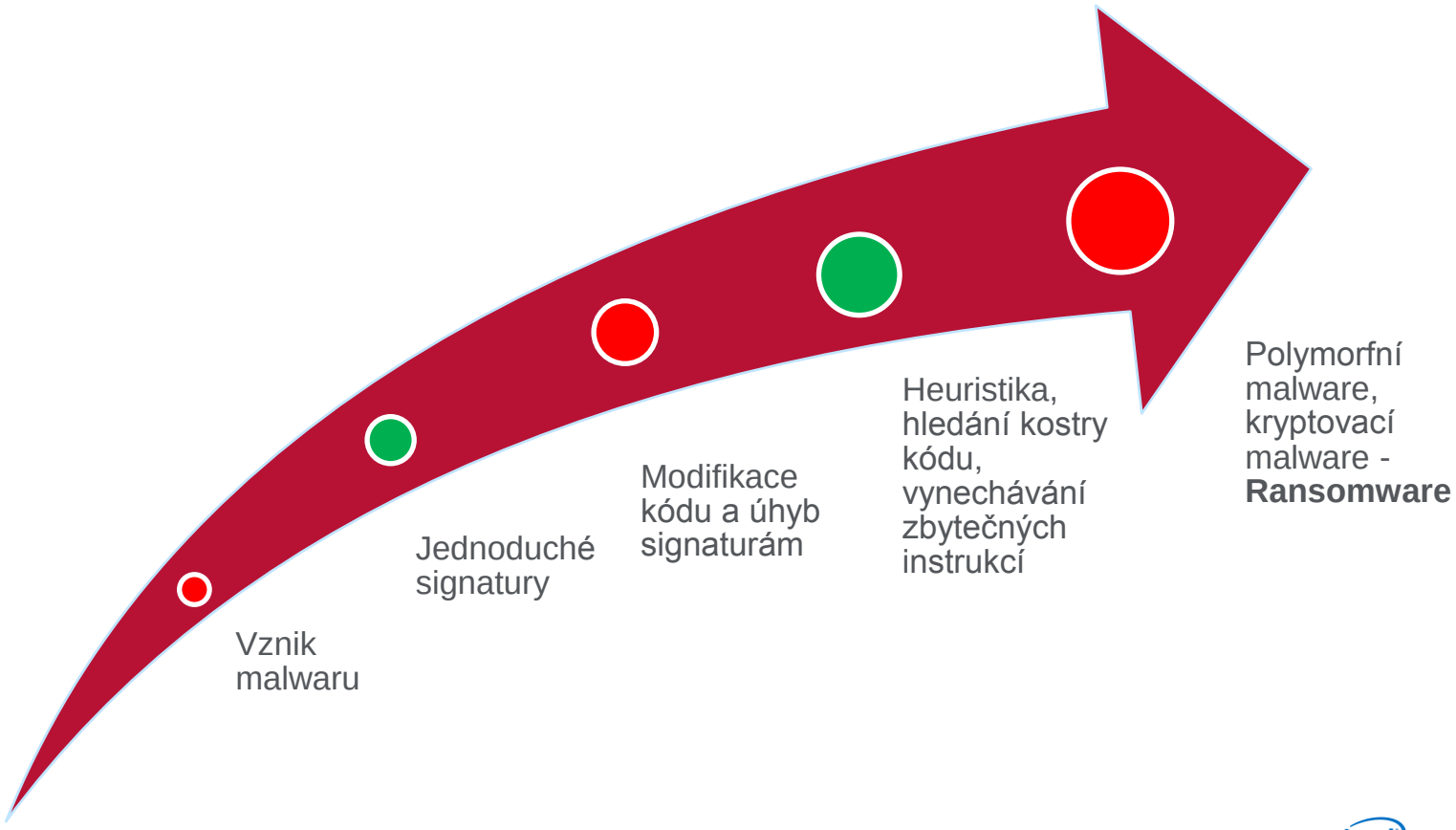
Kryptoviry a malware pod 100% kontrolou

Alena Řezníčková, Territory and Channel Manager, IntelSecurity
Jan Strnad, Sales Engineer, Intel Security
Jiří Endršt, Senior Technical Consultant, PCS - divize DataGuard

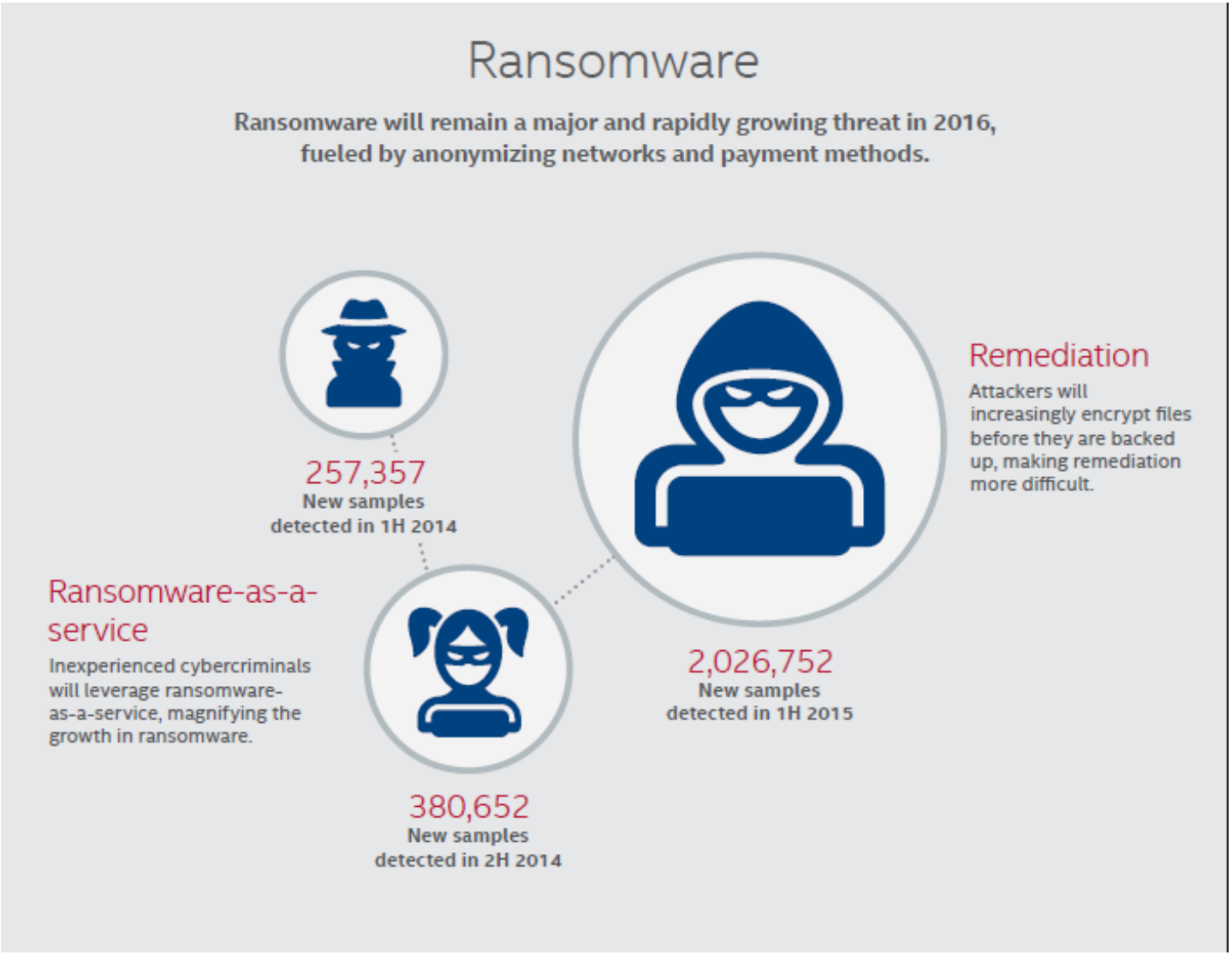
TM

Malware vs. Antimalware

Nekonečný boj, ve kterém nezvítězí ani jedna strana, ale malware bude vždy o krok napřed, protože reaguje na aktuálně dostupné bezpečnostní technologie



Ransomware – predikce Intel Security 2016

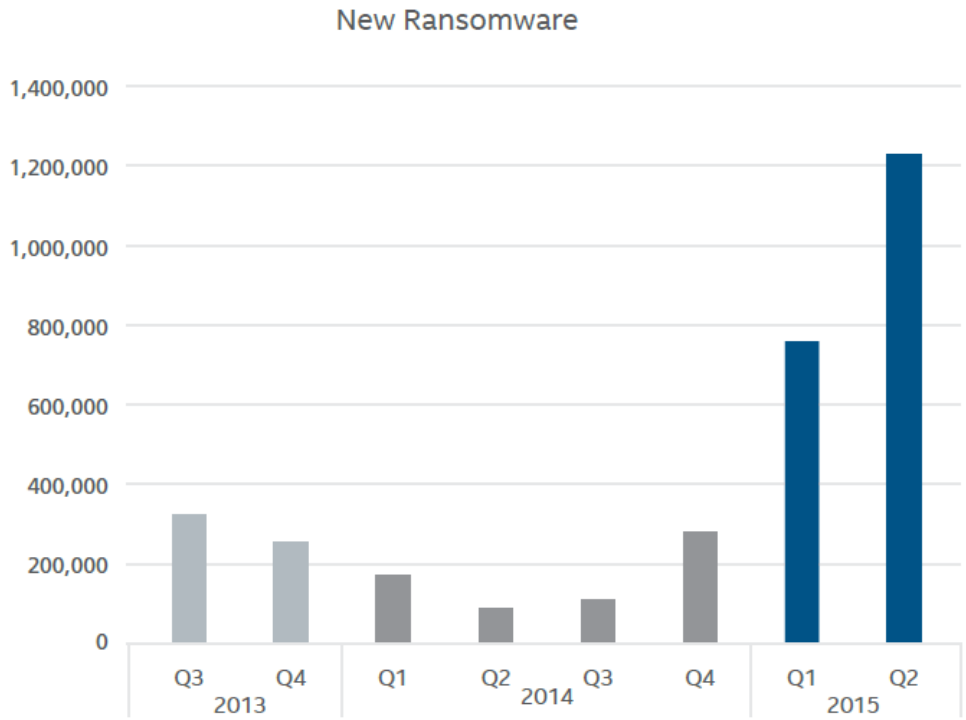


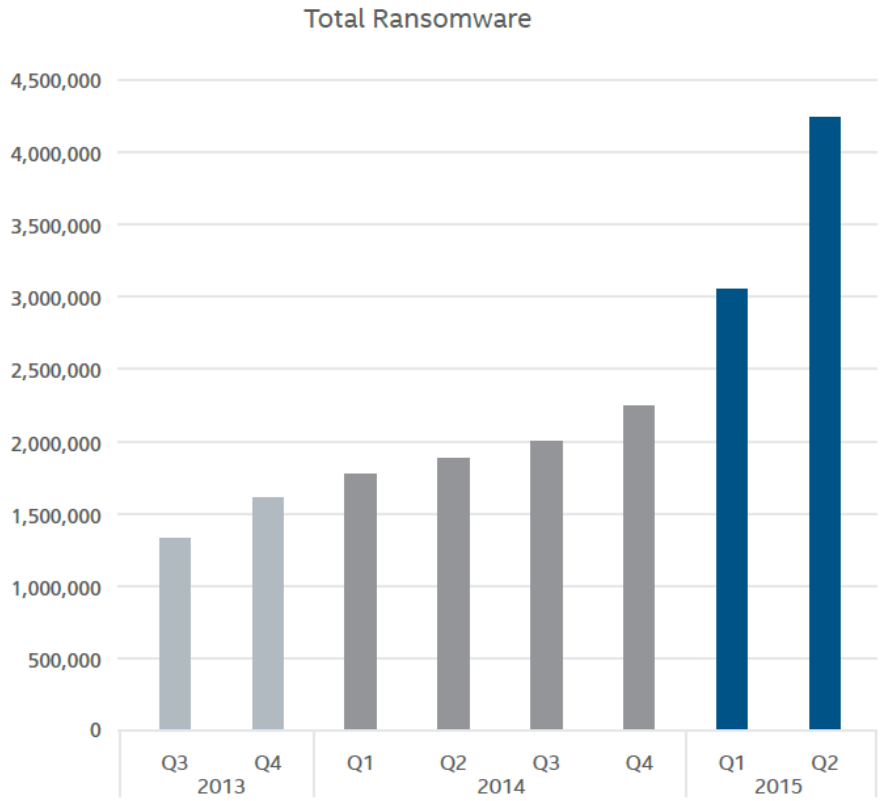
McAfee Labs 2016 Threats Predictions

Ransomware

Ransomware zůstává hlavní a rychle rostoucí hrozbou v roce 2016, využívající anonymitu sítě a nových platebních metod – bitcoin.

Nezkušení útočníci využijí Ransomware-as-a-service, čímž zvyšují množství útoků Ransomware.





Problémy s Ransomware útoky ve světě

BANK INFO SECURITY

Authentication | Compliance | Fraud | Governance | Mobility | Pay

News | Blogs | Interviews | Webinars | White Papers | Memberships | Resources | Events

Home > Articles

Ransomware Attacks' New Focus: Businesses

Why Experts Say Employee Education Is Critical

By Tracy Kitten, March 15, 2015.

Credit Eligible | Email | Tweet | Like | Share

Home / Security

Ransomware authors streamline attacks, infe rise

Ransomware authors continue improving file-encrypting programs for Windows and Android, making these nightmarish attacks harde

The biggest ransomware threat for Windows users is CryptoWall, malware program that encrypts a wide range of files and demands

The Register®
Biting the hand that feeds IT

DATA CENTER | SOFTWARE | NETWORKS | SECURITY | BUSINESS | HARDWARE | SCIENCE | BOOTNOTES | VIDEO

Ransomware holds schools hostage: 'Now give us Bitcoin worth $129k, er, $124k, wait ...'

says district boss

278 | 32 | 31

S has been held hostage by ransomware that has apparently nd the situation.

InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home | News & Commentary | Authors | Slideshows | Video | Radio | Reports | White Papers | Events | Black

ATTACKS/BREACHES | APP SEC | CLOUD | ENDPOINT | MOBILE | PERIMETER | RISK | OPERA

BBC | Sign in | News | Sport | Weather | iPlay

NEWS

Home | UK | World | Business | Election 2015 | Tech | Science | Hea

Technology

Gamers targeted by ransomware v

13 March 2015 | Technology

ATTACKS/BREACHES

3/13/2015
06:00 PM

Hackers Breaking New Ground With Ransomware

The tools and tactics being used to go after victims reveal growing sophistication, and gamers need to look out, security researchers say.

Jai Vijayan
News

The enormous success which hackers have had extracting millions of dollars from individuals and businesses using ransomware appears to be driving more sophisticated tools and tactics from them.

ETWORKWORLD | Most read:

somware: Pay it or fight it?

Cryptolocker – fáze nákazy a obrana

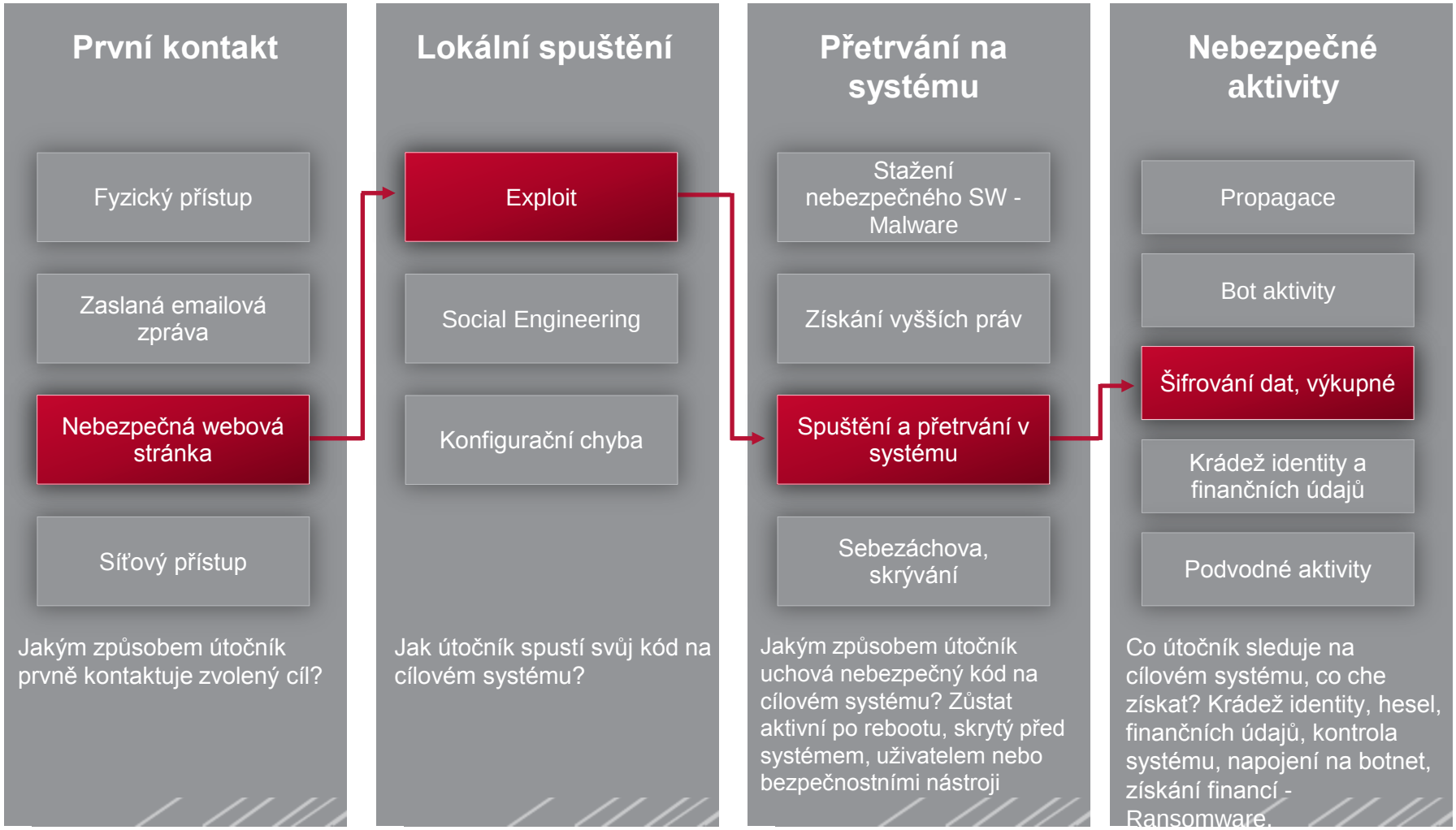
Jaký je další krok?

- Výrobci bezpečnostních technologií musí reagovat
- Detekovat malware bez signatur podle jeho chování, protože
  - Velmi často se jedná o jednoduché modifikace stejného malwaru
  - Malware provádí velmi podobné operace, např.:
    - Zajišťuje své znovuspuštění po restartu
    - Spojuje se se svým Command&Control centrem
    - Vykrádá informace z dalšího softwaru a z klávesnice
    - …
- Detekce před samotnou infekcí koncového stroje
  - Detekce malware na perimetru pomocí síťových prvků
  - Propojení síťová a endpoint bezpečnosti

Ochrana před Cryptolocker a dalším malwarem

- Standardní antivirové řešení nestačí
  - Základní kámen bezpečnosti, nikoliv hradba....
    - AV skenuje soubory porovnámím s DAT databází – blacklistig
    - Co je v DAT databázi - je nalezeno, co není v DAT databázi - je povoleno
    - AV není schopen v reálném čase reagovat na nové nebo modifikované hrozby
- Základní řešení
  - Antivirové a antispamové řešení na bráně i endpointu
  - Host nebo Network IPS
  - Pravidelná záloha souborů
  - Vzdělávání uživatelů – neotevírat přílohy podezřelých emailů
  - Kontrola URL adres při webové komunikaci
  - **Vyšší úroveň bezpečnosti pomocí Adaptivní inteligence při vyhledávání hrozeb**
    - **McAfee Application Control**
    - **McAfee Threat Inteligence Exchange / Data Exchange Layer – TIE/DXL**
    - **McAfee Advanced Threat Defense – ATD**
    - **McAfee Active Response – MAR, McAfee SIEM**

Čtyři fáze útoku na koncový systém - Ransomware




První kontakt
Lokální spuštění
Přetrvání na systému
Nebezpečné aktivity
McAfee® SiteAdvisor®
Website Filtering
Mobile Device Management
McAfee Device Control
Physical File Transfer
McAfee Desktop Firewall
McAfee Desktop Firewall
McAfee Web Gateway a Network IPS
Web Filtering
Email Filtering
On-Access Scanning
Buffer Overflow Prevention
McAfee Endpoint Protection
File Scanning
McAfee Database Activity Monitor
Database Vulnerability Blocking
McAfee Endpoint protection
Rootkit Prevention
McAfee Host Intrusion Prevention
Behavioral Prevention
McAfee Application Control, Threat Inteligence Exchange
Install and Execution Prevention
Write Blocking
Change Protection

McAfee Application control

McAfee Application Control

Bezpečnostní nástroj využívající inteligentní whitelisting

Dynamický whitelisting		Ochrana před spuštěním neautorizované aplikace
Ochrana paměti		Ochrana operační paměti proti útokům a manipulací s aplikacemi - buffer overflow útoky
Reputace souborů		Integrace s GTI a TIE pro klasifikaci aplikací jako Good, Bad a Unknown
Integrace		Napojení na ADT pro kontolu souborů pomocí sandbox technologie, Desktop Firewall integrace

Princip funkce whitelistingu

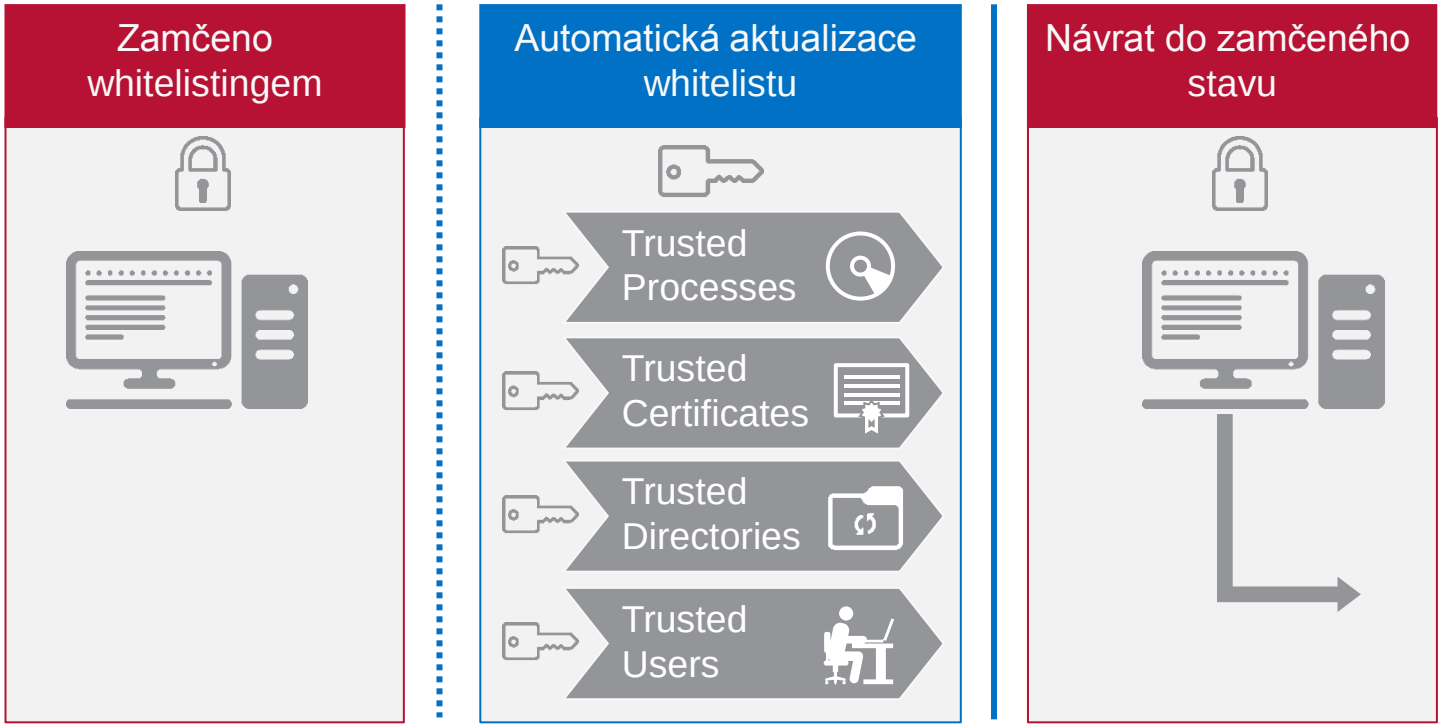
Whitelist je vytvářen po instalaci produktu skenováním systému – aplikací, knihoven, ovladačů a skriptů

1. Pokus o spuštění programu
   - Spustitelný soubor nebo komponenta OS

2. MAC porovnává binární kód s whitelistem

3. Pokud soubor není ve whitelistu, spuštění programu se zablokuje.
   - Událost je logována, alertována nebo auditována

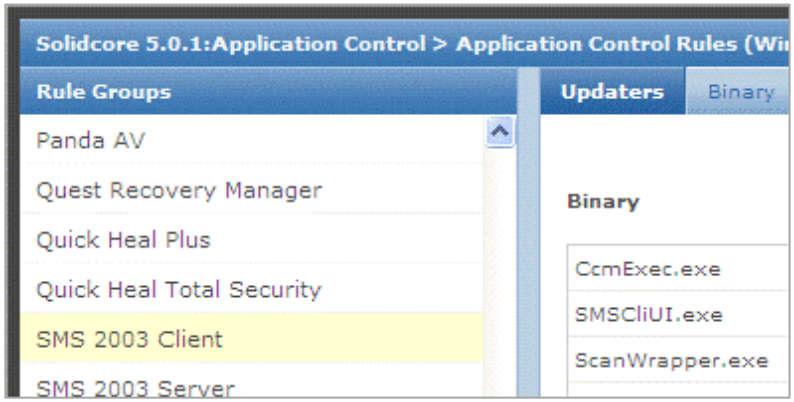
Dynamický model Application Controlu



Dynamický model whitelistingu

1. Důvěryhodné procesy

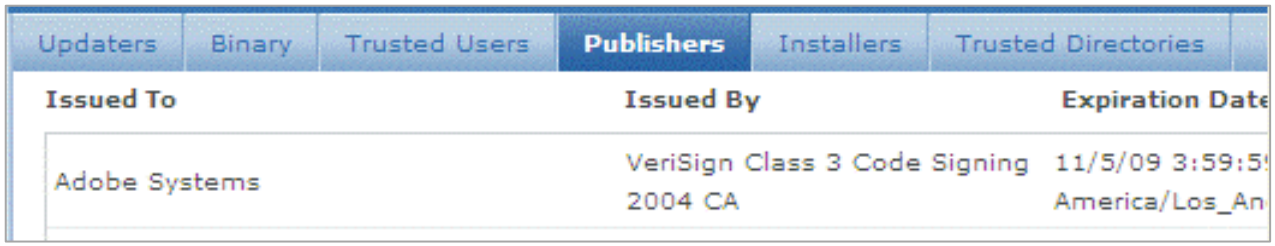
- Nově vytvořená nebo modifikovaná aplikace je přidána do whitelistu
- Podpora standardních updaterů jako MS SMS, SCCM, atd.
- Běžně používané updatery jsou přednastavené
- **Observation-mode** pomáhá vyhledávat updatery



