

Ochrana koncových zařízení

Chraňte všechna svá zařízení před malware, spam, ztrátou dat a dalšími hrozbami pomocí jediné licence pro ochranu koncových zařízení. Produkty Sophos pro ochranu koncových stanic jsou licencovány na uživatele bez ohledu na to, kolik zařízení používá.

Hlavní součásti řešení - Endpoint Protection – Advanced

Sophos Antivirus | Jednotný engine, který poskytuje ochranu proti všem druhům malwaru, detekuje viry, spyware, adware, podezřelé soubory, chování rootkitů a potenciálně nebezpečné aplikace. Je napojen na cloudovou technologii Active Protection, která poskytuje filtrování URL adres a anti-virus. Technologie Genotype detekuje a proaktivně blokuje skupiny virů ještě před tím, než je vydána specifická signatura. Dokáže identifikovat malware nebo spam podle jejich chování a extrahovat jejich vzorky, kterým je přiděleno skóre dle závažnosti.



Host Intrusion Prevention (HIPS) | Provádí behaviorální analýzu a skenování souboru ještě před jeho samotným spuštěním. Dále nabízí ochranu proti hrozbám typu „zero-day“ a chrání proti útokům buffer overflow zaměřeným na zranitelnosti operačních systémů nebo aplikací. Dalším stupněm ochrany je detekce podezřelého chování (Suspicious Behavior Detection), která sleduje veškeré systémové procesy a hledá podezřelé akce, které mohou být projevem malwaru (zápis do registrů, kopie souborů, atd.) Přitom lze nastavit zaslání varování na podezřelé procesy nebo jejich blokování.

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 proti rozsáhlé databázi v cloudu. Pokud je identifikován potenciálně nebezpečný soubor, je poslán jeho kontrolní součet do Live Protection Database, kde se ověřuje, zda jde o škodlivý nebo bezpečný soubor. Pokud je soubor označen jako potenciálně nebezpečný, může SophosLabs požádat o zaslání souboru na hlubší analýzu.

> **Sophos Live URL filtering:** provádí porovnávání URL adres oproti databázi, ve které jsou vedeny stránky, které obsahují 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 Client Firewall | Centrálně spravovatelný firewall, který chrání koncové stanice proti síťovým hrozbám a slouží také k vynucení bezpečnostních politik. Poskytuje proaktivní ochranu proti červům, hackerům, nechtěným aplikacím nebo proti komunikaci mezi neautorizovanými aplikacemi. Monitoruje veškeré aktivní porty a uzavírá neaktivní. Dokáže skrýt koncové zařízení, aby nebylo vidět z vnější sítě, a tím zabraňuje hackerům ve skenování stanic a hledání otevřených portů.

Na firewallu lze také zapnout stavovou inspekci, která monitoruje komunikaci mezi pakety, takže pouze autorizované pakety mohou odejít do sítě. Firewall nabízí jednoduchého průvodce nastavením politik a využití dvou předvolené módů (interaktivní a monitorovací). Politiky lze aplikovat na zařízení také dle toho, zda se nachází uvnitř podnikové sítě nebo mimo ni.

Sophos Application Control | Jedná se o součást antivirového engine a nevyžaduje tedy instalaci separátního agenta na zařízení. Zamezuje instalaci aplikací, které představují bezpečnostní či právní hrozby pro společnost. Pro detekci aplikací je využit antivirový on-access nebo on-demand skener, což snižuje nároky na výkon PC. Administrátoři mohou uživatelům povolit pouze specifické aplikace nebo celé kategorie aplikací, jejichž seznam je pravidelně aktualizován a přístupný přes SophosLabs™

Přínosy Sophos Endpoint Protection

- Všechna zařízení chráněná pomocí jediné licence
- Ochrana kdekoli – bez ohledu na to, kde se právě nacházíte
- Komplexní ochrana proti hrozbám – antivirus, správa zařízení, aplikací, dat, síťových a webových přístupů
- BYOD jednoduše – bezpečný přístup k firemním emailům a datům pomocí MDM řešení s intuitivní správou
- Snadná správa
- Licencování na uživatele – bez ohledu na to, kolik zařízení využívá
- Špičkový servis – upgrady, podpora 24/7



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

Sophos Device Control | Device Control umožňuje definovat, jaké počítače mají přístup ke specifickým vyjímatelným zařízením. Řešení dovoluje spravovat přenositelná úložiště, přenositelná šifrovaná úložiště, CD a DVD zařízení, zařízení využívající rozhraní infrared, Wi-fi zařízení a rozhraní bluetooth.

