

Sophos Mobile Control

Sophos Mobile Control umożliwia bezpieczną pracę na urządzeniach mobilnych oraz nieograniczone możliwości współpracy dla firmy.

Sophos upraszcza system zarządzania typu Enterprise Mobility Management (EMM) dla środowisk, w których korzysta się z telefonów prywatnych (BYOD) przy jednoczesnej maksymalizacji bezpieczeństwa danych. Sophos Mobile Control (SMC) oferuje intuicyjną konsolę zarządzania, aby móc zarządzać aplikacjami, urządzeniami i danymi. SMC zapewnia kompleksową ochronę, poczynając od systemu antywirusowego aż do szyfrowanego współdzielenia plików zawierających wrażliwe dane korporacyjne.

Najważniejsze informacje

- ▶ Jedno rozwiązanie dla wszystkich najnowszych platform mobilnych
- ▶ Konsola zarządzająca dostępna z przeglądarki wraz z wbudowanymi rolami
- ▶ Zdalne instalowanie polityk i aplikacji
- ▶ Dystrybucja dokumentów korporacyjnych na urządzenia użytkowników
- ▶ Zwiększone bezpieczeństwo współpracy poprzez aplikację Secure Workspace
- ▶ Możliwość filtrowania stron internetowych oraz instalacji oprogramowania antywirusowego dla urządzeń z systemem Android
- ▶ Dwa rodzaje wdrożenia – w chmurze lub we własnej sieci

Zarządzanie wszystkimi urządzeniami mobilnymi

Urządzenia mobilne to telefony, fablety lub tablety z systemem iOS, Android lub Windows Mobile, które są własnością firmy lub prywatną użytkowników. Sophos umożliwia zarządzanie wszystkimi tymi urządzeniami z prostej i intuicyjnej konsoli. Administratorzy mogą w łatwy sposób zarządzać różnymi urządzeniami, definiować polityki bezpieczeństwa i polityki zgodności z ustalonymi normami, jednocześnie kontrolując bezpieczeństwo poczty i dokumentów korporacyjnych. Ponadto, poprzez Portal Serwisowy użytkownicy mogą sami wykonywać wiele czynności w dowolnym momencie - gdy urządzenia są zagubione lub skradzione, mogą je być zablokowane lub ich zawartość może zostać całkowicie skasowana. Zasady bezpieczeństwa i zgodności z polityką są egzekwowane automatycznie.

Szyfrowanie

SMC gwarantuje, że dokumenty korporacyjne pozostaną bezpieczne dzięki ich zaszyfrowaniu. Nawet, gdy pliki są współdzielone, rozpowszechniane lub zostają umieszczone w chmurze, pozostają bezpieczne. Jest to najwyższa ochrona danych firmowych, która wykracza poza urządzenie, kontener danych czy chmurę.

Zintegrowane zabezpieczenia

Sophos jest jedynym producentem, który zapewnia zintegrowane oprogramowanie antywirusowe i filtrowanie stron internetowych dla urządzeń z systemem Android zarządzanych w taki sam sposób, jak tradycyjne komputery. Nasza aplikacja Mobile Security integruje się z konsolą SMC i pozwala na centralne zarządzanie ochroną antywirusową, chroniąc użytkowników Android przed złośliwymi aplikacjami, stronami internetowymi i innymi zagrożeniami. Nasze wbudowane filtrowanie stron internetowych powstrzymuje użytkowników przed dostępem do zainfekowanych stron internetowych.

Kontrola dostępu do sieci – NAC

Pozwala zmniejszyć ryzyko utraty danych poprzez wykorzystanie ustawień SMC do blokowania dostępu do sieci firmowej w oparciu o status urządzenia. Automatycznie wykrywa urządzenia, które nie spełniają wymogów ustalonej polityki bezpieczeństwa podczas próby połączenia z siecią i blokuje dostęp do WiFi oraz do vpn. SMC idealnie integruje się z Sophos UTM oraz wspiera urządzenia Checkpoint i Cisco.

Kompleksowe bezpieczeństwo

Tylko Sophos może dostarczyć zintegrowanego i kompleksowego rozwiązania bezpieczeństwa, które może chronić sieć firmową, komputery i urządzenia klienckie, urządzenia mobilne, serwery, dane w chmurze oraz szyfrować dane.

Jeden użytkownik = jedna licencja i niski koszt

Nasze rozwiązanie pozwala na zmniejszenie kosztów przy zastosowaniu uproszczonego licencjonowania względem liczby użytkowników. Jeden użytkownik = jedna licencja, bez względu na to, ile urządzeń mają i wykorzystują. SMC pomaga także obniżyć koszty operacyjne ze względu na bardzo prostą instalację i późniejsze aktualizacje, a także ze względu na minimalne wsparcie dla użytkowników dzięki wykorzystaniu portalu serwisowego – Self Service Portal.

