



Prevenca úniku dát (DLP)

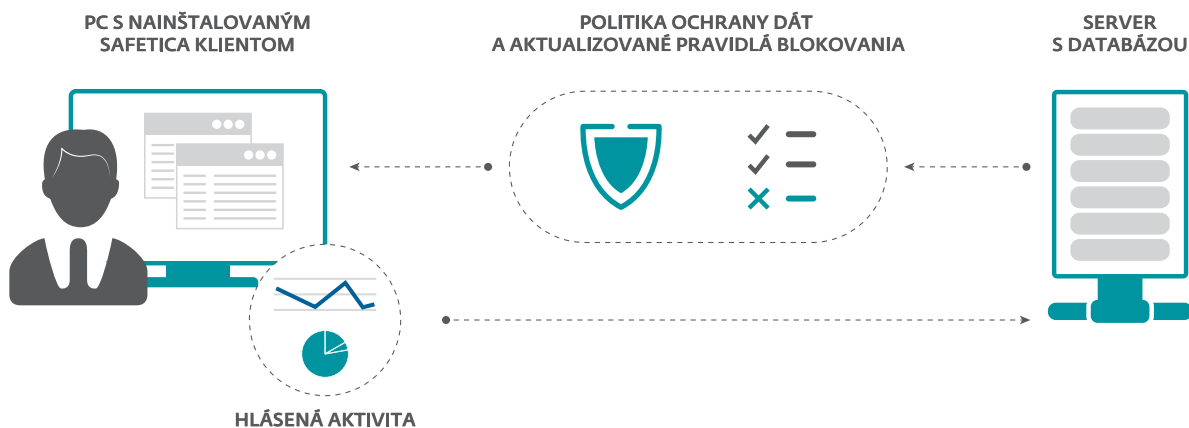


Hlavné výhody

Komplexné DLP riešenie	Pokrýva všetky hlavné cesty úniku dát. Safetica predstavuje DLP riešenie pre koncové zariadenia, ktoré zároveň disponuje schopnosťami prevencie úniku dát v rámci siete.
Rýchle nasadenie	Flexibilný prístup pri blokovaní úniku dát umožňuje najrýchlejšie nasadenie v tejto kategórii produktov.
Vysoká úroveň ochrany pred nedovoleným konaním	Zaisťuje konzistentnú úroveň zabezpečenia aj pri používateľoch s administrátorskými právami.
Ochrana pred únikom dát využitím špecializovaných funkcií	Safetica chráni pred únikom dát s použitím funkcií ako PrintScreen, kopírovanie do schránky, virtuálna tlač, transformácia súboru, archivovanie a šifrovanie.
Univerzálny prístup	Ochrana dát prostredníctvom riešenia Safetica nie je obmedzená len na určité protokoly a aplikácie.
Jasne definované dátové politiky	S funkciou bezpečných zón si stačí zvoliť miesta, z ktorých nesmú uniknúť žiadne citlivé dáta, a Safetica sa postará o všetko ostatné.
Presné sledovanie času	Otvorené neznamená aktívne používané. Výpisy aktivity ukazujú čas, ktorý používatelia skutočne strávili na webových stránkach alebo v aplikáciách.
Automatické výpisy a upozornenia	Safetica vyberá najdôležitejšie zaznamenané informácie a posiela ich súhrnný výpis vybraným adresátom. Kompletné informácie sú v prípade potreby k dispozícii.

Ako to funguje?

Väčšina práce s dátami sa odohráva na koncových pracovných staniciach. Používatelia tu pracujú s dôležitými firemnými dátami, prístupujú na internet, čítajú e-maily, posielajú dokumenty do tlačiarne a pripájajú vymeniteľné médiá. Safetica nasadí na želané koncové pracovné stanice agenta (**Safetica Endpoint Client**) a udržuje s nimi pravidelné spojenie prostredníctvom servera (**Safetica Management Service**). Tento server vytvára databázu informácií o dianí na pracovných staniciach a distribuuje nové bezpečnostné politiky a nariadenia ochrany dát na jednotlivé pracovné stanice.



