ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 5.2.0.0

Prevence ztráty dat & správa mobilních zařízení

Vhodná pro sítě všech velikostí a všechna odvětví

DLP pro Windows, Mac a Linux

Chrání celou síť

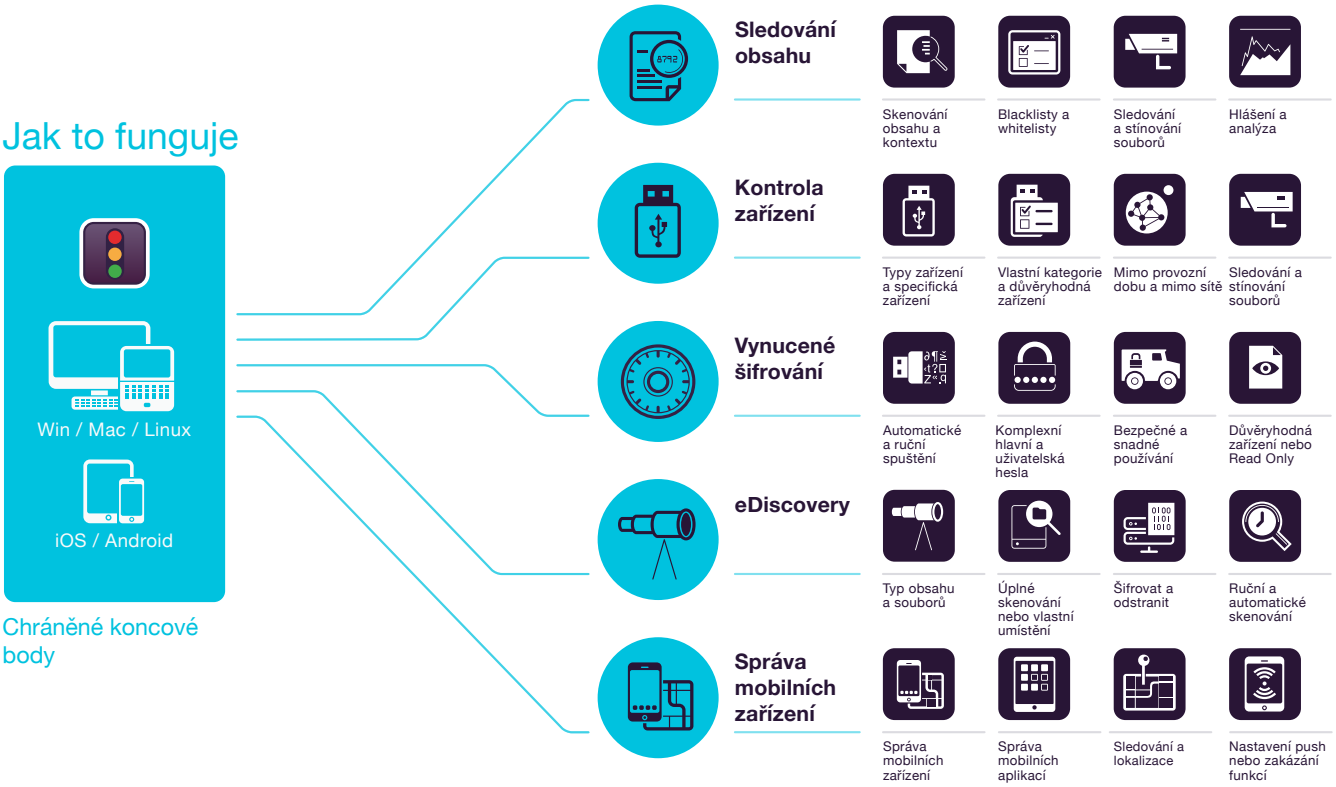
ENDPOINT PROTECTOR

by CoSoSys

Inovativní řešení pro zabezpečení citlivých dat před hrozbami, hrozbami na přenosných paměťových zařízení, v cloudových službách a mobilních zařízení.

