

Safetico Endpoint Security Datasheet

Každý den je vaše společnost poškozována vlastními zaměstnanci. Předstírají práci, zneužívají firemní zdroje, kradou a ztrácejí citlivé informace. Bezpečnostní software Safetico jako jediný na světě ochrání vaši společnost před všemi hlavními následky selhání vlastních zaměstnanců: Únikem citlivých informací, finančními ztrátami i poškozením dobrého jména. Zároveň preventivně odhaluje rizikové chování zaměstnanců dlouho před tím, než jejich jednání ohrozí společnost.

- Ochráníte vaši společnost proti následkům selhání vlastních zaměstnanců.
- Odhalíte váš chování zaměstnanců poškozující vaši společnost.
- Získáte přehled o pracovní aktivitě a produktivitě zaměstnanců.
- Zajistíte, aby citlivá firemní data zůstala tam, kde mají – uvnitř společnosti.
- Ochráníte zájmy vaší společnosti s ohledem na soukromí vašich zaměstnanců.
- Zajistíte, aby zaměstnanci nakládali s citlivými informacemi pouze požadovaným způsobem.
- Získáte bezpečnostní software, který nenaruší vaše stávající firemní procesy.
- Snadněji dosáhnete shody s průmyslovými standardy, normami a zákony.



Moduly Safetico Endpoint Security

Bezpečnostní software Safetico Endpoint Security se skládá ze tří modulů, které vzájemně spolupracují.

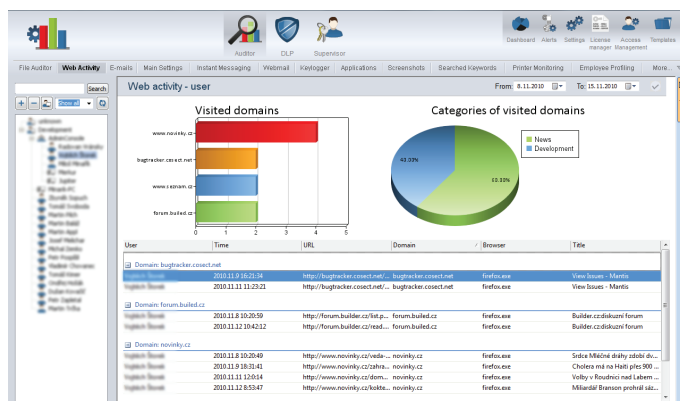
Safetico Endpoint Auditor

Safetico Endpoint Auditor automaticky odhaluje rizikové chování zaměstnanců. Analyzuje jejich činnost a varuje management před hrozcím nebezpečím. Poskytuje přehledné informace o skutečné produktivitě zaměstnanců a odhaluje změny v jejich chování, způsobené například ztrátou motivace nebo lepší nabídkou konkurence. V případě potřeby poskytuje detailní informace o veškeré činnosti zaměstnanců: Které aplikace spouštěli, jaké stránky navštívili, s kým si psali a s jakými soubory pracovali.

Internet Usage Monitoring

Vaši zaměstnanci si v práci vyřizují osobní poštu a navštěvují neproduktivní stránky a sociální sítě. Platíte jim tak zbytečně za práci, kterou nevykonají. Odhalte, které stránky rozptylují vaše zaměstnance nejvíce a kolik času na nich tráví. Získáte tak přehled o tom, kdo a kdy kterou stránku navštívil, kolik rozeslal e-mailů a jak dlouho strávil chatováním.

- Monitoring přístupu na webové stránky.
- Podrobná kategorizace webů.
- Monitoring e-mailů.
- Monitoring webmailů.
- Univerzální záznam IM komunikace.
- Sledování práce se soubory.
- Sledování šifrovaného HTTPS spojení.



Activity Monitoring

Máte přehled o tom, co přesně zaměstnanci dělají na počítači během pracovní doby? Jste si jistí, že skutečně pracují? Sledováním pracovní aktivity zaměstnanců získáte detailní přehled o průběhu jejich pracovní doby. Spolehlivě odhalíte ty, kteří nepracují naplno. Včas se dozvíte o všech nebezpečných aktivitách, které mohou ohrozit vaši společnost a bezpečnost firemních informací.

- Inteligentní záznam obrazovky.
- Kompletní historie zaměstnanecké aktivity.
- Sledování práce se soubory.
- Zachytávání kláves – Keylogger.
- Monitoring vyhledávání.

Printer Monitoring

Spoléhají vaši zaměstnanci na to, že společnost neřeší, kdo si co vytiskne? Víte, kolik citlivých dokumentů vytisknou během jednoho dne a kdo z nich používá firemní tiskárny pro osobní potřebu?

Získejte kompletní přehled o využití firemních tiskáren. Zjistěte, kteří zaměstnanci spotřebují nejvíce tiskového materiálu, odhalte únik citlivých dokumentů a ušetřete významné provozní náklady.

Intelligent Employee Profiling

Zjistěte, kdo jsou vaši zaměstnanci a jaké mají úmysly. Snaží se vaši zaměstnanci opustit společnost, hledají si jinou práci nebo ztratili chuť pracovat? Stráví denně příliš mnoho času nepracovní činností? S pomocí přehledných výstupů a okamžitého varování získáte rychlý přehled o možných personálních a bezpečnostních problémech v dostatečném předstihu.

- Sledování produktivity zaměstnanců.
- Profilování zaměstnanců.
- Automatická upozornění.

Safetica Endpoint Supervisor

Safetica Endpoint Supervisor důsledně dohlíží na to, aby zaměstnanci dělali pouze svou práci. Blokuje nežádoucí činnosti a upozorňuje management na vzniklé problémy. S pomocí Safetica Endpoint Supervisor tak snížíte mzdové náklady, ušetříte firemní prostředky a eliminujete problémy plynoucí z nežádoucí činnosti vašich zaměstnanců.

Application control

Vaši zaměstnanci ohrožují firemní bezpečnost instalací nelegálních a často škodlivých aplikací. Zbavte se pirátských programů, malware, her a další nežádoucích aplikací, které nemají ve firemním prostředí co dělat. Zabraňte vašim zaměstnancům ohrožovat vaši společnost a sami určete, které aplikace jsou vhodné pro plnění jejich pracovních úkolů.

- Blokování aplikací.
- Rozsáhlá databáze aplikací.

	Ředitel	Asistentka	Účetní
Internet			
facebook.com	✓	✓	✗
youtube.com	✓	✗	✗
times.com	✓	✓	✓
Aplikace			
Hledání min	✓	✗	✗
MS Word	✓	✓	✓
Tiskárny			
Kancelář	✓	✗	✗
Vstupní hala	✓	✓	✓

Name	Program	Category	From	To	Logging	Modification	Running	Running other
Adobe Reader	C:\Program ...	-	-	-	✓ Allow	✓ Allow	✓ Allow	✓ Allow
Crashing ap...	C:\Program ...	-	-	-	✗ Deny	✗ Deny	✗ Deny	✗ Deny
IE	C:\Program ...	-	-	-	✗ Deny	✗ Deny	✗ Deny	✗ Deny
Software	C:\Windows	-	12:00	12:30	✗ Deny	✗ Deny	✓ Allow	✗ Deny

Web Control

Vaši zaměstnanci mohou trávit velkou část dne prohlížením webových stránek nesouvisejících s jejich prací. Zabraňte jim v neproduktivní činnosti a zastavte jejich plýtvání vašimi penězi. Pomocí Safetica Endpoint Supervisor spolehlivě zablokujete všechny nežádoucí internetové stránky. Zaměstnanci tak nebudou cítit nutkání krádit si pracovní dobu hraním webových her a návštěvami sociálních sítí.

- Blokování webových stránek dle kategorie a klíčových slov.
- Podrobná kategorizace webů.
- Blokování HTTPS spojení.

Print Control

Omezte zbytečný tisk dokumentů a zabraňte neoprávněnému tisku citlivých dokumentů. Jsou vaši zaměstnanci přesvědčeni, že si mohou v práci volně tisknout pro osobní potřebu? Mějte využití firemních tiskáren pod kontrolou. Dohledem na využití tiskáren snížíte náklady na tisk a zabráníte neoprávněnému tisku citlivých dokumentů.

- Blokování přístupu k tiskárně.
- Blokování tisku vybraných dokumentů ve spojení se Safetica Endpoint DLP.

Safetica Endpoint DLP

Safetica Endpoint DLP ochrání citlivé informace Vaší společnosti před zneužitím pověřenými pracovníky i přístupem třetích osob. Zabraňuje tak finančním ztrátám a poškozování dobrého jména vaší společnosti. Ve spolupráci se Safetica Endpoint Auditor vás informuje i ochrání před nežádoucí činností vašich zaměstnanců dlouho před tím, než se problém projeví.

