Trellix MVISION Endpoint

Pokročilé zabezpečení napříč cloudovou i on-premise infrastrukturou

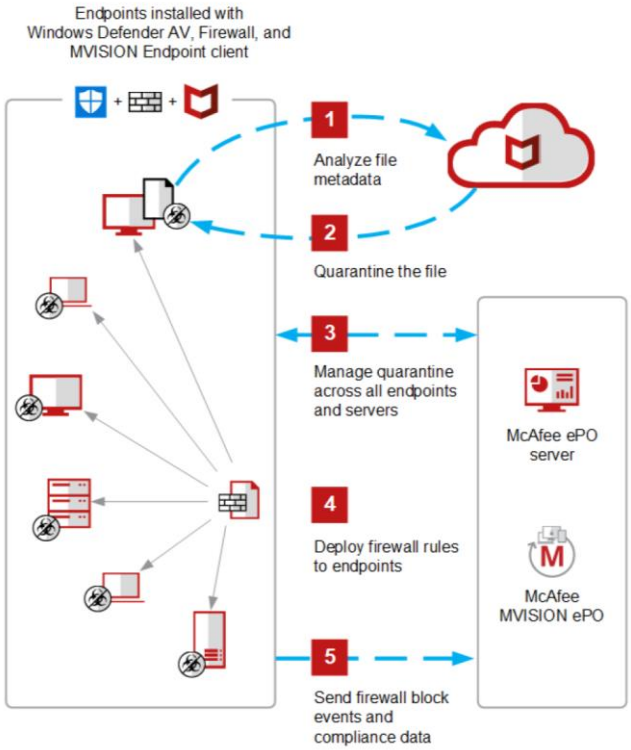
*Platforma Windows již dlouhodobě převažuje v korporátním prostředí, pro mnohé společnosti je tedy nasnadě využití nativní AV ochrany **Microsoft - Windows Defender**. Je však tato ochrana dostačující? Trellix přichází s odpovědí - novou produktovou rodinou **Trellix MVISION**, která doplňuje nativní ochranu Windows Defender zejména o pokročilé techniky strojového učení a možnosti centrální správy na korporátní úrovni. Výsledkem je **plně spolupracující bezpečnostní systém,** který klade minimální nároky na koncový bod a nabízí široké možnosti další integrace.*

MVISION Endpoint

Trellix MVISION Endpoint

Jedná se o odlehčeného klienta, který **doplňuje nativní AV engine Windows Defender**. MVISION Endpoint poskytuje ochranu zejména proti pokročilým hrozbám, a to pomocí behaviorální analýzy, tedy strojového učení (tzv. AI Machine Learning). Centrální správu řešení na korporátní úrovni zajišťuje ePolicy Orchestrator, který lze nasadit jak on-premise, tak i jako cloudovou konzoli. V MVISION ePO lze spravovat samozřejmě také nativní AV engine Windows Defender, ale i Defender Exploit Guard a Windows Firewall – pro všechny zmíněné je možné nastavit jednotné politiky z jediné administrativní konzole!

V rámci balíčku MVISION Protect je mimo jiné k dispozici také plnohodnotné modulární řešení ochrany koncových zařízení **Trellix Endpoint Security 10.X** včetně tradiční On-premise konzole Trellix ePolicy orchestrátor.



*Vylepšete **zabezpečení Windows 10** pomocí Trellix MVISION.*

MVISION ePO

Trellix MVISION ePO (SaaS)

Jedná se o **cloudovou konzoli**, která vychází ze svého on-premise předchůdce, vlajkové lodi společnosti Trellix – ePO neboli ePolicy Orchestrator. Díky cloudovému nasazení MVISION ePO významně šetří náklady na implementaci a následnou údržbu, systém je vždy aktuální. Spravovat lze produkty z portfolia Trellix, ale také produkty jiných výrobců (např. Windows Defender), kromě jednotné správy je možné nastavovat také jednotné bezpečnostní politiky. Další silnou stránkou MVISION ePO jsou nastavitelné dashboardy a přehledný reporting. Uživatelsky přívětivý dashboard „Protection Workspace" poskytuje přehledné vizualizace, monitoruje hrozby, poskytuje informace o shodě a dokáže spravovat zařízení pomocí zjednodušených workflow.

