SOPHOS

Sophos Safeguard Encryption

SafeGuard Enterprise to kompleksowe rozwiązanie do zabezpieczania danych, które wykorzystuje strategię szyfrowania opartą na zasadach w celu zapewnienia niezawodnej ochrony danych na stacjach roboczych, udziałach sieciowych i urządzeniach mobilnych. Pozwala użytkownikom bezpiecznie udostępniać informacje i pracować z plikami na Windows, Mac OS X, iOS i Android przy pomocy aplikacji Sophos Secure Workspace.

W Centrum zarządzania SafeGuard można zarządzać zasadami zabezpieczeń, kluczami i certyfikatami, korzystając ze strategii administrowania opartej na rolach. Dzięki szczegółowym dziennikom i funkcjom raportów zawsze masz przegląd wszystkich wydarzeń.

Po stronie użytkownika szyfrowanie danych i ochrona przed nieautoryzowanym dostępem to główne funkcje bezpieczeństwa SafeGuard Enterprise. SafeGuard Enterprise można bezproblemowo zintegrować z normalnym środowiskiem użytkownika.

Full Disk Encryption

Aby zapewnić najszybsze, najłatwiejsze i najbardziej niezawodne szyfrowanie pełnych dysków, SafeGuard Enterprise korzysta z technologii wbudowanej w system operacyjny. Bezproblemowe zarządzanie kluczami i funkcjami odzyskiwania na zaszyfrowanych dyskach 2 BitLocker i FileVault z SafeGuard Management Center.

Zapewnia centralne zarządzanie pełnym szyfrowaniem dysków za pomocą Windows BitLocker i Mac FileVault, korzystając z technologii wbudowanej w systemy operacyjne. Bezproblemowe zarządzanie kluczami i funkcjami odzyskiwania z SafeGuard Management Center. Aby jeszcze bardziej uprościć przepływ pracy, możesz teraz zarządzać pełnym szyfrowaniem dysków Windows i macOS w Sophos Central.

Location-Based Encryption

Po przypisaniu zasad szyfrowania plików na podstawie lokalizacji, pliki w lokalizacjach objętych polityką są w przejrzysty sposób szyfrowane bez interakcji użytkownika:

Cloud Storage

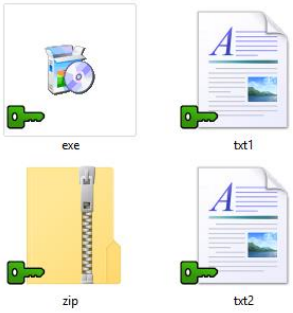
Usługi przechowywania w chmurze pomagają użytkownikom uzyskać dostęp do swoich danych, niezależnie od tego, gdzie się znajdują, na jakimkolwiek urządzeniu, z którego korzystają. Zwiększenie produktywności użytkowników jest ważne, ale równie ważne jest zapewnienie poufności poufnych informacji po przejściu do chmury. SafeGuard Enterprise automatycznie i niewidocznie szyfruje / odszyfrowuje pliki podczas ich przesyłania lub pobierania z usług w chmurze.

- Szyfruje pliki przesłane do usług przechowywania w chmurze
- Umożliwia bezpieczne udostępnianie danych wszędzie
- Automatycznie wykrywa i obsługuje najpopularniejsze usługi przechowywania w chmurze, takie jak Box, Dropbox, OneDrive i Egnyte

File Encryption

Szyfrowanie polega nie tylko na upewnianiu się, że dane pozostają bezpieczne przed ciekawskimi spojrzeniami spoza firmy. Jest to również użyteczne w celu umożliwienia bezpiecznej współpracy i kontrolowania plików wewnątrz niego. SafeGuard Enterprise wykracza poza proste uprawnienia do folderów i gwarantuje, że tylko właściwe osoby będą mogły odczytać właściwe pliki, jednocześnie umożliwiając działom IT zarządzanie plikami i kopiami zapasowymi.

