McAfee Secure Virtualization MOVE-AV

Prověřené nástroje pro efektivní ochranu virtuálního prostředí

Virtuální technologie maximalizují využití hardwaru serverů a pracovních stanic a tím značnou mírou přispívají ke snížení provozních nákladů. Důkladné zabezpečení jejich provozu se však stalo nevyřešenou výzvou pro mnoho organizací všech velikostí a typů. Hlavní bezpečnostní úskalí spočívají ve zranitelnostech, které pramení ze složitosti patchování offline virtuálních serverů a nedořešeném propojení bezpečnosti virtuálních a fyzických serverů. McAfee proto vyvinulo produkty splňující nejpřísnější nároky pro stoprocentní zabezpečení sítě integrací bezpečnostních prvků jak pro ochranu fyzických, tak virtuálních zařízení s pomocí jediné řídící konzole McAfee ePolicy Orchestrator.

Management for Optimized Virtual Environments - MOVE-AV

Díky nástroji McAfee MOVE-AV nyní můžete snadně a hardwarově nenáročně zabezpečit virtuální prostředí ve vaší společnosti. Tento nástroj je navržen tak, aby se snížila potřebná režie tradičních antivirových řešení, při plně zachované bezpečnostní úrovni. Toho McAfee MOVE-AV dosahuje díky rozdělení virtuálního prostředí dle požadavků jeho jednotlivých prvků - virtuálních desktopů a virtuálních serverů. Na rozdíl od virtuálních desktopů mají servery podstatně odlišné nároky na optimalizaci výkonu a provozních nákladů ve virtuálním prostředí, už jen vzhledem k době provozu, zátěži a objemu dat, který zpracovávají.

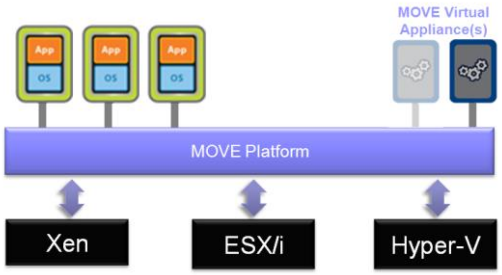
Optimalizace zátěže hostitelského stroje

MOVE-AV je nadstavbou k nástroji VirusScan Enterprise, který modifikuje do většiny běžně používaných virtuálních prostředí. Ať už používáte virtualizační prostředí od VMware, Citrixu nebo Microsoftu, McAfee MOVE-AV je tu pro Vás. V hostujícím prostředí běží MOVE-AV 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 s již skenovanými soubory, 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 tradičních AV řešení a MOVE-AV	AV na VM stroji	McAfee MOVE-AV
Využití paměti (každá VM)	60-120MB+	~20MB
Max. využití CPU hypervizoru	80-100%	<10%
Zatěžuje VM při skenování	ANO	NE
Zátěž při updatu databáze	ANO	NE

Integrace do různorodých prostředí

Vzhledem variabilitě virtuální infrastruktury je samozřejmostí multiplatformní přístup – součástí každé licence je verze McAfee VirusScan Enterprise pro operační systémy **Windows i Linux**. Navíc, pokud používáte virtualizaci společnosti VMware, máte možnost využít integrace s vestavěným bezpečnostním řešením VMware vShield Endpoint. MOVE AntiVirus Security Virtual Appliance (SVA) pak provádí skeny z vnějšku hostovaného stroje, **bez nutnosti agenta na stroji samotném**. Každý nový virtuální stroj je pak automaticky chráněn již od svého vytvoření, i v případě, že je přesunut na jiného hostitele. Ve VMware vCenter pak můžete sledovat i stav SVA, nebo přijímat alerty v případě potíží s jejím připojením.



Klíčové vlastnosti:

- **Nejkompletnější škálovatelné bezpečnostní řešení zahrnující fyzické i virtuální servery, desktopy a sítě**
- **První a jediný bezpečnostní výrobce chránící online i offline virtuální stroje**
- **ePolicy Orchestrator, jediná integrovaná platforma pro fyzické i virtuální prostředí**
- **Multiplatformnost a možnost nasazení bez agenta na virtuálním stroji**

Vlastnosti MOVE AV pro:

Virtuální servery

- **Skenování na základě reálné zátěže -** snížení HW nároků
- **Plánování skenů –** optimalizace zátěže hostitelského HW
- **Skenování virtuálních serverů v offline režimu**

Virtuální desktopy

- **McAfee Host Intrusion Prevention**
- **McAfee SiteAdvisor® Enterprise**
- **McAfee Web Filtering**

- **McAfee VirusScan Enterprise pro Windows a Linux**
- **Centrální správa pomocí McAfee ePolicy Orchestrator**

