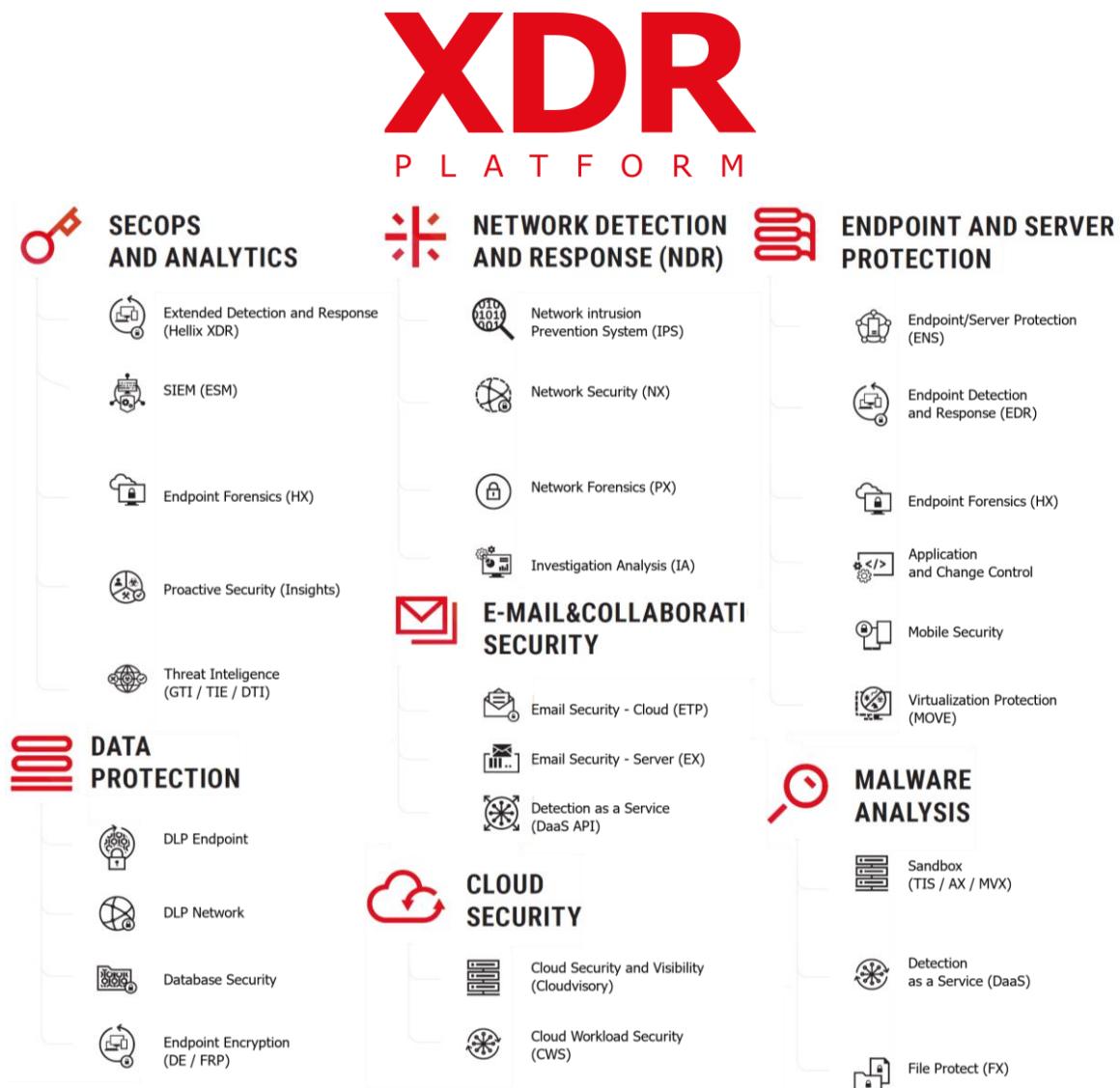


# XDR Platform

Dnešní svět je plný dynamických kybernetických hrozob, kdy každá další je komplexnější než ta předchozí. S nárůstem počtu těchto hrozob, se zvyšuje i počet alertů, kterým musí SOC týmy čelit. V důsledku toho jsou SOC týmy často velmi přetížené a hrozí, že přehlédnou skutečně důležitá upozornění. Mohou za to především fragmentované bezpečnostní nástroje, které spolu nekooperují, což znesnadňuje SOC týmům reagovat včas. Výsledkem je zvýšené riziko kompromitace bezpečnosti celé organizace.

