COMGUARD

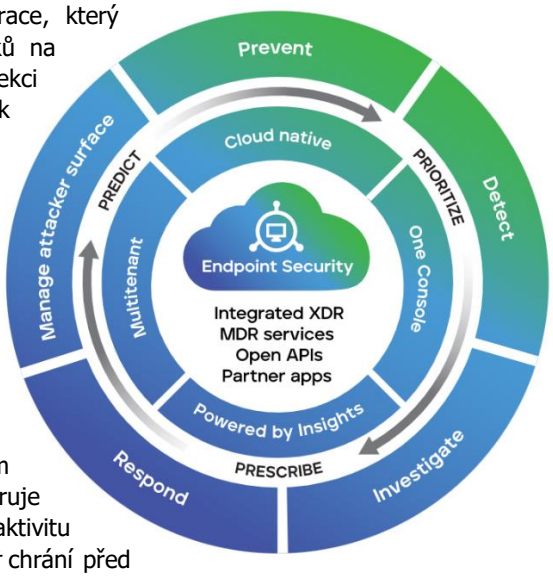
Trellix

Endpoint Protection

Trellix Endpoint Security představuje integrované bezpečnostní řešení pro stanice i servery kombinované s desktopovým IPS a Firewallem. Robustní konzole 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.

Threat Prevention • Firewall • Web Control • Adaptive Threat Protection

Trellix Host IPS & Desktop Firewall je ucelený systém nové generace, který 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.



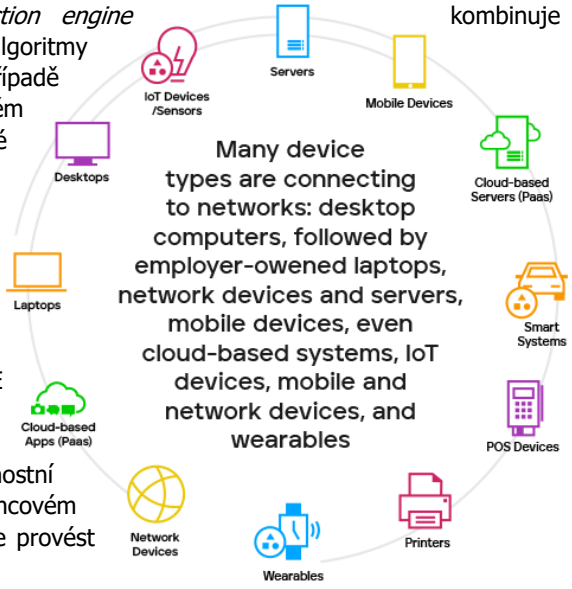
Web Control zabezpečuje, reguluje a sleduje veškerou činnost webového prohlížeče. Blokuje přístup uživatelů na webové stránky s nevhodným obsahem a které mohou obsahovat spyware, phishing scams nebo spam agenty. Rozšiřuje ochranu tradičních URL filtrů a zabraňuje uživatelům prohledávání nebezpečných webových serverů.

Adaptive Threat Protection je 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* chrání 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 dokážou obejít.

Pokročilé zabezpečení pro cloudovou i on-premise infrastrukturu

Trellix ePolicy Orchestrator (ePO): Díky integraci s Trellix ePolicy Orchestratorem jsou komponenty Trellix Endpoint Protection centrálně spravovány z jediné konzole. ePO umožňuje vzdálenou instalaci a správu, distribuci bezpečnostních politik, nebo rozesílání pravidelných aktualizací. 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.

Trellix Mobile Technologie *Mobile Threat Detection engine* kombinuje vysoce výkonný anti-malware pro iOS a Android s algoritmy strojového učení, které detekují nestandardní chování mobilního zařízení. V případě připojení 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.



Trellix EDR nepřetržitě monitoruje a shromažďuje data, čím poskytuje bezpečnostním administrátorům potřebný vhled a kontext nutný k detekci a reakci na pokročilé hrozby. Poskytuje nástroje pro investigaci a automatizaci založené na bázi AI, to umožní provádět bezpečnostní analýzu i technikům na juniorské úrovni. 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, anebo celou vybranou skupinu.

COMGUARD
communication security

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

COMGUARD

Trellix

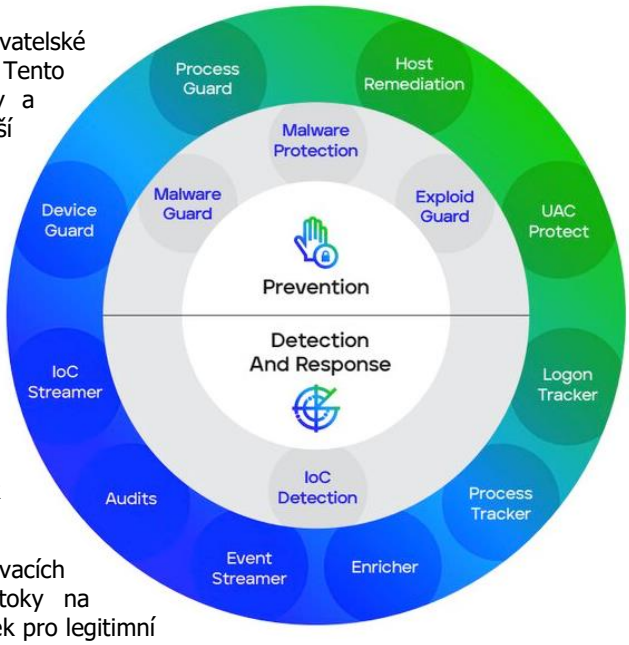
Endpoint Protection

Další alternativa řešení ochrany koncových zařízení je Trellix Endpoint Protection, který je postaven na strategi „Protect, Detect & Respond", která dokáže zabránit kybernetickému útoku hned v několika fázích jeho životního cyklu. Dohromady tedy vytváří komplexní řešení ochrany koncových stanic a poskytuje nástroje pro forenzní analýzu i ThreatHunting.

