SOPHOS

END USER PROTECTION

Zabezpečení mobilních zařízení

Sophos Mobile Control (SMC) je „nutnou" podmínkou bezpečné, produktivní a přitom neomezené komunikace či výměny informací v rámci organizace. Zjednodušuje management mobilních zařízení (EMM) v prostředích využívajících BYOD/CYOD a zároveň maximalizuje bezpečnost dat. Intuitivní konzole nabízí přehled o aplikacích, zařízeních i datech. Součástí SMC je také oceňovaný antimalware Sophos či šifrování souborů pro zabezpečení citlivých informací organizace.

Mobile Management | Mobilní zařízení mají mnoho podob z hlediska hardwaru, OS i to, zda jej vlastní organizace či uživatel. Sophos nabízí jednoduchou, intuitivní konzoli, která zajistí konsolidované řízení mobilní komunikace. Administrátoři mohou snadno spravovat různá zařízení, nastavovat a automaticky vynucovat politiky a pravidla pro dosažení shody s požadavky i zabezpečovat přístup k emailu a citlivým dokumentům. Nyní také Sophos nabízí správu skrze Sophos Central, tedy konzoli přes kterou se dají spravovat i další produkty od Sophos. Při krádeži či ztrátě je možné zařízení vzdáleně smazat či uzamknout.

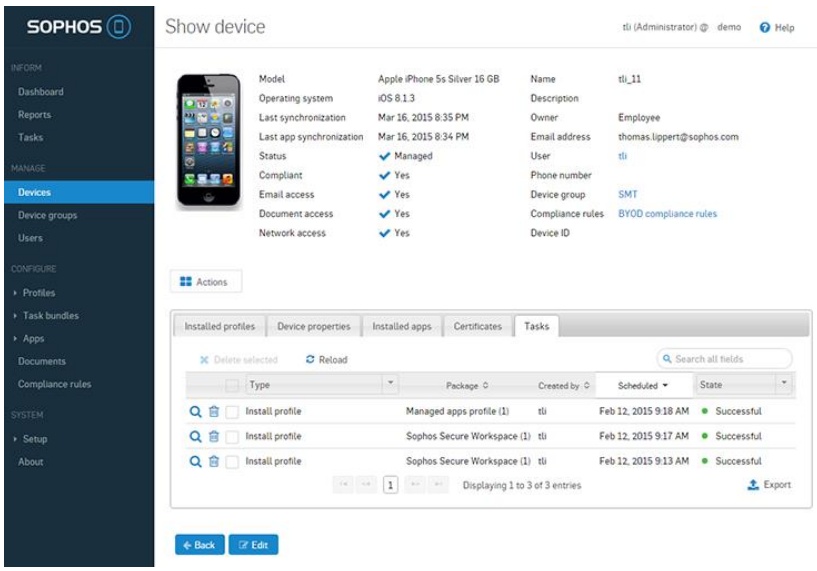
Ochrana citlivých informací | SMC zajišťuje bezpečnost korporátních dokumentů pomocí šifrování, i když jsou soubory sdíleny, umístěny v cloudu, nebo jinak distribuovány. Ochrana informací tak jde za hranice zařízení či kontejneru a nezaniká ani v cloudu.

Integrovaná bezpečnosti pro Android | Sophos je jediným výrobcem, který poskytuje integrovaný antivirus a webový filtr pro Android spravovaný stejně jako pro stolní počítače. Aplikace „Mobile Security" je integrována v rámci SMC konzole a tím je zajištěna centrální správa antimalwarové ochrany. Spolu s webovou filtrací pak pokrývá celé spektrum hrozeb pocházejících z nechtěných či nebezpečných aplikací a webový stránek.

Network Access Control | SMC významně snižuje riziko bezpečnostních incidentů díky řízení přístupu do sítě na základě posouzení shody zařízení s požadavky. Automaticky detekuje neshodná mobilní zařízení ve chvíli, kdy se snaží připojit do sítě a blokuje jejich připojení k Wi-Fi či VPN. SMC je možné integrovat se Sophos UTM, podporovány jsou rovněž platformy Checkpoint a Cisco.

Přínosy Sophos Mobile Control

- Jedno řešení pro všechny nejnovější platformy
- **1 licence = 1 uživatel | 1 uživatel = více zařízení |** nízké režijní náklady
- Webová konzole s přístupem dle rolí
- Vzdálené řízení politik a aplikací
- Možnost správy přes Sophos Central či SMC
- Automatické monitorování shody zařízení
- Vzdálená lokace, uzamčení a mazání
- Distribuce aplikací, dokumentů na uživatelská zařízení
- Umožňuje bezpečnou spolupráci přes „Secure Workspace"
- Webový filtr a antimalware (Security Control) pro zařízení s OS Android
- Nasazení v rámci vlastní infrastruktury (On-premise) či formou služby (SaaS)
- Nově nabízí i Sophos Mobile Security for iOS



Sophos Secure Workspace

- Napojení a přístup ke všem hlavním poskytovatelům ukládání dat a „WebDAV" službám
- Přístup k souborům z definovaných firemních úložišť
- Šifrování pomocí AES 256 bit
- Centrální správa klíčů
- Možnost přidat vlastní klíč a šifrovat nové soubory na mobilním zařízení
- Prohlížení HTML, obrázků a videí
- Prohlížení a úprava textu a PDF
- Zvýšení ochrany přístupu k aplikacím pomocí dalšího hesla

Sophos = integrované zabezpečení sítě, koncových zařízení, serverů, cloudu, dat a mobilních zařízení.

COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

SOPHOS

END USER PROTECTION

Mobile Device Management (MDM)

- Správa a řízení pro iOS, Android (vč. Samsung KNOX) a Windows Phone zařízení
- Konfigurace a vzdálené nasazení politik
- Vynucuje vestavěné bezpečnostní funkce jako je šifrování, aspasscodes apod.
- Plná ochrana a eliminace dopadů ztráty či zcizení (lokalizace, uzamčení, smazání dat)
- Nastavení politik dle skupin uživatelů

Mobile Content Management (MCM)

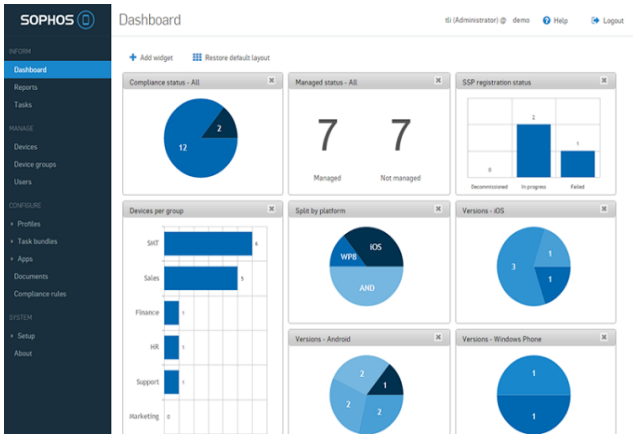
- Transparentní šifrování každého souboru, dokumentu či informace chrání data nejen v kanceláři, ale kdekoliv se uživatel pohybuje
- Centrální distribuce dokumentů na zařízení
- Řídí kontejner pro korporátní citlivé dokumenty s možností uzamknutí či smazání při kompromitaci
- Umožňuje přístup k obsahu cloudových služeb jako je Dropbox, Google Drive, MS OneDrive, a dalších „WebDAV" kompatibilních řešení

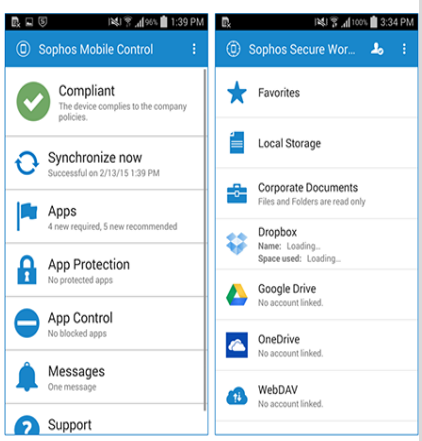
Mobile Application Management (MAM)

- Bezpečně distribuuje aplikace na jednotlivé uživatele nebo skupiny
- Nasazuje iOS řízené aplikace pro větší kontrolu nad aplikačními daty
- Hesla chránící aplikace přistupující k datům organizace
- Blacklist pro aplikace, které mohou být nebezpečné, nebo konzumující firemní zdroje
- Podporuje pořizování aplikací skrze Apple Volume Purchasing (VPP)

Mobile Email Management (MEM)

- Distribuuje nastavení emailové komunikace pro okamžitý přístup uživatele k poště
- Řídí přístup k emailu skrze emailovou bezpečnostní bránu dle stavu uživatelského zařízení
- Selektivně maže všechny firemní emaily v případě krádeže či ztrátě zařízení nebo ukončení pracovního vztahu (u BYOD)





Sophos Secure Email

- Nabízí bezpečné řešení za využití konteinerů pro email, kalendář a kontakty, odděleně od dalších email aplikací
- Maily, kontakty a události jsou synchronizovány pomocí Exchange ActSync.
- Veškerá data v kontejneru jsou šifrována (nabízí i možnost additional Password Protection)
- Dostupný pro iOS, Andriod i Windows Phone

Klíčové funkce Sophos Mobile Security (aplikace pro Android)		**V řízeném módu (SMC) navíc**
Antivirus	„On-demand" sken celého úložiště, plánovaný sken, skenování každé nové aplikace vč. SD karty, detekce potenciálně nechtěných aplikací a aplikací s nízkou reputací, okamžitá karanténa pro malware	Konzole reportuje jaký malware byl nalezen, zda byl odstraněn, okamžité reakce na narušení shody s požadavky
Ztráta a krádež	Alarm, lokace, zamknutí/odemknutí, smazání dat i vzdáleně, detekce výměny SIM karty	Provádí všechny akce z konzole a sleduje výsledek
Bezpečnostní poradce	Kontrola zdrojů aplikací, USB debugging, uzamykání obrazovky, šifrování zařízení, NFC, Bluetooth	Zapracovává kterékoli z těchto nastavení do bezpečnostních politiky, kontroluje vývoj v reportech, přijímá varování o důležitých událostech
Ochrana aplikací	Přidává další úroveň ochrany pro důležité aplikace a nastavení pro zabránění manipulace. Definuje dobu odkladu	Rozšiřuje bezpečnostní politiku na úroveň aplikací, rozpoznává narušení, definuje automatické reakce.
Webový filtr	Rozpoznává nebezpečný obsah, kategorizuje stránky, definuje reakce a whitelisty	Implementuje firemní politiky a reakce v této oblasti
Ochrana proti spamu	Blokuje nechtěné telefonáty a SMS, definuje nechtěné volající nebo typy telefonátů, kontroluje URM v SMS	
Ochrana soukromí	Analyzuje všechny aplikace a varuje před nečekanými náklady, narušení soukromí, přístupem na internet	

COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz