Risk&Compliance

FIM - Configuration – Change – Application Control

Ochrana integrity systému a dat

Organizace všech velikostí a typů se dennodenně potýkají s dosažením shody firemního IT s nastavenou politikou, a to jak korporátní, tak i určenou mezinárodními standardy. Důvodů je hned několik, ať už je to na jedné straně závod o udržení kroku s neustále se měnícími požadavky a standardy a na straně druhé časté změny v systému (databáze, servery, aplikace,…) s nedohledatelnou a nejasnou historií. Tato kombinace prakticky znemožňuje dosáhnout kvalitního výsledku bez využití sofistikovaných řešení. Z těchto důvodů společnost McAfee vyvinula řadu nástrojů, které IT administrátorům, auditorům a dalším osobám zapojených do výše popsaného procesu napomohou splnit tento nelehký úkol.

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.

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.

Jednoduché nasazení

Díky tzv. *pozorovacímu módu*, je možné Application Control nasadit tak, že nic neblokuje, ale hlásí do ePO, jaké aplikace by zablokoval, pokud by byl aktivní. To přináší velkou výhodu při ladění politik během implementace.

Klíčové výhody

- **Absolutní kontrola nad využívanými aplikacemi.**
- **Minimální náročnost administrace uzamčeného systému.**
- **Nemožnost spuštění škodlivého kódu.**
- **Hladký chod aktualizací systému i v případě jeho uzamčení.**
- **Integrace s GTI – administrátor dostává informace o důvěryhodnosti aplikací.**
- **Přímočará tvorba výjimek – Administrátor přímo z události o blokaci může přidat výjimku do politiky.**

Dostupné verze řešení Application Control

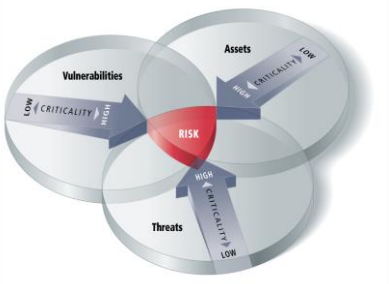
- Application Control for Servers
- Application Control for Devices

McAfee Change Control

Přináší nepřetržitou detekci změn na úrovni systému, a to i v distribuovaných sítích. V případě nasazení v preventivním módu blokuje neautorizované změny důležitých systémových souborů, adresářů a konfigurací. McAfee Change Control sleduje a prověřuje každý pokus o změnu v reálném čase. Následně je jednoduché dohledat, kdy a kým byla změna provedena. Je tak zajištěna nepřetržitá kontrola integrity souborů (FIM). Tato průběžná kontrola minimalizuje dopad neoprávněně provedených změn.

Shoda s mezinárodními standardy

Dosažení shody s mezinárodními standardy je poměrně složitý úkol. Například v případě PCI DSS, je nutné splnit přibližně 180 požadavků rozdělených do 12 kategorií a právě kategorie zaměřující se na sledování integrity souborů se v praxi ukázali jako nejnáročnější k dodržení. McAfee Change Control ovšem poskytuje nástroj, jak tyto požadavky splnit, a to účinným a nákladově efektivním způsobem. Díky integraci s centrální správou ePolicy Orchestrator to nyní dokážou nejen velké korporace, ale i malé společnosti.



Klíčové výhody

- **Audit změn konfigurací s dohledatelnou hitorií pro případnou forenzní analýzu.**
- **Kontrola integrity souborů a ochrana proti změnám.**
- **Ochrana proti narušení shody (PCI DSS, SOX, …).**
- **Jednotná správa pomocí ePolicy Orchestrator.**
- **Možnost zaznamenávat změny provedené na vybraných datech (konfiguračních a log souborech) - Kdo, kdy, jak a co změnil.**

Dostupné verze řešení Change Control

- Change Control for PCs
- Change Control for Servers

COMGUARD
security & networking

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

FIM - Configuration – Change – Application Control

McAfee Integrity Control

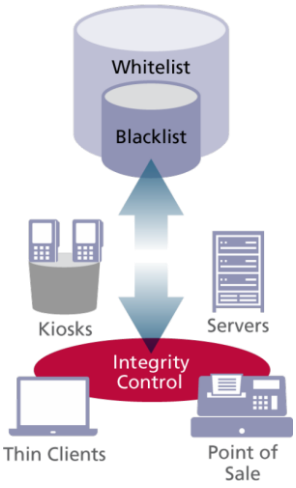
Nástroj sloužící k monitorování aktivit probíhajících v systému. Tato nepřetržitá kontrola je nezbytná k testování bezpečnosti a udržení shody se standardy, jako je Payment Card Industry Data Security Standard (PCI DSS).

