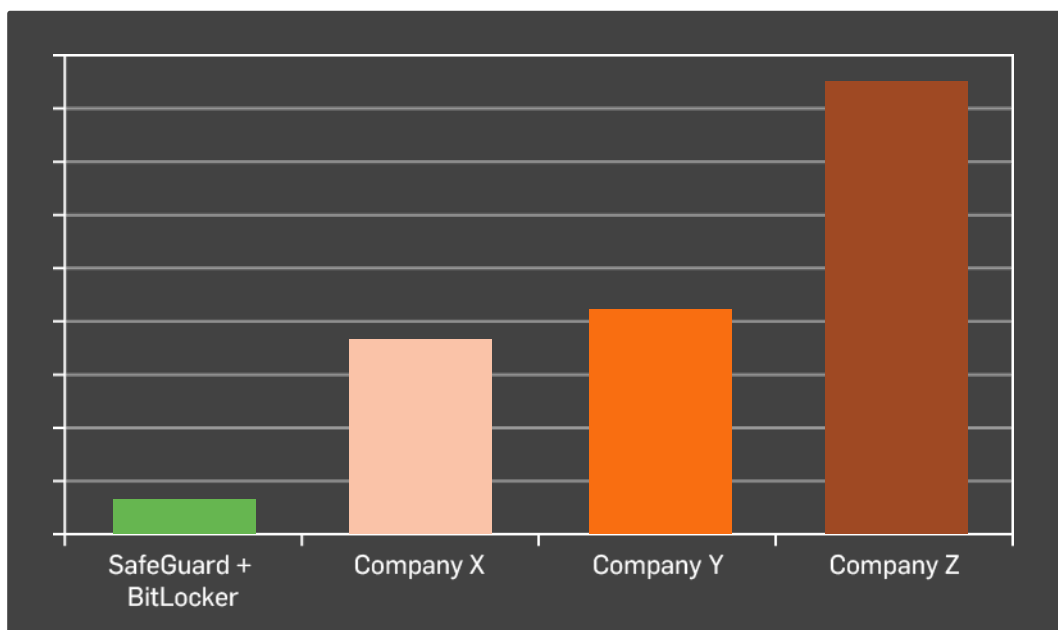
Average boot time



SafeGuard Native Device Encryption

Natywne szyfrowanie dysków

- Znacznie krótszy czas szyfrowania wstępnego



Czas szyfrowania wstępnego

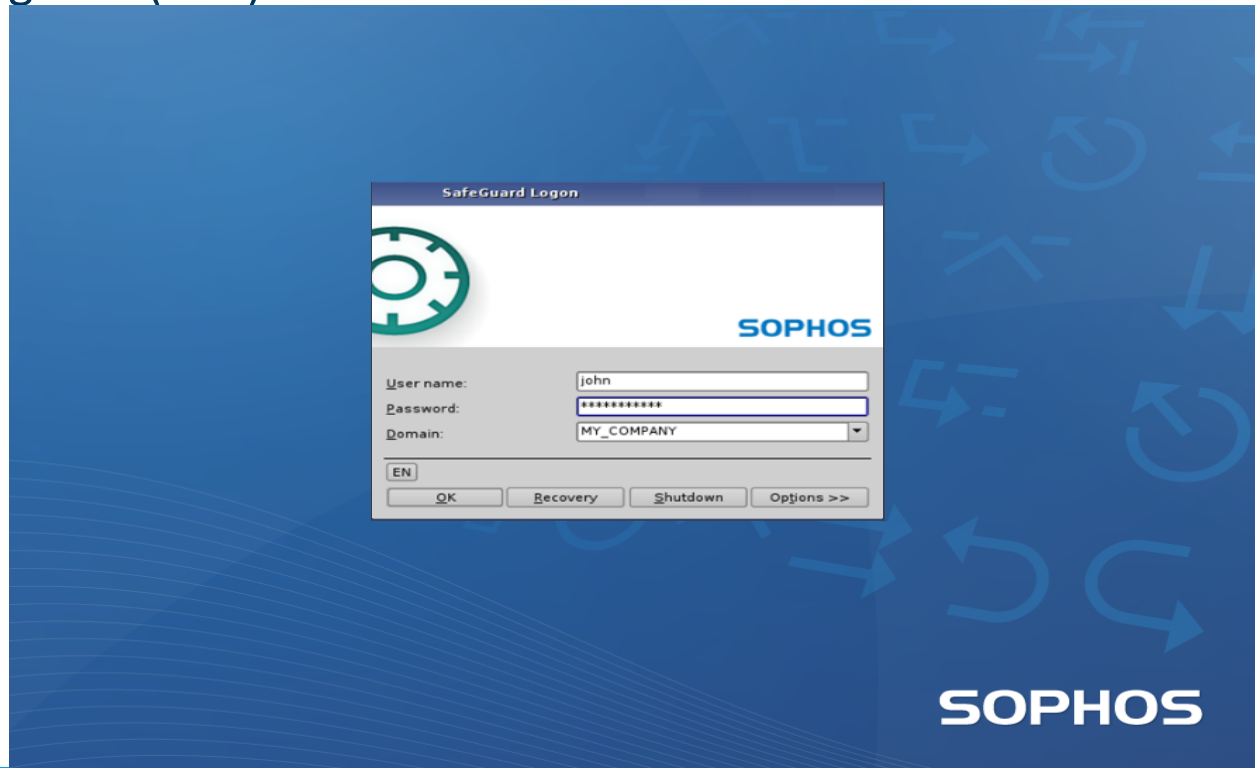