Ve světě, ve kterém přenosná, lifestylová zařízení a cloud mění náš způsob práce a života, Endpoint Protector je navržen tak, aby chránil důvěrná data před vnitřními útoky, zatímco udržuje produktivitu a dělá práci snadnější, bezpečnější a zábavnější. Přístup fungující na základě blacklistu a whitelistu umožňuje flexibilitu při tvorbě bezpečnostních zásad. Organizace mají možnost zakázat používání konkrétních vyměnitelných zařízení a datových přenosů prostřednictvím aplikací pro sdílení cloudových souborů a dalších online služeb, skenovat určitá PII, ale mohou povolit přenosy pro specifické URL a jména domén pro určité počítače/uživatele/skupiny, a vyhnout se tak přerušení pracovních úloh.
Dostupná jako hardware nebo jako virtuální zařízení, Endpoint Protector může být zprovozněn během několika minut. Navíc, responzivní rozhraní pro správu umožňuje nastavení zásad a kontrolu hlášení z jakéhokoli zařízení, od stolního počítače až po tablet. Endpoint Protector dramaticky snižuje rizika představovaná vnitřními hrozbami, která by mohla vést k úniku, krádeži nebo jinému způsobu ohrožení dat. Navíc je v souladu se všemi různými pravidly a předpisy

Jak to funguje



Ochrana sledující obsah
pro Windows, macOS a Linux

Průběžná kontrola a monitoring dat, možnost rozhodování, která data můžou či nemůžou společnost opustit přes různé komunikační body. Filtry mohou být nastaveny na Typ souboru, Aplikace, Předdefinovaný a vlastní obsah, Regex, a další.

Kontrola zařízení
pro Windows, macOS a Linux

Sledujte a kontrolujte USB a periferní porty. Nastavujte oprávnění na Zařízení, Uživatele, Počítač, Skupinu nebo Globálně.

Vynucené šifrování
pro Windows a macOS

Automaticky zabezpečte data zkopírovaná na paměťová zařízení USB pomocí šifrování AES 256bit. Fungující croos - platform, pasword - based, snadné k využití a velmi účinné.

eDiscovery
pro Windows, macOS a Linux

Skenujte data na koncových bodech ve zbytku síťové architektury a aplikujte nápravná opatření, jako je šifrování nebo odstranění v případě, že důvěrná data byla identifikována na neoprávněných počítačích.

Správa mobilních zařízení
pro Android, iOS a macOS

Spravujte, kontrolujte a upravujte úroveň zabezpečení na smartphonech a tabletech. Protlačujte nastavení zabezpečení, nastavení sítě, aplikace atd.

Sledování obsahu

pro Windows, macOS a Linux

Emailoví klienti: Outlook / Thunderbird / Lotus Notes • Internetové prohlížeče: Internet Explorer / Firefox /Chrome / Safari • Rychlé posílání zpráv: Skype / Microsoft Communicator / Yahoo Messenger • Cloudové služby & sdílení souborů: Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa • Další aplikace: iTunes /Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer • DALŠÍ

Blacklisty výstupních bodů

Filtry můžete nastavit na základě rozsáhlého seznamu monitorovaných aplikací. Obsah lze monitorovat na vyměnitelných zařízeních USB, síťově sdílených položkách a dalších výstupních bodech.

Blacklisty pro typy souborů

Filtry pro typy souborů můžete využít k blokování dokumentů na základě typu jejich přípony, a to i když tyto byly upraveny některým z uživatelů.

Blacklisty pro předdefinovaný obsah

Filtry můžete vytvořit na základě předem definovaného obsahu, jako jsou čísla kreditních karet, čísla sociálního zabezpečení a mnoho dalších.

Blacklisty pro vlastní obsah

Filtry lze vytvořit také na základě vlastního obsahu, jako jsou klíčová slova a výrazy. Je možné vytvořit Různé blacklistové slovníky.

Blacklisty názvů souborů

Můžete vytvořit filtry založené na názvech souborů. Mohou být nastaveny podle názvu souboru a jeho typu přípony, nebo pouze podle názvu, nebo pouze podle přípony.

Blacklisty a whitelisty umístění souborů

Filtry založené na umístění souborů na místním pevném disku. Mohou být nastaveny tak, aby buď zahrnovaly, nebo vylučovaly podsložky.

Blacklisty pro časté výrazy

Můžete vytvořit vlastní pokročilé filtry, které hledají určitá opakování v datech přenášených přes chráněnou síť.

Whitelisty povolených souborů

Zatímco jsou všechny ostatní pokusy o přenos souborů blokovány, můžete vytvářet whitelisty pro vyhnutí se nadbytku a zvýšení produktivity.

Whitelisting domén & URL

Prosazujte podnikové zásady zabezpečení, ale umožněte zaměstnancům flexibilitu, kterou potřebují ke své práci. Přidejte na whitelist firemní portály a emailové adresy.

Monitorování snímků obrazovky a schránky

Zakažte možnosti snímání obrazovky. Eliminujte datové úniky citlivého obsahu skrze Kopírovat & Vložit / Vyjmout & Vložit a posilte tak zásady zabezpečení dat.

