Endpoint Protection & Encryption®

Porozumění a automatizace procesu ochrany důvěrných dat

Důvěrné informace mohou opustit organizaci mnoha způsoby: emailem, přes web, IM, FTP, atd. Eliminace těchto hrozeb je jednou z klíčových oblastí informační bezpečnosti v rámci organizace. Některá data vyžadují šifrování, některá musí být blokována díky své povaze nebo reputaci adresáta. Nastavení a vynucení správných pravidel uvnitř společnosti není triviální záležitostí, a proto nabízí McAfee řešení pro maximální usnadnění této výzvy – McAfee DLP (Data Loss Prevention).

McAfee Host DLP

McAfee Data Loss Prevention Endpoint je centrálně řízené „host-based" řešení ochrany firemních dat před jejich ztrátou a zneužitím. Politiky ochrany datových toků jsou nastaveny přes McAfee ePolicy Orchestrator konzoly a automaticky propagovány na koncové stanice skrze infrastrukturu MS Active Directory, Novell NDS nebo PKI. Každé porušení těchto zásad ze strany koncových uživatelů je monitorováno a preventivně regulováno v reálném čase, přičemž bezpečnostní politiky jsou kontinuálně prosazovány na úrovni koncových stanic i v případě, kdy je koncová stanice odpojena od LAN společnosti. Poté, co se stanice opět připojí do vnitřní sítě, jsou události postoupeny reportovacímu serveru.

Klíčové charakteristiky

- Možnost integrace s Threat Intelligence Exchange a Data Exchange Layer pro lepší viditelnost a real-time monitoring.
- **Možnost nasazení na Windows servery a virtuální desktopy.**
- Napomáhá chránit integritu dobrého jména společnosti.
- Preventivně brání hrozbám ztrát dat ještě před jejich vznikem.
- Redukuje riziko ztráty a zneužití dat vyplývající ze zranitelností na koncových stanicích.
- Poskytuje vedení úplnou transparentní kontrolu nad datovými toky.
- Snadno se nasazuje do stávající IT infrastruktury.
- Pokročilé možnosti ochrany: Vynucení fingerprinting, klasifikace a označování souborů s cílem zabezpečit citlivá data a ochránit tím tak kritické informace a intelektuální vlastnictví.
- Prosazuje mnohostranné, vysoce flexibilní politiky s možností využití sofistikovaných předvoleb pro shodu se standardy.

Ztráta zákaznických & citlivých dat

- Záznamy o kreditních kartách
- Osobní data zaměstnanců a zákazníků
- Finanční data

Ztráty intelektuálního vlastnictví

- Patenty
- Zdrojové kódy
- Obchodní informace

Shoda se standardy

- HIPAA
- EU Data Protection Directive
- SOX
- GLBA
- SB 1386
- Basel II

Klasifikace citlivých dat

Řešení McAfee Data Loss Prevention Endpoint implementuje patentovaný algoritmus klasifikace obsahu, který analyzuje jak strukturovaná, tak nestrukturovaná data. Klasifikace může být například založena na umístění dokumentu na file serverech, dle klíčových slov a regulárních výrazů nebo dle aplikací, ve kterých byla data vytvořena. Po klasifikování a označkování, zůstává označení spojeno s těmito daty po celou dobu jejich životního cyklu, samozřejmě včetně změn. Tato procedura umožňuje přesné vystopování citlivých dat nezávisle na tom, jaké změny v dokumentech či jejich derivátech byly provedeny.

McAfee Network DLP

DLP Discover

McAfee Network DLP napomáhá organizacím chránit se proti únikům dat. Na rozdíl od řešení jiných výrobců, které od zákazníků očekávají informace o tom, co mají chránit, McAfee Network DLP přináší komplexní pokrytí pro zjevně důvěrná data a usnadňuje odhalit data, jejichž závažnost není ihned zřejmá.

DLP Monitor

McAfee Network DLP Monitor sbírá, stopuje a reportuje informace o datech přenášených v rámci sítě v reálném čase. Zároveň poznává, jaké informace se jakým způsobem přenáší mezi uživateli i vnějšími subjekty. Díky výkonné specializované appliance, která unikátním způsobem detekuje více než 300 typů obsahu na jakémkoli portu či protokolu, pomáhá odhalit hrozby úniku dat a provézt příslušnou akci. Navíc umí upozorňovat uživatele a vzdělávat je v oblasti ochrany důvěrných informací.

DLP Discover	Napomáhá nalézt, vyhodnotit a klasifikovat citlivé informace.
DLP Monitor	Pasivně monitoruje všechen síťový provoz, analyzuje jeho obsah a reportuje události, které mohou způsobit ztrátu dat.
DLP Prevent	Na síťové úrovni blokuje aktivity, které mohou vést ke ztrátě důvěrných informací.

McAfee Network DLP napomáhá organizacím automatizovat proces ochrany jejich dat.

Identifikace a náprava rizikových procesů.

Identifikace a prevence neúmyslných úniků dat.

Poskytování mechanismů pro udržování shody s bezpečnostní politikou, standardy a pro audit.