Działanie i recovery - POA



Szyfrowanie dysków

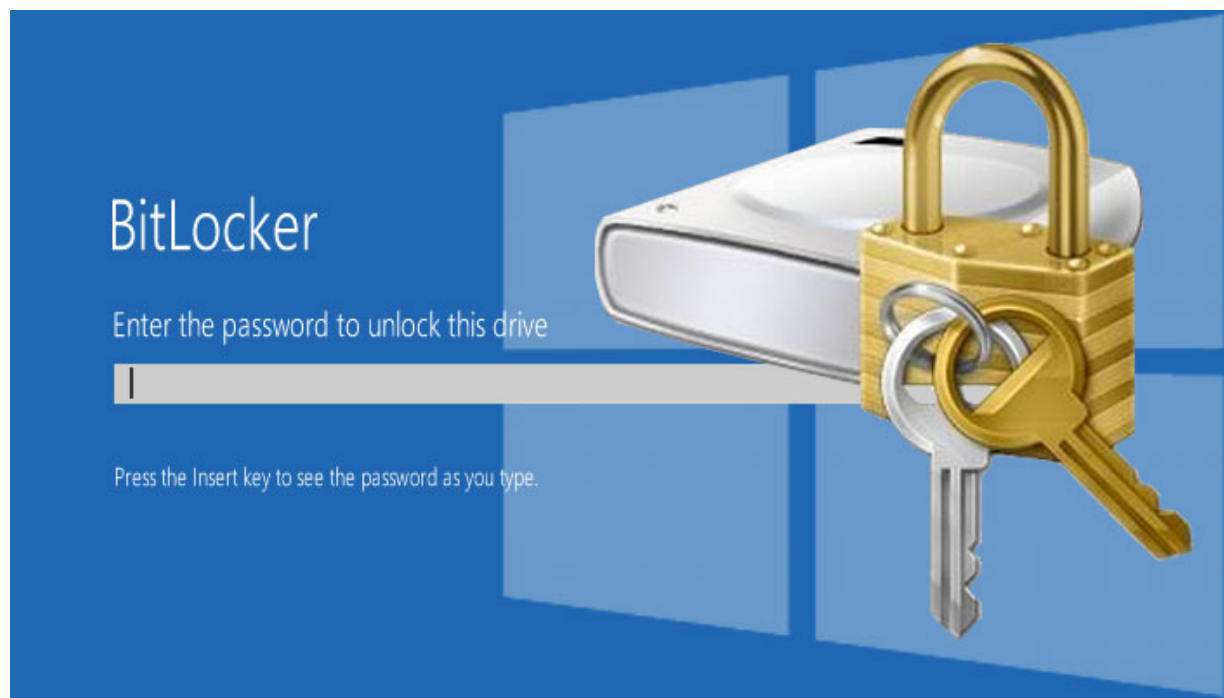
- Power-on authentication (POA)
- Mechanizm Challenge/response oraz lokalny mechanizm odzyskiwania hasła przez użytkownika Self Help
- Single sign-on (SSO)



