McAfee Endpoint Security 10

Nové řešení společnosti McAfee Endpoint Security 10 přináší kompletně přepracovaný a optimalizovaný anti-malware engine „AMCore" (NextGeneration anti-malware engine), který nezatěžuje uživatele skenováním celého disku a který má rozšířené funkce firewallu a ochrany webového provozu. To vše je sjednoceno pod GUI, které je připravené i pro dotykové displeje. Řešení umožňuje společný reporting v ePO konzoli (přístup „on-premise" nebo cloud) s možností napojení na Threat Intelligence Exchange a další přídavné moduly. Migrace z původních produktů pro endpointy je díky připravenému migračnímu nástroji otázkou několika minut.

endpoint Security Moduly

- **Threat Prevention modul** – zahrnuje několik pokročilých funkcí na zjišťování škodlivého malware. Funguje jako obrana proti vznikajícím a cíleným útokům. Je to nástupce VirusScan Enterprise (VSE).
- **Web Control modul** – zabraňuje uživatelům navštěvovat nebezpečné nebo nedůvěryhodné internetové stránky. Prostřednictvím Web Filtering kategorizuje webové stránky na lokální úrovni. Jedná se o nástupce Site Advisor Enterprise (SAE).
- **Firewall modul** – Monitoruje veškerou komunikaci. Zastavuje škodlivý příchozí nebo odchozí síťový provoz. Obsahuje Stateful Firewall, Adaptive Mode a DNS Blocking.
- **Přídavné moduly** – volitelné rozšíření bezpečnostních nástrojů

Vše přehledně na jednom místě

McAfee Endpoint Security má centralizovaný management, který umožňuje celkovou správu z jediné konzole (možnost správy on-premise nebo cloud).

Inteligentní ochrana

Spolupracuje a sdílí informace (souborový hash, URL,…) s dalšími zařízeními v reálném čase, což vede k rychlejší identifikaci podezřelého chování a umožňuje lepší koordinaci obrany (ochrana před cílenými útoky a zero-day hrozbami).

Silný a efektivní výkon

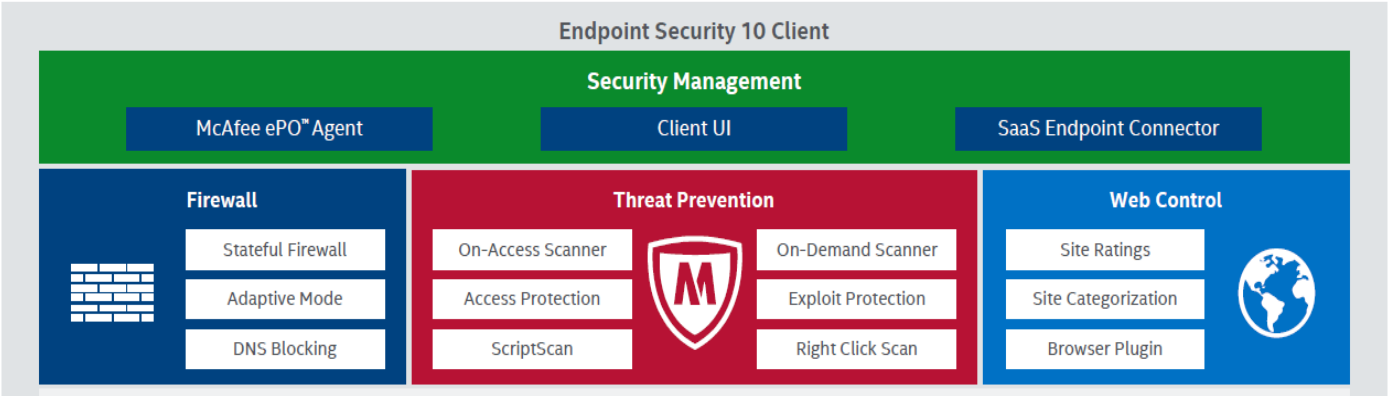
Zvyšuje výkon optimalizovaným skenováním (zaměřuje se na podezřelé procesy a důvěryhodné procesy neprochází), aktualizacemi a maximalizací výkonu CPU.

Security Framework

Eliminuje redundanci v podobě duplicitních technologií a množství řešení pro správu. Umožňuje napojit přídavná řešení (např. McAfee TIE, MAR, GTI) a zvýšit tím zabezpečení. Pro komunikaci využívá Data Exchange Layer (DXL).

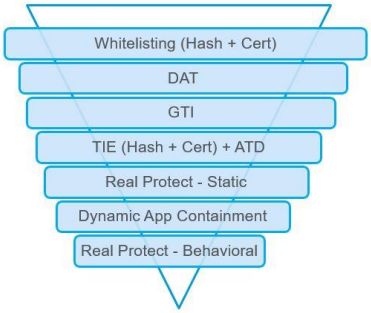
Společná architektura

Společná architektura umožňuje efektivní spolupráci všech modulů, což vede k zvýšení bezpečnosti zabezpečení, např. po stažení nějakého souboru odešle Web Control hash souboru Threat Prevention, který okamžitě spustí jeho prověřování. Na základě výsledků této kontroly jsou provedeny nezbytné kroky. V McAfee ePolicy Orchestrator (ePO) lze nastavit požadovanou úroveň citlivosti Global Threat Intelligence.