Bezpečnostný softvér Safetica ponúka kompletné DLP riešenie (zamerané na prevenciu úniku dát), ktoré chráni pred širokou škálou bezpečnostných hrozieb spôsobených ľudským faktorom. Safetica poskytuje ochranu pred úmyselným aj náhodným únikom dát, ohrozujúcim konaním zvnútra spoločnosti, problémami v rámci produktivity, hrozbami spojenými s využívaním súkromných zariadení v pracovnej sieti (BYOD) a mnohými inými.

Filozofia bezpečnostného riešenia Safetica stojí na troch pilieroch: úplnosť, flexibilita a jednoduchosť používania.

Safetica poskytuje komplexné riešenie prevencie úniku dát na podnikovej úrovni, ktoré manažerom ponúka aj kompletný výpis aktivity. Navyše pomáha uplatniť bezpečnostné nariadenia spoločnosti na jednotlivých používateľoch. Safetica prináša v jednom softvérovom balíku širokú ponuku bezpečnostných nástrojov, ktoré by ste inak museli zakúpiť jednotlivo od viacerých poskytovateľov.

Hlavné funkcie

Komplexná prevencia úniku dát	Safetica zabezpečuje všetky potenciálne cesty úniku dát, no napriek tomu je jednoduchá na inštaláciu a ovládanie. Dôkaz o komplexnosti riešenia Safetica nájdete v sekcii Zabezpečenie na koncových zariadeniach.
Sledovanie trendov a produktivity	Upozorní vedenie spoločnosti v prípade náhlych zmien v aktivite zamestnancov a pri dlhodobom poklese produktivity jednotlivých oddelení. Obe zmeny sú indikátorom možného bezpečnostného rizika.
Reportovanie aktivity	Kontrolovaním všetkých používateľských aktivít na znaky potenciálnej hrozby odhaľuje bezpečnostné priestupky na viacerých frontoch ešte pred tým, ako prebehne samotný prenos dát.
Prevencia úniku dát cez e-mail	Zaisťuje, že sa chránené dáta nedostanú do nepovolaných rúk prostredníctvom e-mailu. Zaznamenáva, kam boli citlivé dáta odoslané a uchováva tieto informácie pre budúce použitie.
Kontrola aplikácií s časovými pravidlami	Povoľuje fungovanie vybraným pracovným aplikáciám a ostatné blokuje až do momentu, keď sa zvýši bezpečnosť prostredia. Aplikácie môžu byť sprístupnené aj na určitý obmedzený čas.
Filtrovanie webu	Pomocou filtrovania dopredu vybraných kategórií a kľúčových slov dokáže Safetica jednoducho uplatniť nariadenia o povolenom používaní (AUP) platné pre danú spoločnosť.
Kontrola tlače	Stanovuje obmedzenie na to, čo smie byť vytlačené a kým. Zároveň umožňuje nastaviť limity, a to pre jednotlivých používateľov aj pre celé oddelenia.
Správa zariadení	Zamedzuje zamestnancom pripájať neoprávnené zariadenia. Porty môžu byť sprístupnené pre vybrané zariadenia, prípadne blokované pre všetky zariadenia.
Riadenie šifrovania	Safetica ponúka úplné šifrovanie disku, šifrovanie celých partícií a vytvára lokálne alebo virtuálne disky na bezpečné uchovávanie súborov. Okrem metód zabezpečenia prístupu heslom a kľúčom ponúka Safetica pre dáta opúšťajúce bezpečnú zónu aj zabezpečené cestovné disky a funkciu šifrovania v prípade kopírovania.
Informatívny a testovací mód	Pomáha spoločnostiam progresívne integrovať ochranu dát prostredníctvom testov pre všetky potenciálne situácie, a to bez obmedzenia či spomalenia firemných procesov.
Okamžitá ochrana utajených dát	Chráni nové informácie okamžite po vytvorení alebo prijatí utajeného súboru.
Zjednotená riadiaca konzola	Riadiaca konzola Safetica umožňuje jednoduché riadenie zabezpečenia a reportovanie z jedného miesta. Integruje ochranu firemných dát, reportovanie a politiky blokovania.
Kontrola šifrovaných spojení SSL/HTTPS	Kontroluje a chráni zabezpečené komunikačné linky vrátane webových stránok využívajúcich HTTPS protokol, IM aplikácií so zabezpečeným spojením a zabezpečenej e-mailovej komunikácie.
Nízke celkové náklady súvisiace s prevádzkou (TCO)	Používatelia si nemusia zakúpiť žiadne dodatočné bezpečnostné zariadenia. Safetica agenty na koncových pracovných staniách poskytujú funkciu prevencie úniku dát aj pre firemné siete.
Flexibilné použitie	Vďaka svojmu univerzálnemu prístupu Safetica zabezpečí každú aplikáciu, protokol rýchlych správ (IM) alebo webmailovú službu.