Działanie i recovery - Bitlocker

Szyfrowanie dysków

- TPM
- TPM + PIN
- Klucz USB
- TPM + klucz USB
- Hasło od win 8 i 8.1
jako metoda zastępcza



SafeGuard Data Exchange



Szyfrowanie urządzeń przenośnych

- Szyfrowanie plików na urządzeniach przenośnych
 - Pamięci USB, płyty CD/DVD, karty pamięci, zewnętrzne dyski twarde etc.
- Ochrona informacji przy przenoszeniu
 - Transparentna wewnątrz organizacji z wykorzystaniem ogólnych polityk i kluczy
 - Dostęp poprzez aplikacje dla użytkowników spoza organizacji*
- Nie wymagana akcja ze strony użytkownika
- Możliwość wykorzystania prywatnych nośników

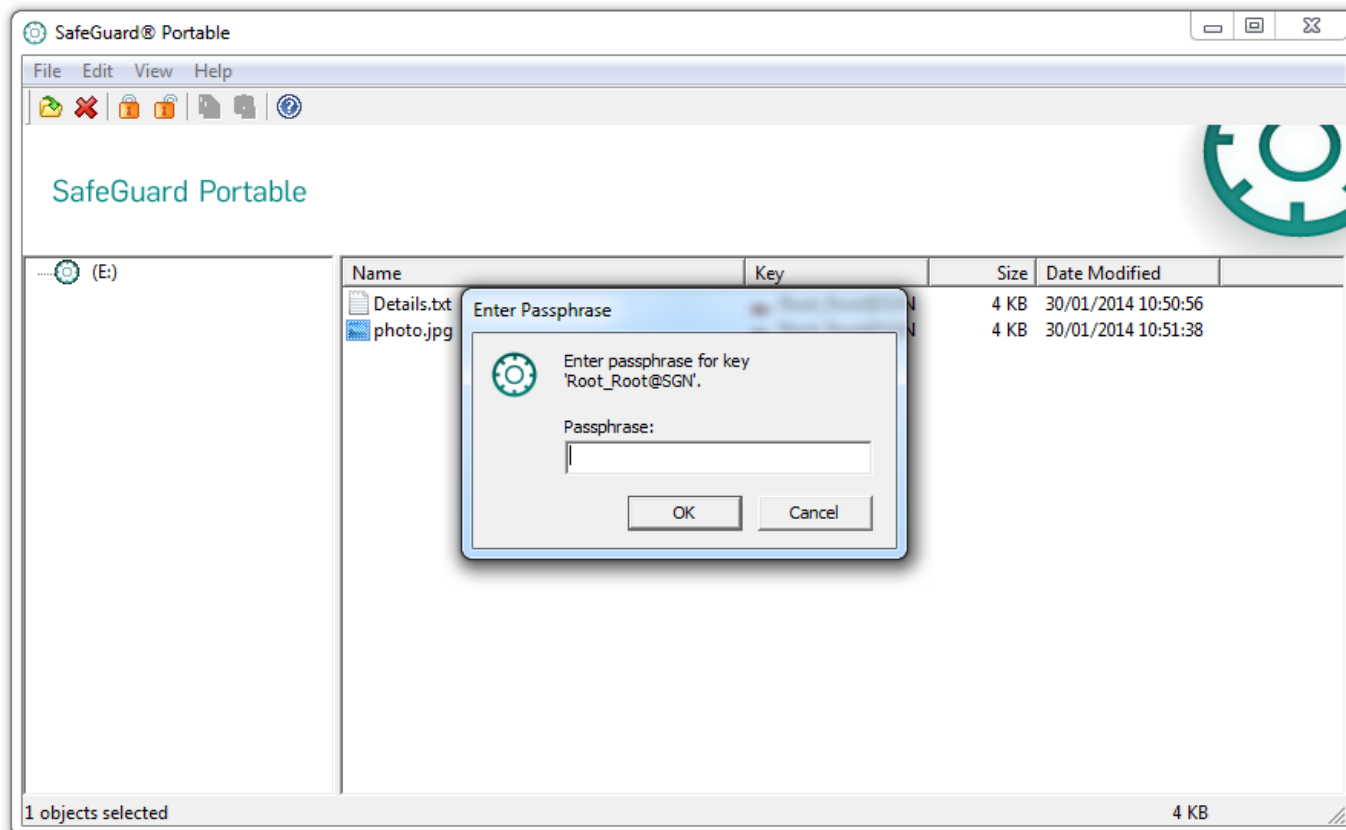


*) SG Portable niedostępny dla Mac OS