Dynamický model whitelistingu

2. Důvěryhodné certifikáty

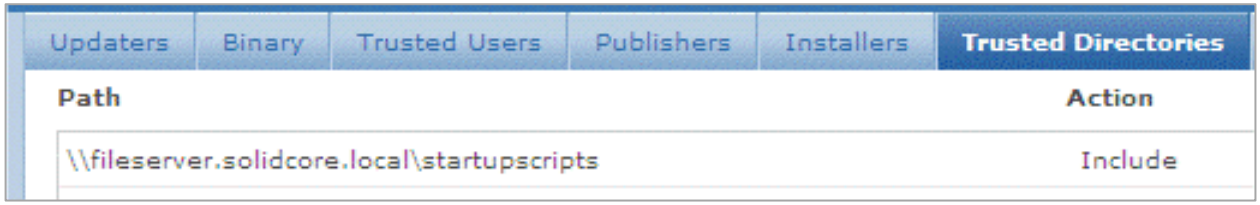
- Důvěra k aplikacím podepsaných známými výrobci
- Self Signing - velmi polulární metoda
  - Vytvoření vlastního certifikátu a podepsání autorizovaných aplikací



Dynamický model whitelistingu

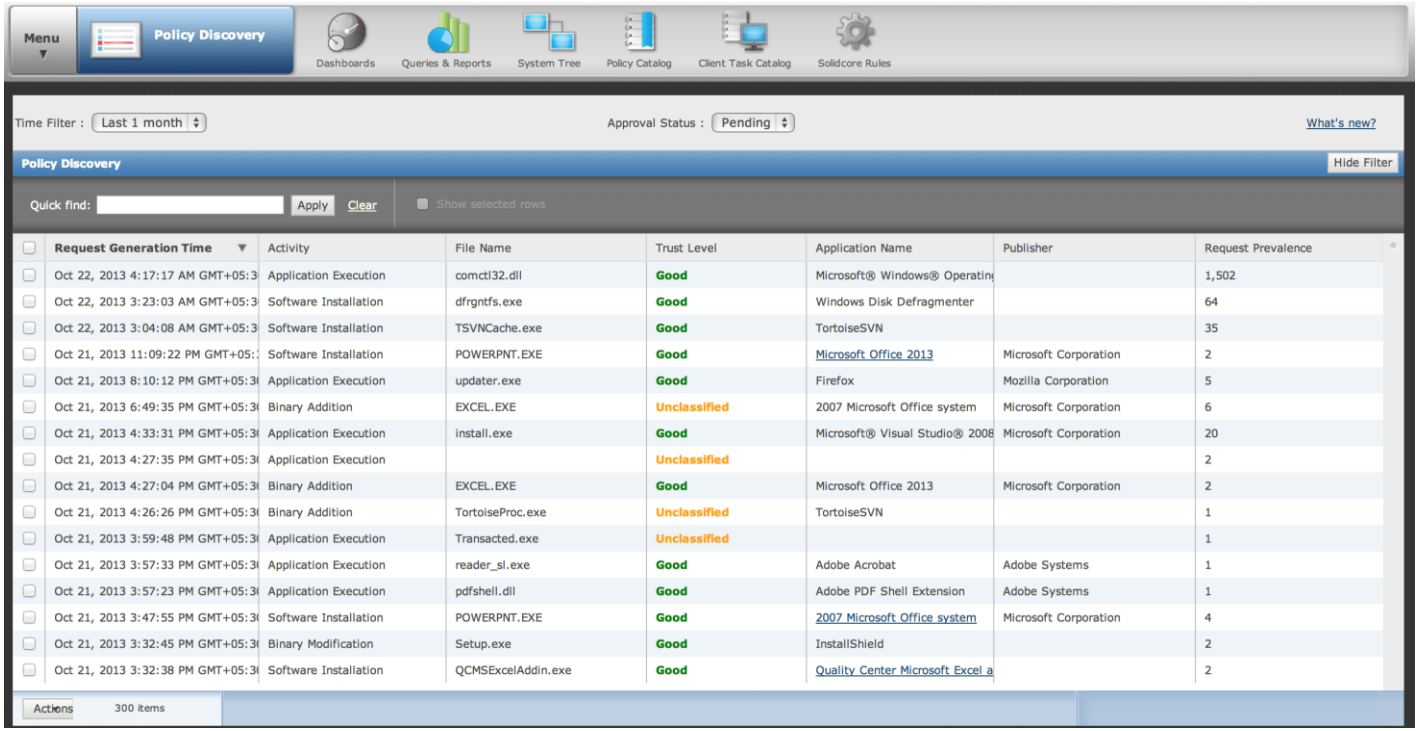
3. Důvěryhodný adresář

- Definuje sdílený adresář, který je důvěryhodný pro instalaci aplikace



Dynamický model whitelistingu

4. Důvěryhodný uživatel (IT Admins)



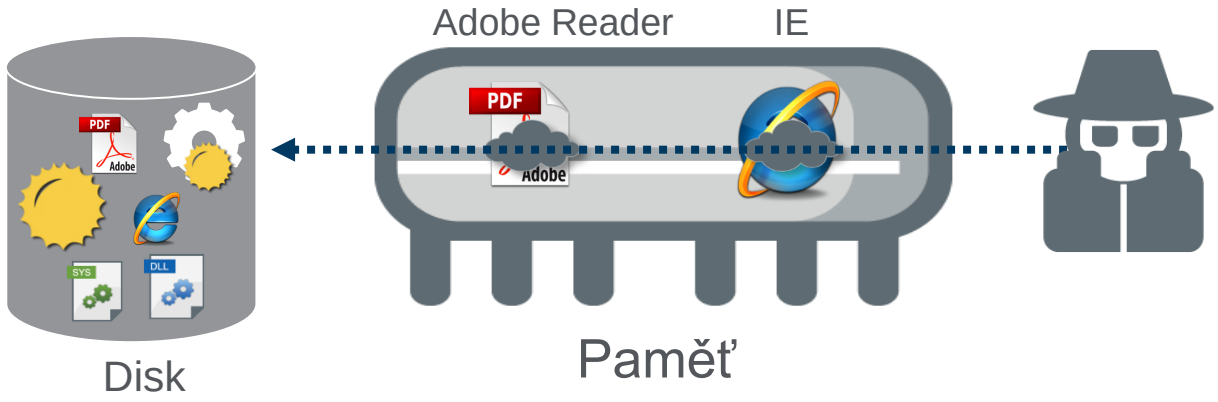
Dynamický model whitelistingu

4. Důvěryhodný uživatel (Koncový uživatel, který si smí schválit spuštění aplikace)

- Aplikace, která není ve whitelistu, může být schválena uživatelem
- Tento model je vhodný pro uživatele/systémy, kde se dějí časté změny (není doporučený pro všechny uživatele)
- Administrátor má možnost auditovat tyto uživatelsky schválené aplikace a může provést změny - povolit/zalázat

Ochrana paměti počítače – proč je nutná?

- Důvěryhodný program je spouštěn v paměti počítače
- Nicméně, tento program má zranitelnost – Acrobat Reader, IE, Firefox....
- Zravitelnost může být útočníkem zneužita vzdáleně
- Skrze zranitelnost změní útočník systémová nastavení a spustí škodlivý kód



Ochrana paměti – Co dělá Application Control

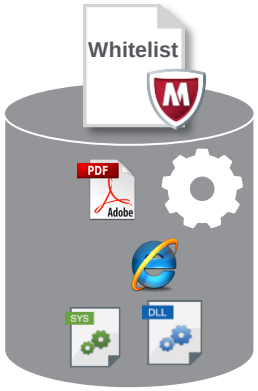
Ochrana aplikace whitelistem

- Program ve whitelistu nemůže být zneužit – nový spouštěný program (malware) nemá záznam ve whitelistu

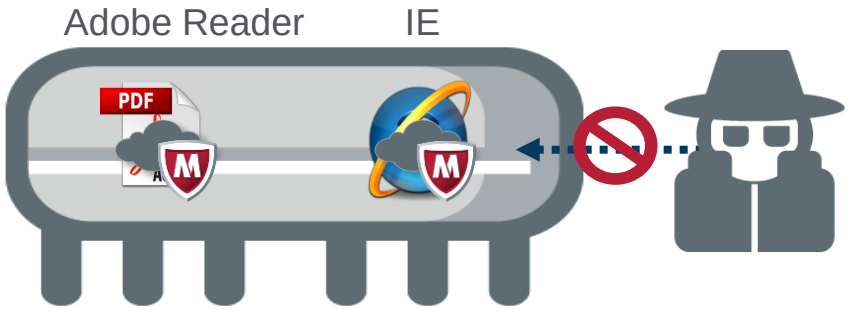
Ochrana paměti pracuje bez signatur

Application Control redukuje nutnost okamžité instalace záplat!

Dostupný pro Windows 32-bit & 64-bit systémy



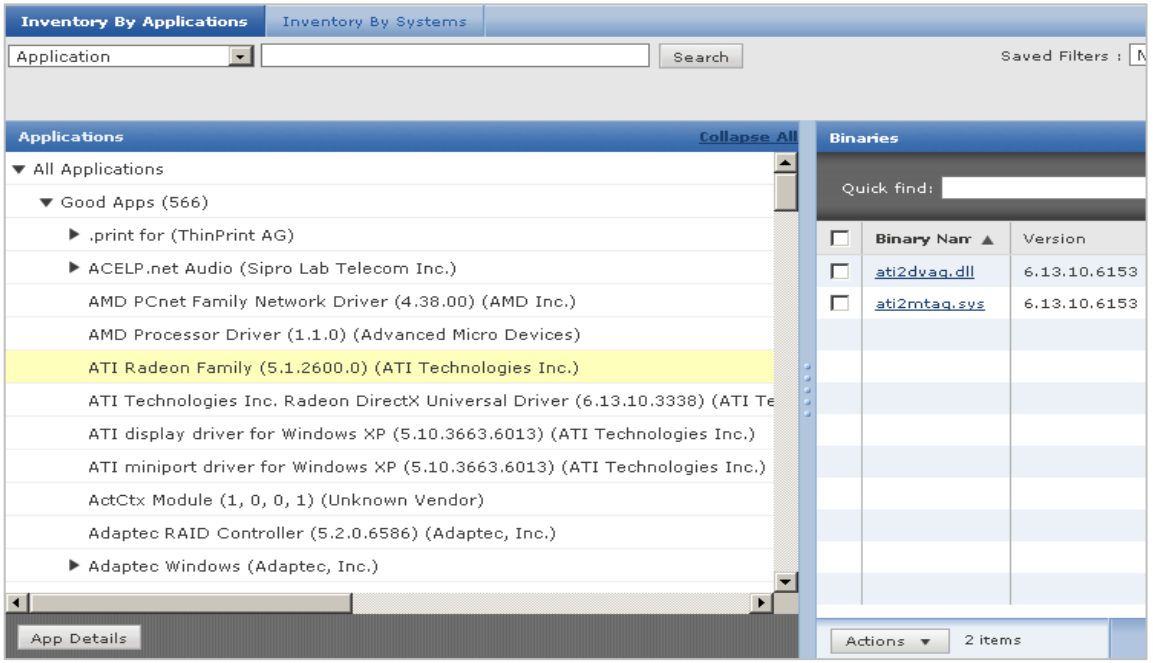
Disk



Paměť

Inventorizace aplikací

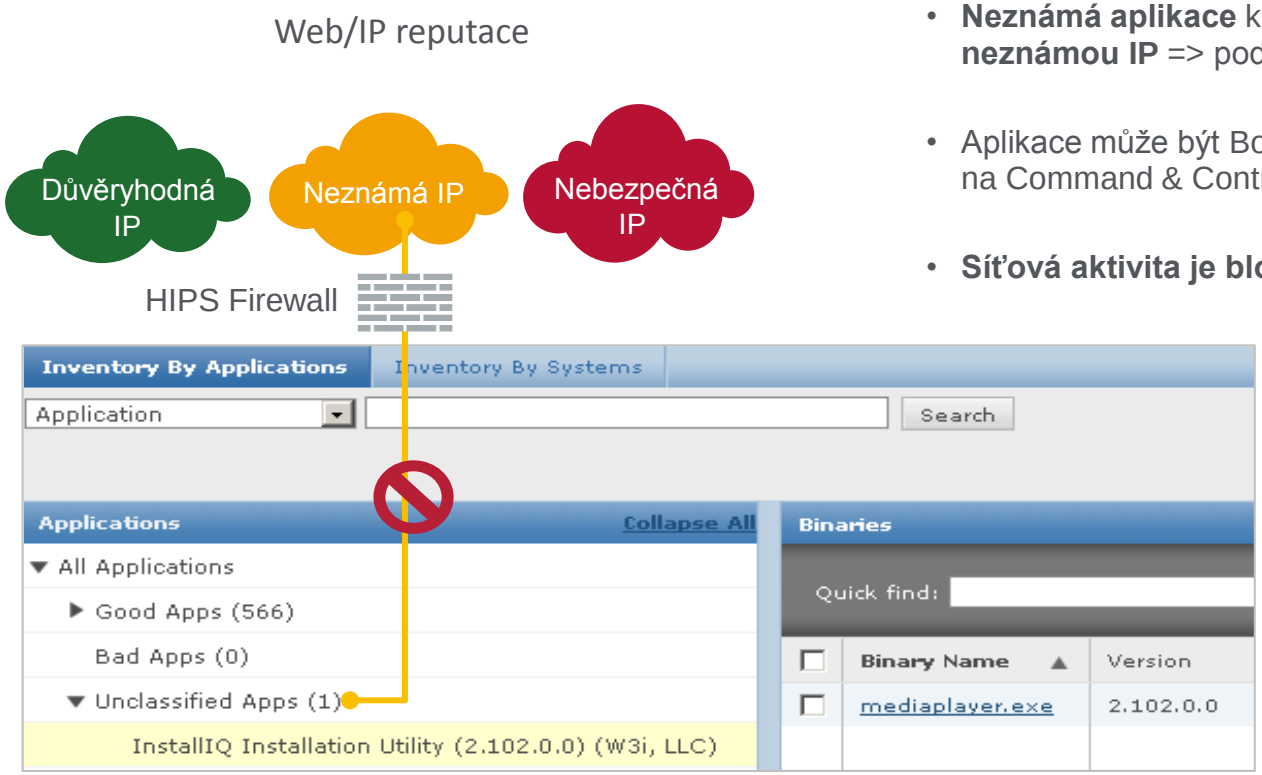
- Ucelený přehled o všech aplikacích na koncových bodech – seznam whitelistů v jedné konzoli
- Kontrola aplikací s Globálním reputčním systémeme GTI – ohodnocení bezpečnosti aplikací
- Seznam aplikací s neznámou reputací – možnost okamžité nápravy – povolit/zakázat
- Seznam zastaralých verzí běžících aplikací – Adobe Reader.....