Device control

Zastavte nekontrolované vynášení citlivých informací ze společnosti. Zabraňte vašim zaměstnancům ukládat si důležité informace na neznámé flash disky, mobilní telefony nebo jiná zařízení. Vyhnete se tak nejen úniku citlivých dat, ale také zabráníte virům a dalším škodlivým aplikacím napadnout vaši síť. Určete, která připojená zařízení mohou vaši zaměstnanci používat pro práci. Veškeré snahy o připojení neschválených zařízení jsou zablokovány a zaznamenány.

- Kontrola nad USB, IrDa, Bluetooth, FireWire, sériovým a paralelním portem.
- Podrobná identifikace USB a Bluetooth zařízení.

Data at Rest Protection

Kdokoliv z vašich zaměstnanců i dalších osob si může odnést citlivé firemní informace, pokud je neukládáte bezpečně. Ochráňte svoji společnost před únikem dat uložených na pracovních stanicích, přenosných počítačích i serverech. Sami určete, kteří zaměstnanci mohou k souborům přistupovat a co s nimi mohou provádět. Safetica Endpoint DLP se také postará o důkladné smazání nepotřebných dat.

- Zabezpečení uložených dat a šifrování disků.
- Datová skartovačka.

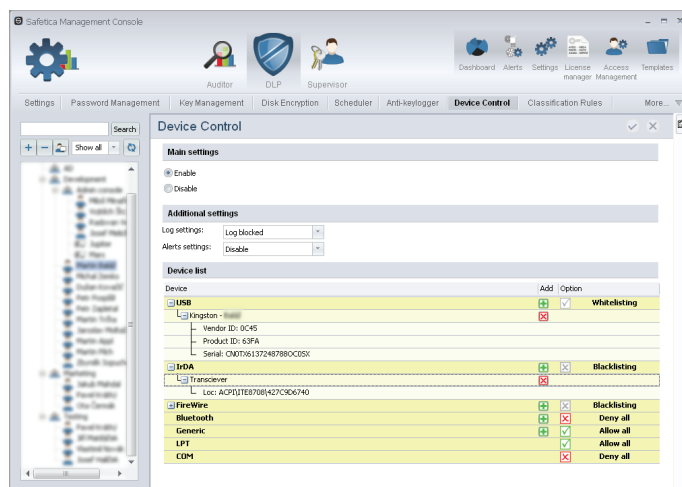
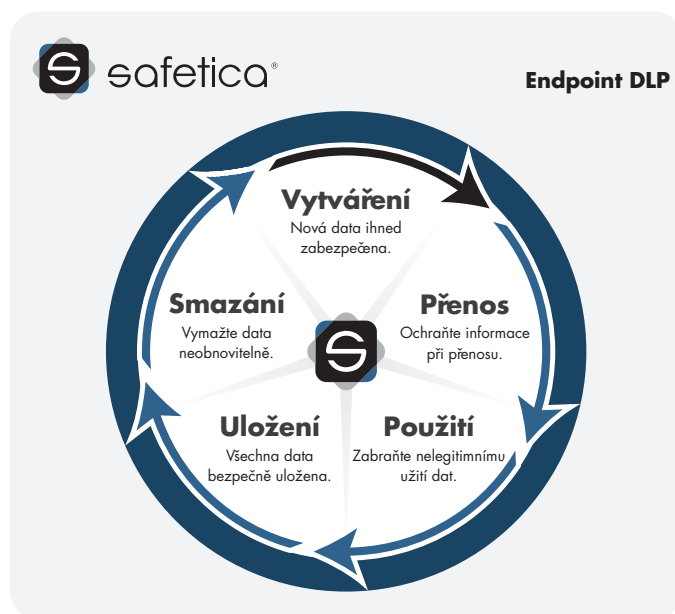
Data in Motion Protection

Ztrácíte přehled v tom, kdo si jaké citlivé údaje odnáší na přenosných zařízeních? Kdo z vašich zaměstnanců už takový disk ztratil nebo mu ukradli přenosný počítač? Ochráňte citlivé firemní informace i v případě, že si je zaměstnanci legitimně berou domů. Přenášená data jsou neustále v bezpečí a nikdo další k nim nemá přístup. Buďte si konečně jistí, že zítra nikdo nenajde na ulici flash disk s důvěrnými informacemi z vaší společnosti.