Safe Guard Portable

- Data Exchange
- Encryption for Cloud Storage

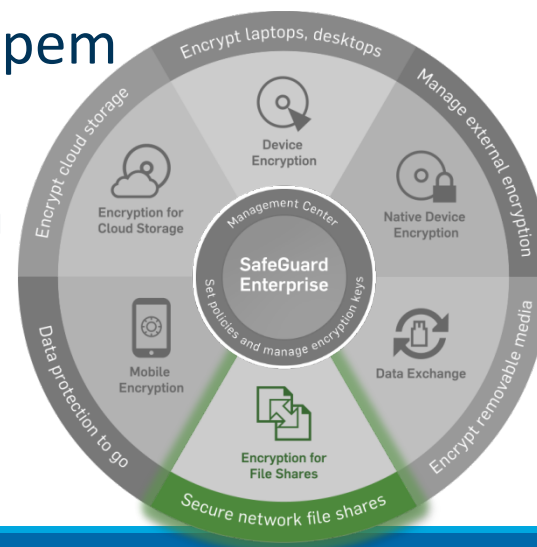


SafeGuard Encryption for File Shares



Szyfrowanie udziałów sieciowych

- Chroni dane przy przesyłaniu i w spoczynku
- Oferuje większe możliwości niż zwykłe uprawnienia do folderów
- Gwarantuje że tylko upoważnione osoby mogą odczytać określone dane
- Pozwala wprowadzić podział obowiązków między administratorami IT i administratorami bezpieczeństwa
- Administrator może zarządzać siecią i dostępem do danych ale nie mieć w nie wglądu
- Szyfrowanie transparentne dla użytkownika
- Szyfrowane pliki możliwe do odczytania na Windows i Mac OS

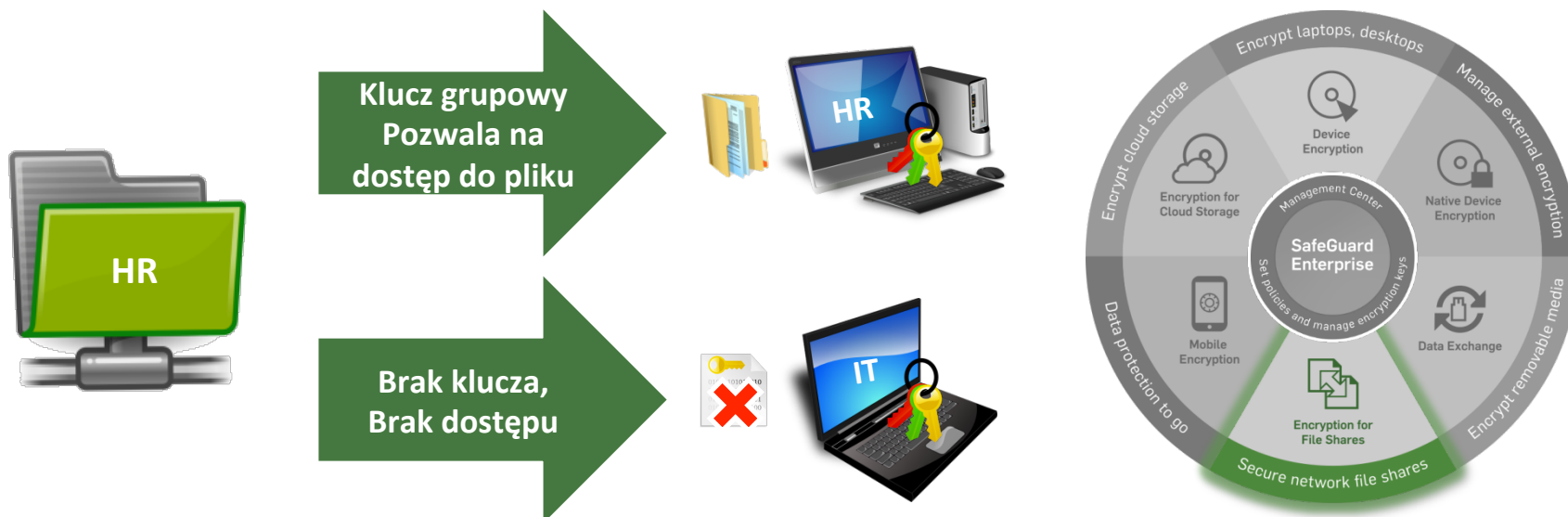


SafeGuard Encryption for File Shares

Szyfrowanie udziałów sieciowych



- Kiedy może się przydać
 - Ochrona przed odczytaniem danych przez pracowników IT
 - Ochrona danych wrażliwych (HR, księgowość)
 - Bezpieczna wymiana informacji w ramach grupy
 - Ochrona danych firmowych na serwerach hostowanych u providera



SafeGuard Encryption for Cloud Storage



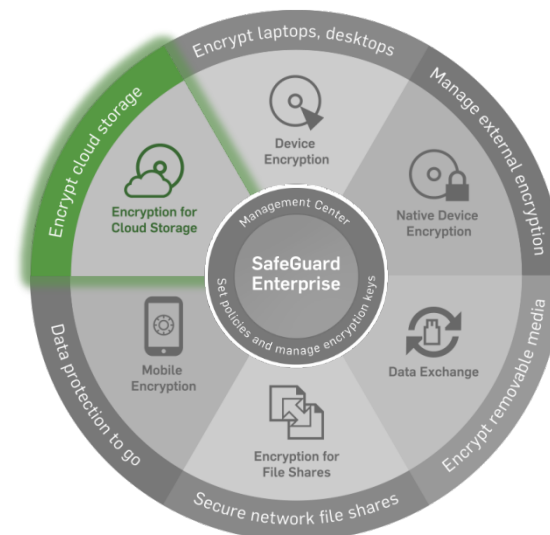
Szyfrowanie danych w chmurze

- Dodatkowy poziom ochrony danych w chmurze
- Szyfrowanie transparentne dla użytkownika
- Kontrola nad kluczami i szyfrowaniem w obrębie organizacji
- Większość serwisów wspieramy “out of the box”
 - Dropbox, Google Drive, Egnyte, OneDrive i więcej
- Wsparcie dla serwisów publicznych i prywatnych