TECHNOLOGICKÁ ALIANCIA

ESET Technologická Aliancia má za cieľ lepšie chrániť firemných zákazníkov pomocou doplnkových riešení pre IT bezpečnosť. Prinášame našim klientom nové možnosti na zaistenie maximálnej bezpečnosti v neustále sa meniacom prostredí. Našu overenú technológiu kombinujeme s ďalšími produktmi, ktoré vo svojej kategórii vynikajú vysokou kvalitou.



Zabezpečenie na koncových zariadeniach

Reportovanie a blokovanie aktivít

- Všetky operácie so súbormi
- Dlhodobé trendy, krátkodobé odchýlky v aktivite
- Webové stránky (podpora všetkých prehliadačov vrátane HTTPS komunikácie) – aktívny a neaktívny čas
- E-mail a webmail (akýkoľvek poskytovateľ)
- Vyhľadávané kľúčové slová (podpora väčšiny prehliadačov, podpora Windows Search)
- Instant messaging (nezávislosť od aplikácie – všetky protokoly)
- Využívanie aplikácií vrátane aktívneho a neaktívneho času
- Virtuálne, lokálne a sieťové tlačiarne
- Aktivita obrazovky (inteligentné zachytenie aktivity)
- Keylogging (zaznamenávanie stlačených klávesov)

Prevenca úniku dát

- Všetky pevné disky, USB, FireWire, SD/MMC/CF karty, SCSI zariadenia
- Prenos súborov po sieti (nezabezpečený i zabezpečený)
- E-mail (protokoly SMTP, POP, IMAP, Microsoft Outlook/MAPI)
- SSL/HTTPS (všetky prehliadače a aplikácie so štandardnou správou certifikátov)
- Funkcie Kopírovať/Vložiť, Skopírovať do schránky, Drag & Drop (presúvanie myšou)
- Virtuálne, lokálne a sieťové tlačiarne
- Bluetooth, IR/LPT/COM/paralelné porty
- CD/DVD/BluRay mechaniky
- Kontrola prístupu aplikácií k súborom

Systémové požiadavky

Safetica klient

- 2,4 GHz dvojjadrový procesor
- 2 GB pamäte RAM
- 10 GB voľného miesta na disku
- Inštalácia na klientskom počítači
- MS Windows 7 a vyšší, 32-bitová a 64-bitová verzia

Safetica server

- 2 GHz dvojjadrový procesor (odporúčame štvorjadrový)
- 4 GB pamäte RAM
- 100 GB voľného miesta na disku
- Inštalácia na aplikačnom serveri alebo dedikovanom serveri (možná je aj virtualizácia)
- Podpora Active Directory
- MS Windows Server 2012 a vyšší, 32-bitová a 64-bitová verzia
- Vyžaduje pripojenie k serveru s MS SQL 2012 R2 a vyšším
- Pri zdieľaní s MS SQL odporúčame minimálne štvorjadrový procesor, 8 GB pamäte RAM a 100 GB voľného miesta na disku

MS SQL (databáza pre server)

- Požiadavky podľa edície MS SQL
- Zdieľaný alebo dedikovaný server, odporúčame minimálne 100 GB voľného miesta na disku
- MS SQL 2012 R2 a vyšší, prípadne MS SQL 2016 Express a vyšší (bezplatná verzia)
- MS SQL 2016 Express je voliteľná súčasť inštalácie
- Pri použití WebSafetica je vyžadovaný MS SQL 2012 a vyšší

Prípady použitia

Zabezpečenie kľúčových firemných informácií

Po tom, ako sa pre všetky chránené dáta vymedzia bezpečné zóny, vykonáva Safetica kontrolu každej interakcie s takýmito súbormi. V prípade nepovolenej operácie ju Safetica zablokuje alebo vykoná inú vopred zvolenú akciu. Medzi týmito akciami môže byť napríklad informovanie bezpečnostného manažéra, zašifrovanie dát či ponúknutie inej, bezpečnej destinácie pre súbor. Dáta na prenosných médiách a počítačoch sú chránené aj mimo priestorov spoločnosti.