Spolupráce s firewallem pro neznámé aplikace

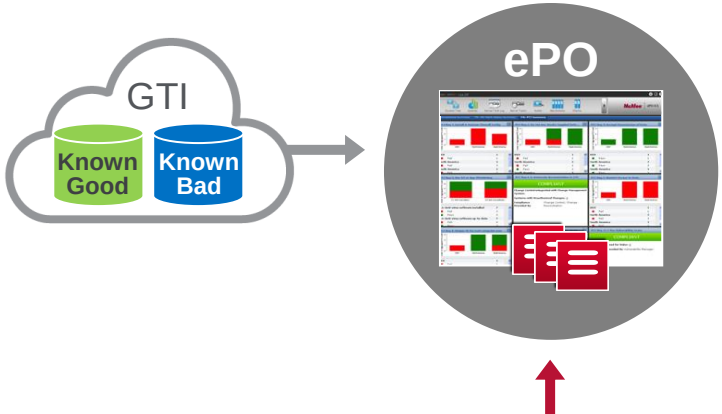
Reputace souborů + IP reputace

- **Neznámá aplikace** komunikuje na **neznámou IP** => podezřelá aktivita!
- Aplikace může být Botnet/APT komunikující na Command & Control Server
- **Síťová aktivita je blokována firewallem**



Application Control v McAfee ekosystému

GTI: Reputace souborů z cloudu



TIE: Lokální reputace souborů

ATD: sandboxová analýza souboru

VSE: Soubor je zapsán do whitelistu po úspěšné kontrole AV

HIPS: Neznámé aplikace (graylist) blokovaná komunikace

Jaké řešení vybrat do prostředí společnosti?

	Jednoúčelové systémy	Servery	COE stanice/notebooky	Dynamické stanice/notebooky
				
	⬅ STATICKÉ			DYNAMICKÉ ➡
Primární Antimalware	MAC	MAC	MAC	TIE, AV
Sekundární Antimalware		ODS	AV	

TIE / DXL
Threat Intelligence Exchange
Data Exchange Layer

Threat Intelligence Exchange - TIE/DXL technologie

Threat Intelligence Exchange (TIE) je systém, který zjišťuje reputaci spouštěných souborů z různých zdrojů a na základě této reputace umožní spustit nebo zablokovat tuto aplikaci.

- Využívá Data eXchange Layer(DXL) k distribuci reputací
- Kombinuje informace z více bezpečnostních zdrojů k určení reputace
- Adaptivní bezpečností snižuje riziko při spouštění souborů

Poskytuje absolutní přehled o spouštěných aplikacích na koncových bodech

- Možnost využití i pro inventarizaci aplikací a jejich využívání na jednotlivých strojích

Propojení s GTI cloud službou

- Okamžité reakce na detekované hrozby oproti rychlosti aktualizaci DAT
- Centrální bod který agreguje požadavky na GTI z interní sítě

Lokální reputace aplikací/souborů

- Eliminování možnosti detekce interního SW jako virus
- Možnost definovat „firemní Image“ jako prověřený systém

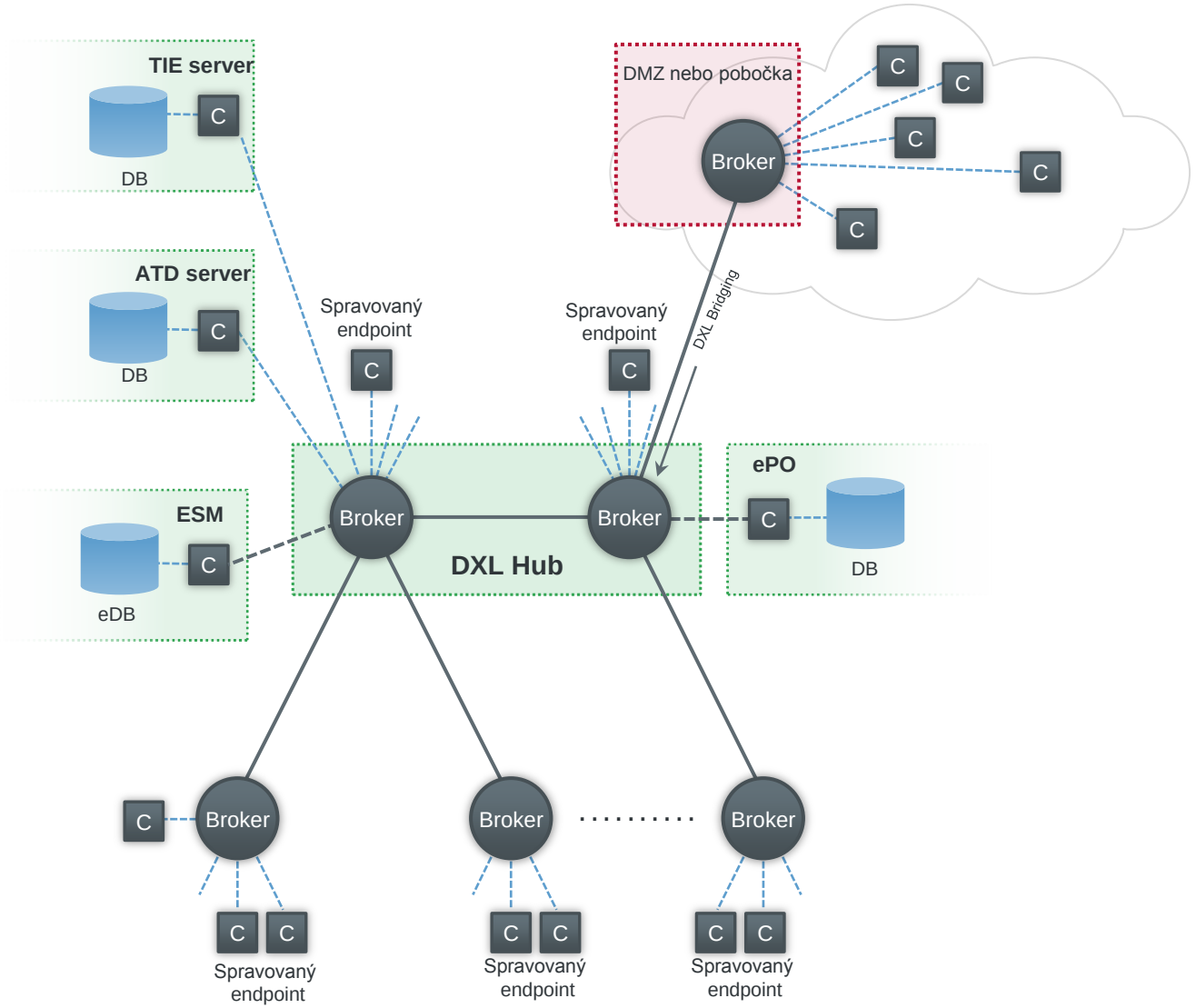
Napojení na službu Virustotal

- Využití 57 skenovacích engine od světových výrobců pro kontrolu spouštěných aplikací

Co je Data Exchange Layer

Data Exchange Layer (DXL) je základní vrstva pro SecurityConnected architekturu

- Vlastností DXL klienta je iniciovat trvalé připojení k serverům pro zasílání zpráv skrze tzv. Brokery
- DXL je založen na protokolu Message Queue Telemetry Transport (MQTT)
- Navržen pro optimalizaci komunikace zařízení na sítích s malou šířkou pásma, vysokou latencí nebo nespolehlivé sítě
- Šifrovaná komunikace pomocí TLS 1.2 na portu 8883
- Server iniciuje komunikaci na dříve nedostupného klienta
- DXL je plně spravován pomocí ePO serveru

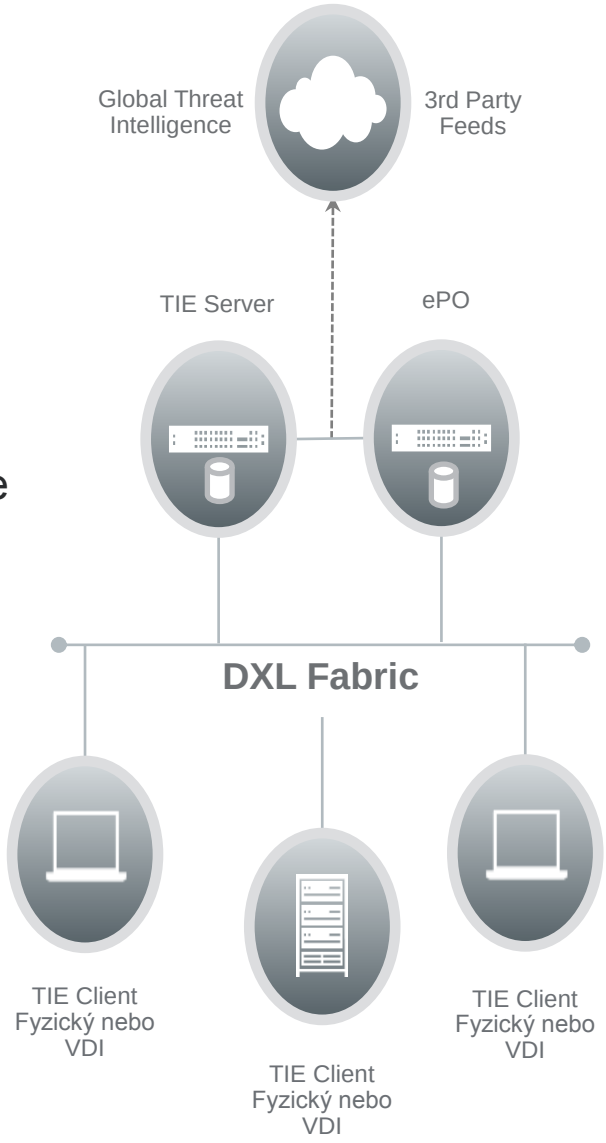

TIE server
C
DB
ATD server
C
DB
ESM
C
eDB
DMZ nebo pobočka
C
C
C
Broker
C
C
DXL Bridging
Spravovaný endpoint
C
Spravovaný endpoint
C
Broker
Broker
DXL Hub
ePO
C
DB
C
Broker
Broker
Broker
C
C
C
C
C
C
Spravovaný endpoint
Spravovaný endpoint
Spravovaný endpoint

TIE/DXL architektura

McAfee Threat Intelligence Exchange

Komponenty řešení

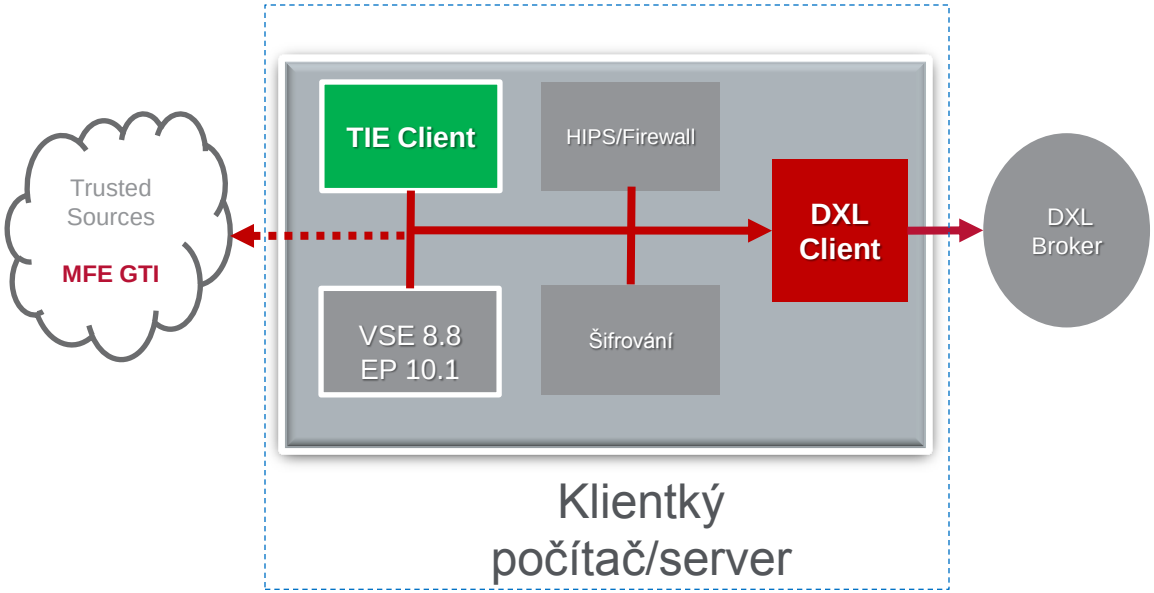
- TIE Server – virtuální image na VMware
- TIE Client
- DXL Fabric



