McAfee Server Security Suites

Jedno integrované zabezpečení pro datová centra

Mnoho organizací transformuje a optimalizuje svoje datová centra a hledají nyní řešení, jak nejlépe zabezpečit tuto klíčovou část IT. Tradiční schémata ochrany jsou velmi drahá a často nevyhovují rozměrům většiny organizací. Proto společnost McAfee přichází s bezpečnostním balíčkem pro servery, datová úložiště a síťovou bezpečnost, kdy si společnost vybírá ze tří typů licencování a má tak možnost zvolit ideální řešení pro organizaci a optimalizovat tak náklady na bezpečnost svého datového centra.

Hlavní součásti řešení:

- **VirusScan Enterprise** - nejnovější verze antivirového enginu s řadou pokročilých funkcí jako blokování infekce, portu a jména souboru, uzamčení adresářů, prohledávání skriptů aj. Dostupný i pro Linux server
- **Change control** – Identifikuje neautorizované změny systému
- **Application Control** - zajišťuje provozování pouze důvěryhodných aplikací (whitelisting) na serverech a koncových zařízeních a tím snižuje riziko neoprávněného využívání softwaru.
- **MOVE-AV** – hardwarově nenáročné zabezpečení virtuálního prostředí.
- **ePolicy Orchestrator** - centrální bod bezpečnosti LAN, jednotná správa, monitoring a analýza bezpečnosti sítě.

McAfee je největší IT bezpečnostní firmou na světě.

McAfeeVirusScan Enterprise

VirusScan Enterprise reaguje na omezení tradičních antivirových systémů a zastavuje hrozby, i když nejsou signatury aktualizovány. Navíc nabízí prevenci narušení pomocí ochrany proti přetečení vyrovnávací paměti specifických aplikací. Tato inovační technologie rozšiřuje ochranu i na dosud neznámá bezpečnostní rizika, čímž snižuje náklady na řízení odezvy v případě napadení. Hlavní charakteristiky:

- **kompletní ochrana proti PUP a Rootkitům,**
- **detekce neznámých útoků v čase nula,**
- **proaktivní ochrana napojená na systém globální inteligence – technologie Artemis,**
- **On-Access skenování,**
- **Buffer Overflow ochrana a blokování portů,**
- **prohledávání skriptů (Java a Visual Basic),**
- **trasování a blokování zdroje infekce.**

McAfee Application control

Zajišťuje provozování pouze důvěryhodných aplikací na serverech a koncových bodech. Což prakticky funguje tak, že na daný stroj nainstalujeme všechny potřebné aplikace a následně stroj uzamkneme. Poté již není možno spustit jinou aplikaci než nainstalovanou. To snižuje riziko neoprávněného užívání softwaru, zvyšuje kontrolu a bezpečnost koncových bodů. V neposlední řadě představuje účinnou hráz proti všem druhům škodlivých kódů, jelikož se nemají jak spustit! Pro hladký chod systému je využíváno unikátní technologie McAfee Application Whitelisting.

Klíčové výhody Application Control

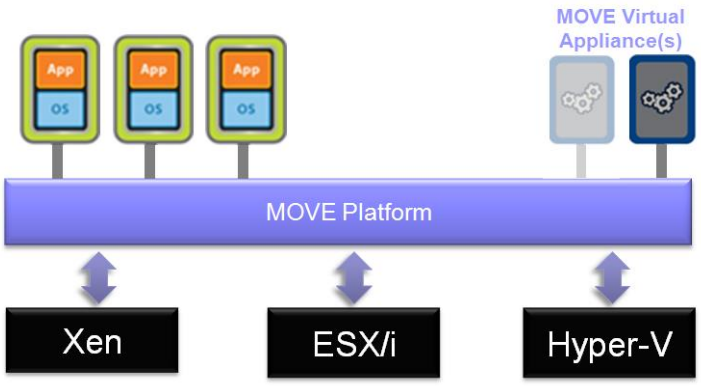
- **Absolutní kontrola nad využívanými aplikacemi.**
- **Minimální náročnost administrace uzamčeného systému.**
- **Nemožnost spuštění škodlivého kódu.**
- **Hladký chod aktualizací systému i v případě jeho uzamčení.**

Jak řešení funguje?

