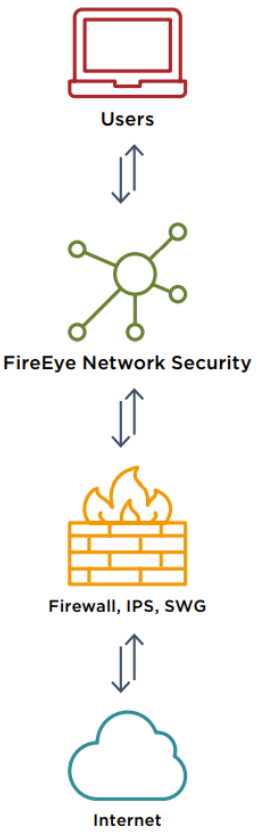
COMGUARD

Trellix

FireEye Network Security

Zacílené kybernetické útoky, pokročilý malware, rozsáhlé ransomware kampaně – to jsou příklady kybernetických hrozeb, na které konvenční ochrana perimetru sítě v dnešní době zkrátka nestačí. Možným řešením je posílení ochrany perimetru o další bezpečnostní vrstvu – ***sandboxingovou ochranu****.*

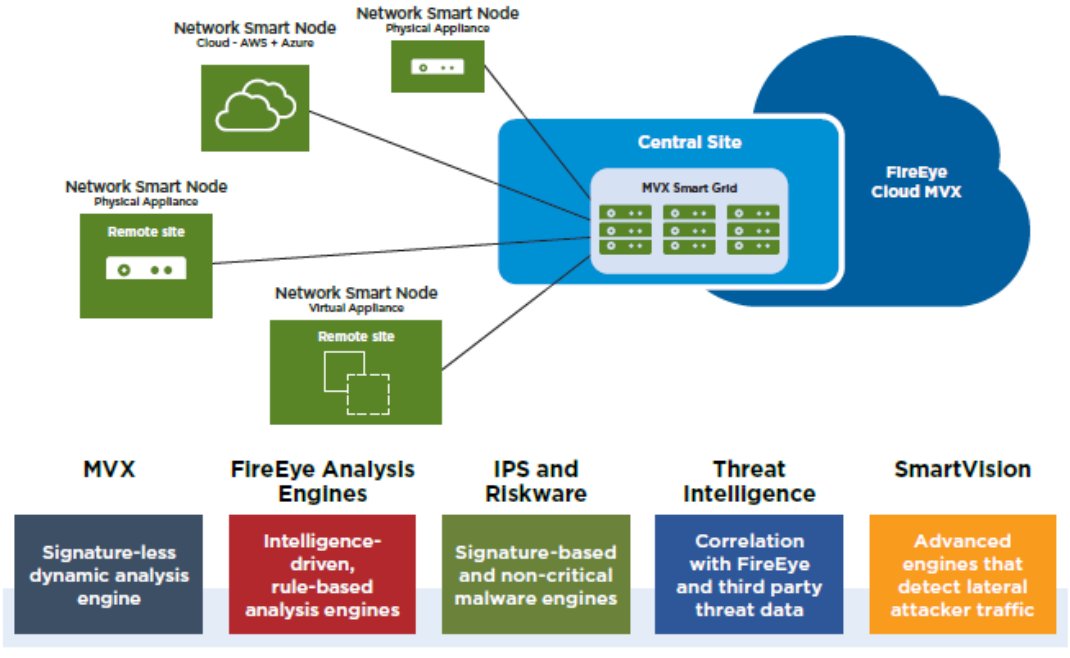


FireEye Network Security je efektivní řešení ochrany perimetru organizace před celou škálou bezpečnostních hrozeb. Díky schopnosti přesné detekce dokáže okamžitě zastavit zacílené kybernetické útoky, nebo dokonce také malware speciálně navržený tak, aby dokázal obejít konvenční bezpečnostní prvky.