TIE Client architektura

Podporované operační systémy

- Microsoft Windows 7 (32-bit and 64-bit)
- Windows 8.0 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 8.1U1/U2 (32-bit and 64-bit)
- Windows 10.0 (32-bit and 64-bit)
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows 10 (32-bit and 64-bit) using Patch 6

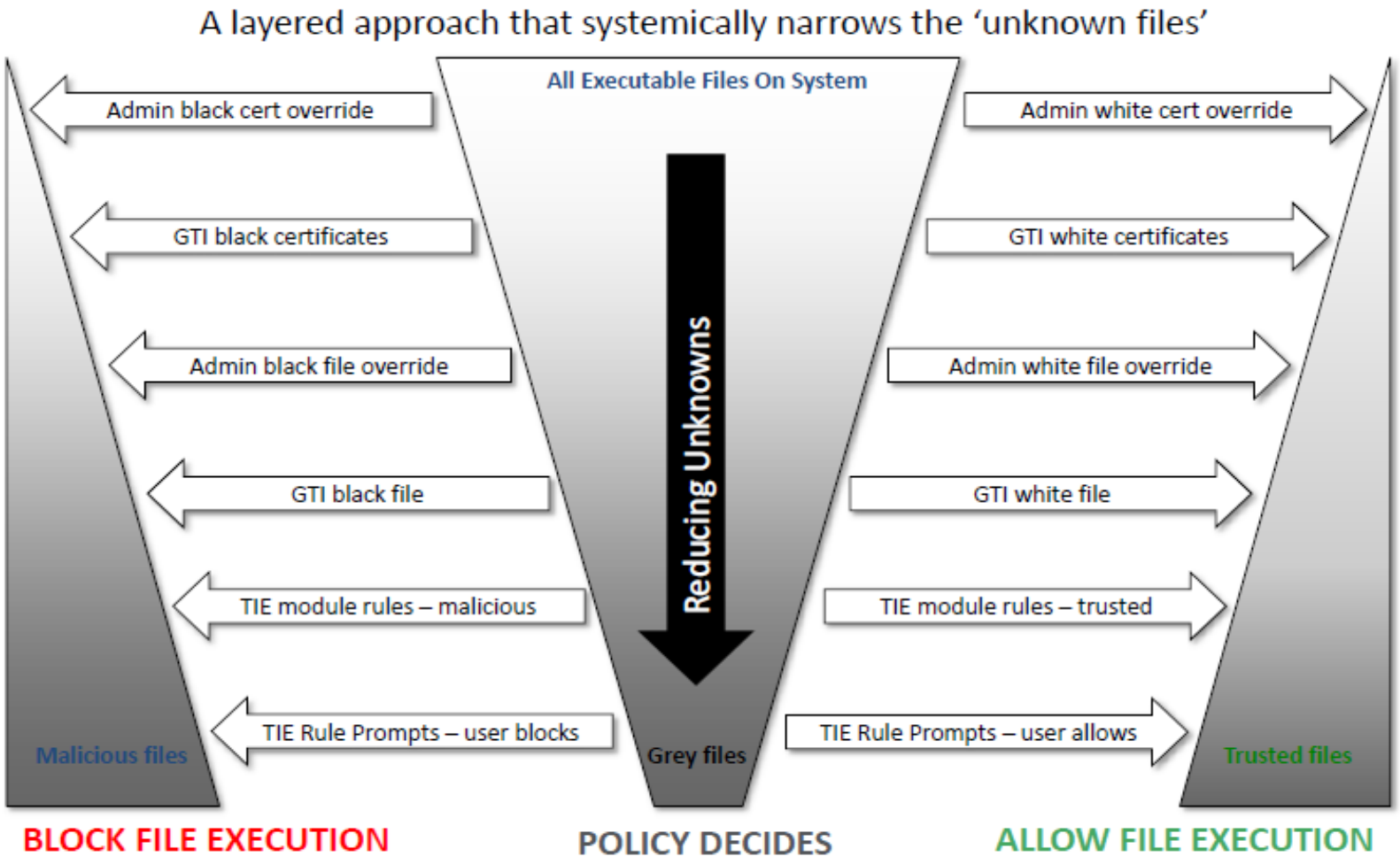


TIE logika - reputace souborů

Metadata, která využívá logika TIE klienta:

- ✓Statická data souboru
  - Hash souboru, velikost, typ souboru, verze .....
- ✓Procesní data o souboru
  - Nadřazený proces / soubor, jaký proces spouští cílový soubor, počet vláken.....
- ✓Data o prostředí souboru
  - Cesta k souboru, instalace služby, spouštění klíčů
  - Souštění souboru z lokální sítě, počítače, z Internetu
  - Počet spuštění soubor v rámci lokální sítě
- ✓Data o certifikátech
  - Seznam certifikátů a jejich řetězení
  - Soubor podepsaný platným/revokovaným certifikátem

TIE logika klienta – filtr pro určení reputace souboru



TIE logika – reputační pravidla

1. Installation Verification (TIE Test sample).
2. Identify that the file is the main component of a trusted installer using the file's certificate reputation.
3. Identify that a file is the main component of a trusted installer using the file's reputation.
4. Identify certificates needing reputation correction.
5. Use certificate reputation to identify trusted or malicious files.
6. Use Enterprise file reputation to identify trusted or malicious files.
7. Use GTI file reputation to identify trusted or malicious files.
8. Identify trusted files with McAfee Privileges.
9. Intelligent Prompt.
10. Identify trusted signed applications.
11. Identify trusted Help resource libraries.
12. Identify trusted help resource libraries.
13. Identify trusted signed utility applications.
14. Identify trusted signed drivers.
15. Identify trusted signed Digital Rights Management (DRM) libraries.
16. Identify trusted signed files.
17. Identify trusted files from a trusted creator.
18. Identify trusted prevalent files.
19. Identify trusted files on the disk that were prevalent in the enterprise prior to installing the TIE module.
20. Identify suspicious files executing from the Recycle bin.
21. Identify suspicious files executing from the roaming folder.
22. Find suspicious files signed with a revoked certificate.
23. Identify a suspicious password stealer.
24. Identify suspicious files that are hidden from the user.
25. Identify suspicious files created by an untrusted process.
26. Identify a suspicious file that hides in a secure location.
27. Identify a suspicious keylogger hiding as an installed program.
28. Identify files that ATD reports as suspicious.
29. Identify web installers.
30. Identify trusted DOTNet assemblies.
31. Identify trusted files on the disk.
32. Identify suspicious files that have odd creation dates and are likely not packed.
33. Identify suspicious files that have odd creation dates and are likely packed.
34. Identify a file as suspicious based on how it is packed.
35. Identify a suspicious key logger.
36. Identify a suspicious file that hides its age.
37. Identify new suspicious files.
38. Identify new suspicious files seen on a small number of systems.
39. Identify suspicious files from the Internet.
40. Trust files based on High Change Systems security level when offline.
41. Trust files based on typical systems security level when offline.
42. Trust files based on Low Change Systems security level when offline.
43. Not Applicable.
44. Generic reputation merge.
45. Identify a file as suspicious when executed by the command shell.
46. Identify a suspicious password stealer (large).
47. Identify a suspicious password stealer (medium).
48. Identify safe files extracted by Windows Installer.

TIE logika – výpočet reputace souborů

Reputation Legend:	Description:	Reputation Value:
Known Trusted Installer	Trusted file installer based on GTI or Enterprise reputation	100
Known Trusted	This is a trusted file	99
Most Likely Trusted	Almost certainly a trusted file	85
Might be Trusted	Appears to be a benign file	70
Unknown	Cannot make a determination at this time	50
Might be Malicious	Appears to be a suspicious file	30
Most Likely Malicious	Almost certainly a malicious file	15
Known Malicious	This is a malicious file	1
Not Set	No reputation available / No Enterprise reputation set	0

Příklad reputace TIE - porovnání třech spouštěných souborů

Microsoft Visio

- ✓ Podepsaný důvěryhodným certifikátem
- ✓ Silná globální reputace z GTI

Důvěryhodnost: Velmi vysoká
Akce: **Povolit**

Zákaznická aplikace

- ▬ Žádný podpis
- ▬ Žádná globální reputace
- ✓ Mnohokrát spouštěný v lokálním prostředí / důvěryhodná lokální aplikace
- ✓ Žádné další atributy bezpečnostní hrozby

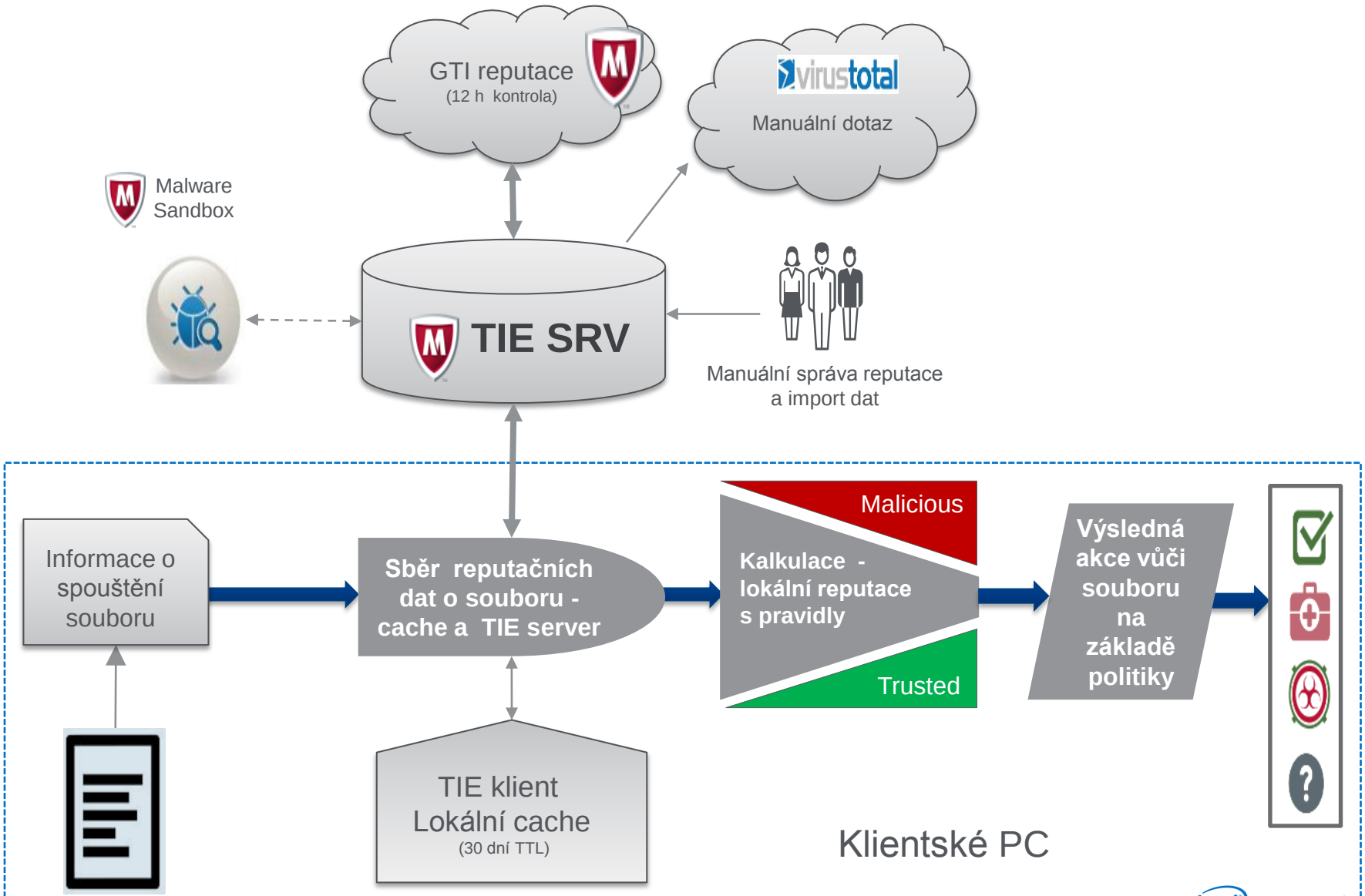
Důvěryhodnost : Vysoká
Akce: **Povolit**