DLP Prevent

McAfee Network DLP Prevent aplikuje a vynucuje politiky pro informace odcházející přes email, webmail, Instant Messaging, „wikis", blogy, portály, HTTP/HTTPS a FTP díky integraci Message Transfer Agentů (MTA) využívajících SMTP nebo ICAP-kompatibilní proxy. V případě narušení bezpečnostních politik umožňuje aplikovat množství akcí, jako je šifrování, blokace, přesměrování, umístění do karantény a mnoho dalších. Tím zaručuje stálou shodu s bezpečnostními politikami organizace i s oborovými standardy v rámci ochrany důvěrných dat.

COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

Endpoint Protection & Encryption®

Bezprecedentní ochrana citlivých informací

Skupina produktů McAfee Endpoint Encryption poskytuje bezprecedentní ochranu důležitých informací, čímž pomáhá organizacím zamezovat únikům důvěrných dat a chránit integritu hlavních činností společnosti. Řešení je výjimečné svou komplexností z hlediska pokrytí všech forem šifrování na koncových zařízeních, které kontinuálně chrání data na pracovní stanici, notebooku či ve sdílených souborech a složkách. Důležitá je rovněž podpora vynucení centrální bezpečnostní politiky organizace a zároveň vyhovění oborovým standardům.

Řešení	Stručná charakteristika
McAfee Drive Encryption	• Šifrování celých disků na noteboocích a mobilních zařízeních chrání preventivně citlivá data před krádeží, zejména formou zcizení samotného zařízení. • Zajišťuje robustní kontrolu přístupu díky autentizaci před bootováním. • Přináší transparentní šifrování bez narušení práce uživatele či zpomalení systémů. • Zaručuje konzistentní ochranu na všech zařízeních. • Vynutitelnost politiky společnosti. • Náhradní přihlášení při ztrátě hesla. • Autentizace pomocí libovolné kombinace hesla, smartkarty (tokeny) a biometriky. • Centrální správa přes **McAfee ePO** dovolující propojení s ostatními produkty
McAfee File & Removable Media Protection	• File&Removable Media Protection automaticky chrání v rámci organizace sdílené / soubory a složky. • Zabraňuje neautorizovanému přístupu k informacím na PC, noteboocích, síťových serverech a přenosných médiích. • Poskytuje mechanismus sdílení klíčů, což umožňuje uživatelům sdílet bezpečný přístup. • Vynucení šifrování při nahrávání dat na externí zařízení (přenosné disky, optická média). • Spolupráce s McAfee Data Loss Prevention Endpoint. • Podporuje virtuálně neomezený počet uživatelů. • Jednoduchá revokace klíčů • Jednoduchá správa práv uživatelů přes **McAfee ePO**.
Management of Native Encryption	• Chrání data pomocí nativního šifrování Apple FileVault pro MAC PC a Microsoft nativní šifrování BitLocker pro MS Windows. • Přímo přes ePO lze spravovat všechny verze OSX X(Mountain Lion, Mavericks, Yosemite a El Capitain) podporující FileVault a verze Windows (7, 8 a 10), které podporují Microsoft BitLocker • Nabízí kompatibilitu s OS X patch, upgrady a firmware updaty vydaných společností Apple • Nabízí single-sign-on z FileVault prebootovacího prostředí přímo do OS X. • Umožní upgrade z jedné verze na druhou, bez nutnosti dešifrovat a zase zašifrovat disk. • Spravuje BitLockeer na Win 7, 8 a 10 přímo z ePO, bez nutnosti Microsoft BitLocker Management and Administration server (MBAM) • Integrace s centrální správou **McAfee ePO**.

Výhody McAfee Endpoint Encryption

- **Prověřené a stabilní řešení,** podporuje i starší verze operačních systémů.
- Má **centrální nástroje pro reporting a vynucování politik** – uživatel s administrátorským oprávněním si na svém stroji nemůže disk svévolně dešifrovat.
- Eliminuje chyby jiných řešení, které nakládají chybně s recovery informacemi tak, že jsou ukládány lokálně i do Active Directory nezašifrovaně a tedy přístupné bez ochrany.
- McAfee šifruje celý disk a pre-boot, **podporuje autentizační tokeny a smartkarty bez omezení**, jiní výrobci často vyžadují ponechat část disku dešifrovanou!
- Nabízí **audit administrátorů** tak, aby nemohli jednoduše získat klíče k šifrovaným datům (včetně univerzálního klíče pro společnost) a použít je kdykoliv v budoucnu. To jiné nástroje často nenabízejí.
- **Obnova dat i při použití čipu Trusted Platform Module** (ten je obsažen ve většině vyšších řad notebooků) – nevyžaduje fyzický přístup k notebooku.
- McAfee je robustní řešení pro ochranu dat, což dokazují i certifikace **FIPS 140-2 a Common Criteria (Level 4).** Disponuje ochranou proti zneužití dat vlastními administrátory, tím se odlišuje od klasických oprávnění k souborům na úrovni souborového systému!

COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz