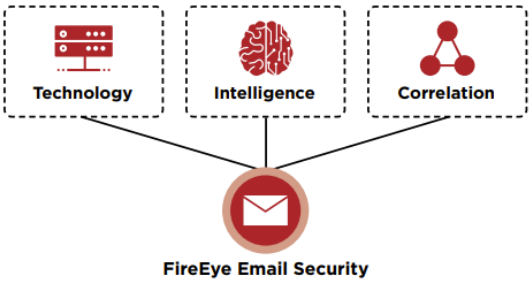
COMGUARD

Trellix

FireEye Email Security

Email je nejzranitelnějším vektorem kybernetických útoků, protože ním denně projde obrovské množství dat. Přizpůsobitelnost vzhledu emailu a možné vkládaní a skrývaní URL adres, na kterých uživatel jednoduše nakazí své zařízení malwarem, je velkým rizikem, se kterým se společnosti denně potýkají. V současné době rozmachu pokročilých hrozeb se Sandboxing stává novým bezpečnostním standardem.



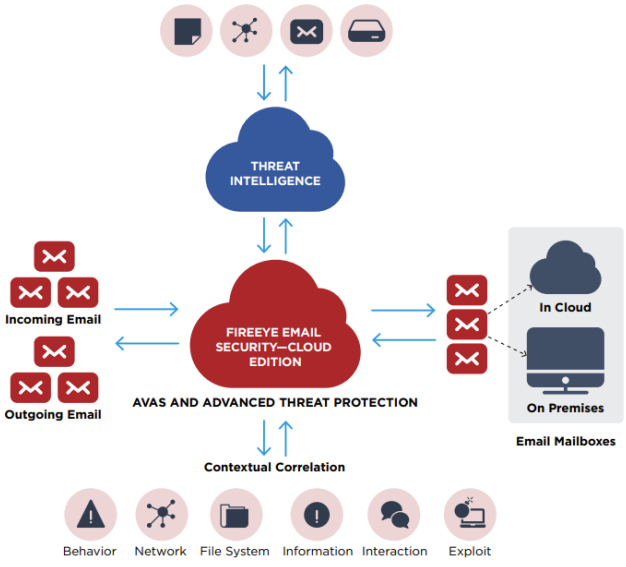
FireEye Email Security je **emailová brána s unikátní sandboxingovou technologií,** která dokáže detekovat a blokovat všechny druhy nevyžádaných e-mailů, zejména zacílené pokročilé útoky. Běžně dokáže odhalit hrozby také v provozu, který konkurenční produkty považují za bezpečné. Společnost FireEye nabízí emailovou ochranu ve dvou verzích – **Cloud edition** a **Server edition**.

FireEye se stalo leaderem v oblasti emailové bezpečnosti díky své technologii, která identifikuje, izoluje a okamžitě zastavuje škodlivé URL. Technologie odhalí imitaci legitimního uživatele/organizace i útoky skryté v příloze mailu ještě před tím, než nebezpečný mail vnikne do infrastruktury organizace. Dokáže také retrospektivně odstranit e-mail, který se stal škodlivým až po jeho přijetí (po kliknutí na link, nebo jinou interakcí). Zároveň kontroluje odcházející poštu z Vaší schránky – abyste nevědomě nepřeposlali škodlivý nebo spamový mail a neocitli se na černé listině.

Klíčové vlastnosti

- Umožňuje Office 365 aby mohl automaticky **odstranit e-maily**, které se **po doručení** stanou **škodlivými**
- Dokáže **spolupracovat** s jakýmkoliv **poskytovatelem e-mailu** třetí strany
- Poskytuje **hluboké znalosti** o útocích a útočnících z předchozích vyšetřování a pozorování
- **Ověřuje autenticitu** jména a e-mailové adresy
- Integrace s FireEye Network Security poskytuje **širší pohled** do více-vektorových útoků a **koordinaci ochrany** v reálnem čase

Za pomocí sociálního inženýrství hackeři dokážou připravit poutavý podvržený e-mail upravený přesně na míru svému cíli. Pravděpodobnost úspěšnosti phishingového útoku tak prudce stoupá. **Multi-Vector Virtual Execution™ (MVX)** je technologie, která k detekci malware místo signatur využívá dynamickou analýzu v bezpečném virtuálním prostředí. Dokáže tak odhalit zero-day útoky, doposud neznámé exploity a malware. Kontroluje skutečně **vše** – přílohy (EXE, DLL, PDF, SWF, DOC/ DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 a ZIP/RAR/TNEF archivy), přílohy zaheslované a zašifrované, URL, PDF a Microsoft Office soubory. Upozorňuje na slabiny v OS, vyhledávači a aplikacích. Nepřehlédne ani škodlivý kód vložený do e-mailů typu spear-phishing.



PhishVision je technologie fungující na bázi **deep learningu**. Porovnává legitimní weby a portály s přiloženými URL v doručených e-mailech. Další vrstvu ochrany před hrozbami z URL poskytuje systém **Skyfeed**, který shromažďuje informace o webovém prostoru jako např. účty na sociálních sítích, blogy, fóra a další).

