

Intercept X

Díky nikdy nekončícímu závodu mezi kybernetickými zločinci a bezpečnostními experty zaznamenala ochrana koncových zařízení za posledních 30 let obrovský pokrok. Klasické antivirové řešení, fungující na principu signatur, je ale pouze nutný základ pro ochranu duševního vlastnictví společnosti. Sophos Intercept X je technologie nové generace, která funguje jako doplnění klasické ochrany - efektivně chrání proti Ransomware, Zero-day útokům a dalším pokročilým hrozbám.

Sofistikovaná ochrana proti pokročilému malwaru

Endpoint Protection

Zatímco na světě existuje nespočet druhů malwaru, efektivních způsobů jak doručit tento malware na koncovou stanici jsou pouze desítky. Proto je specializace na přerušení těchto cest velice efektivním způsobem ochrany. Technologie **Exploit prevention** rozpozná všechny nejčastěji zneužívané zranitelnosti v internetových prohlížečích, flash playerech apod. a následně systém ochrání proti jejich zneužití. Proto dokáže zastavit hrozby ještě předtím, než se do systému vůbec dostanou. Díky této technologii Sophos Intercept X dokáže účinně chránit mimo jiné i proti „Zero Day“ útokům a neznámým hrozbám.

Ochrana proti ransomware

Technologie **CryptoGuard** detekuje spontánní škodlivé šifrování dat, ihned po jeho zahájení. Dokonce i v případě, že ověřený systémový proces nebo soubor je zneužit ransomwarem, CryptoGuard dokáže odhalit škodlivou aktivitu a šifrování ihned zastavit. Soubory, které ransomware stihl zašifrovat předtím, než byl zastaven, převede Intercept zpět do nezašifrovaného stavu. Veškerá aktivita CryptoGuardu se děje automaticky a bez interakce koncového uživatele. CryptoGuard dokáže efektivně zastavit nejen šifrování lokálních souborů, ale i souborů uložených na síťových úložištích.

Vyčištění systému od malwaru

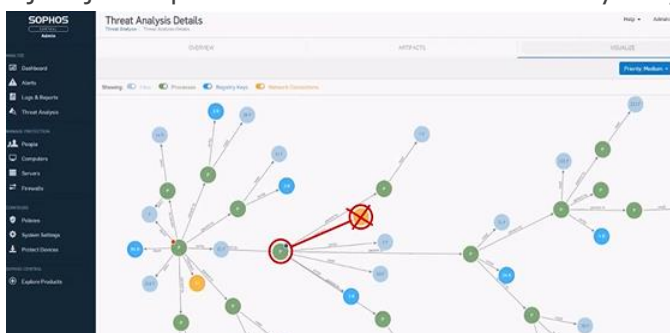
Sophos Clean je nástroj využívající regresní analýzu chování a forenzní inteligenci k objevení a odstranění „zero-day“ hrozeb, trojských koní, rootkitů, ransomware a polymorfního malware. Díky tomu, že Sophos Clean nespolehá pouze na signatury, ale zkoumá podezřelé chování souborů a procesů, dokáže Sophos Clean odhalit i pokročilé hrozby a následně je i trvale odstranit. Sophos Clean také obsahuje funkcionality, které mohou odstranit bezprostřední ohrožení a všechny systémové změny jako je zapisování do registru, obnovení systému apod.

Detekce podezřelého provozu

Pokročilejší malware vyžaduje komunikaci se vzdálenými servery, od kterých získává instrukce a následně jim pak zasílá informace z nakaženého stroje. **Sophos Malicious Traffic Detection** je komponenta, která monitoruje HTTP provoz a hledá náznaky pokusu o spojení se škodlivými URL jako jsou například Command and Control servery. Díky tomuto modulu je docíleno vrstvené ochrany proti ransomware.

Analýza útoku

Nástroj **Root Cause Analysis (RCA)** poskytuje administrátorům detailní přehled infekcí, které se v systému objevily za posledních 90 dní. Grafická analýza útoku pomáhá administrátorům porozumět odkud se infekce do systému dostala, jaké události ji doprovázely a co přesně způsobila, než se jí podařilo odstranit.



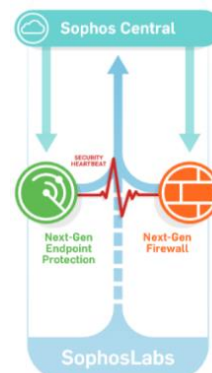
Klíčové vlastnosti Sophos Intercept X

- Ochrana proti „Zero-day“ exploitům
- Technologie **CryptoGuard** chrání proti Ransomware
- Inovativní **Anti-malware, HIPS** a **malicious traffic** detektor
- Web filter pro uživatele na síti i **mimo kancelář**
- **Grafická analýza** původu útoku a jeho průběhu
- Odstranění i **skrytého malwaru** pomocí technologie **Sophos Clean**
- Možnost integrace s firewalley díky **Synchronized Security**
- **Velká výkonost** také na starších systémech
- Jednoduchá a **centralizovaná správa**
- Paralelní fungování s antiviry jiných výrobců

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 i prostřednictvím mobilního telefonu.



Sophos Synchronized Security

Security Heartbeat nabízí sdílenou inteligenci mezi koncovými stanicemi a XG firewallem (v reálném čase). Security Heartbeat synchronizuje inteligenci mezi jednotlivými bezpečnostními produkty, které byly dříve provozovány nezávisle, pomáhá tím vytvářet účelnější ochranu před pokročilým malwarem a cílenými útoky tak, že 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 agent podnikne potřebné kroky proti zanesení nákazy směrem do firemní sítě. Security Heartbeat automaticky izoluje nakaženou stanic.

Integrace se Sophos Central Advanced



Sophos Intercept X je rozšíření aktivní obrany, které funguje paralelně i s antiviry jiných výrobců. Doporučená je však spolupráce s řešením Sophos Central Endpoint Advanced. V případě tohoto nasazení lze vše spravovat z jediné cloudové konzole a je zajištěno kompletní pokrytí všech vektorů útoku.

			Intercept X	Central Endpoint Advanced + Intercept X
		pricing	per user	per user
Prevence	Zabraňuje doručení malwaru na zařízení	Web Security		✓
		Download Reputation		✓
		Web Control / Category-based URL Blocking		✓
		Device Control (např. USB)		✓
		Application control		✓
		Browser Exploit Prevention	✓	✓
Prevence	Zabraňuje spuštění malwaru na zařízení	Anti-Malware File Scanning		✓
		Live Protection		✓
		Pre-execution Behaviour Analysis / HIPS		✓
		Potentially Unwanted Application (PUA) Blocking		✓
		Exploit Prevention	✓	✓
Detekce	Zastavuje běžící hrozbu	Runtime Behavior Analysis / HIPS		✓
		Malicious Traffic Detection (MTD)	✓	✓
		CryptoGuard Ransomware Protection	✓	✓
Reakce	Vyšetřuje rozsah škod a odstraňuje malware	Automated Malware Removal	✓	✓
		Synchronized Security Heartbeat	✓	✓
		Root Cause Analysis	✓	✓
		Sophos Clean	✓	✓