**Trellix XDR Platform** poskytuje organizacím jednotnou centralizovanou platformu, která je vybavena přehledným UI a zároveň poskytuje granulární vhled do veškerých upozornění napříč celou bezpečnostní infrastrukturou nasazenou on-premise i v cloudu (uživatelské stanice, síťový provoz, servery). Tento vhled se vztahuje jak na portfolio Trellix, tak i na podporované produkty výrobců třetích stran. Trellix XDR Platform dává organizacím nástroje pro rychlé a přesné detekování hrozob a pomáhá k zastavení útoků ještě předtím, než k nim stihne dojít.



# XDR Platform

## Bezpečnostní ekosystém Trellix

**Trellix Endpoint Security** poskytuje ochranu zejména proti pokročilým kybernetickým hrozbám, a to pomocí behaviorální analýzy, tedy strojového učení (tzv. AI Machine Learning).

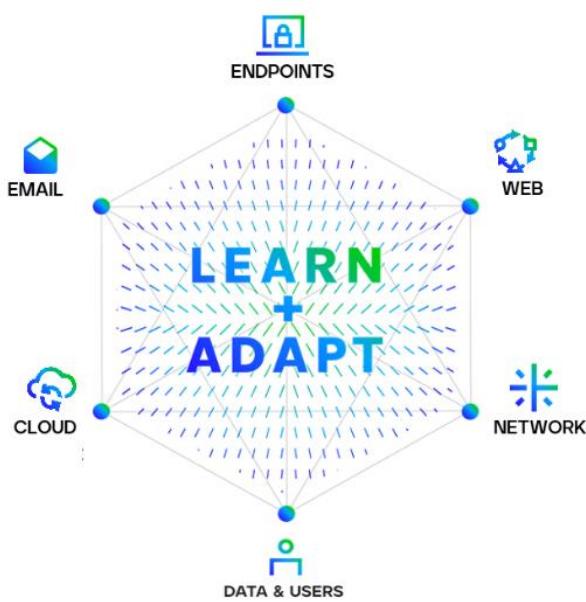
**Trellix Change Control** přináší nepřetržitou detekci změn na úrovni systému, a to i v distribuovaných sítích.

**Trellix 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.

**Trellix Email Protection** je komplexní bezpečnostní řešení zaměřené na ochranu organizací před škodlivými e-maily a kybernetickými útoky. Toto řešení poskytuje pokročilou detekci, analýzu a ochranu proti phishingu, malware, ransomware, spamu a dalším hrozbám přicházejícím skrze e-mailovou komunikaci.

## Hlavní výhody řešení

- Snižuje riziko vzniku kybernetického bezpečnostního incidentu pomocí špičkové detekční technologie
- Optimalizuje zdroje SOC díky prioritizaci bezpečnostních alertů
- Zjednodušuje práci SOC expertů – poskytuje nástroje pro investigaci a automatizaci založené na bázi umělé inteligence (AI)
- Díky cloudové architektuře lze jednoduše nasadit a je nenáročné na údržbu
- Nabízí široké možnosti integrace pomocí API
- Poskytuje jednotný vhled napříč celou bezpečnostní infrastrukturou, ekosystémem Trellix i dalších bezpečnostních výrobců.



**Trellix 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 umožňují reagovat na hrozby v reálném čase.

**Threat Intelligence Exchange** je nástroj pro reputační hodnocení souborů a výměnu informací o hrozbách mezi endpointy, globální databází hrozeb, sandboxy a dalšími zdroji dat.

**Trellix SIEM** (Security Information and Event Management) je komplexní bezpečnostní řešení, které kombinuje pokročilou analýzu a centralizované správy logů pro detekci a reakci na hrozby v reálném čase.

**Trellix Data Loss Prevention** systematicky monitoruje a chrání informace před jejich neoprávněným užitím vlastními uživateli, či kompromitovanými účty. Tímto způsobem pokrývá a zabezpečuje síťovou komunikaci (email, webmail, Instant Messaging atd.), fyzická zařízení (tiskárny, USB zařízení aj.), peer-to-peer aplikace a další...). IPS/IDS síťové sondy **Trellix Network Security Platform** preventivně chrání vnitřní síť před známými/ neznámými/ spyware, malware, botnety, DoS/DDoS útoky, VoIP hrozbami atd. Kombinuje několik stupňů detekce narušení od rozpoznání útoků na základě signatur přes pravidla chování, anomálií provozu, rozpoznání aplikací a „Zero Day Attack“ ochran.

**Cloudvisory** přináší monitorování, správu a kontrolu složitých multi-cloudových prostředí. Centrální správu všech Trellix řešení na korporátní úrovni zajišťuje **ePolicy Orchestrator**, který lze nasadit jak on-premise, tak i formou SaaS.

Lze jednoduše integrovat například s:

