KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Technologie šifrování

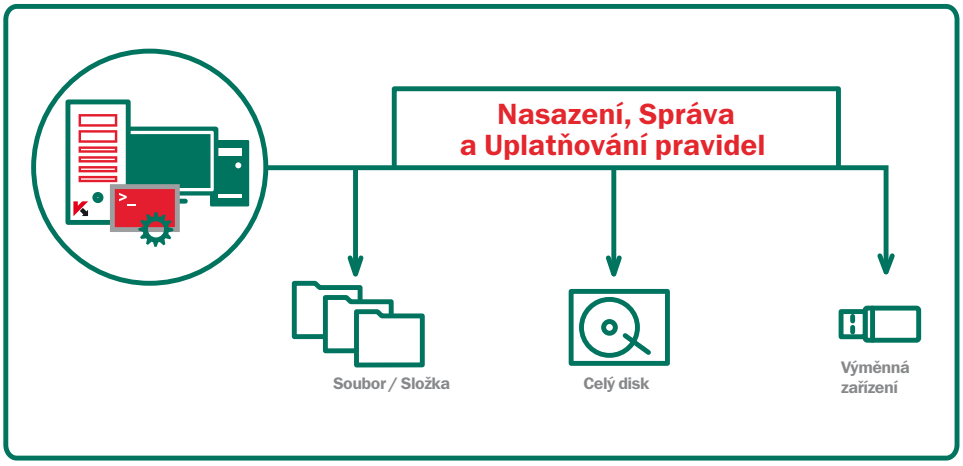
Šifrování zabraňuje neoprávněnému přístupu k datům v případě náhodné ztráty počítače nebo nosiče dat.

Technologie šifrování společnosti Kaspersky Lab chrání cenná data při náhodné ztrátě nebo krádeži zařízení. Toto řešení kombinuje silné šifrování organicky integrované s předními technologiemi na trhu pro ochranu koncových zařízení společnosti Kaspersky. A protože je dodává firma Kaspersky, vyznačuje se snadným zaváděním, správou z centrální správní konsole a použitím jedné sady pravidel.

Chraňte svá data jednoduše a bezpečně šifrovací technologií firmy Kaspersky:

- CELÝ DISK
- NA ÚROVNI SOUBORU/SLOŽKY
- NA VYMĚNITELNÝCH / INTERNÍCH ZAŘÍZENÍCH

SPRÁVA PROSTŘEDNICTVÍM JEDNÉ SPRÁVNÍ KONSOLE.



PRAXÍ PROVĚŘENÁ, BEZPEČNÁ KRYPTOGRAFIE

Firma Kaspersky pro šifrování využívá algoritmus standardu AES s klíčem o délce 256 bitů