- Konfiguruje szyfrowanie plików dla folderów współdzielonych
- Upewnia się, że tylko niektórzy użytkownicy lub grupy mają dostęp do danych
- Nie wymaga interakcji ze strony użytkowników
- Zapewnia dodatkową warstwę ochrony, jeśli / kiedy serwery korporacyjne przejdą do chmury



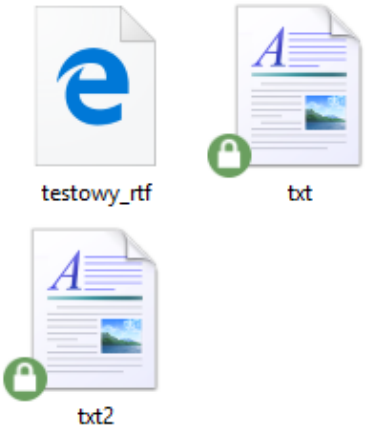
Data Exchange

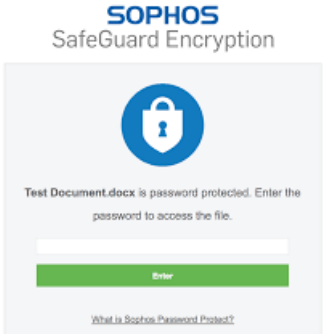
SafeGuard Enterprise automatycznie i transparentnie szyfruje pliki na nośnikach wymiennych, takich jak pamięci USB, karty pamięci i płyty CD / DVD.

- Udostępniaj zaszyfrowane dane na nośnikach wymiennych w całej organizacji bez wpływu na użytkowników
- Za pomocą przenośnej aplikacji i hasła można łatwo i bezpiecznie udostępniać zaszyfrowane nośniki wymienne użytkownikom, którzy nie używają SafeGuard Enterprise
- Biała lista nośników umożliwia łatwiejsze i bardziej elastyczne zarządzanie szyfrowaniem

Szyfrowanie plików w oparciu o aplikacje (Application-based)

SafeGuard Enterprise Synchronized Encryption może szyfrować dowolny plik utworzony za pomocą aplikacji określonej w polityce, niezależnie od lokalizacji pliku. Na przykład, jeśli Microsoft Word zostanie określony jako aplikacja, dla której aktywne jest szyfrowanie plików, każdy plik tworzony lub zapisywany za pomocą programu Microsoft Word jest automatycznie szyfrowany przy użyciu klucza zsynchronizowanego szyfrowania. Każda osoba, której pęk kluczy zawiera ten klucz, może uzyskać dostęp do pliku. Zasada definiuje listę aplikacji, dla których szyfrowanie plików jest wykonywane automatycznie.





Wtyczka Outlooka

Aby ułatwić życie użytkownikowi końcowemu, Synchronized Encryption zapewnia dodatek Outlook, który automatycznie wykrywa pocztę e-mail wysyłaną poza organizację za pomocą załącznika do pliku. Następnie zapyta, która opcja (hasło chronione, niezabezpieczone) użytkownik chce wybrać. W razie potrzeby użytkownik może ustawić hasło w wyświetlonym oknie dialogowym. Alternatywnie można użyć strategii do zdefiniowania domyślnej akcji wykonywanej automatycznie bez interwencji użytkownika.

Udostępnij pęk kluczy pomiędzy SafeGuard Enterprise i Sophos Mobile Control

Klucze szyfrowania z pęku kluczy SafeGuard Enterprise można udostępnić w aplikacji Sophos Secure Workspace (SSW) zarządzanej przez Sophos Mobile Control. Użytkownicy aplikacji mogą następnie używać kluczy do odszyfrowywania i przeglądania dokumentów lub szyfrowania dokumentów. Pliki te mogą być następnie bezpiecznie udostępniane wszystkim użytkownikom SafeGuard Enterprise i SSW.

Integracja z Sophos Central Endpoint Protection - usuwanie kluczy na zaatakowanych komputerach

W połączeniu z Sophos Central Endpoint Protection klucze można usuwać automatycznie, jeśli wykryje szkodliwe działanie na punktach końcowych.