Neznámý soubor - malware

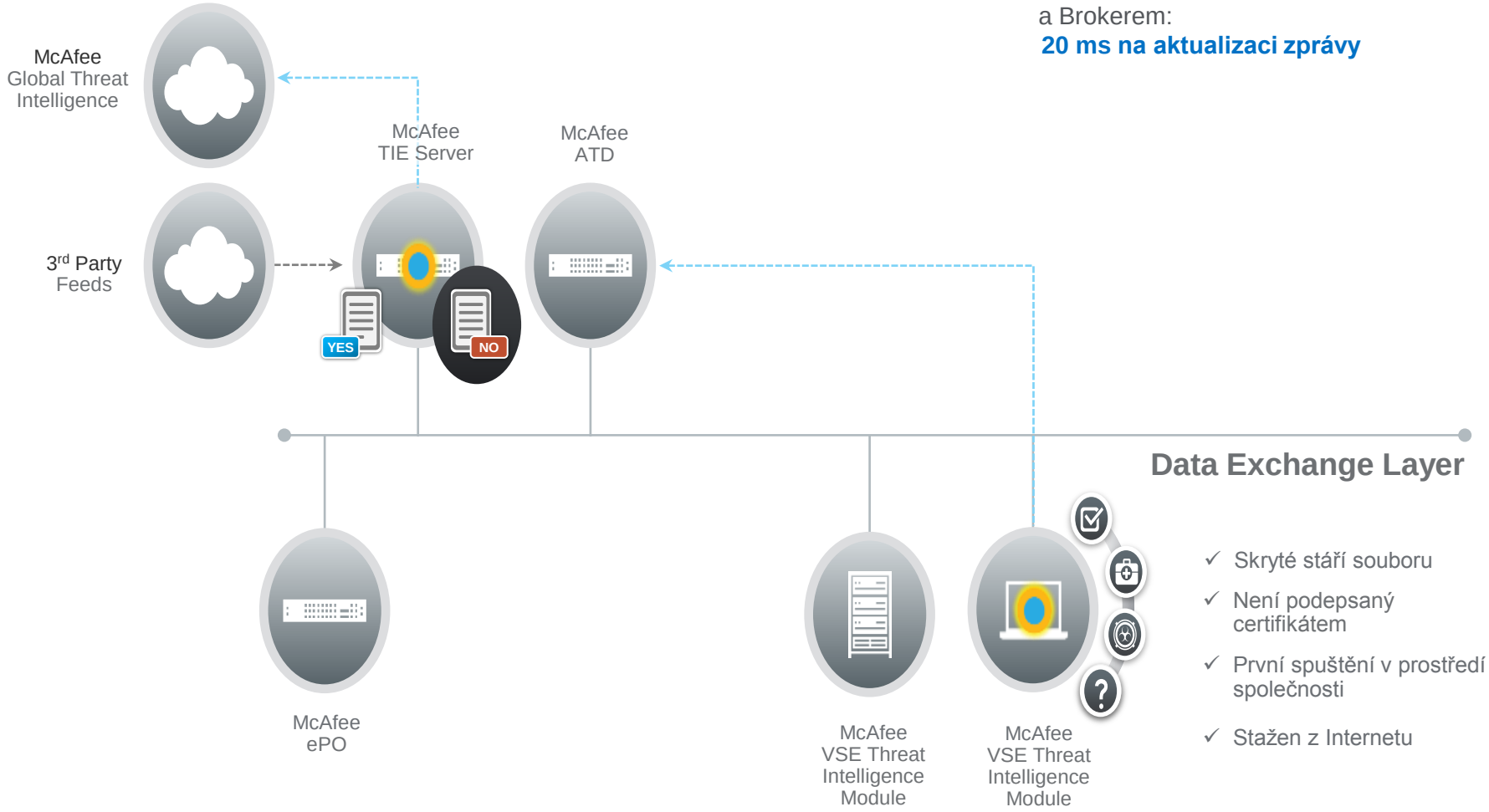
- ▬ Žádný podpis
- ▬ Žádná globální ani lokální reputace
- ✗ První spuštění v lokálním prostředí
- ✗ Podezřelý atribut – download z Internetu

Důvěryhodnost : Nízká
Akce: **Blokovat**

Logika TIE technologie



- Rychlost odbavení zpráv Brokerem:
  20K zpráv za sekundu
- Průměrná doba komunikace mezi klientem a Brokerem:
  20 ms na aktualizaci zprávy



ATD
Advanced Threat Defense

McAfee Advanced Threat Defense

Specializovaná appliance určená na detekci známého i neznámého (tzv. zero-day) malwaru

Detekci neznámého malware zařizuje kombinace několika metod, jednou z hlavních je **sandboxing**

- Soubor je otevřen/spuštěn ve virtuálním prostředí, které simuluje klientský stroj a ATD sleduje veškeré jeho činnosti

McAfee Advanced Threat Defense
Architektura řešení

Jádro

Admin VM
Linux 64bit:

Administration
Scheduler
Task manager
File input / Server
Results output

Communication
HTTP/HTTPS
FTP/SFTP
Restful API
Socket

Engine

- Lokální B/W listy
- GAM engine
- GTI reputace
- MFE Antivirus

Zákaznicky definovatelné Sandbox image

Windows XP SP2/SP3

Server 2003 SP1/SP2

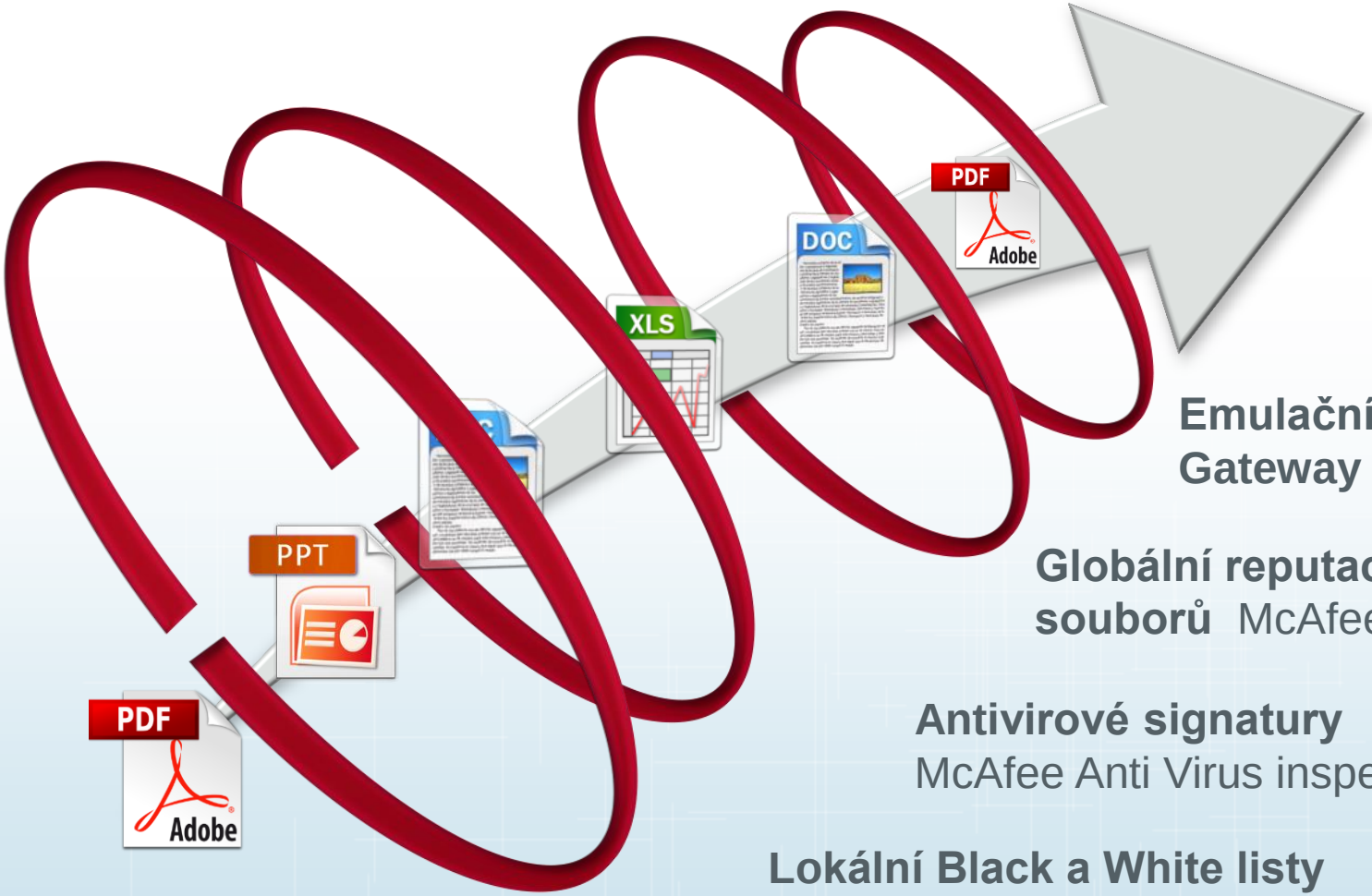
Server 2008 64bit

Windows 7 32bit/64bit

Android

Type-I Hypervisor

Intel-based Hardware Platform



Sandboxing
Statická a dynamická analýza

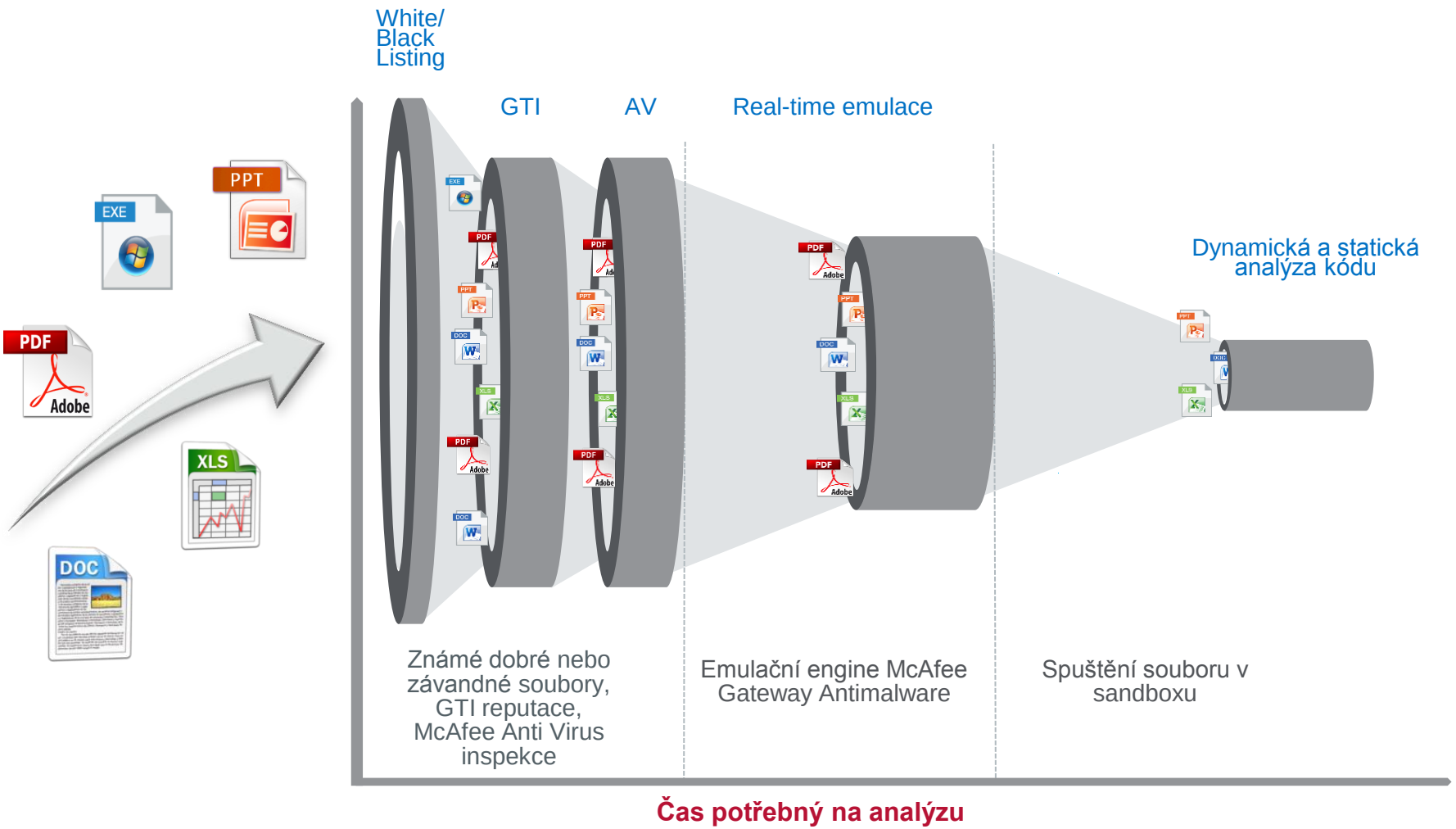
Emulační engine – Gateway Anti- Malware

Globální reputace souborů McAfee GTI

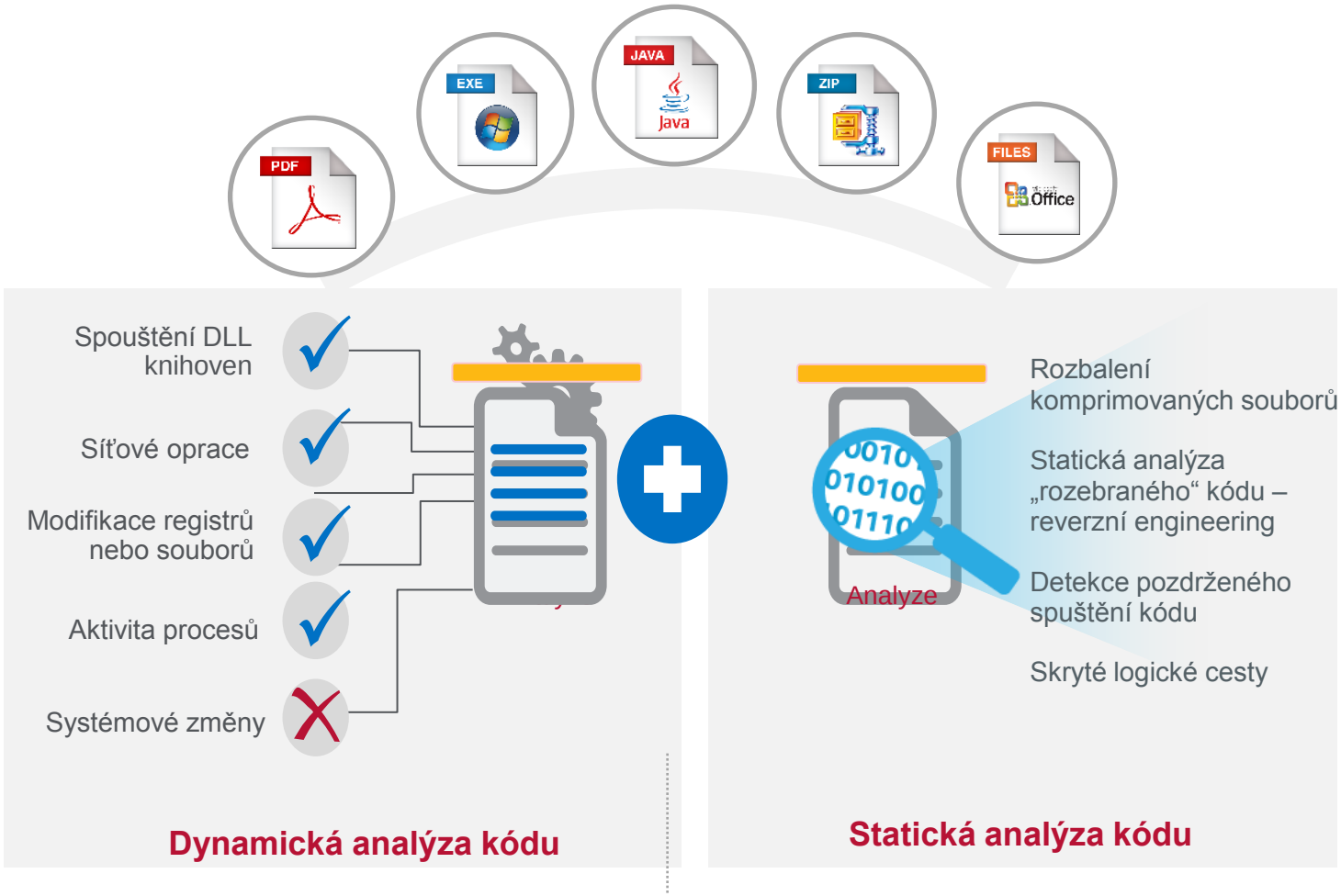
Antivirové signatury
McAfee Anti Virus inspekce