- Šifrování přenosných disků.
- Nejbezpečnější šifrovací algoritmy.

Data in Use Protection

Vaše citlivé informace jsou nejvíce ohroženy v okamžiku, kdy s nimi pracují zaměstnanci. Pokud k nim mají legitimní přístup, nic jim nebrání zkopírovat si data na flash disk nebo přeposlat e-mailem. Nedovolte vašim zaměstnancům zneužít jejich přístupu k citlivým datům. Zabraňte jim provádět s daty nepovolené operace a pečlivě kontrolujte, zda je skutečně využívají k práci. Zabraňte špionážním aplikacím v zachytávání vašich důvěrných informací při zpracování na klientských stanicích.



- DLP pravidla.
- Anti-KeyLogger.
- Inteligentní klasifikace dat.
- Řízení chování a přístupu aplikací k datům.

Time Efficient Security

Zapomeňte na pomalý a složitý proces integrace bezpečnostního softwaru do stávajících firemních procesů a podnikové sítě. Software Safetica Endpoint Security je navržen tak, aby vás ani vaše zaměstnance nijak neomezoval při práci. Jeho nasazení výrazně ušetří vašemu bezpečnostnímu manažerovi čas strávený nastavováním bezpečnostních politik. Běžní zaměstnanci nebudou provozem bezpečnostního softwaru při své obvyklé práci nijak omezovali. Správci vaší sítě mohou téměř okamžitě nastavit bezpečnostní software do shody se zákony a průmyslovými standardy.

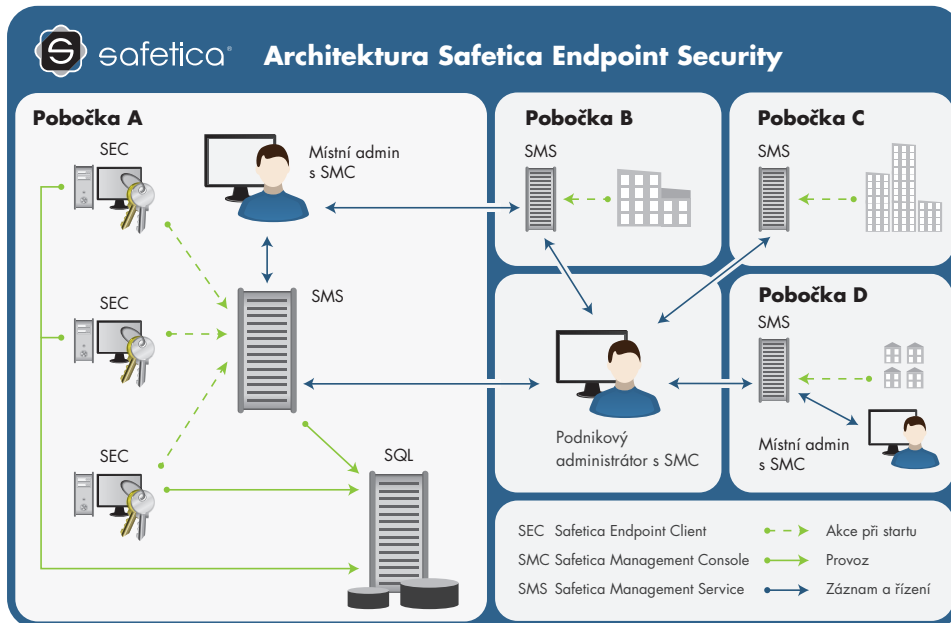
- Snadná aplikace šablon nastavení.
- Plánovač pro opakované úlohy.
- Automatická upozornění.
- Vzdálená správa klientských stanic.
- Detailní řízení přístupu ke správě a dohledu.
- Optimalizace pro nasazení ve velkých sítích.