Rozpoznání optických znaků

Kontrolujte obsah fotek a obrázků a odhalte důvěrné informace z naskenovaných dokumentů a jiných podobných souborů.

Sledování a stínování souborů

Zaznamenává všechny přenosy souborů nebo jejich pokusy k různým online aplikacím a dalším výchozím bodům. Uložením kopie souborů získáte jasný přehled o těchto činnostech.

Threshold pro filtry

Definujte, jaký maximální počet porušení bude u přenosu souborů povolen. To platí pro každý typ obsahu nebo součtu všech porušení.

Limit přenosu

Nastavte limit přenosu ve specifickém časovém intervalu. Může být založen na počtu souborů nebo na jejich velikosti. Upozornění emailem na dosažení limitu je k dispozici.

Kontextuální skenování obsahu

Povolte pokročilý inspekční mechanismus pro ještě přesnější detekci citlivého obsahu, jako jsou PII. Kontext je možné upravovat.

Dočasné offline heslo

Dočasné povolení přenosu souborů počítačům odpojeným od sítě. Zajistěte bezpečnost a produktivitu.

Ovládací panely, hlášení a analýza

Monitorujte činnost související s přenosem souborů pomocí silného nástroje pro hlášení a analýzu. Záznamy a hlášení mohou být také exportována do řešení SIEM.

Soulad (GDPR, HIPAA, atd.)

Dodržujte pravidla odvětví a zásady jako PCI DSS, GDPR, HIPAA, atd. Vyhněte se pokutám a jiným předsudkům.

DLP pro tiskárny

Zásady pro místní a síťové tiskárny pro blokování tisku důvěrných dokumentů a pro prevenci ztrát a krádeží dat.

DLP pro tenké klienty

Chraňte data na terminálových serverech a zabraňte ztrátě dat v prostředí tenkých klientů stejně jako v kterémkoli jiném typu sítě.

Kontrola zařízení

pro Windows, macOS a Linux

USB jednotky / Tiskárny / Zařízení Bluetooth / MP3 přehrávače / Externí pevné disky / Vývojové desky / Digitální fotoaparáty / Webkamery / Thunderbolt / PDA / Síťově sdílené položky / FireWire / iPhony / iPady / iPody / Disketové jednotky / Sériový port / Paměťová zařízení PCMCIA / Biometrická zařízení / DALŠÍ

Podrobné nastavení oprávnění
Oprávnění zařízení mohou být nastavena globálně, na skupinu, počítač, uživatele a zařízení. Používejte původní nastavení, nebo si je přizpůsobte dle potřeby.

Typy zařízení a specifické zařízení
Nastavte oprávnění – zakázat, povolit, pouze pro čtení atd. – pro Typy zařízení nebo Specifická zařízení (s použitím VID, PID a Sériového čísla).

Vlastní kategorie
Můžete vytvořit oprávnění na základě kategorií zařízení, což usnadňuje správu zařízení od stejného prodejce.

Zásady mimo provozní dobu
Zásady ovládání zařízení mohou být nastaveny tak, aby platily mimo běžnou provozní dobu. Můžete nastavit začátek & konec pracovní doby.

Zásady mimo produkční síť
Zásady ovládání zařízení mohou být nastaveny tak, aby platily mimo firemní síť. Jejich vynucení funguje na základě názvů domén DNS a IP adres.

Import & Synchronizace Active Directory
Využívejte výhod AD a zjednodušte rozsáhlá zavádění. Udržujte subjekty aktuální s ohledem na síťové skupiny, počítače a uživatele.

Informace o uživatelích a počítačích
Získejte lepší viditelnost díky informacím, jako jsou ID zaměstnanců, Týmy, Poloha, přesné kontaktní údaje a více (IP, MAC adresy, atd.)

Sledování souborů
Zaznamenejte všechny přenosy souborů nebo jejich pokusy k různým paměťovým zařízením USB a mějte jasný přehled o činnosti uživatelů.

Stínování souborů
Uložte kopii souborů přesunutých na ovládaná zařízení a později může být využita k auditu.

Dočasné offline heslo
Dočasné povolení přístupu k zařízení počítačům odpojeným od sítě. Zajistěte bezpečnost a produktivitu.

Vytvoření emailových upozornění
Můžete nastavit předdefinovaná a vlastní emailová upozornění a buďte informováni o těch nejdůležitějších událostech týkajících se užívání zařízení.