Správa vymeniteľných médií

Safetica umožňuje spravovať práva používateľov pri pripájaní vymeniteľných médií do firemných počítačov. Eliminuje sa tak ďalšia cesta možného úniku dát a výrazne sa znižuje počet potrebných zásahov servisného tímu.

Súlad s bezpečnostnými nariadeniami

S nainštalovaným Safetica klientom na firemných počítačoch a s aktivovanou správou politík v riadiacej konzole Safetica bude pre vás jednoduché zaručiť súlad s nariadeniami o používaní citlivých dát.

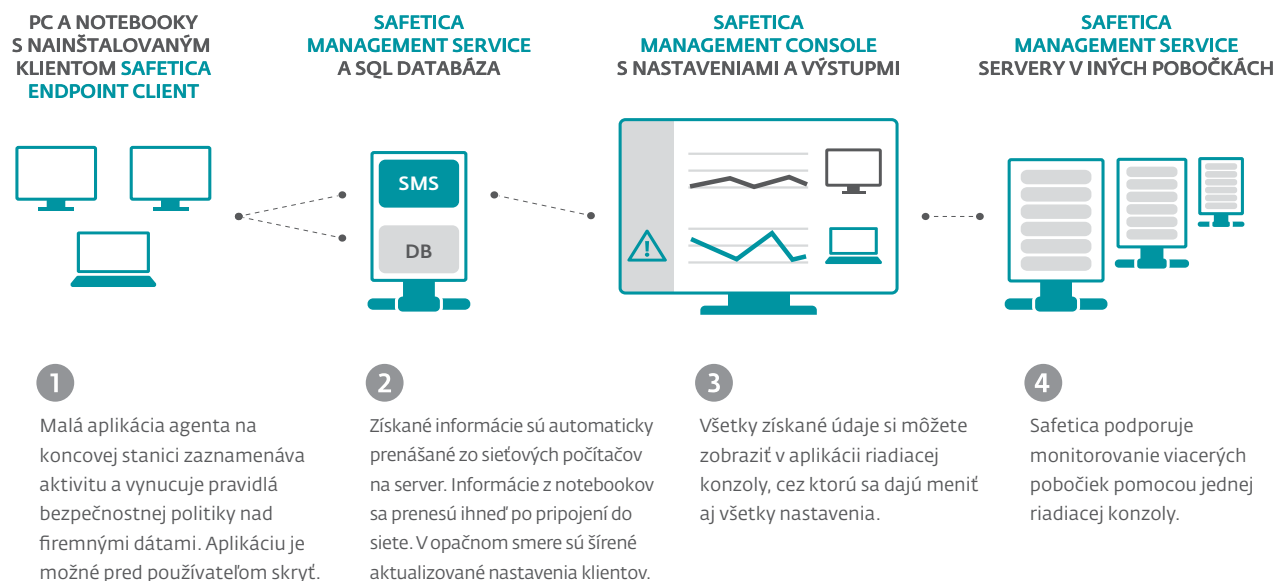
Šifrovanie dát

Safetica ponúka úplné šifrovanie disku, dokáže dohliadať na zašifrované úložisko súborov, spravovať prístupové kľúče a predchádzať ukladaniu dát na nezabezpečených miestach.

Dohľad nad produktivitou

Manažéri môžu prostredníctvom e-mailu dostávať pravidelné súhrnné správy o produktivite vybraných používateľov alebo skupín, a to aj bez toho, aby museli priamo použiť grafické rozhranie riadiacej konzoly Safetica.

Architektúra



Copyright © 1992 – 2018 ESET, spol. s r. o. ESET, ESET logo, ESET android, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, LiveGrid logo alebo iné tu uvedené produkty spoločnosti ESET sú registrovanými ochrannými známkami spoločnosti ESET, spol. s r. o. Windows® je registrovanou ochrannou známkou spoločnosti Microsoft. Ostatné názvy tu uvedených spoločností alebo produktov môžu byť registrovanými ochrannými známkami ich príslušných vlastníkov. Vyrobené v súlade so štandardom ISO 9001:2008.