Ilość użytkowników korzystająca z chmury w ubiegłym roku

700

Source: IHS iSuppli Research

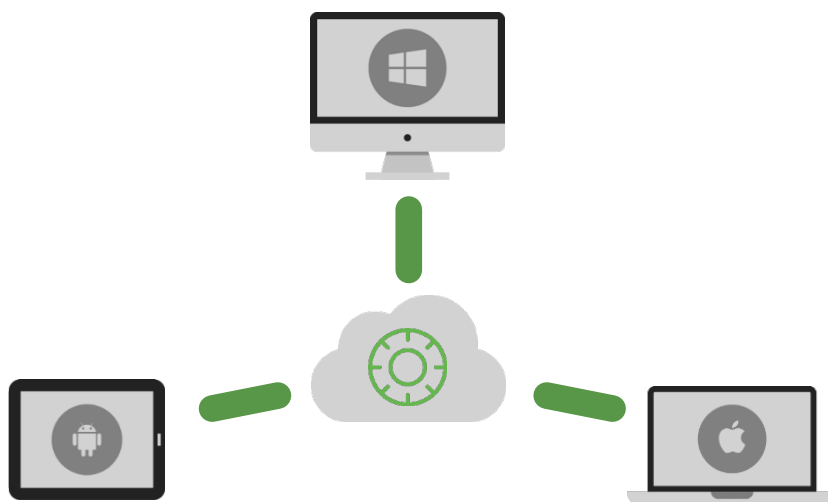


SafeGuard Encryption for Cloud Storage



Szyfrowanie danych w chmurze

- Nie musisz się bać przechowywania danych w chmurze
- Twoje dane są bezpieczne w momencie gdy opuszczają stacje
- Zapewnia możliwości audytowania i weryfikacji zgodności z politykami organizacji
- Pozwala współdzielić dane w ramach organizacji i poza nią

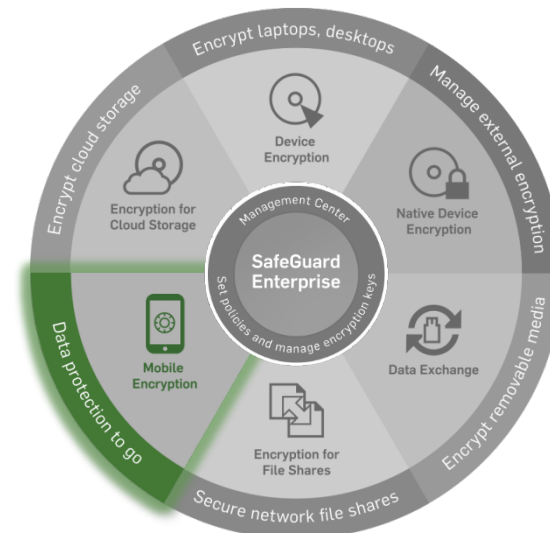
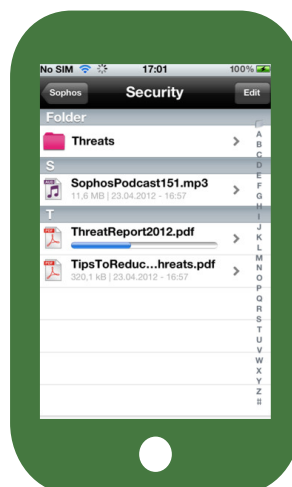
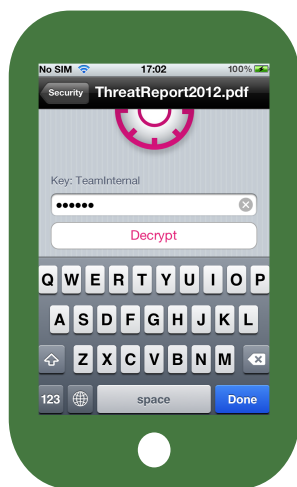
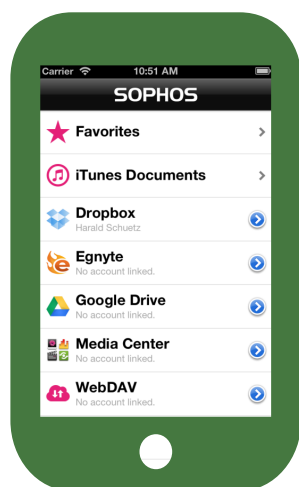


Sophos Mobile Encryption

Mobilna aplikacja do podglądu danych



- Możliwość odczytania danych zaszyfrowanych w chmurze
- Zapewnia dostęp do danych na większej ilości platform
- Dostęp do plików zaszyfrowanych hasłem
- Bezpłatna aplikacja na iOS i Android



SafeGuard Encryption Licencjonowanie

Elastyczne opcje licencjonowania



- Licencjonowanie na zasadzie subskrypcji lub wieczyste
- Produkty dostępne jak bundle “all-in-one” lub osobne moduły
- Subskrypcje licencjonowane na użytkownika, licencje wieczyste licencjonowane na urządzenie
- Aplikacje na urządzenia mobilne bezpłatne
- Uwaga na dodatki, uwierzytelnianie Smart Card
wsparcie tokenów,