Monitorování se zaměřuje se na tři klíčové oblasti:

- **Aktivita**: například je kontrolováno přihlašování a odhlašování uživatelů, změny hesel, práva uživatelů, atd.
- **Změna schémat**: například vytváření a úprava tabulek, indexování, atd.
- **Změna dat**: Vkládání, mazání a úprava citlivých dat.

Výsledky lze později využít k určení kdo, kdy a jak provedl danou změnu pro případnou forenzní analýzu, kde tyto informace mohou mít zásadní význam pro určení, zda byla změna korektní či ne. V neposlední řadě je třeba uvést, že monitoring má minimální nároky na výkon celé infrastruktury.

Integrace s Global Threat Intelligence – nabízí jediněčný způsob ja k se vypořádá s globálními hrozbami pomocí McAfee Global Threat Intelligence (GTI). Jedná se o technologii, které sleduje reputaci souborů, zpráv a odesílatelů v reálném čase (zapomocí senzorů po celém světě). GTI využívá znalosti cloud-based informační databáze a pomáhá tím určit pověst všech souborů (kvalifikuje je jako dobrý, špatný a neznámé).



McAfee Integrity Monitor for Fixed Function Devices

Nástroj, určený pro úzce specializovaná zařízení, u kterých je třeba omezit funkčnost ke konkrétním účelům. Nabízí možnost omezit využití přístroje a přístupu k datům jeho prostřednictvím. Proto je zejména vhodný například pro zákaznické terminály či kiosky. Nemusíte se tak bát průniku do infrastruktury pomocí terminálu, nad kterým není stálý dohled, a můžete svým zákazníkům umožnit přístup k datům, která potřebují.

McAfee Policy Auditor

Potřebujete spolehlivé důkazy o splnění regulatorních i jiných firemních požadavků? McAfee Policy Auditor umožňuje automatizaci procesů potřebných pro vnitřní a vnější audity IT. Jedná se o řešení na bázi agenta s rozsáhlou podporou obsahu norem a plnou integrací s McAfee ePolicy Orchestrator (ePO™). Poskytuje přesný a efektivní audit, kdykoliv je zapotřebí, takže se můžete vrátit k řízení rizik, ne papírování.

Jak řešení funguje?

Policy Auditor je nástroj, který kontroluje nastavení a softwarové vybavení stanic a serverů. Kontrolu provádí agent na stanici na základě výrobcem předdefinovaných pravidel a auditů (popř. dalších testů definovaných administrátorem). K dispozici jsou audity pro všechny podporované operační systémy a obvyklé softwarové vybavení. V reportu je možné jednoduše dohledat chybně nastavené stroje a zastaralé softwarové vybavení (od serverových aplikací po browsery a kancelářský software), které se může stát vstupní branou pro útočníky.

Dostupné verze řešení Application Control:

- Policy Auditor for Server
- Policy Auditor for Desktop

Klíčové výhody

- **Udržení shody se standardy.**
- **Integrace s dalšími McAfee nástroji, např. s centrální správou McAfee ePO.**
- **Využití pro audity systémů.**
- **Vynucení centrální politiky u všech spravovaných stanic.**
- **Variabilní nastavení pro každý typ společnosti.**

Centralizovaný Management

Díky integraci s McAfee ePolicy Orchestratorem (ePO) jsou komponenty centrálně spravovány z jediné konzoly. ePolicy Orchestrator umožňuje vzdálenou instalaci a správu, distribuovat bezpečnostní politiky či rozesílat pravidelné aktualizace produktů. Součástí systému jsou nástroje pro monitoring v reálném čase i analýzu historických událostí s množstvím předdefinovaných reportů.

Přehled produktů McAfee Risk and Compliance

DIAGNOSTIKA	OCHRANA	SPRÁVA
POLICY AUDITOR	CHANGE CONTROL INTEGRITY CONTROL APPLICATION CONTROL	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