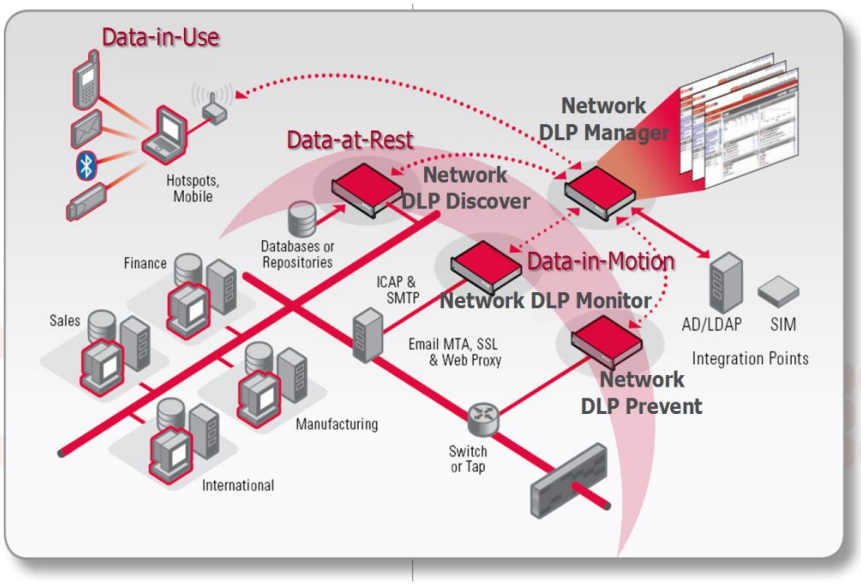
McAfee Network DLP

Porozumění a automatizace procesu ochrany důvěrných dat

Riziko kompromitace dat je a bude neustále přítomné. Čím více lidí sdílí informace elektronicky, tím větší je např. riziko, že někdo úmyslně či neúmyslně pošle důvěrné informace neoprávněné osobě. Ty však mohou nechtěně 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 McAfee nabízí řešení pro maximální usnadnění této výzvy – McAfee DLP (Data Loss Prevention).

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.



Identifikace a náprava rizikových procesů.

Identifikace a prevence neúmyslných úniků dat.

Poskytování mechanismů pro udržování shody s bezpečnostní politikou a standardy.

Centrální správa pomocí jediné konzole McAfee ePolicy Orchestrator® (ePO™) lze spravovat **DLP Endpoint** i **DLP Network**.

Jednotné nastavení politik u network i endpoint DLP řešení.

Podpota Mac OS X vč. Mac OS Sierra.

DLP Discover

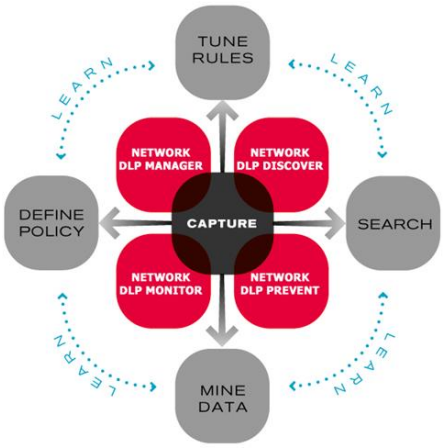
McAfee DLP napomáhá organizacím chránit se proti únikům dat. Na rozdíl od řešení jiných výrobců, které od zákazníků očekávají informace o tom, co mají chránit, McAfee Network DLP přináší komplexní pokrytí pro zjevně důvěrná data a usnadňuje odhalit data, jejichž závažnost není ihned zřejmá.

DLP Monitor

McAfee 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 Prevent

McAfee DLP Prevent aplikuje a vynucuje politiky pro informace odcházející přes email, webmail, EAS (Exchange ActiveSync), Instant Messaging, „wikis", blogy, portály, HTTP/HTTPS a FTP díky integraci Message Transfer Agentů (MTA) využívajících SMTP nebo ICAP-kompatibilní proxy (viz obrázek). **DLP Prevent for mobile** navíc skenuje obsah emailů, které odchází nebo přichází na mobilní zařízení. 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.



McAfee DLP v Leader kvadrantu Gartnera

Gartner

Závěry Gartnera:

- Integrace s McAfee Web Gateway podporuje dešifraci a opětovnou šifraci webového provozu včetně emailových služeb a cloudových produktů
- Unikátní schopnost napomoci rozpoznat citlivá data.
- Integrace s Titus či Boldon James pro klasifikaci dat.
- Výhodou je samostatná monitorovací appliance (McAfee DLP Monitor).

COMGUARD security & networking

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

McAfee DLP Endpoint

Chrání důvěrné informace před jejich neoprávněným užitím

McAfee® Data Loss Prevention Endpoint systematicky monitoruje a chrání informace před jejich neoprávněným užitím vlastními uživateli. Tímto způsobem pokrývá a zabezpečuje síťovou komunikaci (email, webmail, Instant Messaging, atd.), fyzická zařízení (tiskárny, USB zařízení aj.), peer-to-peer aplikace, trojské koně, červy, viry atp. Všechny pokusy o neautorizované přesunutí chráněných dat jsou monitorovány, reportovány a v případě potřeby blokovány – vždy na základě bezpečnostních politik společnosti.

Klíčové charakteristiky

- ✓ Monitoring i restrikce v reálném čase nad všemi uživatelskými aktivitami
- ✓ Sdílené politiky s DLP Discover appliancí (nástroj pro klasifikaci citlivých informací)
- ✓ Řízení souborů při ukládání na cloudové služby jako jsou OneDrive, Office 365, apod.
- ✓ **Možnost nasazení na Windows servery a virtuální desktopy**
- ✓ Pokročilý reporting incidentů a monitoring se sběrem důležitých dat pro analýzu
- ✓ Návaznost na uživatele či uživatelské skupiny a související politiky DLP
- ✓ Nabízí zpětnou vazbu pomocí pop-up výukového modulu.
- ✓ Centrální správa pomocí jediné konzole McAfee ePolicy Orchestrator® (ePO™)
- ✓ Prosazuje mnohostranné, vysoce flexibilní politiky s možností využití sofistikovaných předvoleb pro shodu se standardy (jednotné nastavení u network i endpoint řešení).
- ✓ Možnost nastavení manuální klasifikace souborů.

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

- ISO 27001
- EU Data Protection Directive
- SOX, HIPAA
- GLBA
- SB 1386
- Basel II

Centrální správa koncových stanic

McAfee Data Loss Prevention Endpoint je centrálně řízené řešení ochrany firemních dat před jejich ztrátou a zneužitím. Politiky ochrany datových toků jsou nastaveny přes McAfee ePolicy Orcheatrator konzolu a automaticky distribuovány 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. Po opětovném připojení jsou události předány reportovacímu serveru.

Klasifikace citlivých dat

Řešení 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 souborových serverech, dle klíčových slov a regulárních výrazů **nebo dle aplikací, ve kterých byla data vytvořena**.

Manuální tagování

Tato funkcionalita umožňuje klasifikovat soubory přímo koncovým uživatelem, což znamená, že klasifikace souboru nemusí být závislá na jeho obsahu. Podle potřeb organizace lze tuto politiku aplikovat plošně na všechny uživatele (každý bude muset nově vytvořenému dokumentu udělit patřičnou klasifikaci), nebo nastavit jako právo pouze administrátorům. Poté, co je obsah klasifikován a označkován, 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 uživatelé provedli.

Prevence ztráty a zneužití dat

Implementovaný soubor reaktivních pravidel je připraven monitorovat a preventivně bránit jakýmkoli porušením politik zacházení s citlivými daty. McAfee Data Loss Prevention Endpoint umožňuje:

- monitorování, analýzu a ochranu před nepovoleným přesouváním dat přes:
  - email, web, IM, cloudové služby
  - neznámé síťové protokoly,
  - vyjímatelná zařízení, tisk, printscreen
  - Aplikace pro sdílení dat, trojské koně, malware,
- monitorování a ochranu před neautorizovaným tiskem dokumentů,
- kontrolu nad fyzickými zařízeními na koncových stanicích (USB, Wi-Fi, Bluetooth, atd.),
- monitorování a ochranu před instalací a užíváním neautorizovaných aplikací.

Průběžné reportování a monitorování

Data Loss Prevention Endpoint využívá integraci s McAfee ePolicy Orchestratorem® (ePO™) a poskytuje tak systémovým administrátorům široké možnosti auditování systému a reportování. Události jsou zobrazovány v reálném čase a obsahují detailní popis každé událostí – porušení bezpečnostních politik. Vysoce flexibilní filtry dovolují rychlé uspořádání událostí dle jejich typu, času a klasifikace dat. Správci mohou také registrovat různé uživatele jako příjemce uživatelsky filtrovaných RSS. Pro úplnost obsahuje také reportování pro výkonné manažery a vedoucí pracovníky.

COMGUARD security & networking

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