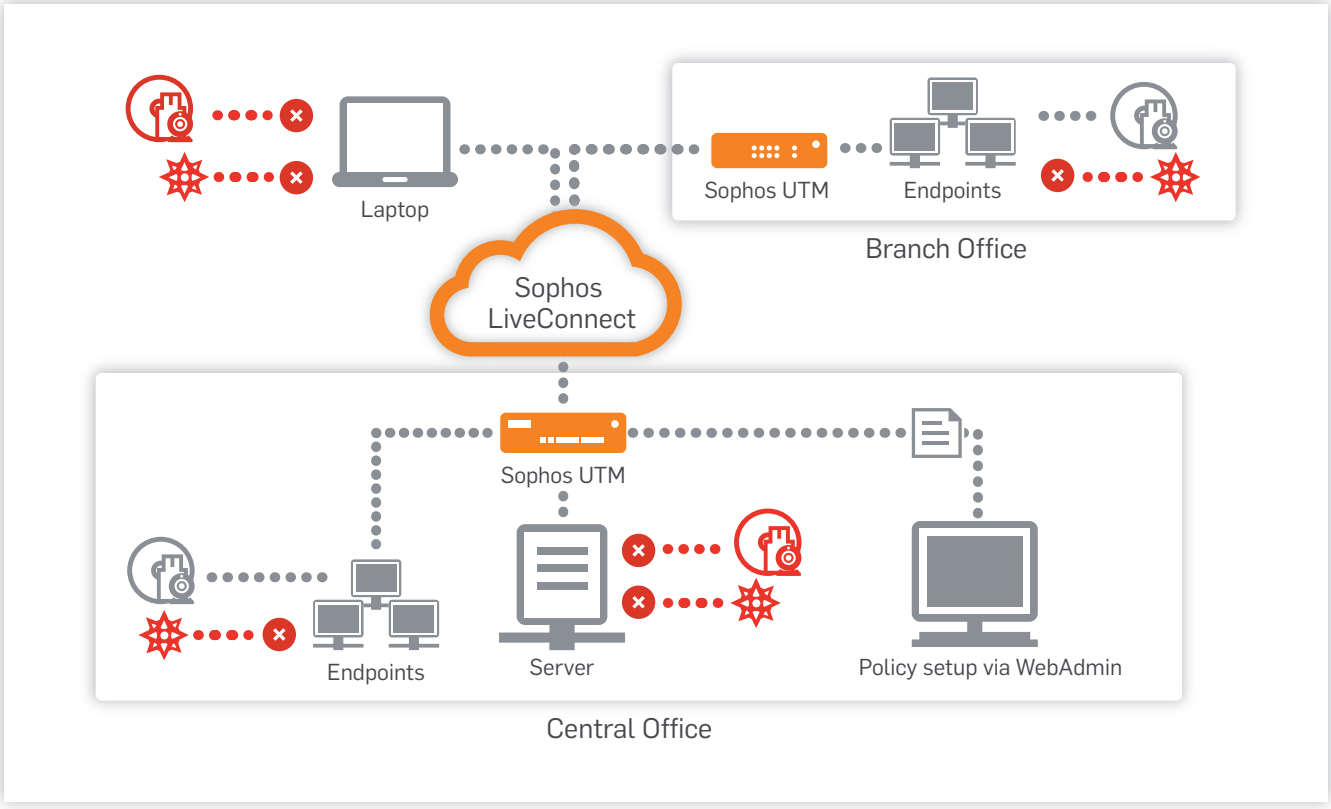
SOPHOS

Sophos UTM Endpoint Protection

Chroni i kontroluje stacje robocze za pośrednictwem centralnego urządzenia UTM

- AV i HIPS: Wykrywają i usuwają wirusy, spyware, rootkity, trojany, adware i potencjalnie niechciane aplikacje (PUA) oraz identyfikują i usuwają nowe zagrożenia za pomocą systemu zapobiegania włamaniom na stacjach roboczych (HIPS).
- Funkcje urządzeń: Wymuszanie kontroli urządzeń peryferyjnych podłączanych na stacjach roboczych. Kontrola dostępu do Internetu zarówno za pomocą mediów bezprzewodowych, jak i przewodowych.
- Ochrona całej sieci: Niezależnie od tego, gdzie znajduje się stacja końcowa, czy jest to komputer w siedzibie firmy, czy w oddziale, czy należy do podróżującego pracownika instalacja agenta na stacjach roboczych odbywa się zawsze bez wysiłku poprzez usługę Sophos LiveConnect i nie wymagane jest posiadanie usług katalogowych.
- Łatwiejsza konfiguracja: Pobranie i instalacja agenta na stacje robocze odbywa się jednym kliknięciem myszki. Polityki bezpieczeństwa są automatycznie wdrażane z centralnego urządzenia Sophos UTM.
- Centralne zarządzanie: Sophos UTM pozwala na centralne tworzenie różnych polityk dla wszystkich stacji roboczych, jednocześnie zapewniając aktualizację informacji o wszystkich zarządzanych komputerach.
- Szczegółowe logi: Możliwość monitorowania obecnej lokalizacji i aktywności wszystkich stacji roboczych. Szczegółowe logowanie wszystkich zdarzeń takich jak odmowa dostępu, próba zmiany polityki czy podłączenie nowego urządzenia.

Sophos UTM Endpoint Protection pozwala w łatwy sposób skonfigurować zabezpieczenia stacji końcowych i zapewnić im ochronę przed malwarem, wirusami oraz utratą danych. Narzędzia raportujące pozwalają na analizowanie sposobu korzystania z urządzeń, a nawet śledzenie ich położenia.



Dystrybucja polityk z użyciem UTM Endpoint Protection

Korzyści

- Ograniczenie rozprzestrzeniania malware'u i wirusów poprzez kontrolę pamięci przenośnych
- Ograniczenie możliwości utraty danych firmowych
- Aktywna rzeczywista ochrona w oparciu o serwisy w chmurze gwarantująca skanowanie podejrzanych plików
- Gwarantowana ochrona również dla komputerów nienależących do domeny
- Szybka lokalizacja komputerów znajdujących się na całym świecie
- Wdrażanie polityk jednym kliknięciem myszki pozwala oszczędzać czas

"Otwarte porty USB są uważane za jeden z najważniejszych czynników wpływających negatywnie na bezpieczeństwo w firmie. Nareszcie znalazłem proste rozwiązanie do ich kontroli, które jest zarządzane centralnie przez Sophos UTM."

Kurt Laux, Właściciel, IT-Consulting & Services

Specyfikacja techniczna

Urządzenie	UTM 110	UTM 120	UTM 220	UTM 320	UTM 425	UTM 525	UTM 625
Zalecana liczba stacji końcowych	10	25	75	200	600	1,300	2,000

Funkcjonalność

Wdrożenie

- Automatyczne tworzenie prekonfigurowanych pakietów instalacyjnych na urządzeniu Sophos UTM
- Proste i globalne wdrożenie wraz z konfiguracją polityk i późniejszymi aktualizacjami agentów z użyciem Sophos Live Connect
- Globalna instalacja bez wymogu posiadania usług katalogowych
- Jeden unikalny pakiet instalacyjny dla wszystkich stacji roboczych
- Wiele metod wdrożenia:
  - USB
  - Poczta elektroniczna
  - Active Directory GPO
  - Standardowe narzędzia do wdrażania oprogramowania
- Automatyczna rejestracja stacji roboczych w Sophos UTM
- Automatyczne aktualizacje agenta
- Serwis typu broker – szyfrowane połączenie https
- Zabezpieczenie przed próbami deinstalacji lub deaktywacji oprogramowania przez nieuprawnionych użytkowników lub złośliwe oprogramowanie

Zarządzanie

- Komunikacja szyfrowana algorytmem AES-256 i podpisana SHA1-HMAC
- Centralne polityki korzystania z urządzeń i transferu plików (odczyt / zapis, tylko odczyt, dostęp zabroniony, logowanie zdarzenia)
- Wsparcie dla grup komputerów
- Tworzenie białych list dla plików i śledzenie lokalizacji stacji
- Wykaz wszystkich stacji roboczych i urządzeń

Kontrola

- Wsparcie dla systemów Microsoft Windows XP SP2, Windows Vista i Windows 7
- Wsparcie dla systemów Microsoft Windows Server 2003 i 2008
- Możliwość korzystanie z zaufanych urządzeń
- Kontrola urządzeń przenośnych pamięci USB, Bluetooth, stacji dyskietek, napędów optycznych, sieci bezprzewodowych, modemów, itd.