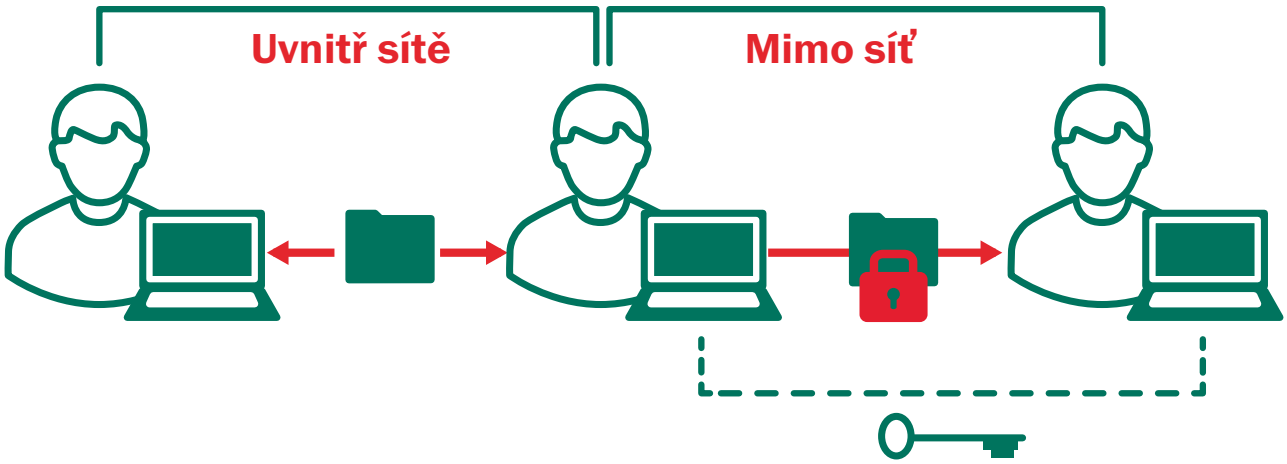
VOLBA ŠIFROVACÍ METODY

Aby byly pokryty všechny možné scénáře použití, je pro ochranu dat uložených na pevných discích i výměnných zařízeních k dispozici jak metoda šifrování na úrovni souborů a složek, tak šifrování celého disku.

TRANSPARENTNOST PRO KONCOVÉ UŽIVATELE

Šifrovací technologie společnosti Kaspersky Lab zůstává transparentní vždy a pro všechny aplikace, včetně nastavování. Tím, že informace jsou chráněny za běhu aplikace, nenarušuje šifrování produktivitu koncových uživatelů. Jedno přihlášení k šifrovanému systému zvyšuje transparentnost pro uživatele.

Při přenosu souboru je šifrování firmy Kaspersky neviditelné a uvnitř sítě transparentní pro uživatele. Data určená externím uživatelům lze ukládat do zásobníků chráněných heslem. Heslo lze příjemci poslat pro dešifrování jiným komunikačním kanálem.



FUNKCE ŠIFROVÁNÍ:

JEDNOTNÝ ZÁKLAD KÓDU
Protože všechny funkce této víceúrovňové ochrany koncových zařízení jsou součástí jednoho softwarového produktu, není nutné zavádět a spravovat samostatná řešení pro ochranu před malwarem, kontrolu koncových zařízení a šifrování.

NAVZÁJEM PROVÁZANÁ A ORGANICKY INTEGROVANÁ PRAVIDLA
Jednotný základ kódu administrátorům umožňuje vytvářet jednotná pravidla. Například: IT může povolit připojení pouze schválených výměnných nosičů dat a také může na stejné zařízení uplatnit pravidlo šifrování (tedy kombinování pravidel pro technologie kontroly zařízení a šifrování).

ZÁKAZNICKY UPRAVITELNÁ NASTAVENÍ PŘÍMO Z INSTALACE
Nastavení pro šifrování jsou předdefinovaná (lze je však zákaznicky upravit) pro běžné složky, jako jsou Dokumenty a Plocha, nové složky, rozšíření jména souboru a skupiny nebo rozšíření jména souboru (např. dokumenty Microsoft Office, archivy e-mailových zpráv).

CENTRÁLNÍ KLÍČ ADMINISTRÁTORA PRO PŘÍPAD MIMOŘÁDNÝCH UDÁLOSTÍ
To je prostředek, který správci zabezpečení umožní dešifrovat data na discích v případě poruchy hardwaru nebo softwaru.

OBNOVENÍ UŽIVATELSKÉHO HESLA
Umožňuje uživateli obnovit heslo pro spuštění před startem systému nebo přistupovat k šifrovaným datům prostřednictvím mechanizmu „výzva/odpověď“.

Způsoby nákupu

Šifrovací technologie Kaspersky se neprodávají samostatně, ale jsou součástí těchto úrovní **Kaspersky Endpoint Security for Business**:

- Endpoint Security, Advanced
- Kaspersky Total Security for Business

NE VŠECHNY FUNKCE JSOU K DISPOZICI NA VŠECH PLATFORMÁCH.
Pro další informace navštivte **www.kaspersky.com**

KESB-ET/Version 0.1/Nov12/Global

KASPERSKY lab