Dynamic Application Containment (DAC)

DAC nabízí ochranu před ransomware, greyware a „patient-zero" hrozbám tím, že bezpečně zkoumá chování a obsah aplikace tak, že spustí podezřelý binární kód v uzavřeném prostředí (aby nedošlo k nákaze celé sítě) a snaží se vysledovat, jaké akce se daná aplikace snaží provést. Pokud jde o nezávadnou aplikaci, povolí ji. Pokud ne, aplikaci zakáže a předejde tím šíření nákazy dále. Neznámým aplikacím, kterým umožní spuštění, omezí akce, které může provádět. DAC umožňuje sledovat vlastnosti a chování souboru i bez nutnosti využití sandboxu, či nutnosti připojení ke cloudu. DAC je součástí Threat Prevention modulu.



COMGUARD
security & networking

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

Real Protect

Jedná se o real-time technologii pro detekci hrozeb, která monitoruje podezřelé činnosti na koncových zařízeních na základě chování. Real-Protect využívá strojové učení pro automatickou klasifikaci na základě chování (v cloudu) a využívá ji pro detekci „zero-day" hrozeb. Dokáže objevit malware či detekovat škodlivou aktivitu a zablokovat ji nebo umístit do karantény. Klasifikace od Real Protect může být využita k vytvoření ukazatele útoky (IoA) nebo indikátor kompromisu (IoC). Real Protect je součástí Threat Prevention modulu.

Konzole ePO v cloudu

ePO cloud je součástí ENS 10 a umožňuje připojit se kdykoliv a kdekoliv, díky tomuto řešení se snižují provozní náklady. V případě cloud řešení není zapotřebí mít vlastní ePO server. Nový a přehlednější dashboard obsahuje více relevantních informací.

Firewall – kontrola provozu

Kontroluje příchozí a odchozí provoz a na základě reputace jej blokuje/povoluje. Firewall má vylepšenou ochranu (DEP, GBOP, Kevlar sigs., SMEP).

Web Control – webová ochrana

Hodnotí a kategorizuje webové stránky, monitoruje aktivitu prohlížečů (plug-inů) apod. Hodnocení bezpečnosti webové stránky zobrazuje již během on-line prohlížení a vyhledávání. Web Control umožňuje správci webu upozorňovat a blokovat přístup na webové stránky na základě hodnocení.

Threat Prevention – adaptivní skenování

Zero-impact scan (skenování s nulovým dopadem pro koncového uživatele) využívá inteligentní skenování, např. skenuje jen ty soubory, které vyhodnotí, že mají být skenovány, a ohodnotí je stupněm důvěryhodnosti. Scan je prováděn pouze v „klidovém stavu" daného zařízení (skenování probíhá, když uživatel nepracuje). Klidový stav je určen monitorováním činnosti disku.

- Automatické skenování stažených souborů
- Variantní skenování – full scan, quick scan, „right-click" scan a nastavitelný scan
- Ochrana heslem proti nežádoucí odinstalaci
- Rozšířené loggování, reporting a hlášení událostí
- Migrační asistent – pomáhá s přenosem dat z VSE 8.8

V3 DAT

V3 DAT obsahuje novou strukturu, která je kompatibilní s produkty AMCore-based. V3 DAT je menší než V2 DAT (přibližně 30MB, komprimované) a lze ho spravovat, nasadit a aktualizovat přes ePO. V3 DAT je kompatibilní s extra .DAT a je řízen stejným způsobem jako V2 DAT.

McAfee Active Response (MAR)

MAR v kombinaci s Threat Inteligence Exchange vytvoří výkonný nástroj v boji proti bezpečnostním incidentů.

„**Discover**" – definuje nepřetržitý sběr dat založený na možnosti vyhledávat a analyzovat systémová data.

„**Detect**" – sleduje a zachycuje události, soubory a systémové změny. Údaje jsou následně odeslány k forenzní analýze a zpracovány.

„**Respond**" – přijímá okamžitá upozornění, takže se dokáže přizpůsobit změnám útočných metodik.

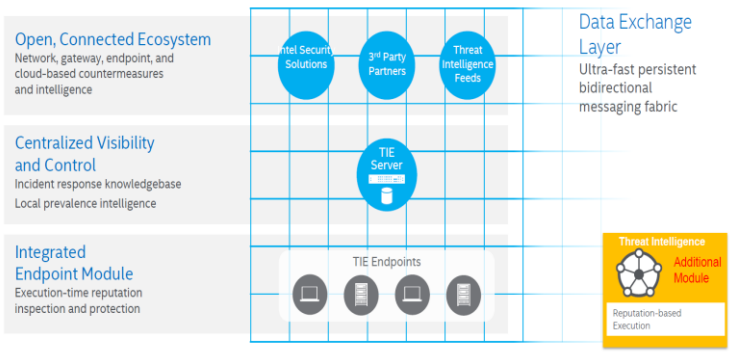
Jako součást integrované bezpečnostní architektury nabízí nepřetržitý a automatizovaný dohled nad koncovými stanicemi.

Klíčové funkce Active Response:

- Vyhledávání a vizualizace systémových dat
- Neustálé sledování kritických událostí a veškerých změn pomocí jedné sady příkazů
- Přednastavené a přizpůsobitelné akce při spuštění
- Kompatibilní s McAfee ePO – využití jediné konzole pro řízení a sledování bezpečnosti.
- Vynucení konzistentních politik – zavádění celopodnikových politik

Threat Intelligence Exchange (TIE)

Přídavný modul, který zvyšuje ochranu koncových stanic pomocí adaptivní prevence hrozeb. Představuje centralizovanou a optimalizovanou detekci hrozeb díky databázi, která kombinuje data z více informačních zdrojů včetně řešení třetích stran.



COMGUARD
security & networking

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