Hlavní výhody řešení:

- Poskytuje ochranu proti pokročilým hrozbám pomocí strojového učení.
- Kontroluje možné zcizení přihlašovacích údajů
- Zajišťuje centrální správu celého řešení na korporátní úrovní pomocí MVISION ePO.
- Centrální správu lze díky cloudové architektuře jednoduše nasadit a je nenáročná na údržbu.
- Agent MVISION Endpoint má jen zanedbatelný vliv na výkon koncové stanice.
- Lze jednoduše rozšířit o funkcionality EDR (Endpoint Detection and Response).
- Nabízí široké možnosti integrace s dalšími bezpečnostními produkty (i třetích stran) pomocí DXL (data Exchange layer).
- Přímá integrace napříč produktovou rodinou MVISION – CASB a Mobile Security

COMGUARD
communication security

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

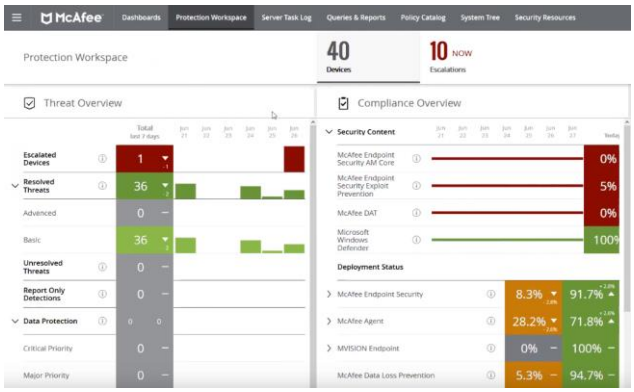
Trellix MVISION Endpoint

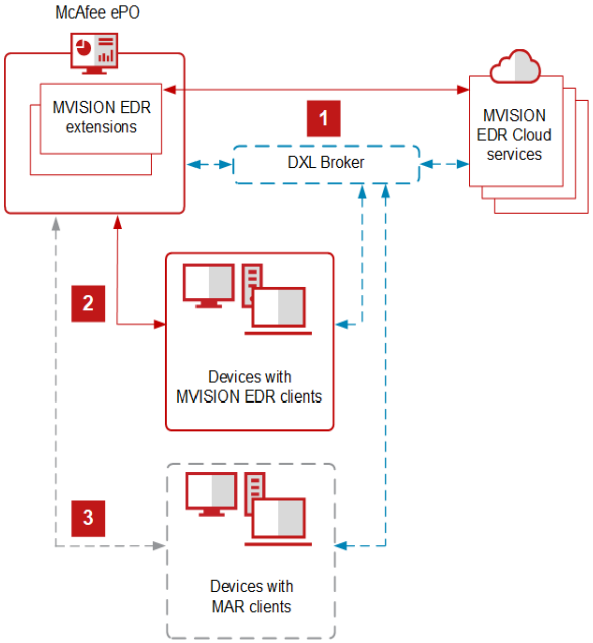
Trellix MVISION EDR

MVISION EDR

MVISION EDR nepřetržitě monitoruje a shromažďuje data, díky čemuž poskytuje hlavně bezpečnostním administrátorům potřebný vhled a kontext nutný k detekci a reakci na pokročilé hrozby. Bez účinného EDR řešení se bezpečnostní týmy často mohou cítit zahlceny až paralyzovány množstvím informací, které je zapotřebí analyzovat. MVISION EDR poskytuje **nástroje pro investigaci a automatizaci založené na bázi umělé inteligence (AI),** to umožní provádět bezpečnostní analýzu i technikům na juniorské úrovni.

MVISION EDR Automaticky detekuje pokročilé hrozby z koncového zařízení nebo dokonce i podporovaného SIEMu. Výsledky následně zobrazuje v MITRE ATT&CK® frameworku (https://attack.mitre.org). Další důležitou funkcionalitou jsou předkonfigurované akceschopné nástroje pro ThreatHunting, které umožnují reagovat na hrozby v reálnem čase. Bezpečnostní administrátoři tak mohou např. ukončit libovolný proces na vybraném koncovém zařízení, umístit zařízení do karantény, nebo smazat zvolený soubor. Akce lze provést buď na jediné zařízení, a nebo celou vybranou skupinu.





	MVISION Protect Standard	MVISION Protect Plus and EDR for Endpoint
ePO on-premise, ePO MVISION	✓	✓
Self-managed	✓	✓
Trellix MVISION Endpoint	✓	✓
MVISION Mobile	×	✓
ENS 10 multiplatform	✓	✓
Host Intrusion Prevention*	✓	✓
Desktop Firewall*	✓	✓
Site Advisor + Web filter*	✓	✓
AntiVirus + AntiSpyware*	✓	✓
Device control	✓	✓
MVISION Insights	×	✓
Application Control	×	✓
TIE - Threat Intelligence Exchange	×	✓
Ochrana před ransomware, greyware a „patient-zero" hrozbám	✓	✓
Data Exchange Layer (DXL)	✓	✓
EDR 30 - 90 days retention	×	✓

*** Je součástí Endpoint Security 10**

Trellix MVISION Mobile

MVISION Mobile

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. V případě připojení mobilního zařízení na nezabezpečenou, nebo dokonce kompromitovanou síť systém upozorní uživatele a případně i administrátora. Stejné upozornění lze také nastavit i pro mobilní aplikace s neznámou reputací. Samozřejmostí je také integrace s Trellix ePO, tedy konzolí pro centrální správu všech zařízení. MVISION Mobile tedy poskytuje stejnou úroveň zabezpečení jako pokročilý antivirový engine u běžných PC umístěných v korporátní síti.

COMGUARD
communication security

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