SafeGuard Enterprise Architektura

Architektura



Wymagania

Platforms supported	x86 32-bit	x64 64-bit	IA-64 (Itanium) 64-bit	Minimum disk space	Minimum memory	
SafeGuard Enterprise - Client						
Windows XP SP3 Professional	✓ ³			300 MB	1 GB ¹	
Windows Vista SP2 Business, Enterprise, Ultimate Edition	✓ ³	✓ ³		300 MB	1 GB ¹	
Windows 7 SP1 HomePremium, Professional, Enterprise, Ultimate Edition	✓	✓		300 MB	1 GB ¹	
Windows 8, 8.1 Pro, Enterprise Edition	✓	✓		100 MB	2 GB ¹	
Windows 10 Pro, Enterprise Edition	✓ ⁴	✓ ⁴		100 MB	2 GB ¹	
SafeGuard - Management Center						
Windows 7 SP1 HomePremium, Professional, Enterprise, Ultimate Edition	✓	✓		1 GB	1 GB ¹	
Windows 8, 8.1 Pro, Enterprise Edition	✓	✓				
Windows Server 2008 SP2		✓		Please follow standard Windows Server installation guidelines		
Windows Server 2008 R2 SP1, SP2		✓				
Windows Server 2012		✓				
Windows Server 2012 R2		✓				
SafeGuard Enterprise - Server						
Windows Server 2008 SP2		✓ ²		Please follow standard Windows Server installation guidelines		
Windows Server 2008 R2 SP1, SP2 **		✓ ²				
Windows Server 2012 **		✓ ²				
Windows Server 2012 R2 **		✓ ²				
Windows Small Business Server and Windows Server Essentials are not supported.						

<https://www.sophos.com/en-us/support/knowledgebase/118646.aspx>

Wdrożenie



Weryfikacja założeń, dobór komponentów, sprawdzenie kompatybilności

Instalacja komponentów serwerowych (SGN Server, baza danych, MGMT Center)

Integracja z AD (opcjonalna)

Stworzenie paczek instalacyjnych

Instalacja paczek centralnie (narzędzia zewnętrzne) lub ręcznie

Wybór metody szyfrowania i modułów do zainstalowania

Safe Guard Easy



- Przeznaczone dla pojedynczych wdrożeń
- Szyfrowanie dysków NTFS, FAT, FAT32, oraz dysków OPAL
- Zarządzanie przez Policy Editor z możliwością upgradu do Management Center po wykupieniu licencji Safe Guard Enterprise
- Wbudowane mechanizmy challenge/response dla prostego recovery (portal www, self help)

<https://www.sophos.com/medialibrary/PDFs/factsheets/sophossafeguardeasydsna.pdf>



**Dlaczego warto wybrać
rozwiązanie Sophos?**

Z nami Twoje dane są bezpieczne zawsze!

#nobackdoors



<https://www.sophos.com/en-us/lp/nobackdoors.aspx>

Nagrody i wyróżnienia

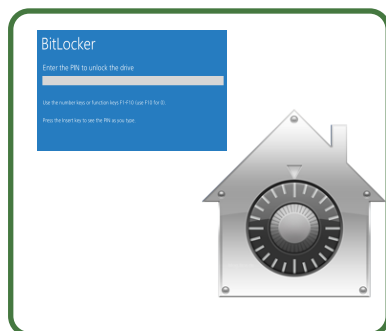
Sophos to najlepsze rozwiązanie do ochrony danych, możecie wierzyć nam na słowo, ale...



- SGN oszczędza Twoje pieniądze (Gartner)
- SGN znacznie szybszy od konkurentów (Tolly)
- Użytkownicy wybrali SGN najlepszym rozwiązaniem do szyfrowania (TechTarget)

Safe Guard to

- Wydajność, bez ograniczania użytkowników
- Wieloplatformowość
- Dedykowany mechanizm szyfrowania i zarządzanie natywnymi mechanizmami szyfrowania
- Szyfrowanie nie tylko dla dysków twardych
- Proste wdrożenie i jedna konsola zarządzania



SOPHOS