Ovládací panel a grafika
Pro rychlý přehled těch nejdůležitějších událostí a statistik jsou k dispozici grafická znázornění a tabulky.

Hlášení a analýza
Monitorujte činnost související s užíváním zařízení pomocí mohutného nástroje pro hlášení a analýzu. Záznamy a hlášení mohou být také exportována.

Přídatné funkce
K dispozici je také mnoho dalších funkcí.
info@endpointprotector.com

Vynucené šifrování

pro Windows a macOS

Vládou schválené šifrování 256bit AES / Anti-manipulační techniky / Integrita aplikací / Posílání zpráv uživatelům / Obnovení do továrního nastavení / Nastavení zásad hesel / další

Vynucené šifrování USB
Autorizujte pouze šifrovaná zařízení USB a zajistěte, že jsou všechna data kopírovaná na vyměnitelná paměťová zařízení automaticky zabezpečena.

Automatické zavedení a pouze pro čtení
K dispozici je jak automatické, tak ruční zavedení. Dokud není šifrování potřebné, můžete nastavit oprávnění pouze pro čtení.

Komplexní hlavní a uživatelská hesla
Komplexnost hesel je nastavitelná dle vaší potřeby. Hlavní heslo zajišťuje plynulost v případech jako je resetování uživatelských hesel.

Přídatné funkce
Šifrování je také dostupné pro cloudové úložiště, místní složky, CD & DVD
info@endpointprotector.com

eDiscovery

pro Windows, macOS a Linux

Typy souborů: Grafické soubory / Soubory Office / Archivní soubory / Soubory programů / Soubory médií / atd. • Předdefinovaný obsah: Kreditní karty / Osobně identifikovatelné informace / Adresy / Sociální sítě / ID / Pasy / Telefonní čísla / DIČ / Čísla zdravotního pojištění / atd. • Vlastní obsah / Název souboru / Časté výrazy / HIPAA / atd.

Šifrování a dešifrování dat

Neměnná fyzicky uložená digitální data obsahující důvěrné informace můžete šifrovat a zamezit tak přístup neautorizovaným zaměstnancům. Dešifrování je také možné.

Odstraňování dat

Dojde-li k jasnému narušení vnitřních bezpečnostních zásad, smažte citlivé informace neprodleně poté, co jsou nalezeny na neoprávněných koncových bodech.

Skenování blacklistů umístění

Na základě předem definovaných umístění můžete vytvářet filtry. Vyhněte se nadbytečnému skenování neměnných fyzicky uložených digitálních dat pomocí cílených inspekcí obsahu.

Automatické skenování

Kromě Čistého a Přírůstkového skenování můžete naplánovat i Automatická skenování – jednorázově nebo opakovaně (každý týden nebo měsíc).

Sledování souborů

Zaznamenejte všechny přenosy souborů nebo jejich pokusy k různým online aplikacím a cloudovým službám a mějte jasný přehled o činnosti uživatelů.

Hlášení a analýza

Monitorujte záznamy o skenování klidových dat a v případě potřeby aplikujte nápravná opatření. Záznamy a hlášení mohou být také exportována do řešení SIEM.

Threshold pro filtry

Definujte, jaký maximální počet porušení bude u přenosu souborů povolen. To platí pro každý typ obsahu nebo součtu všech porušení.

Soulad (GDPR, HIPAA, atd.)

Dodržujte průmyslová pravidla a zásady jako PCI DSS, GDPR, HIPAA, atd. Vyhněte se pokutám a jiným předsudkům.

Integrace SIEM

Využijte produktů Bezpečnostních informací a Správy událostí pomocí externalizace záznamů. Zajistěte bezproblémové využívání bezpečnostních produktů.

Blacklisty pro typy souborů

Filtry pro typy souborů můžete využít k blokování dokumentů na základě typu jejich přípony, a to i když tyto byly upraveny některým z uživatelů.

Blacklisty pro předdefinovaný obsah

Filtry můžete vytvořit na základě předem definovaného obsahu, jako jsou čísla kreditních karet, čísla sociálního zabezpečení a mnoho dalších.

Blacklisty pro vlastní obsah

Filtry lze vytvořit také na základě vlastního obsahu, jako jsou klíčová slova a výrazy. Je možné vytvořit Různé blacklistové slovníky.

Blacklisty názvů souborů

Můžete vytvořit filtry založené na názvech souborů. Mohou být nastaveny podle názvu souboru a jeho typu přípony, nebo pouze podle názvu, nebo pouze podle přípony.