Sophos Mobile Control

Mobile Device Management (MDM)

- ▶ Zarządza i kontroluje urządzenia z systemem iOS, Android (w tym Samsung KNOX) oraz Windows Phone 8.1
- ▶ Zdalne konfigurowanie polityk i wdrożenie
- ▶ Egzekwowanie wbudowanych funkcji bezpieczeństwa, takich jak hasła i szyfrowanie urządzenia
- ▶ Pełna ochrona w przypadku utraty lub kradzieży urządzenia – możliwość zablokowania, usunięcia wszystkich danych oraz zlokalizowania urządzenia
- ▶ Polityki zgodności z regulacjami bezpieczeństwa konfigurowane względem grup

Zarządzanie dokumentami

- ▶ Transparentne szyfrowanie każdego pliku powoduje że dokumenty i dane są bezpieczne – nie tylko w biurze, ale wszędzie, gdzie są użytkownicy
- ▶ Centralne miejsce dystrybucji dokumentów zapewnia centralną dystrybucję dokumentów do wszystkich urządzeń
- ▶ Centralne zarządzanie kontenerami z dokumentami firmowymi wraz z możliwością ich blokowania lub usuwania w przypadku, gdy urządzenie zostanie skompromitowane
- ▶ Dostęp do danych z Dropbox, Google Drive, Microsoft OneDrive, Egnyte i innych rozwiązań oferujących przechowywanie danych w chmurze

Zarządzanie aplikacjami

- ▶ Dystrybucja ustawień poczty korporacyjnej umożliwiającą rozpoczęcie pracy w ciągu kilku minut
- ▶ Kontrola dostępu do poczty w oparciu o stan urządzenia za pomocą bezpiecznej bramki pocztowej
- ▶ Usuwanie zawartości korporacyjnej skrzynki pocztowej w przypadku utraty lub kradzieży urządzenia lub jeśli pracownik odchodzi wraz ze swoim urządzeniem w modelu BYOD

Ochrona antywirusowa oraz filtrowanie stron internetowych dla systemu Android

- ▶ Automatycznie skanuje wszystkie nowo instalowane aplikacje w poszukiwaniu wirusów i złośliwego oprogramowania
- ▶ Urządzenia posiadające wirusy lub inne złośliwe oprogramowanie automatycznie trafiają do kwarantanny
- ▶ Chroni użytkowników przed stronami internetowymi ze złośliwym kodem oraz blokuje dostęp do stron internetowych w oparciu o kategorie stron
- ▶ Kontroluje ustawienia WiFi, NFC oraz Bluetooth, a także dostęp do sklepów z aplikacjami oraz ustawienia szyfrowania urządzenia

Kontrolowany dostęp do sieci

- ▶ Produkt Sophos stale kontroluje stan urządzeń i wykrywa włamania do systemu operacyjnego, aplikacje znajdujące się na czarnej liście administratora oraz inne ustawienia uznane za niebezpieczne
- ▶ Integracja z urządzeniem klasy UTM firmy Sophos pozwala administratorowi na blokowanie sieci WiFi oraz dostępu poprzez vpn w oparciu o status zgodności z polityką bezpieczeństwa
- ▶ Predefiniowany interfejs kontroli dostępu do sieci poprzez Cisco ISE oraz Checkpoint

Nowe funkcjonalności w wersji 5

- ▶ Centralne miejsce dystrybucji dokumentów
- ▶ Możliwość edycji dokumentów
- ▶ Nowy interfejs użytkownika pozwala na szybsze wykonywania typowych zadań administracyjnych
- ▶ Wsparcie dla Windows Phone 8.1
- ▶ Wsparcie dla Samsung KNOX
- ▶ Portal serwisowy dla użytkowników w pełni przygotowany w wersji mobilnej ułatwia wdrożenie
- ▶ Zarządzanie produktem Secure Workspace dla iOS i Android

Wymagania systemowe oraz inne techniczne informacje na temat produktu Sophos Mobile Control można znaleźć pod adresem sophos.com/mobile.

Możliwość pełnej integracji silnika antywirusowego Sophos w dowolnej aplikacji. Wiodący na rynku silnik antywirusowy Sophos jest dostępny także jako pakiet SDK aby zapewnić maksimum bezpieczeństwa aplikacjom biznesowym. Więcej informacji można uzyskać od działu sprzedaży Sophos OEM.

Wypróbuj bezpłatnie

Zarejestruj się, aby bezpłatnie wypróbować przez 30 dni: sophos.com/mobile

Dział sprzedaży w Polsce
Tel: +48 22 548 0005
Email: salesee@sophos.com

Oxford, Wielka Brytania | Boston, USA
© Copyright 2015. Sophos Ltd. Wszystkie prawa zastrzeżone.
Spółka zarejestrowana w Anglii i Walii pod numerem 2096520 i adresie: The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos jest zarejestrowanym znakiem towarowym spółki Sophos Ltd. Wszystkie inne wymienione produkty i nazwy firm są zarejestrowanymi znakami towarowymi ich prawowitych właścicieli.

2015-08-27 DSPL (RP)

SOPHOS