McAfee Endpoint Protection

Jedno integrované zabezpečení koncových zařízení, jediná řídící konzole

Dnešní sofistikované útoky si žádají ucelený systém ochran. Řízení systémové bezpečnosti s pomocí decentralizovaných bezpečnostních systémů je zastaralé a neúčinné. McAfee Endpoint Security představuje integrované zabezpečení před soudobými útoky pro stanice i servery kombinované s desktopovým IPS a Firewallem. Díky integračnímu prvku ePolicy Orchestrator navíc poskytuje nejen centralizaci správy, ale také jednotný monitorovací systém s rozsáhlými možnostmi reportů a analýz. Přináší tolik potřebný přehled nad bezpečností sítě, nutný pro zajištění nepřetržité dostupnosti služeb LAN pro zaměstnance, zákazníky i obchodní partnery.

Hlavní součásti řešení:

- **Endpoint Security** – jediný agent pro komplexní ochranu koncového zařízení pre Windows, Mac a Linux
- **Anti-Spyware** – integrovaná ochrana proti moderním škodlivým kódům – malwaru.
- **Host IPS & Desktop Firewall** – víceúrovňová detekce a prevence hrozeb včetně ochran před DoS útoky a útoky v čase nula (Zero-Day).
- **Web Control** – proaktivní ochrana zajišťuje bezpečné prohlížení webových stránek v prohlížeči a kategorizuje weby na úrovni lokální stanice, tj. i ve chvíli kdy je stanice mimo LAN.
- **Ochrana email serverů proti virům a spamu** – kontrola příchozího i odchozího emailového provozu na existenci spamu, virů a jiného nežádoucího obsahu s téměř 100% úspěšností a nulovou „false positive".
- **Device Control** – řídí přístup k připojitelným komunikačním kanálům (Bluetooth, wifi) a výměnným médiím (USB disky).
- **Endpoint Encryption** – šifrování disků, složek a souborů s vynucením a dohledem centrálních politik na pracovních stanicích.
- **Global Threat Intelligence** – globální reputační systém poskytující informace o výskytu malware na webu, v emailu, IP adresách a dalších entitách.
- **Application Control** – zajišťuje provozování pouze důvěryhodných aplikací na koncových stanicích pomocí Application Whitelisting agenta.
- **Security for Email Servers with AntiSpam** – ochrana email serverů (Microsoft Exchange a Lotus Domino) proti virům a spamu.
- **Policy Auditor** – dohled a vynucení centrálních politik na pracovních stanicích.
- **ePolicy Orchestrator** – centrální konzole pro správu bezpečnostní infrastruktury.

Nová produktová řada MVISION

Pokročilá ochrana pro Windows 10 – spolupráce **MVISION Endpoint** a Windows Defender vytváří efektivní ochranu pro koncové body proti sofistikovaným hrozbám. Jednotná správa produktů je zabezpečená prostřednictvím **MVISION ePO** platformy.

Zabezpečení mobilních zařízení – Technologie **Mobile Threat Detection engine** kombinuje vysoce výkonný antimalware pro iOS a Android s algoritmy strojového učení (Machine learning), které detekují nestandardní chování mobilního zařízení.

McAfee Endpoint Security (ENS)

Jedná se o zcela výkonný engine, který se skládá ze čtyř modulů – Threat Prevention Module (Antimalware), Web Control Module (Web filter), Firewall Module (Desktop firewall a IPS) a doplňkový Adaptive Threat Protection Module. Mezi klíčová zdokonalení můžeme zařadit zejména Zero-impact sken, který probíhá pouze v případě, kdy uživatel s PC nepracuje. Dále také framework, který umožňuje integraci více bezpečnostních řešení. Podporovány jsou také systémy Mac a Linux. Pro přenesení stávajícího nastavení bezpečnostních politik do nového prostředí je připraven Migration tool, který zajistí bezproblémovou automatickou migraci.

Adaptive Threat Protection (ATP)

Jedná se o doplňující modul určený k ochraně proti pokročilým hrozbám. Technologie Real Protect detekuje chování malware, a monitoruje podezřelé činnosti programů nebo aplikací na koncových zařízeních. Škodlivou aktivitu zablokuje a malware umístí do karantény. Dynamic Application Containment ochraňuje před ransomware, greyware a „patient-zero" hrozbám – podezřelý binární kód spouští v omezeném módu (tak aby nemohl dokončit svůj záměr) a zkoumá jeho chování. Eliminuje nevýhody sandboxingu, který některé typy malware dokáží obejít.

McAfee Host IPS & Desktop Firewall

Tento ucelený systém nové generace kombinuje několik stupňů detekce narušení od rozpoznání známých útoků na základě automaticky aktualizovaných signatur, přes pravidla chování pro detekci neznámých útoků (včetně DoS útoků, anomálií provozu a Zero Day Attack ochran), s možnostmi desktop firewallů. Mezi hlavní vlastnosti patří SQL/HTTP Injection Protection, ochrana pro zveřejněné zranitelnosti Microsoft, zabránění kompromitace aplikací, nebo blokování přístupu stanic či serverů na síť v případě, že nejsou aktualizované.

Web Control

Zabezpečuje, reguluje a sleduje veškerou činnost webového prohlížeče. Technologie Web Control blokuje přístup uživatelů na webové stránky s nevhodným obsahem. Rozšiřuje ochranu tradičních URL filtrů a zabraňuje uživatelům prohledávání nebezpečných webových serverů. Blokuje a upozorňuje na webové stránky, které mohou obsahovat spyware, phishing scams nebo spam agenty. Poskytuje granulární přehledy pro veškerou činnost související s webem.

McAfee Application Control

Tento produkt funguje tak, že 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.

COMGUARD
security & networking

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

McAfee Endpoint Protection

Global Threat Intelligence

McAfee Global Threat Intelligence (GTI) je komplexní cloudově založená služba, která umožňuje zákazníkům McAfee využít jedinečné technologie pro ochranu celé informační infrastruktury a pomáhá čelit kybernetickým hrozbám napříč všemi vektory.

Device Control & Endpoint Encryption

Device Control umožňuje řídit přístupy k přenosným médiím (CD, USB disky) a připojitelným kanálům (Bluetooth, IR nebo wifi). Některé balíčky McAfee navíc nabízí funkce pro zašifrování celých disků, adresářů a souborů, včetně přenosných zařízení jako jsou USB klíčenky bez nutnosti využívat specializovaných nástrojů dalších výrobců.

McAfee ePolicy Orchestrator (ePO)

Díky integraci s McAfee ePolicy Orchestratorem jsou komponenty McAfee Endpoint Protection centrálně spravovány z jediné konzole. ePolicy Orchestrator umožňuje vzdálenou instalaci a správu, distribuci bezpečnostní politiky, nebo rozesílání pravidelných aktualizací produktů. Vše je podpořeno úzkou spoluprací s MS Active Directory. Součástí systému jsou nástroje pro monitoring v reálném čase i analýzu událostí s množstvím předdefinovaných reportů.

McAfee Active Response (MAR)

je odpověď na nejpokročilejší kybernetické hrozby a útoky. Jedná se o klíčovou součást integrované bezpečnostní architektury, která umožňuje neustálý přehled o všech koncových zařízeních, čímž je docíleno aktivní ochrany v reálném čase. Z centrální konzole může operátor posílat dotazy nebo příkazy na koncové stroje, např.: Který proces komunikuje s IP adresou a.b.c.d. a tak eliminovat právě probíhající nebezpečí.

Threat Intelligence Exchange (TIE)

spolupracuje se všemi bezpečnostními prvky, které vystupují jako jeden celek. Integrovaná inteligence z různých zdrojů dat (i ze zdrojů třetích stran) v kombinaci s kontextovými daty a signaturami umožňuje snadnější a rychlejší rozhodovací proces. Kombinuje data z GTI, řešení třetích stran a STIX souborů s informacemi, které shromažďují lokální bezpečnostní zařízení. Poté tyto informace vyhodnocuje a sdílí napřímo skrz všechna řešení.

	MVISION Standard (MV1)	MVISION Plus (MV2)	Endpoint Threat Protection (ETP)	Endpoint Protection Advanced Suite (EPA)	Complete Endpoint Threat Protection (CTP)	Complete Endpoint Protection Business (CEB)
ePO - centrální správa (cloud i on-premise řešení)		✓	✓	✓	✓	✓
ePO MVISION	✓	✓	✓	✓	✓	✓
Endpoint Security (ENS)	✓	✓	✓	✓	✓	✓
MVISION Endpoint	✓	✓				
MVISION Mobile		✓				
SiteAdvisor			✓	✓	✓	✓
Anti-spyware			✓	✓	✓	✓
Desktop Firewall			✓	✓	✓	✓
Web Filter for Endpoint			✓	✓	✓	✓
Adaptive Threat Protection modul	✓	✓			✓	✓
Email server: anti-virus, anti-spam			✓	✓	✓	✓
Device Control			✓	✓	✓	✓
Ochrana pro servery			✓	✓	✓	✓
Endpoint security pro Mac a Linux			✓	✓	✓	✓
Host IPS				✓	✓	✓
Policy Auditor				✓		✓
Application Control					✓	✓
Drive Encyption						✓
Management of Native Encryption						✓
File & removable media protection						✓
TIE – Threat Intelligence Exchange		✓				
Správa a ochrana pro Sharepoint						✓
Ochrana pro datová úložiště						✓
Dynamic Application Containment (DAC) a Real Protect	X / ✓	X / ✓			✓	✓

COMGUARD security & networking

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