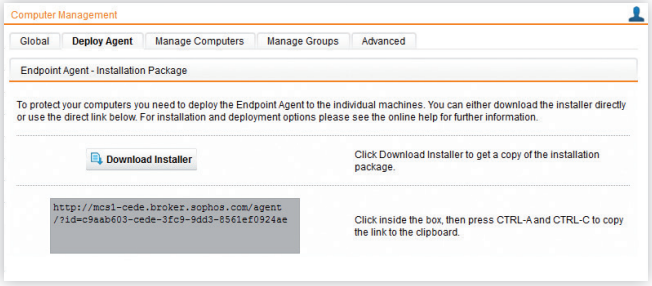
Antywirus i HIPS

- Wykrywanie i usuwanie wirusów, spyware, rootkitów, trojanów, adware oraz potencjalnie niechcianych aplikacji (PUA)
- Identyfikacja nowych zagrożeń, usuwanie ich i minimalizacja liczby fałszywych alarmów z użyciem lokalnego systemu zapobiegania włamaniom (HIPS)
- Blokowanie dostępu do zainfekowanych stron internetowych poprzez filtrowanie adresów URL w czasie rzeczywistym

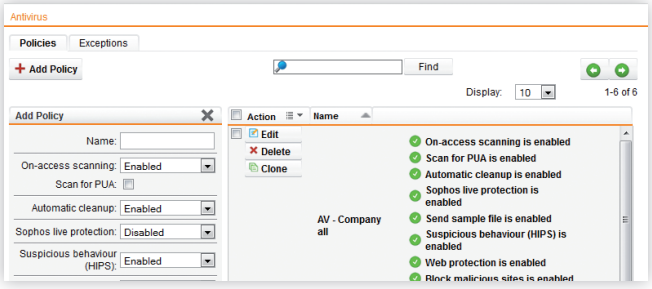
Logowanie / raportowanie

- Logowanie adresów IP, zdarzeń typu logowanie się stacji klienckiej, podłączanych urządzeń, użytkowników, itp.
- Lokalizowanie stacji roboczych znajdujących się na całym świecie
- Monitorowanie używanych urządzeń w czasie rzeczywistym
- Monitorowanie pamięci USB w całej organizacji
- Monitorowanie podłączania nowych urządzeń
- Analizowanie polityk

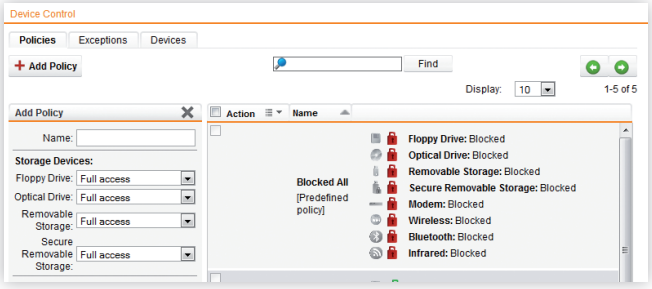
Interfejs użytkownika



Łatwa instalacja agentów na stacjach roboczych



Niezbędne polityki antywirusowe



Polityki kontroli urządzeń

W celu uzyskania dodatkowych informacji należy się zarejestrować:

sophos.com/utm-meets-endpoint

Licencjonowane moduły

Każda sieć firmowa i spoósb jej funkcjonowania jest inny. Sophos zapewnia Państwu różne moduły, spośród których można wybrać te, które odpowiadają obecnym potrzebom.

Niezbędny firewall sieciowy

Oferuje podstawowe funkcje bezpieczeństwa, by pomóc chronić sieć firmową.

UTM Network Protection

Ochrona sieciowa broni przed wyszukanymi typami ataków złośliwego malware'u, robaków i hakerskich exploitów, które mogą ominąć firewall.

UTM Email Protection

Ochrona firmowej poczty elektronicznej przed niechcianymi wiadomościami, wirusami oraz ochrona danych wrażliwych przed cyberprzestępcami.

UTM Web Protection

Ochrona internetowa chroni pracowników przed zagrożeniami internetowymi poprzez kontrolę stron internetowych.

UTM Webserver Protection

Ochrona serwera webowego chroni serwer i uruchomione na nim usługi i aplikacje takie jak np. Outlook Web Access (OWA) przed nowoczesnymi atakami hakerskimi.

UTM Wireless Protection

Ochrona sieci bezprzewodowych ułatwia zarządzanie i zabezpieczanie sieci bezprzewodowych.

RED (Remote Ethernet Device)

Zdalne urządzenie sieciowe jest najłatwiejszym i najbardziej wygodnym sposobem na zabezpieczenie oddziałów firmy.

Sophos Poland
Tel: +48 22 548 0005
Email: salesee@sophos.com

Boston, USA | Oksford, Wielka Brytania

Sophos datasheet 12.12.v1.dPL

SOPHOS