Základem FireEye Network Security je **Multi-Vector Virtual Execution™ (MVX)**, **strojové učení** a **umělá inteligence**. MVX je technologie která k detekci malware místo signatur využívá dynamickou analýzu vzorku kódu v bezpečném virtuálním prostředí, dokáže tak odhalit zero-day útoky, doposud neznámé exploity a malware. Kontroluje podezřelý síťový provoz za účelem identifikace útoků, které se vyhýbají tradičním obranným mechanismům založených na signaturách a bezpečnostních politikách. Škodlivou aktivitu blokují v reálnem čase i retrospektivně.

Další důležitou součástí řešení je technologie **IPS** (Intrusion Prevention System), která detekuje běžné síťové útoky využitím konvenčního porovnávaní signatur.

FireEye Network Security je k dispozici v různých variantách rozdělených dle typu nasazení, dokáže tedy pokrýt i specifické požadavky náročnějších organizací. Typické nasazení je sériové zapojení za zařízení určené k ochraně perimetru (např. next-generation firewall, IPS nebo secure web gateway). Zabezpečení perimetru rozšířené o další vrstvu ochrany v podobě FireEye Network Security je připraveno čelit všem výzvám moderního kybernetického prostoru.



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

FireEye Network Security

Capabilities	Benefits
Detection	
Accurate detection of advanced, targeted and other evasive cyber attacks	Minimizes risk of costly cyber breaches
Modular and scalable security architecture	Provides investment protection and supports business growth.
Consistent level of protection for multi-OS environments and all Internet access points	Creates a strong defense across the entire organization for all types of devices
Integrated, distributed, physical, virtual, on-premise and cloud deployment options	Offers flexibility to align with organizational preferences and resources
Multi-vector correlation with Email and Content Security	Provides visibility across wider attack surface
Prevention	
Immediate blocking of attacks at line rates from 250 Mbps to 10 Gbps	Gives real-time protection against evasive attacks
Visibility into encrypted traffic	Built-in TLS 1.3 decryption support available on appliances without an additional license fee
Response	
Low rate of false alerts, riskware categorization and mapping to MITRE ATT&CK framework	Reduces operational cost of triaging unreliable alerts
Pivot to investigation and alert validation, endpoint containment and incident response	Automates and simplifies security workflows
Execution evidence and actionable threat intelligence	Accelerates prioritization and resolution of detected security incidents

Možnosti rozšíření:

FireEye Network Security lze rozšířit o další moduly, díky kterým lze automatizovat proces reakce na generované aletry, provádět hloubkovou investigaci zachycených packetů, nebo také umožní provádět nápravná opatření přímo na samotných koncových stanicích.

Možnosti nasazení:

- ***Integrované síťové zabezpečení*** – standalone, all-in-one HW appliance, který má v sobě integrovaný nástroj MVX. Díky tomu se z jednoho místa řeší zabezpečení síťového vstupního bodu. Jde o snadno ovladatelné řešení, nevyžaduje pravidla, politiky nebo ladění.
- ***Distribuované síťové zabezpečení*** – rozšiřitelná appliance s centrálně sdílenou službou MVX. Zabezpečení síťového vektoru vhodné i pro náročnější organizace, které se skládá z:
  - ***Network Smart Node*** – virtuální senzory, které analyzují síťový provoz. Detekují a blokují škodlivý, zároveň ho odesílají MVX službě pro finální analýzu.
  - ***MVX Smart Grid*** – on-premise, centralizovaná flexibilní MVX služba, která nabízí transparentní škálovatelnost a nasazení v režimu vysoké dostupnosti s automatickým vyvažováním zátěže. Přechod z integrovaného hardwarového zařízení na MVX Smart Grid poskytuje další kapacitu pro detekci a analýzu síťových hrozeb.
  - ***FireEye Cloud MVX*** – předplatné služby MVX zajišťuje soukromí analýzou provozu na on-premise Network Smart Node. Službě MVX se skrz šifrované připojení posílají pouze podezřelé soubory, kdy jsou objekty odhalené jako benigní následně propuštěny.

Form Factor	Performance
Integrated Network Security	50 Mbps to 5 Gbps
Physical Network Smart Node	50 Mbps to 10 Gbps
Virtual and Public Cloud Network Smart Node	50 Mbps to 8 Gbps

COMGUARD
communication security

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