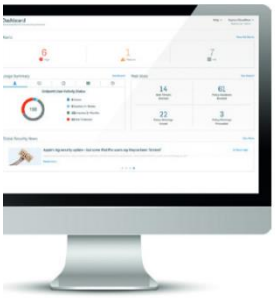
SOPHOS

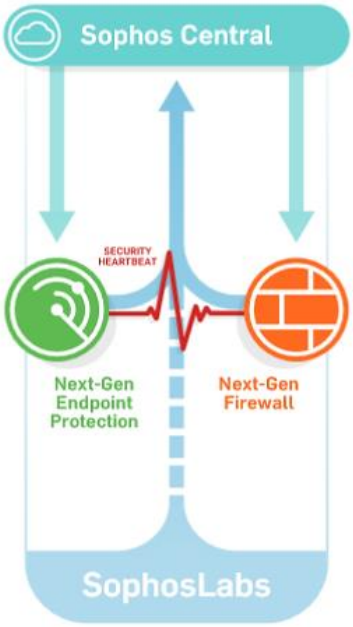
CLOUD PROTECTION

Sophos Central Protection

Vývoj v podnikovém prostředí nabral v posledních letech jasný směr. Přesun informačních systémů do cloudu s sebou přinesl pozitiva ve formě úspory času a peněz, ale přináší i bezpečnostní rizika. Sophos se logicky zaměřil právě i na tuto oblast a vytvořil několik bezpečnostních produktů, které jsou poskytovány jako služba a přinášejí dodatečnou ochranu napříč celým portfoliem Sophos. Všechny cloud produkty mohou být spravovány pomocí Sophos Central, unikátní konzole umožňuje správu všech Sophos produktů jako jsou: ochrana pro koncová zařízení, mobilní zařízení, webová a emailová ochrana, servery a bezdrátové technologie.

Sophos Central Console – centrální konzole, která umožňuje IT administrátorům pohodlně spravovat všechny Sophos produkty přehledně pomocí webového rozhraní. Díky jednotné platformě Sophos nazvané Synchronized Security je možné jednoduše sdílet potřebné informace mezi bezpečnostními řešeními, vytvářet politiky, jednoduše nastavovat všechna zařízení a získat přehled pomocí reportů. Sophos Central je přístupný jak přes webový prohlížeč, tak prostřednictvím mobilního telefonu.





Sophos Synchronized Security with Security Heartbeat

Security Heartbeat nabízí sdílenou inteligenci mezi koncovými stanicemi a XG firewallem (v reálném čase). Pro zastavení čím dál více sofistikovaných útoků je potřeba spolupracující ekosystém. Security Heartbeat tak synchronizuje inteligenci mezi bezpečnostními produkty, které byly dříve provozovány nezávisle, a tím vytváří účelnější ochranu před pokročilým malware a cílenými útoky. Security Heartbeat nabízí přímou komunikaci mezi ochranou koncových stanic a XG firewallem. Jakmile je zjištěno podezřelé chování, Sophos Firewall OS začne komunikovat s podezřelým systémem a Sophos next-generation endpoint protection agent podnikne kroky k zamezení nákazy směrem do firemní sítě a automaticky izoluje nakaženou stanici. Security Heartbeat vyžaduje spolupráci mezi Central Endpoint Protection, či Intercept X a Next Generation XG Firewall.

Live Protection - Zahrnuje Sophos Live Anti-Virus a Sophos Live URL Filtering s možností přímého napojení na SophosLabs. Snižuje nároky na aktualizace lokální databáze signatur a škodlivých stránek.

- **Sophos Live Anti-Virus** – kontroluje podezřelé soubory oproti rozsáhlé databázi v cloudu. Pokud je identifikován potencionálně nebezpečný soubor, je poslán jeho kontrolní součet do LiveProtection Database, kde se ověřuje, zda jde o škodlivý nebo bezpečný soubor. Pokud je soubor označen jako potencionálně nebezpečný, může SophosLabs požádat o zaslání souboru na hlubší analýzu.
- **Sophos Live URL filtering** – porovnává URL adresy oproti databázi, ve které jsou vedeny stránky obsahující malware. Databáze je neustále aktualizována a denně přibývá 20000 až 40000 nově prověřených stránek. Pokud je stránka, na kterou se chce uživatel připojit, identifikována jako škodlivá, je mu automaticky zablokován přístup.

Sophos Intercept X – Next Generation Technology na posílení ochrany proti exploitům

Jedná se o zcela unikátní technologii, která nevyužívá signatur a je určena k ochraně proti pokročilému malware, ransomware, exploitům a cíleným hackerským útokům. Intercept X vychází z principů umělé inteligence tzv. **Machine Learning,** která funguje na bázi neuronové sítě. Poskytuje také grafickou analýzu útoku a pokročilé možnosti odstranění škodlivého kódu z infrastruktury. Lze také rozšířit o technologii **EDR (Endpoint Detection and Response)** poskytující bezpečnostním administrátorům nástroje pro aktivní vyhledávání hrozeb v infrastruktuře. Dokonce lze také celé řešení povýšit na úroveň služby, kdy v rámci zakoupených licencí výrobce poskytuje tým zkušených profesionálů, kteří proaktivně vyhledávají hrozby vyskytující se ve Vaší IT infrastruktuře a navrhují nápravná i preventivní opatření.