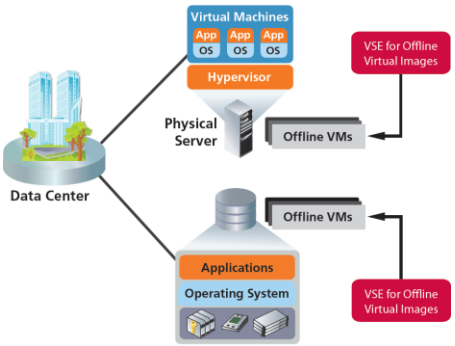
COMGUARD security & networking

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

McAfee Secure Virtualization MOVE-AV

McAfee VirusScan Enterprise for Offline Virtual Images

Řešení pokrývá situace, kdy nákaza nemůže být odstraněna za běhu systému, nebo případy virtuálních serverů převedených do režimu offline, které a zůstaly tak bez pravidelných bezpečnostních updatů, čímž se mohou nechtěně vyhnout nezbytným aktualizacím. Řešení automaticky skenuje, čistí a provádí updaty zabezpečení virtuálních serverů bez nutnosti jejich převedení do online režimu. Před svojí opětovnou aktivací jsou tak plně aktualizovány a **chráněny proti aktuálním hrozbám, které vznikly během jejich offline seance nebo které v online režimu nemohly být odstraněny**.



McAfee VirusScan Enterprise

Nástroj pro ochranu před hrozbami jako jsou viry, červi, trojské koně, spyware, buffer-overflow attacks i jejich kombinacemi. Zvládne v reálném čase sledovat a blokovat veškeré kanály pro šíření těchto hrozeb – soubory, web, emaily včetně příloh i síťovou komunikaci. K rychlejší detekci a odhalování škodlivého softwaru využívá globální databázi hrozeb McAfee Global Threat Intelligence, díky které také přenáší velkou část zátěže mimo Váš počítač. Je také centrálně spravovatelný pomocí McAfee ePolicy Orchestratoru, kterému zároveň reportuje veškeré události.

McAfee ePolicy Orchestrator

Díky integraci s McAfee ePolicy Orchestratorem (ePO) **jsou bezpečností komponenty (pro virtuální i fyzická zařízení) spravovány centrálně 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.

KOMPLEXNÍ OCHRANA PRO VIRTUALIZOVANÉ SERVERY – POVÝŠENÍ AV OCHRAN

McAfee Integrity Monitor (FIM) je nástroj pro kontinuální monitorování integrity (celistvosti, neporušenosti) souborů se schopností **sledovat změny obsahu i přístupových práv** u souborů a adresářů atp.

McAfee Application Control pro Servery zajišťuje kontrolu nad spuštěnými procesy a aplikacemi na serverech. To snižuje riziko neoprávněného spuštění malware nebo softwaru, zvyšuje kontrolu a bezpečnost! Provádí aplikační audit serveru s vynucením spuštění jen autorizovaných aplikací, spolupracuje s update systémy Microsoft aj.

McAfee Change Control pro Servery eliminuje rozdíl mezi autorizovanou zdokumentovanou změnou a skutečnou změnou nastavení IT služeb. McAfee Change Control zviditelňuje učiněné změny v reálném čase, prokazuje odpovědnost za změnu a vynucuje politiky v oblasti změn nastavení. Zabraňuje tak nežádoucím či neoprávněným změnám. Hlídá neautorizované změny v konfiguracích, souborech, lozích a registrech včetně preventivní ochrany a blokování.

McAfee Integrity Monitor pro Databáze – nástroj sloužící k monitorování aktivit probíhajících na databázích. Tato nepřetržitá kontrola je nezbytná k testování bezpečnosti a udržení shody se standardy jako PCI DSS. Monitorování se zaměřuje se na tři klíčové oblasti: **Aktivity:** Prověřuje přihlašování a odhlašování uživatelů, změny hesel, práva uživatelů. **Změny schémat:** Vytváření a úprava tabulek, indexování, atd. **Změna dat:** Vkládání, mazání a úprava citlivých dat v databázi. **McAfee Database Activity Monitoring** je navíc doplněn o databázové IPS nástroje a detekci zranitelností.

McAfee Datacenter Security Suite for Database – balíček obsahující produkty McAfee Databases Activity Monitoring a McAfee Vulnerability Manager for Databases se zvýhodněným licencováním. Oproti samotnému produktu McAfee Database Activity Monitoring tak získáte navíc sledování a reportování aktuálních patchů, detekovaných zranitelností, slabých hesel, nebezpečných kódů, rootkitů a jiného malware.

McAfee Datacenter Security Suite – balíček produktů dodávaný ve třech verzích, **pro server, pro hypervisor** a **pro virtuální desktop**, optimalizovaný pro konkrétní potřeby a problémy daného systému. S tímto balíčkem získáváte pokročilou ochranu proti virům, malware, trojským koním, červům a dalším škodlivým kódům ať už ve virtuálním nebo reálném prostředí. Navíc obsahuje také McAfee Application Control, díky kterému máte možnost zařízení po prvotní instalaci „uzamčít" pro jakékoli další instalace nebo změny nastavení. Tím také spolehlivě zabráníte zavlečení škodlivých kódů do systému stroje.

COMGUARD
security & networking

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