Blacklisty a whitelisty umístění souborů

Filtry založené na umístění souborů na místním pevném disku. Mohou být nastaveny tak, aby buď zahrnovaly, nebo vylučovaly podsložky.

Blacklisty pro regulérní výrazy

Můžete vytvořit vlastní pokročilé filtry, které hledají určitá opakování v datech přenášených přes chráněnou síť.

Whitelisty povolených souborů

Zatímco jsou všechny ostatní pokusy o přenos souborů blokovány, můžete vytvářet whitelisty pro vyhnutí se nadbytku a zvýšení produktivity.

Whitelisting domén & URL

Prosazujte podnikové zásady zabezpečení, ale umožněte zaměstnancům flexibilitu, kterou potřebují ke své práci. Přidejte na whitelist firemní portály a emailové adresy.

Whitelist typu MIME

Vyhněte se nadbytečnému skenování na globální úrovni vyloučením kontroly obsahu pro určité typy MIME.

Přídatné funkce / K dispozici je také mnoho dalších funkcí. / info@endpointprotector.com

Správa mobilních zařízení

pro Android, iOS a macOS

Registrace over-the-air pro iOS & Android

Zařízení je možné registrovat na dálku prostřednictvím SMS, E-mailu, odkazu URL nebo QR kódu. Zvolte si pro vaši síť ten nejvýhodnější způsob.

Hromadná registrace

Pro efektivitu instalačního procesu lze registrovat až 500 smartphonů a tabletů najednou.

Zámek na dálku

Povolte okamžité uzamčení na dálku pro případ jakýchkoli souvisejících incidentů. Vyhněte se ztrátě dat způsobené ztracenými nebo zapomenutými zařízeními.

Sledování & lokalizace

Pozorně sledujte firemní mobilní zařízení a mějte vždy přehled o tom, kde se citlivé údaje vašeho podniku právě nacházejí.

Zákaz vestavěných funkcí

Spravujte povolení pro vestavěné funkce, jako je fotoaparát, a vyhněte se tak narušení a ztrátě citlivých dat.

Přehrání zvuku při hledání ztracených zařízení

Hledejte ztracené mobilní zařízení pomocí přehrávání hlasitého vyzvánění aktivovaného na dálku, dokud ho nenajdete (podporováno pouze pro Android).

Správa mobilních aplikací

Spravujte aplikace v souladu s podnikovými zásadami bezpečnosti. Instalujte okamžitě neplacené i placené aplikace na registrovaná zařízení.

Push nastavení sítě

Push pro síťová nastavení jako e-mail, Wi-Fi a nastavení VPN nebo je zakažte, včetně Bluetooth, nastavení režimu vyzvánění, atd.

Upozornění

K dispozici vám jsou rozšířená přednastavená systémová upozornění, nebo si můžete nastavit vlastní systémová upozornění.

Hlášení a analýza

Monitorujte činnost související s užíváním zařízení pomocí silného nástroje pro hlášení a analýzu. Záznamy a hlášení mohou být také exportována.

Kiosk Mode se Samsung Knox

Uzamkněte nebo omezte přístup zařízení k určitým aplikacím. Zajistěte bezpečnost vašich mobilních zařízení a proměňte je v důvěryhodná zařízení.

Správa macOS

Pro rozšíření funkcí DLP mohou být Macy také registrovány do modulu MDM a využívat výhod přidaných možností správy.

Zesílení hesla

Proaktivní ochrana důležitých podnikových dat uložených na mobilních zařízeních díky vynucení silných bezpečnostních zásad pro hesla.

Vymazání obsahu na dálku

V kritických situacích, kdy lze datovému úniku zabránit jedině vymazáním veškerého obsahu zařízení, tak můžete provést na dálku.

Geofencing

Definujte prostor virtuálního okruhu v zeměpisné oblasti a získejte tak lepší přehled o zásadách MDM, které platí pouze pro specifickou oblast.

iOS omezení

Ujistěte se, že je zařízení využitelné pouze k pracovním účelům. Pokud neodpovídají podnikovým zásadám, zakažte iCloud, Safari, App Store, atd.

Push vCards na Androidu

Přidávejte a používejte push na kontakty na zařízeních Android a ujistěte se tak, že jsou vaše mobilní pracovní síly schopné rychle kontaktovat ty správné lidi.

Monitorování aplikací

Mějte dohled nad tím, jaké aplikace vaši zaměstnanci stahují na svá mobilní zařízení a udržujte tak diskrétní hranici mezi prací a volným časem.