Endpoint Security Tools

K čemu jsou špičkové bezpečnostní systémy, když zaměstnanci používají jednoduchá hesla nebo si je píšou na papírky? Naučte je dodržovat správné bezpečnostní návyky. Ulehčete práci vaší IT podpoře, která řeší každý den mnoho žádostí o zapomenuté heslo. Umožněte zaměstnancům dále nepotřebná data bezpečně a neobnovitelně smazat a zamknout jejich počítač, když odcházejí na oběd. Zabráníte tak náhodným kolemjdoucím využívat jejich

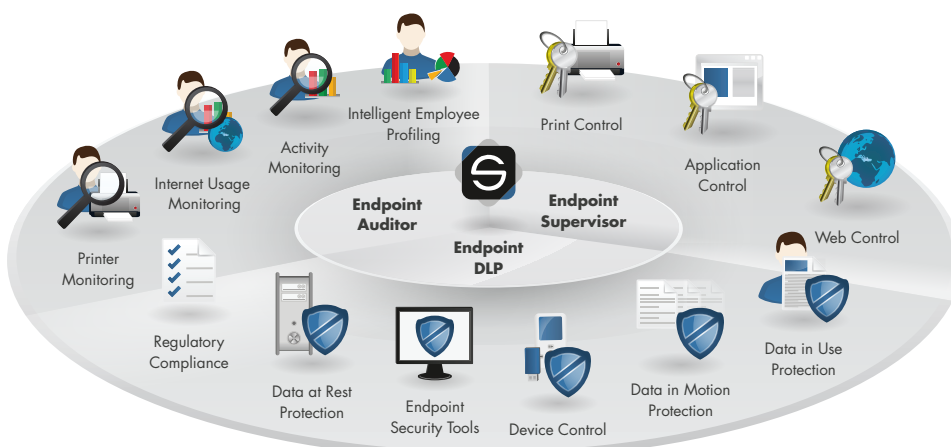
počítač a přistupovat k citlivým firemním informacím.

- Bezpečný správce hesel.
- Podpora běžných typů archivů.
- Generátor hesel.
- PC zámek.
- Bezpečnostní klíče.
- Šifrování přenosných disků.
- Datová skartovačka.
- Anti-keylogger.
- Odeslání zabezpečených dat e-mailem.



Software Safetica Endpoint Security je založen na architektuře klient-server. Na koncových stanicích je spuštěna klientská aplikace (Safetica Endpoint Client – SEC), která komunikuje se serverovou komponentou Safetica Management Service (SMS). Bezpečnostní manažer a nebo správce využívají ke vzdálenému připojení konzoli (Safetica Management Console – SMC).

Data získaná monitoringem jednotlivých koncových stanic jsou ukládána na databázový server. Software je optimalizován pro provoz v rozsáhlých sítích, včetně podpory poboček, a to i mezinárodních.



Licenční model

Software Safetica je licencován pomocí modelu ročního předplatného za využívání software (subscription model). Počet zakoupených licencí určuje počet klientských operačních systémů, na kterých může software Safetica Endpoint Security běžet najednou. Pro rozšíření dříve pořízené a stále platné licence slouží mechanismus rozšiřování licencí.

Shoda se standardy

Safetica Endpoint Security vám pomůže splnit legislativní požadavky a průmyslové standardy, které jsou po vaší společnosti vyžadovány. Nastavení software je snadno přizpůsobitelné pro konkrétní nařízení, regulace a zákony. Umožňuje chránit zájmy vaší společnosti v souladu s místními zákony a s ohledem na soukromí vašich zaměstnanců.

- Snadné dosažení shody se zákony a průmyslovými normami.
- Aktivace vybraných komponent produktu v souladu s příslušnými normami.
- Přednastavené šablony pro konkrétní standardy a zákony.
- Dokumentace pro snadné dosažení shody se standardy.
- Import a export šablon pro rychlé nastavení.

Technické požadavky Safetica Endpoint Client

Doporučené požadavky:

- 1,6 GHz dvoujádrový procesor 32-bit (x86) nebo 64-bit (x64)
- 1 GB paměti RAM
- 2 GB volného místa na pevném disku
- Instalace na klientskou stanicí
- Skrytý agent (volitelně GUI)
- MS Windows XP SP3, Vista, 7, 32-bit i 64-bit
- MSI instalační balíček

Safetica Management Service

Doporučené požadavky:

- 2,4 GHz dvoujádrový procesor 32-bit (x86) nebo 64-bit (x64)
- 2 GB paměti RAM
- 10 GB volného místa na pevném disku
- Sdílený nebo vyhrazený server, pomocí více serverů lze rozložit zátěž
- MS Windows Server 2003 SP2, 2008, 2008 R2, 32-bit i 64-bit
- MS SQL nebo SQLite u menších sítí
- Podpora Active Directory nebo bez AD