FireEye Email Security poskytuje ochranu i v dalších fázích **ransomware** útoku. Dokáže zachytit komunikaci s command-and-control servery pokus o útok si zapamatuje. V dalším incidentu podobný útok rychle identifikuje. Další důležité funkcionality jsou **anti-spam** a **antivirová ochrana** (AVAS). Důvěryhodnost mailu zjišťuje také ověřením stáří a aktivitou domény odesilatele.

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 Email Security

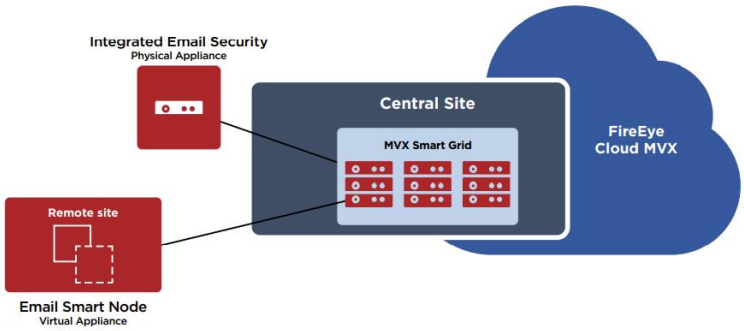
MalwareGuard je technologie postavena na základě **Machine Learning (AI)** čímž doplňuje další již zmíněné vrstvy ochrany. Ještě před samotným spuštěním dokáže předpovědět, zda je soubor systému Windows pravděpodobně škodlivý, a může tedy zabránit malwaru v propagaci. Data využívána pro strojové učení se opírají o 15 milionů koncových zařízení a více než milion hodin strávených analyzováním nejrůznějších útoků.

FireEye Email Security kategorizuje i **riskware** na nebezpečné a méně nebezpečné hrozby, s prioritním odstraněním hrozeb nejzávažnějších. Z FireEye **Dynamic Threat Intelligence (DTI)** cloudu se až k zařízení dostávají v reálnem čase všechny potřebné informace o aktuálních hrozbách.

FireEye Helix poskytuje viditelnost napříč celou infrastrukturou a obohacuje alerty o investigativní tipy, korelaci s endpointy a inteligenčními feedy. Nabízí i možnosti automatizace. Tímto způsobem FireEye Helix upozorňuje na neviděné hrozby a napomáhá učinit kvalifikovaná rozhodnutí.

Ochrana před tzv. **impersonation** je další funkce, kterou **Email Security (ES)** disponuje. Tato funkce je založená na určení důvěryhodných odesílatelů a porovnávání odesílatelů s důvěryhodnými kontakty. ES disponuje také e-mailovou karanténou, tedy odděleným prostředím určeným pro emaily, které neodpovídají explicitnímu seznamu blokování či povolení. Všechny e-mailové atributy mohou být použity pro vyhledávaní, analyzování a mohou být doručeny skrze intuitivní dashboard.

Cloudová verze je zabezpečená e-mailová brána ideální pro migraci e-mailové bezpečnosti do cloudu. Jednoduše se integruje s Microsoft Office 365 a dalšími cloudovými e-mailovými platformami. Poskytuje ochranu před útoky, které se vyhýbají konvenčním bezpečnostním technologiím. Tento produkt získal řadu certifikací, nejznámější je **ISO 27001**, dále získal i FedRAMP autorizaci díky AVAS a SOC 2 Type 2.



Serverová verze se liší typem nasazení (on-premise) a navíc nabízí kontrolu obrázků v e-mailu, které požadují zadání hesla a mohou být potenciální hrozbou. Skenuje URL odkazy v archivech (ZIP, LZIP, JAR) i dokumenty, které si z nich můžete stáhnout (někdy i nevědomě). V této verzi také naleznete pokročilé hrozby ve vyhledávačích a zranitelnosti aplikací.

Pro nasazení v režimu monitoringu lze nastavit transparentní BBC pravidlo k odesílaní kopie e-mailů na analýzu do Email Security.

Flexibilní možnosti nasazení – aby si každý našel to, co hledá:

- ***Integrované e-mailové zabezpečení*** – standalone, all-in-one HW appliance. Z jediného místa zabezpečuje a chrání vstupní bod e-mailového provozu. Jde o snadno ovladatelné řešení, které lze nasadit za méně než 60 minut. Nevyžaduje pravidla, politiky nebo ladění.
- ***Distribuované e-mailové zabezpečení*** – rozšiřitelná appliance s centrálně sdílenou službou MVX, která je určená k ochraně e-mailového provozu pro náročnější organizace. Skládá se z:
  - ***Email Smart Node*** – virtuální senzory, které analyzují e-mailový provoz a detekují i blokují ten 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 e-mailových hrozeb.
  - ***FireEye Cloud MVX*** – předplatné služby MVX zajišťuje soukromí analýzou provozu na on-premise Email Smart Node. Službě MVX se skrz šifrované připojení posílají pouze podezřelé soubory, kdy jsou objekty odhalené jako benigní následně propuštěny.

COMGUARD
communication security

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