

## 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 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

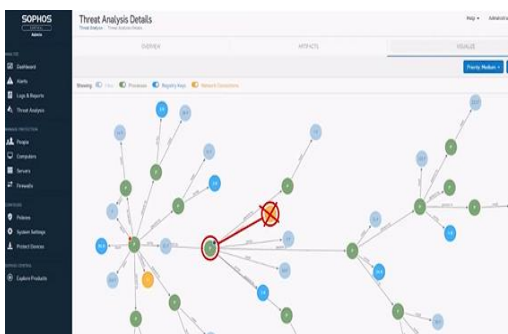
Technologie **CryptoGuard** detekuje spontánní škodlivé šifrování dat, ihned po jeho zahájení. Dokonce i v případě, že ověřený systémový proces nebo soubor je zneužit ransomwarem, CryptoGuard dokáže odhalit škodlivou aktivitu a šifrování ihned zastavit. Soubory, které ransomware stihl zašifrovat předtím, 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 malwaru. 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** chráníci 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 XG firewally díky **Synchronized Security** Jednoduchá a **centralizovaná správa**
- Paralelní fungování s antiviry jiných výrobců

#### Technologie Deep Learning

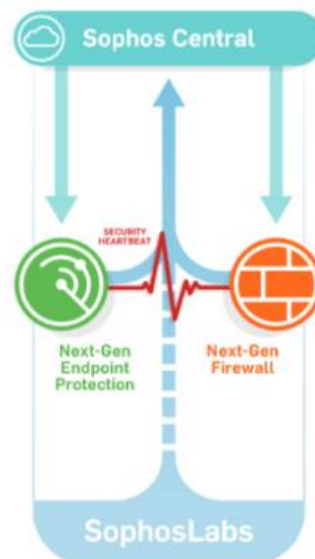
- Pokročilá forma technologie **Machine Learning** fungující na bázi neuronové sítě.
- Zabraňuje mimo jiné také neautorizovanému zvyšování oprávnění procesů
- Ochrana proti útokům typu **AtomBombing** a metodám Code Cave
- Zabraňuje zneužívání aplikací (HTML, PowerShell) pomocí internetového browseru

## Sophos Central Console

Centrální konzole, která umožňuje IT administrátorům pohodlně spravovat všechny Sophos produkty přehledně pomocí webového rozhraní. Díky technologii Sophos Synchronized Security je možné jednoduše sdílet potřebné informace skrz bezpečnostní infrastrukturu, vytvářet politiky, jednoduše nastavovat všechna zařízení a získat přehled pomocí reportů. Sophos Central je přístupný i prostřednictvím mobilního zařízení.

## 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 stanici.



## Endpoint Detection and Response – EDR

EDR je moderní technologie, která administrátorům poskytuje prostředky k včasné identifikaci hrozby a zabránění jejímu dalšímu šíření. Jakmile je soubor označen jako podezřelý, EDR izoluje předmětnou koncovou stanici od okolní sítě tak, aby nedošlo k šíření hrozby dál. Pomocí Sophos Central může administrátor odeslat soubor k prozkoumání do Sophos Labs, přičemž celý tento proces kontroly nezabere více než 2 minuty. Výsledkem zkoumání je přehledná analýza souboru specifikující míru jeho nebezpečí. Pomocí EDR může administrátor zjistit, zdali se podezřelý soubor nevyskytuje také na jiných stanicích v síti a případně tento soubor jednoduše odstranit ze všech stanic spravovaných přes Sophos Central.

## Sophos Managed Threat Response - MTR

Jedná se o pokročilou službu určená k detekci a eliminaci kybernetických hrozeb poskytovaná výrobcem 24x7. Za službou stojí dedikovaný tým špičkových etických hackerů, bezpečnostních analytiků, threat hunterů a dalších zkušených profesionálů. MTR nabízí tzv. Threat Hunting i těch nejkompexnějších a nejsložitějších hrozeb a proaktivní návrhy na změny konfigurací a řešení slabých míst v zabezpečení sítě. Základ MTR tvoří Intercept X s EDR, kde služba provádí pravidelné kontroly nastavení a dává případné doporučení pro změny politik. Nedělnou součástí je také pravidelný reporting, kde jsou přehledně zpracovány všechny potřebné informace pro vedoucí pracovníky. Díky proprietárním investigativním technikám dokáže tým kybernetických odborníků odlišit legitimní uživatelské chování od hackerských taktik a technik. Po potvrzení incidentu dostane zákazník přímé telefonní spojení na dedikovanou osobu, která s ním na řešení incidentu bude pracovat.

## Integrace se Sophos Central Endpoint Protection

Základní balík Sophos Intercept X je rozšíření aktivní obrany, které funguje paralelně i s antiviry jiných výrobců. Doporučená je však spolupráce s řešením Sophos Central Endpoint Protection (dostupné také jako výhodný balík Sophos Central Intercept X Advanced, případně pak další rozšíření s EDR a MTR).

	Sophos Intercept X Advanced	Sophos Intercept X Advanced with EDR	Sophos MTR Standard	Sophos MTR Advanced
Foundational techniques	✓	✓	✓	✓
Deep learning	✓	✓	✓	✓
Anti-exploit	✓	✓	✓	✓
CryptoGuard anti-ransomware	✓	✓	✓	✓
Endpoint detection and response (EDR)		✓	✓	✓
24/7 Monitoring and Response			✓	✓
Lead-driven threat hunting			✓	✓
Advanced lead-less threat hunting				✓