Asset Management

Evidence a inventarizace mobilních zařízení vašeho podniku, co se týče názvů zařízení, typů, modelů, kapacity, verzí operačních systémů, operátorů, IMEI, MAC adres atd.

Vytvoření emailových upozornění

Můžete nastavit předdefinovaná a vlastní emailová upozornění, abyste byli informováni o těch nejdůležitějších událostech týkajících se užívání zařízení.

Ovládací panel a grafika

Pro rychlý přehled těch nejdůležitějších událostí a statistik jsou k dispozici grafická znázornění a tabulky.

Přídatné funkce

K dispozici je také mnoho dalších funkcí.
info@endpointprotector.com

100% flexibilita při implementaci

Vhodné pro všechny typy sítí, naše produkty mohou využívat podnikoví zákazníci, malé a střední podniky a dokonce i domácí uživatelé. Díky architektuře klient-server je snadné je zavést a řídit centrálně prostřednictvím webového rozhraní. Kromě hardwarové a virtuální verze, instance služby Amazon Web Services a Cloudové verze, je tu pro ty, kteří hledají spíše základní funkce, k dispozici také Stand-alone verze.

Endpoint Protector

Ochrana sledující obsah, eDiscovery, Kontrola zařízení a Šifrování jsou k dispozici pro počítače s různými verzemi a distribucemi operačního systému Windows, macOS a Linux. Pro mobilní zařízení s iOS a Android jsou dostupné také Správa mobilních zařízení a Správa mobilních aplikací.

Můj Endpoint Protector

Ochrana sledující obsah, Kontrola zařízení a Šifrování jsou k dispozici pro počítače s operačními systémy Windows a Mac. Pro mobilní zařízení s iOS a Android jsou dostupné Správa mobilních zařízení a Správa mobilních aplikací.

Hardwarové zařízení

Virtuální zařízení

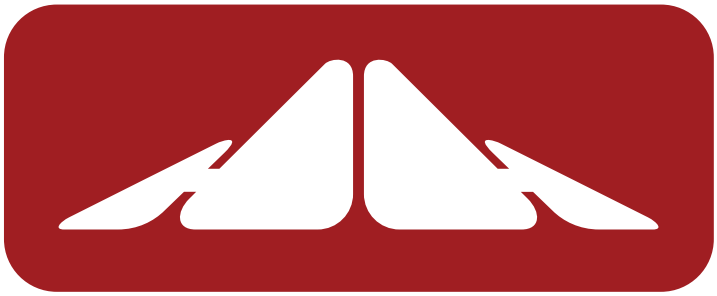
Amazon Instance

Cloudové řešení

Moduly

		Chráněné koncové body				
Windows	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●	
	Windows Server 2003 - 2016	(32/64 bit)	●	●	●	●	
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●	
macOS	macOS 10.13	High Sierra	●	●	●	●	
	macOS 10.12	Sierra	●	●	●	●	
	macOS 10.11	El Capitan	●	●	●	●	
	macOS 10.10	Yosemite	●	●	●	●	
	macOS 10.9	Mavericks	●	●	●	●	
	macOS 10.8	Mountain Lion	●	●	●	●	
	macOS 10.7	Lion	●	●	●	●	
Linux	Ubuntu		●	●	●	n/a	
	OpenSUSE / SUSE		●	●	●	n/a	
	CentOS / RedHat		●	●	●	n/a	
	Fedora		●	●	●	n/a	
iOS	iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9, iOS 10, iOS 11						●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+), Marshmallow (6.0+), Nougat (7.0+), Oreo (8.0+)						●

*Prosím podívejte se na podrobnosti týkající se podporovaných verzí a distribucí na endpointprotector.com/linux



COSOSYS

HQ (Romania)

E-mail sales@cososys.com
Sales +40 264 593 110 / ext. 103
Support +40 264 593 113 / ext. 202

Germany

vertrieb@endpointprotector.de
+49 7541 978 26730
+49 7541 978 26733

Korea

E-mail contact@cososys.co.kr
Sales +82 70 4633 0353
Support +82 20 4633 0354

North America

sales.us@endpointprotector.com
+1 888 271 9349
+1 877 377 6475

IS4 security
Feel Real Trust

IS4 security s.r.o.

Jordánská 391, 198 00 Praha 9
Česká republika

Web: www.is4security.cz
Email: info@is4security.cz
Tel.: +420 272 048 006

Oficiální Partner pro ČR