SOPHOS
Security made simple.

Sophos Sandstorm

Pokročilá a snadná next-gen ochrana před hrozbami

Sophos je lídrem bezpečnostního trhu v boji s pokročilým malwarem. Využívá vysoce efektivní technologie, jako je emulace JavaScriptu v reálném čase nebo analýza chování. Zatímco konvenční antimalwarová ochrana je i nadále důležitou součástí první obranné linie, organizace potřebují další nástroje k boji proti současnému cílenému malwaru.

Sophos Sandstorm je bezpečnostní řešení proti pokročilým vytrvalým hrozbám (APT) a zero-day malwaru a doplňuje bezpečnostní produkty společnosti Sophos. Rychle a přesně detekuje, blokuje a reaguje na skryté hrozby, které jiná řešení nezachytí, pomocí výkonné cloudové sandboxingové technologie nové generace.

Hlavní výhody

- Snadná integrace s vaším bezpečnostním řešením Sophos
- Uvedeno do provozu během několika minut
- Chrání před pokročilými vytrvalými hrozbami (APT), neznámým malwarem a cílenými útoky
- Informace o hrozbách pro vaše potřeby
- Komplexní pokrytí platforem
- Granulární reporty zaměřené na incidenty

Pokročilá ochrana před cílenými útoky

Ochrání vaši síť před neznámým malwarem, který by jinak mohl ukrást vaše data. Výkonná cloudová sandboxingová technologie příští generace umožňuje rychle a přesně detekovat, blokovat a reagovat na APT a zero-day hrozby.

Vše je tak snadné

Sophos Sandstorm je plně integrován do vašeho bezpečnostního řešení Sophos. Jednoduše aktualizujte své předplatné, použijte politiky Sandstorm a jste okamžitě chráněni proti cíleným útokům. Vše jednoduše a během několika minut.

Blokování skrytých hrozeb, které jiní nevidí

Detekuje neznámé hrozby, které jsou speciálně navržené tak, aby se vyhnuly první generaci sandboxingových zařízení. Naše komplexní emulace poskytuje nejdetailnější pohled na chování neznámého malwaru a detekuje škodlivé útoky, které jiní prostě nevidí.

Hloubkový forenzní reporting

Analýza incidentů urychluje reakci na pokročilé hrozby a poskytuje vám i důležité informace o možných APT hrozbách. Tento přístup zefektivňuje ochranu a šetří čas.

Komplexní analýza

Zjistí potenciálně podezřelé chování napříč všemi vašimi koncovými uživatelskými zařízeními a kritickou infrastrukturou, včetně vašich operačních systémů (Windows, Mac OS X a Android), fyzických a virtuálních hostitelských strojů, služeb, uživatelů, síťové infrastruktury a webových, e-mailových, souborových a mobilních aplikací. Navíc hrozby bezpečně zneškodní v cloudovém prostředí Sandstorm a izoluje vaše datová centra od nebezpečného malwaru.

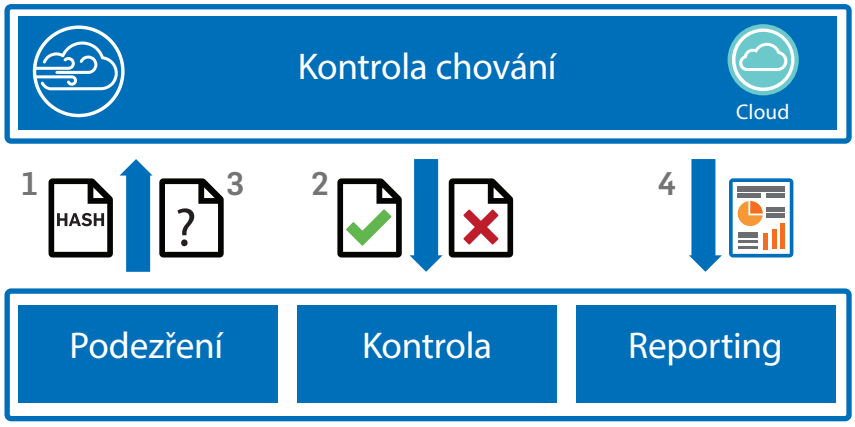
Bleskový výkon

Vaše bezpečnostní řešení Sophos pečlivě předfiltruje provoz, takže Sandstorm už prověřuje jen podezřelé soubory, což zajišťuje minimální vliv na koncové uživatele.

Funkce Sophos Sandstorm

- Plná integrace do vašeho bezpečnostního dashboardu Sophos
- Prověřuje spustitelné soubory a dokumenty obsahující spustitelný obsah
  - Soubory spustitelné ve Windows (včetně .exe, .com a .dll)
  - Wordové dokumenty (včetně .doc, .docx, docm a .rtf)
  - PDF dokumenty
  - Archivy obsahující jakýkoli z výše uvedených typů souborů (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
  - Podporuje více než 20 typů souborů
- Dynamická analýza chování malwaru spouští soubory v reálném prostředí
- Detailní reporty o škodlivých souborech a možnost vytvářet dashboardové soubory
  - Průměrná doba analýzy je méně než 120 sekund
  - Flexibilní uživatelské a skupinové možnosti politik podle typu souboru, výjimek a pokynů k analýze
  - Komplexní pokrytí systémových prostředí, včetně Windows, Mac a Android
  - Podporuje odkazy na jedno stáhnutí

Jak to funguje



1. Bezpečnostní řešení Sophos skenuje soubory všemi běžnými bezpečnostními kontrolami (například hledá malwarové signatury, špatné URL adresy, atd.). Pokud je soubor spustitelný nebo je spustitelný obsah a není stažen z bezpečné webové stránky, soubor je považován za podezřelý. Bezpečnostní řešení Sophos odešle podezřelý souborový hash do Sophos Sandstorm, aby se zjistilo, zda byl již dříve analyzován.
2. Pokud byl hash již dříve analyzován, Sophos Sandstorm předá informace o hrozbě bezpečnostnímu řešení Sophos. Zde je soubor doručen na uživatelské zařízení nebo blokován v závislosti na informacích poskytnutých Sophos Sandstorm.
3. Pokud nebyl hash nikdy dříve detekován, kopie podezřelého souboru je odeslána do Sophos Sandstorm. Zde je soubor spuštěn a je sledováno jeho chování. Jakmile je plná analýza dokončena, Sophos Sandstorm předá informace o hrozbě bezpečnostnímu řešení Sophos. Opět platí, že soubor je doručen na uživatelské zařízení nebo blokován v závislosti na informacích poskytnutých Sophos Sandstorm.
4. Bezpečnostní řešení Sophos využívá detailní informace ze Sophos Sandstorm a vytváří hloubkové forenzní reporty o každém bezpečnostním incidentu.

Vyzkoušejte zdarma

Zaregistrujte si 30denní zkušební provoz na Sophos.com/Sandstorm

Obchodní zastoupení pro východní Evropu
E-mail: salesee@sophos.com

2015.12.9 DS-NA (SM)