Sophos Web Protection | Poskytuje ochranu uživatelům proti hrozbám na internetu nezávisle na tom, zda jsou uvnitř nebo mimo podnikovou síť. Web LENS technologie (Web Lightweight Endpoint Scanner) není závislá na typu webového prohlížeče a je automaticky instalována jako součást ochrany koncových zařízení pro Windows. Zahrnuje analýzu obsahu staženého webovým prohlížečem pomocí Sophos LSP (Layer Service Protocol), ještě než je obsah prezentován v prohlížeči. Tento proces je nezávislý na použitém prohlížeči a byl přímo testován v prohlížečích Internet Explorer, Firefox, Chrome, Safari a Opera. Stejně jako u jiných modulů integrovaných do koncového zařízení, nemůže být odpojen uživatelem, protože jeho aktivace (deaktivace) běží v chráněném režimu. Sophos LENS je využíván Sophos Live URL Filteringem jak pro odhalení infikovaných webových stránek, tak i pro řízení přístupu k webovým stránkám na základě kategorií.

Sophos Data Loss Prevention | Umožňuje blokovat dokumenty označené jako důvěrné, aby nemohly být zaslány přes email, webový prohlížeč nebo nahrány na šifrované USB disky. Pro zjednodušení implementace politik a identifikace citlivých dat lze využít Content Control List (CCL) umístěný na SophosLabs™. CCL kontroluje data v souborech během pokusů o jejich transfer a v závislosti na politice umožňuje akci blokovat, zaslat událost do Sophos Enterprise Console nebo upozornit uživatele, zda si opravdu přeje odeslat soubor s citlivými údaji. Ve všech případech jsou informace o přenosech zaznamenávány. CCL nabízí širokou škálu předdefinovaných seznamů, které zahrnují čísla kreditních karet, bankovní účty, adresy, telefonní čísla nebo např. směrovací čísla. Pokud není tento seznam dostačující, lze jej snadno pomocí průvodce doplnit o vlastní signatury pro citlivá data.

Sophos Patch Assessment | Slouží k identifikování chybějících záplat systémů a k přiřazení priority v závislosti na tom, jak velké hrozbě mohou zabránit. Aplikování jednotlivých záplat je plně transparentní pro koncové uživatele. Přes Sophos Enterprise Console lze identifikovat veškeré hrozby a zranitelnosti a s nimi souvisejícími záplaty včetně odkazu na stránky Sophos a cve.mitre.org pro každou zranitelnost (Common Vulnerabilities and Exposure (CVE)).

Řešení má minimální dopad na výkon jednotlivých virtuálních strojů. Využívá sdílení paměti RAM v prostředí VMware na úrovni hypervisoru, tím snižuje požadavky na využívání RAM jednotlivých strojů. Pro virtuální prostředí nabízí plnohodnotnou ochranu v podobě antiviru, antispywaru, runtime HIPS, Application Control, Device Control, Data a Web Control, Compliance a Patch assessment. Celé řešení je spravováno pomocí Enterprise Console a nabízí napojení na VMware vShield.

Sophos for Network Storage | Ochrana pro síťová úložiště od výrobců NetApp, EMC nebo Sun. Antivirový skener je umístěn na separátním serveru a provádí kontrolu všech souborů, které jsou na úložiště zaslány přes jednotlivé podporované agenty.

Sophos Mobile Control Advanced | Sophos Mobile Control poskytuje flexibilitu, která umožňuje zaměstnancům pracovat i mimo kancelář bez ohledu na to, jaký typ telefonu používají. Budete mít plnou kontrolu nad tím, kdo přistupuje k firemnímu mailu, díky zabezpečené bráně do Exchange Active, která umožní vstup pouze vyhovujícím zařízením. Budete rovněž schopni zajistit dodržování pravidel, pokud jde o instalování aplikací uživateli. Centrální přehled zařízení zobrazuje model, verzi OS, nainstalované aplikace a mnoho dalších podrobných specifikací spravovaných zařízení.

Virtualization Protection

Sophos nabízí ochranu pro následující platformy:

- > VMware vSphere / ESX, VMware Workstation, VMware View,
- > Microsoft Hyper-V Server,
- > Citrix XenServer, Citrix XenDesktop, Citrix XenApp.



Klíčové vlastnosti Mobile Control Advanced

- Jednotné řešení pro všechny mobilní platformy
- Webová konzole pro správu uživatelských identit
- Vzdálená instalace aplikací a prosazení pravidel
- Propojení se skupinami Active Directory
- Pravidelné ověřování, zda mobilní zařízení vyhovují firemním standardům
- Vzdálená lokalizace, zamykání a vymazání dat

Název balíčku	Endpoint Protection Advanced	Sophos Mobile Control Advanced	Sophos Mobile Control Standard	SafeGuard Disk Encryption Advanced	SafeGuard File Encryption Advanced	Web Protection Advanced	Email Protection Advanced
Enduser Protection Web, Mail and Encryption Bundle	✓		✓	✓		✓	✓
Enduser Protection Web and Mail	✓		✓			✓	✓
Enduser Protection Mail and Encryption	✓		✓	✓			✓
Enduser Protection	✓		✓				
Enduser Protection and Encryption Enterprise	✓	✓		✓	✓		
Enduser protection and mail	✓		✓				✓
Enduser protection and Encryption	✓		✓	✓			
Endpoint protection Advanced and mail	✓						✓
SMC Advanced and Encryption Enterprise		✓		✓	✓		