Agent Application Whitelisting po instalaci na počítač provede oskenování disků a do svého unikátního seznamu si zapíše všechny spustitelné soubory a scripty. Poté přejde do stavu blokování a umožní uživateli spustit pouze aplikace, které byly v rámci prvního skenu detekované. Uživatel tedy není schopen instalovat ani spouštět nové aplikace. To samé platí i pro škodlivé kódy, které se taktéž nespustí. Každý počítač má svoji databázi spustitelných aplikací, která vznikla při prvotním skenu. Z tohoto důvodu zde není potřeba žádný administrátorský zásah, systém pracuje zcela automaticky. Zajišťuje provozování pouze důvěryhodných aplikací na serverech a koncových bodech.

Rozšíření do cloudu

S rozšířením využívání cloudových služeb, je čím dál obtížnější zajistit dodržování firemních politik. McAfee pomáhá tyto problémy řešit prostřednictvím dashboardu, kde poskytuje plnou viditelnost o stavu ochrany a bezpečnostních incidentů veřejných i soukromých cloudů.



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

McAfee Server Security Suites

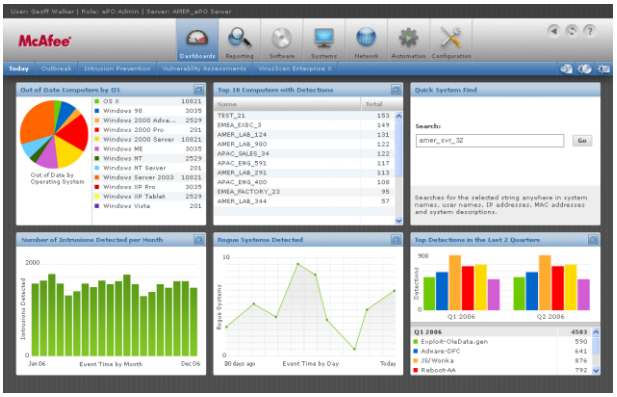
McAfee MOVE-AV je nadstavbou k nástroji VirusScan Enterprise, který modifikuje do virtuálního prostředí. Zde běží jako virtuální stroj, na kterém jsou prováděny veškeré skeny, což oproti konkurenčním řešením, kde na každém virtuálním stroji běží jeden antivirový systém, podstatně snižuje hardwarové nároky. Dalším prvkem, který vede k optimalizaci výkonu virtuálních strojů, je využívání cache, což podstatně zvyšuje rychlost testování (stejné soubory nejsou skenovány dvakrát). Toto řešení je dodáváno ve dvou variantách a to **pro virtuální desktopy a pro servery**. Srovnání s tradičními antivirovými řešeními pro virtuální prostředí naleznete v tabulce níže.

Samozřejmostí u McAfee je univerzální centrální správa McAfee ePolicy Orchestrator, kterou jsou tyto produkty rovněž spravovány. Díky tomu je možné z jediné konzoly řídit bezpečnost celé organizace, respektive provádět veškerá nastavení, plánování skenů jednotlivých virtuálních strojů, vyhodnocování reportů, úpravu bezpečnostních politik, atd.

	AV na VM stroji	McAfee MOVE-AV
Využití paměti (každá VM)	**60-120MB+**	**~20MB**
Využití CPU hypervizoru ve špičce	**80-100%**	**<10%**
Zatěžování VM při skenování	**ANO**	**NE**
Zátěž při aktualizaci DAT databáze	**ANO**	**NE**

McAfee ePolicy Orchestrator

Díky integraci s McAfee ePolicy Orchestratorem (ePO) jsou komponenty McAfee Total Protection for Endpoint centrálně spravovány z jediné konzoly. ePolicy Orchestrator umožňuje vzdálenou instalaci a správu, distribuovat a měnit bezpečnostní politiky či rozesílat pravidelné aktualizace produktů. Vše je podpořeno úzkou spoluprací s MS Active Directory. Součástí systému jsou nástroje pro monitoring v reálném čase i analýzu historických událostí s množstvím předdefinovaných reportů. Centrální management zajišťovaný ePolicy Orchestratorem tak šetří administrátorům čas, kapacitu linek a výrazně snižuje celkové náklady na zajištění kontinuity služeb sítě.



Porovnání balíčků	Server Security Suites Advanced	Server Security Suite Essentials	Security Suite pro Virtual Desktop
VirusScan Enterprise / for Linux Server / Desktop	•/•/-	•/•/-	•/-/•
Datacenter connector for VMware/ vSphere/ AWS/ Azure/ OpenStack	•/•/•/•/•	•/•/•/•/•	-/-/-/-/-
Host IPS for servers	•	•	desktop
Application Control-Server	•		desktop
Change Control - Server	•		
MOVE- Virtual infrastrusture	server	server	desktop
Centrální správa ePO	•	•	•
Licence per:	OS instance	OS instance	virtual machine

COMGUARD security & networking

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