Signature-based EPP • MalwareGuard • ExploitGuard • Process Guard

Protect

Endpoint Protection Platform (EPP) engine chrání uživatelské stanice před běžným malwerem využitím klasických signatur. Tento engine tedy odfiltruje všechny známé viry, trojany červy a podobné typy malware. Díky této základní filtraci nejsou další moduly zahlceny a fungují efektivněji.



MalwareGuard pomocí strojového učení a využitím statické analýzy dokáže odhalit ransomware, trojany, zero-day útoky a další neznámé hrozby.

Dalším modulem, které napomáhá dotvoření komplexní ochrany je **ExploitGuard**. Ten se zaměřuje na detekci, blokování a prevenci pokusů o útoky na zranitelnosti softwarových aplikací. Propojuje behaviorální analýzu se informacemi o aktuálních zranitelnostech k detekci útoků typu „memory corruption" nebo „code injection". Vytváří tedy další vrstvu ochrany proti cíleným útokům. Pozoruje běžně využívané aplikace a na základě jejich aktivit uděluje proprietární „risk skóre".

Modul **Process Guard** byl vyvinut, aby dokázal zastavit exfiltraci přihlašovacích údajů (credentials). Chrání systém přímo v LSASS paměti, kde útoky na přihlašovací údaje probíhají. Samozřejmostí je možnost nastavení výjimek pro legitimní procesy.

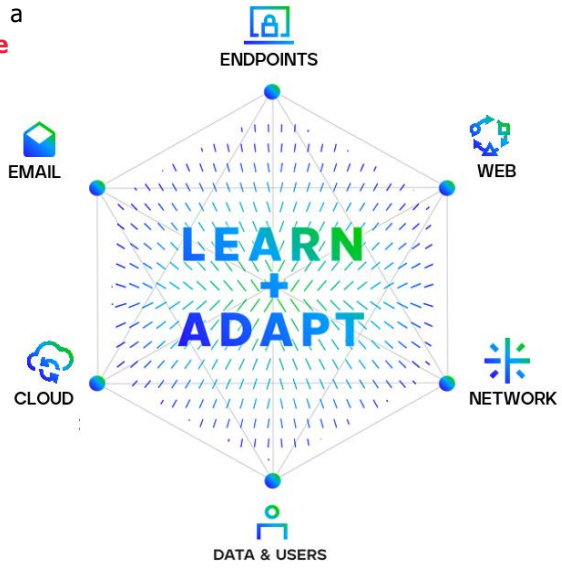
Detect Respond

V případě, že přeci jen dojde k prolomení ochrany, Trellix Endpoint Protection (HX) poskytuje nástroje k odhalení kde, kdy a jak byl systém kompromitován. Díky těmto automatizovaným nástrojům lze konkrétní hrozby odhalit a přímo na ně reagovat. Následně je možné jednoduše provést sanaci v celé organizaci.

Indicator of Compromise Engine (IOC) využívaná denně aktualizovanou knowledge base obsahující nejnovější indikátory útoků shromážděné z *Dynamic Threat Intelligence*. Tento engine dokáže rychle odhalit aktivitu kompromitované uživatelské stanice, když je nalezena aktivní hrozba. Jedná se tedy o nástroj, který pomáhá analytikům odhalit rozsah dopadu útoku v infrastruktuře. Propojuje vhled do aktivit na koncovém zařízení s kontexty síťového provozu.

Získejte jedním agentem přístup k vícero bezpečnostním nástrojům

Forenzní vyšetřování na uživatelských stanicích a serverech umožňuje provádět funkce **Enterprise Search**. Kromě toho umožňuje také bezpečnostním týmům provádět tzv. ThreatHunting. Bezpečnostní analytik má tedy kompletní viditelnost koncových bodů, včetně aktivních procesů, síťových připojení a všech systémových změn. V rámci ThreatHuntingu má analytik k dispozici dokonce i aktivitu na klávesnici útočníka.



Dynamic Threat Intelligence Trellix Endpoint Protection (HX) získává informace o hrozbách z *Global Threat Intelligence*, která nepřetržitě shromažďuje a analyzuje data z různých zdrojů, včetně rozsáhlé Trellix customer base a systémů pro analýzu malwaru. Od *Global Threat Intelligence* se tato *Dynamic Threat Intelligence* liší tím, že se nespoléhá na přirazenou reputaci souborů a kódů, ale všechny potenciální hrozby si ve svém vlastním virtuálním sandboxu spustí a jejich škodlivost si sama ověří.

COMGUARD
communication security

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