Klíčové výhody Intercept X:

- **Pokročilá ochrana proti ransomware**. Jakmile Intercept detekuje útoky typu ransomware, je schopen automaticky útok zastavit ještě dříve, než dojde k šifraci či poškození systému.
- **Anti-exploit technologie blokuje „zero-day" útoky** bez nutnosti potřeby tradičního skenování souborů či updatu signatur.
- **Real-time automatické forenzní zprávy,** které nabízí normativní vodítko k původu nákazy a pomáhá tím tak posílit bezpečnost celé organizace.
- **Grafická analýza útoku** vede k zobrazení všech událostí, které vedly k nákaze.
- Ochrana proti útokům typu AtomBombing, metodám Code Cave a PowerShell exploit

COMGUARD security & networking

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

SOPHOS

CLOUD PROTECTION

Sophos Central Device Encryption

Šifrování souborů spravovatelné pomocí Sophos Central nabízí „always-on" (automaticky šifruje vytvořený obsah) šifrování souborů a dat. Sophos jako první výrobce defaultně nabízí perzistentní, transparentní a proaktivní šifrování pro Windows, Mac, iOS a platformu Android. SafeGuard ve verzi 8 nabízí synchronizované řešení na ochranu dat před malware, cílenými útoky či úniky dat. Sophos nabízí nejlepší praktiky z „always-on" šifrování pro data pocházející z mobilních zařízení, laptopů, desktopů či cloudových aplikací. Jako součást Sophos synchronizované bezpečnostní strategie je Sophos SafeGuard napojen na Endpoint Security a automaticky tak reaguje na bezpečnostní události. Sophos SafeGuard také synchronizuje tyto šifrovací klíče se Sophos Mobile Control a zabezpečuje tím přístup k souborům pro chytré telefony a tablety. Šifrování, dešifrování a přístup k datům je pro uživatele transparentní.

Sophos Sandstorm

Sophos SandStorm je komplementární řešení proti Advanced Persistent Threats (ATP), „Zero-Day" a neznámým útokům. Využívá cloudový next-generation sandbox, který doplňuje stávající bezpečnostní produkty od Sophos o rychlou a přesnou detekci, blokaci a snižuje časovou odezvu na skryté útoky (evasive threats). Analyzuje spustitelné soubory (*.exe, *.com, *.dll a další), Windows dokumenty (*.xls, *.doc(x), *.rtf a další) PDF dokumenty a další. SandStorm podporuje analýzu více než 20 typů souboru. Jedná se o samostatnou licenci pro Sophos Email a Web protection, Cloud Web Gateway, UTM 9.5 a Sophos XG Firewall.

Sophos Clean – malware removal Tool

Technologie Sophos Clean využívá regresní analýzu chování, forenzní inteligenci k objevení a odstranění „zero-day" hrozeb, trojských koní, rootkitů, ransomware a polymorfního malware. Sophos Clean obsahuje funkcionality, které mohou odstranit bezprostřední ohrožení a všechny systémové změny jako je zapisování do registru, obnovení systému apod.

Sophos Central Phish Threat je unikátní cloudová platforma sloužící k posílení nejslabšího článku bezpečnostního řetězce všech organizací – koncového uživatele. Tento simulátor phishingových útoků pomáhá měnit chování a návyky uživatelů pomocí tréninkových phishingových kampaní, jejichž výstupem je přehledný reporting. Celé řešení je spravováno z centrální konzole.

Central Endpoint Protection – Next-Generation ochrana koncových stanic, která proaktivně detekuje a blokuje malware, exploity a „zero-day" útoky. Balíček Central Endpoint Protection obsahuje Anti-malware, Live protection, Web security, Malware removal, HIPS, DLP, Malicious Traffic Detection, Download Reputation, Device Control, Security Heartbeat.

Central Web Gateway – Snadno ovladatelná, globálně-nasaditelná webová brána v cloudu a navržena pro rychlé nasazení a dosažení maximální ochrany webového provozu. Central Web Gateway nabízí jak web filtering tak anti-malware, SSL sken, skenování klíčových slov a reporting

Central Mobile Control - jedná se o Enterprise Mobility Management (EMM) řešení, které pomáhá chránit mobilní zařízení a ochránit firemní data. Verze Standard obsahuje Mobile Device Management (MDM), Mobile Application management (MAM) a Mobile Email Management (MEM). Verze Advanced dále nabízí Mobile Content Management (MCM), Secure Workspace a Secure Email container apps, Mobile Security a Sophos Mobile SDK.

Central Mobile Security – nástroj na ochranu před Malware a dalším hrozbám, určený výhradně pro operační systém Android. Obsahuje Anti-malware, PUA detekci, detekci aplikací s pochybnou reputací, detekci rootkitů a další.

Central Email Protection – díky neustálým aktualizacím ze Sophos Labs udržuje Central Email Gateway stále aktuální ochranu proti malware, phishingu, podvodným stránkám, spamu a dalších hrozeb cílených na uživatele pomocí emailu.

Central Server Protection – jedná se o multiplatformní (Windows, Unix, Linux) ochranu serverových stanic. Nabízí application whitelisting, rozšířený anti-malware engine, Synchronized Security Heartbeat, Data Loss Prevention, Malicious Traffic Detection, Application control, Web Control, Peripheral Control, analýzu chování apod.

Central Wireless – základní uživatelské rozhraní pro administraci pomáhá udržovat přehled v podnikových bezdrátových sítích. Umožní dynamické vytváření sítí, kompletní vizualizaci sítí (i geograficky oddělených).

Sophos Central Firewall Reporting (CFR) – CFR nabízí široké možnosti přizpůsobení historických reportů síťové aktivity, které zabezpečí potřebný vhled do již proběhlých procesů, jejich hlubší pochopení, nastavitelné politiky a pravidla. Díky množství filtrů nabízí lehké a rychlé prohledávání logů z XG firewallu, granulárnost dat v přizpůsobitelných tabulkách a grafech za období až jednoho roku.

COMGUARD
security & networking

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