Lokální Black a White listy
Známé dobré a závadné soubory

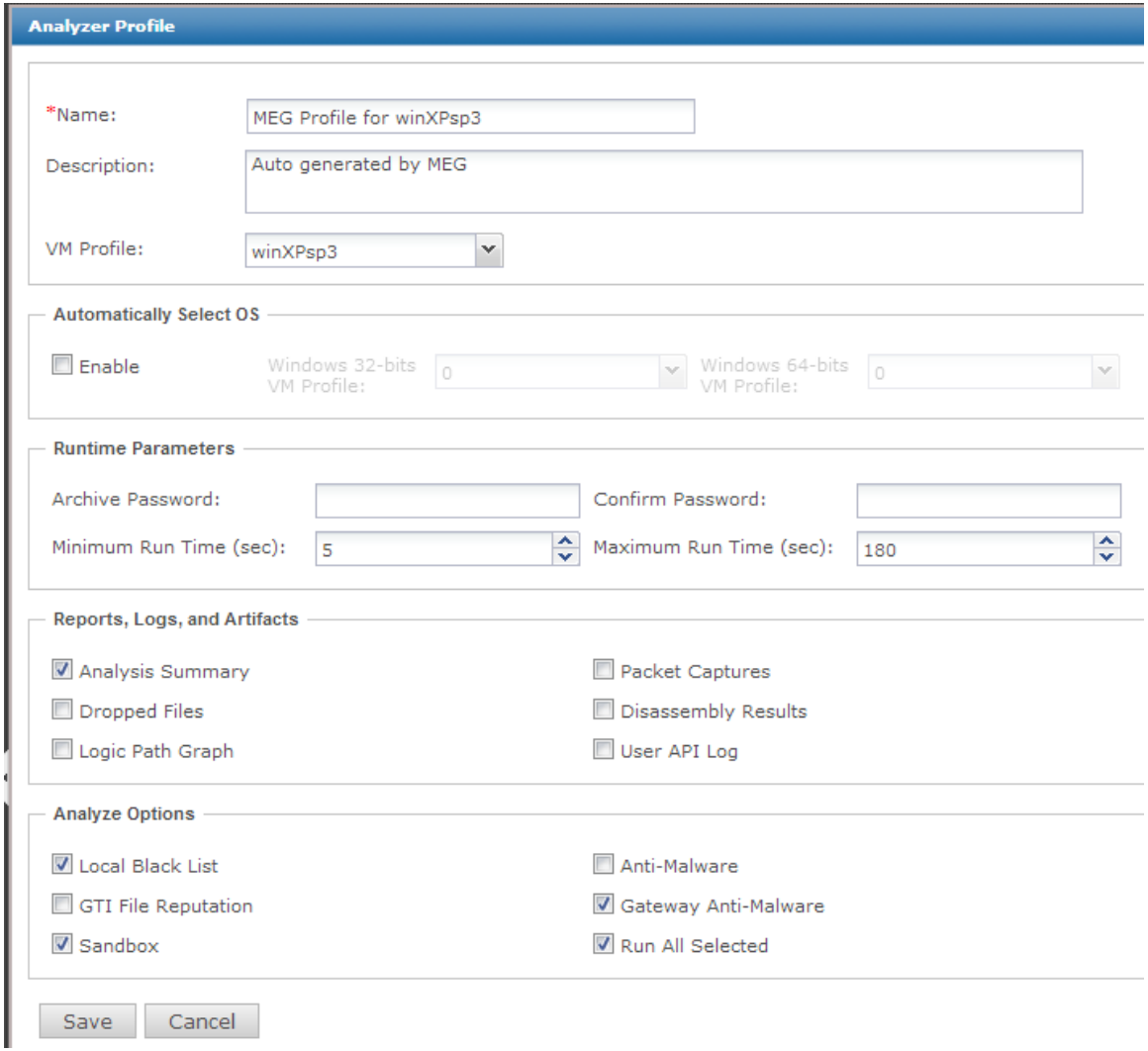
Detekce malware na více úrovních



Dynamická a statická analýza kódu

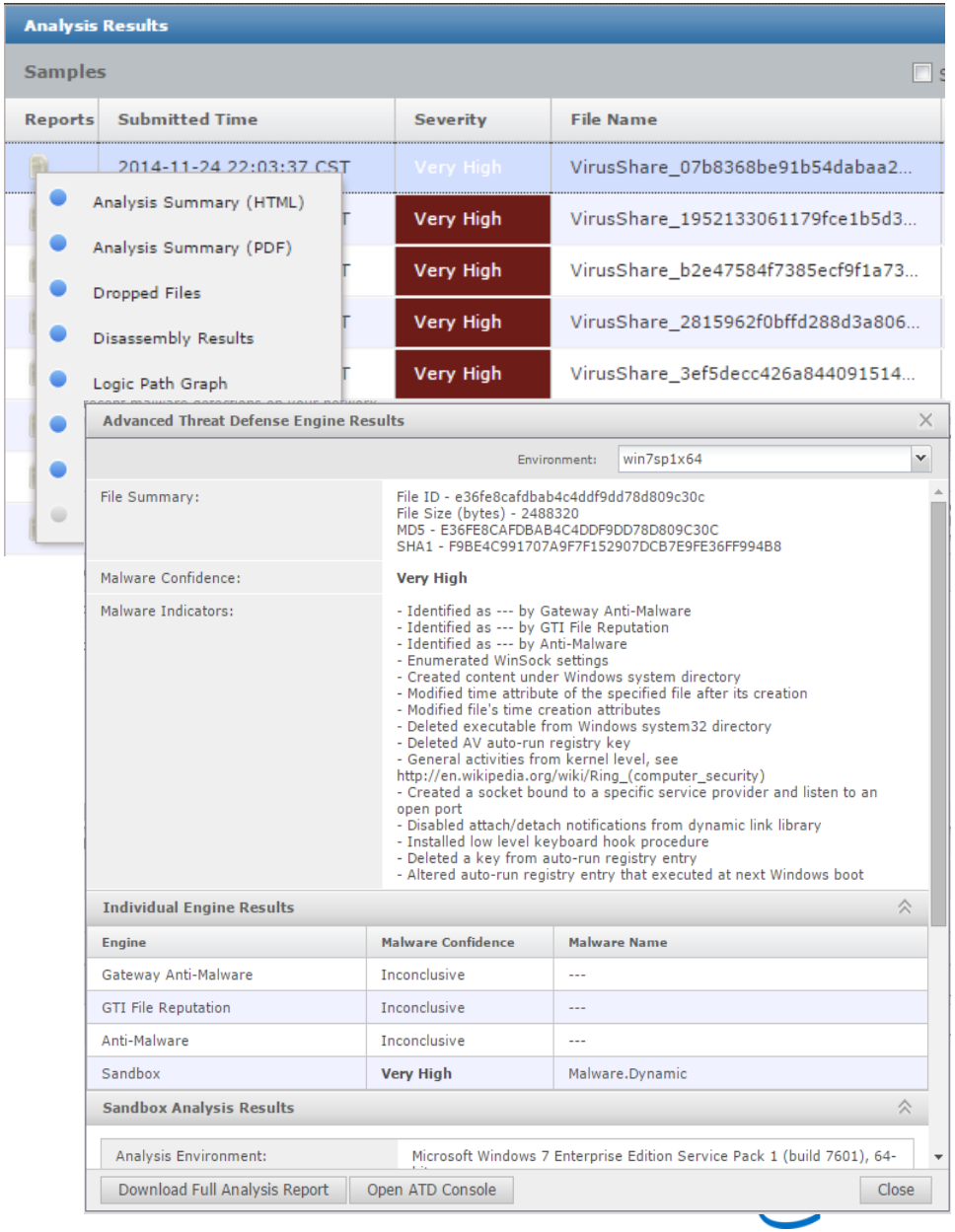


Profil pro hloubkovou analýzu na ATD



ATD reporty

- Možnost sortování pro všechny sloupce
- Každý report má více možností výstupu
  - Sumární report obsahuje grafický výstup výsledku skenování
  - Dropped files je zobrazení souborů, které byly stahovány malwarem
  - Disassembly - výsledek statické analýzy kódu – rozebrání kódu
  - Logic Path je grafické znázornění výstupu statické analýzy
  - Kompletní report obsahuje veškeré výsledky skenování včetně packet traces a IOC/STIX informací



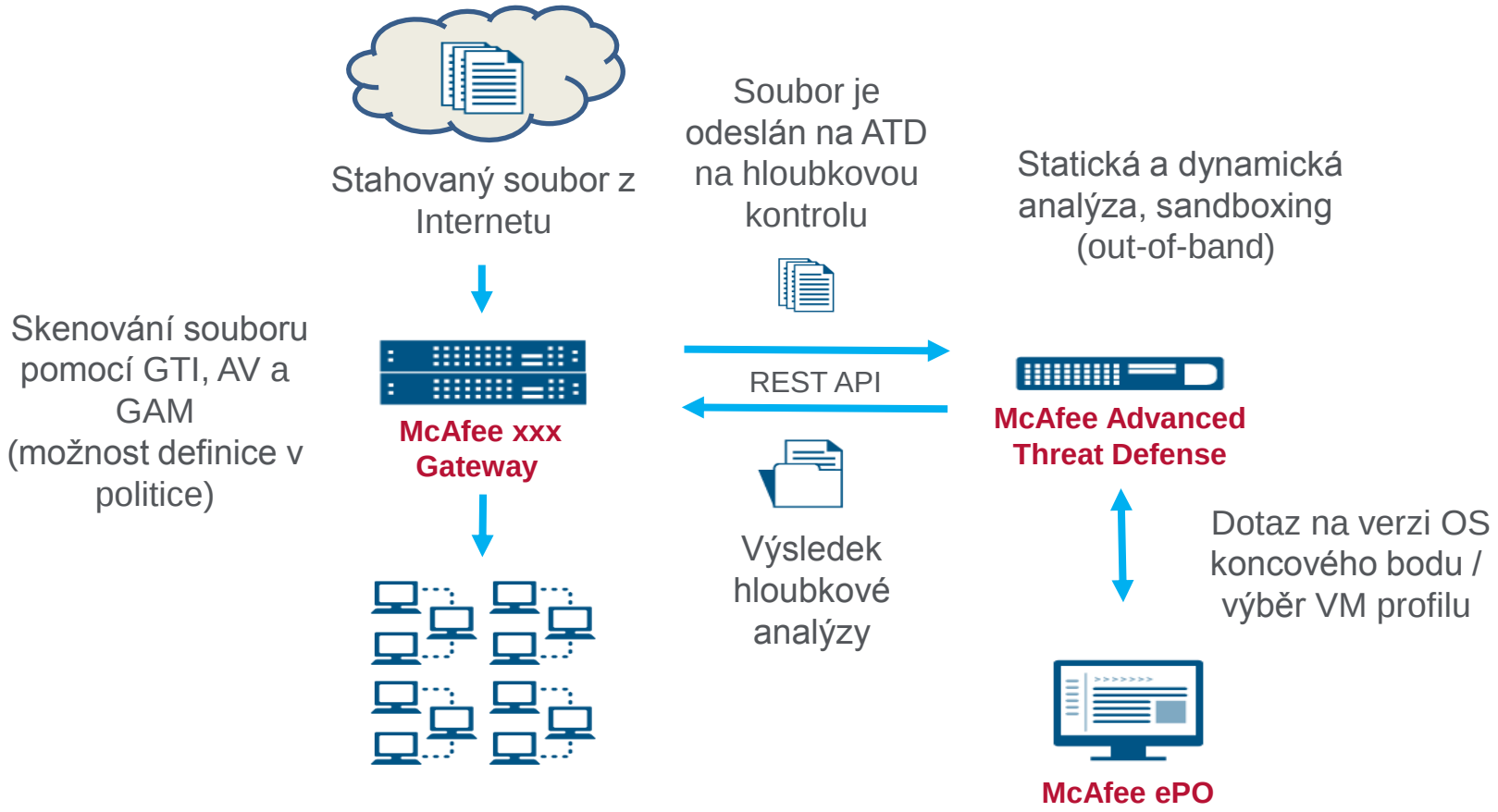
Integrace McAfee ATD

Přímá integrace na úrovni konfigurace

- **McAfee TIE/DXL technologie**
  - TIE client přeposílá podezřelé spustitelné soubory na hloubkovou analýzu
- **McAfee Web Gateway**
  - Přeposílá pouze podezřelé soubory, typicky to budou applety, dokumenty, programy, apod.
- **McAfee Network Security Platform**
  - Vytahuje soubory z protokolů smtp a http (popř. https, pokud je aktivní dešifrace)

REST API – jakékoliv další řešení může poslat soubory na otestování skrz API

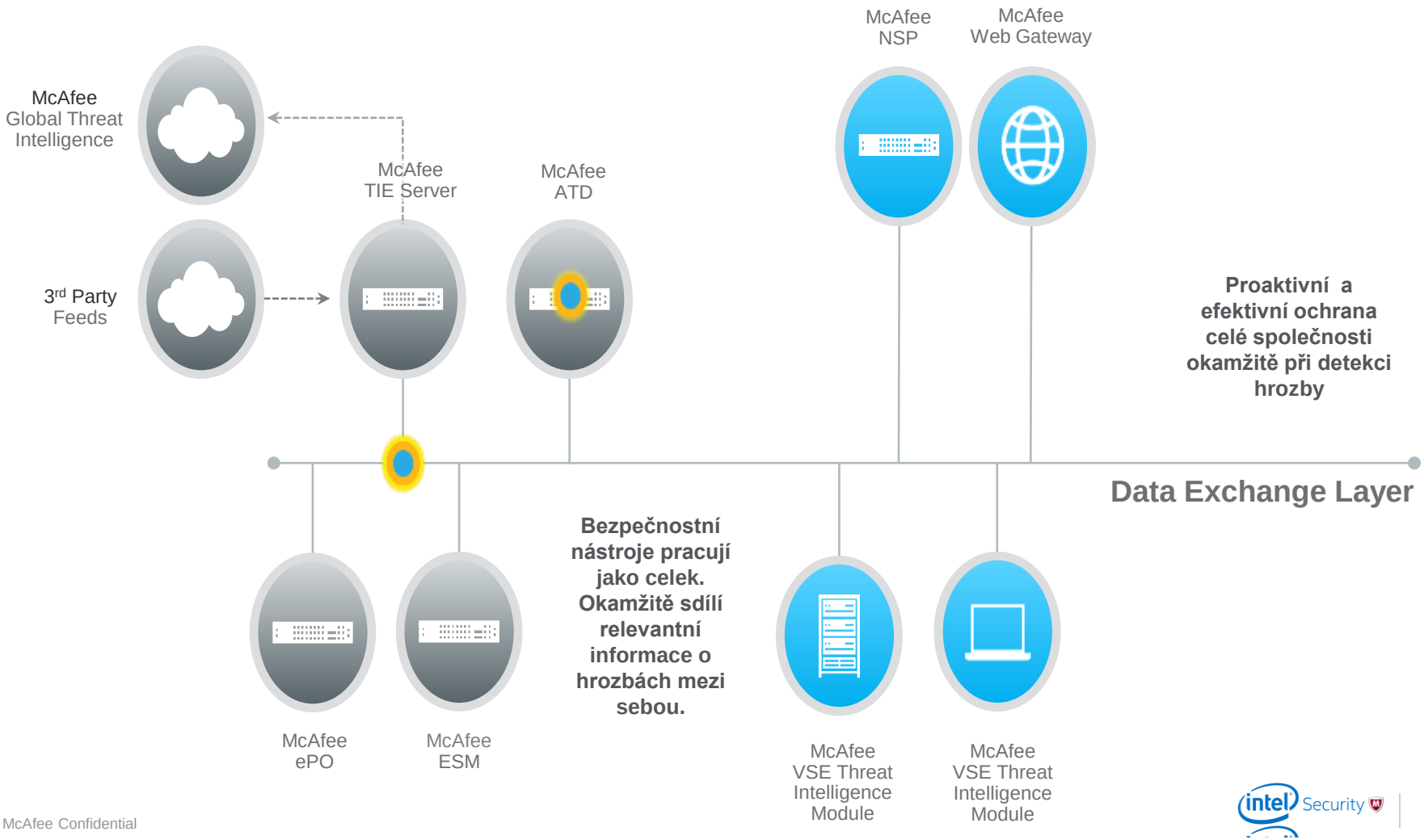
Architektura MWG, IPS a ATD



Threat Intelligence Exchange

Itegrace s branovým řešením bezpečnosti

Bránové nástroje blokují přístup do interní sítě společnosti na základě detekce na koncových stanicích

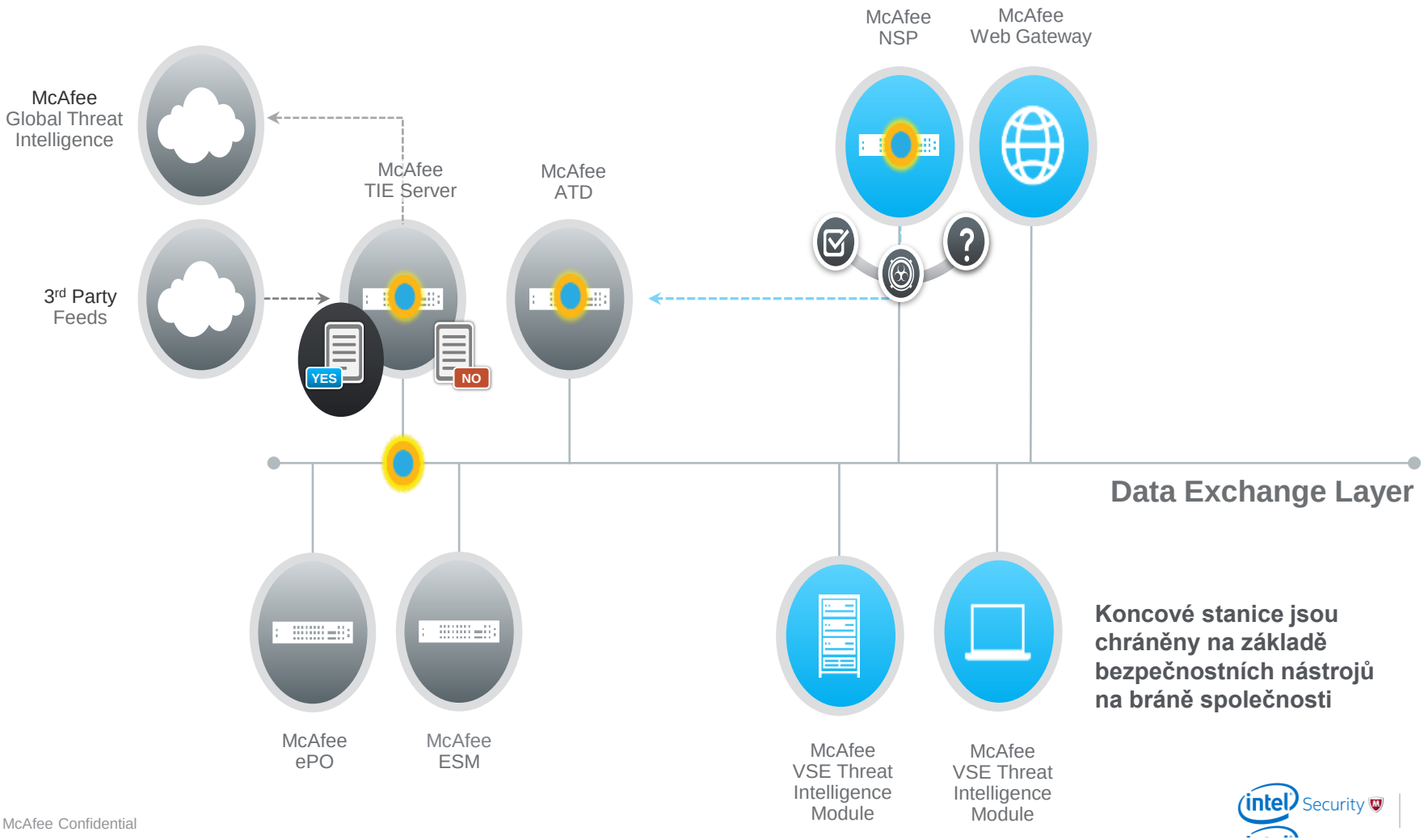


Proaktivní a efektivní ochrana celé společnosti okamžitě při detekci hrozby

Bezpečnostní nástroje pracují jako celek. Okamžitě sdílí relevantní informace o hrozbách mezi sebou.

Threat Intelligence Exchange

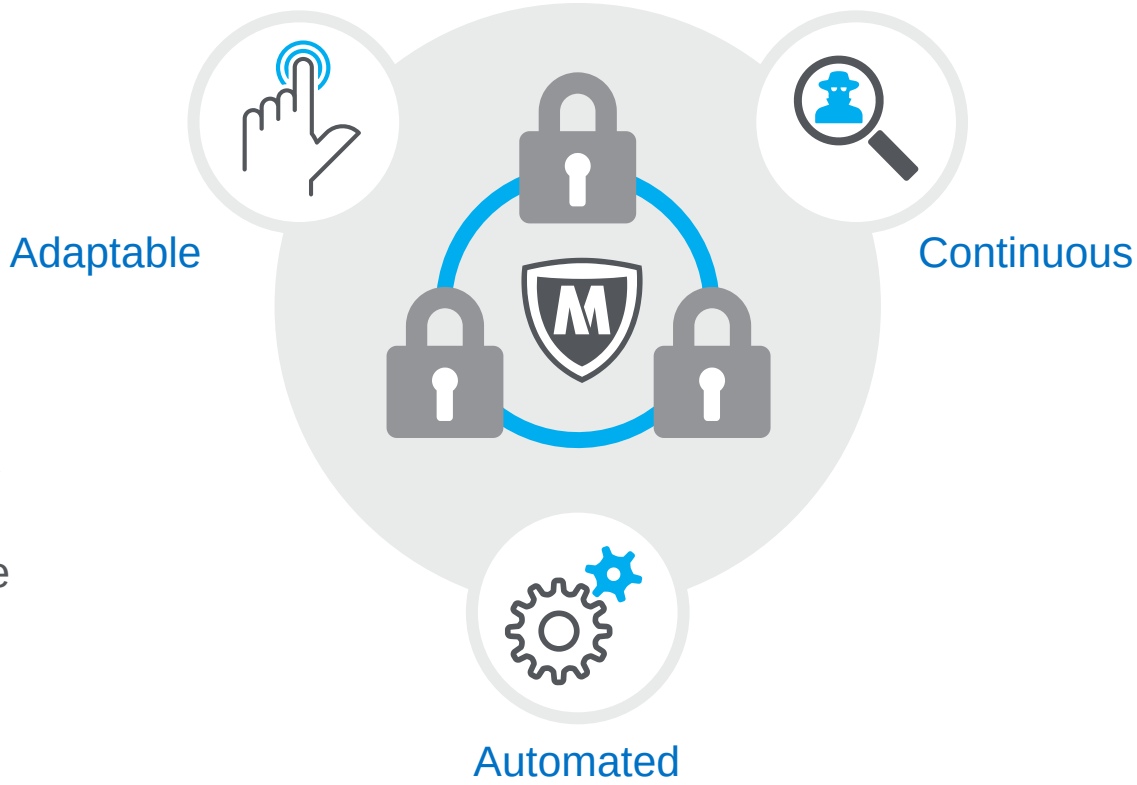
Itegrace s branovým řešením bezpečnosti



McAfee Active Response

McAfee Active Response

- On-line sledování procesů, souborů a komunikace.
- Vyhledávání souborů, které mohou být nebezpečné – spuštěné aplikace nebo uložené soubory
- Pomocí triggerů provádí automatizované akce na detekované události, soubory nebo komunikace – smazání souboru, blokace komunikace
- Správa celého řešení z jedné management konzole – ePO serveru

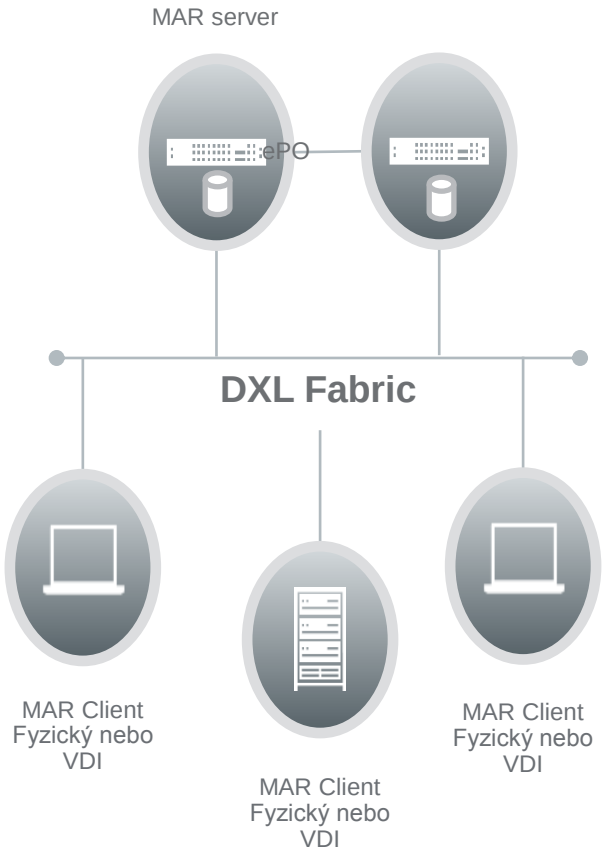


MAR/DXL architektura

McAfee Active Esponse

Komponenty řešení

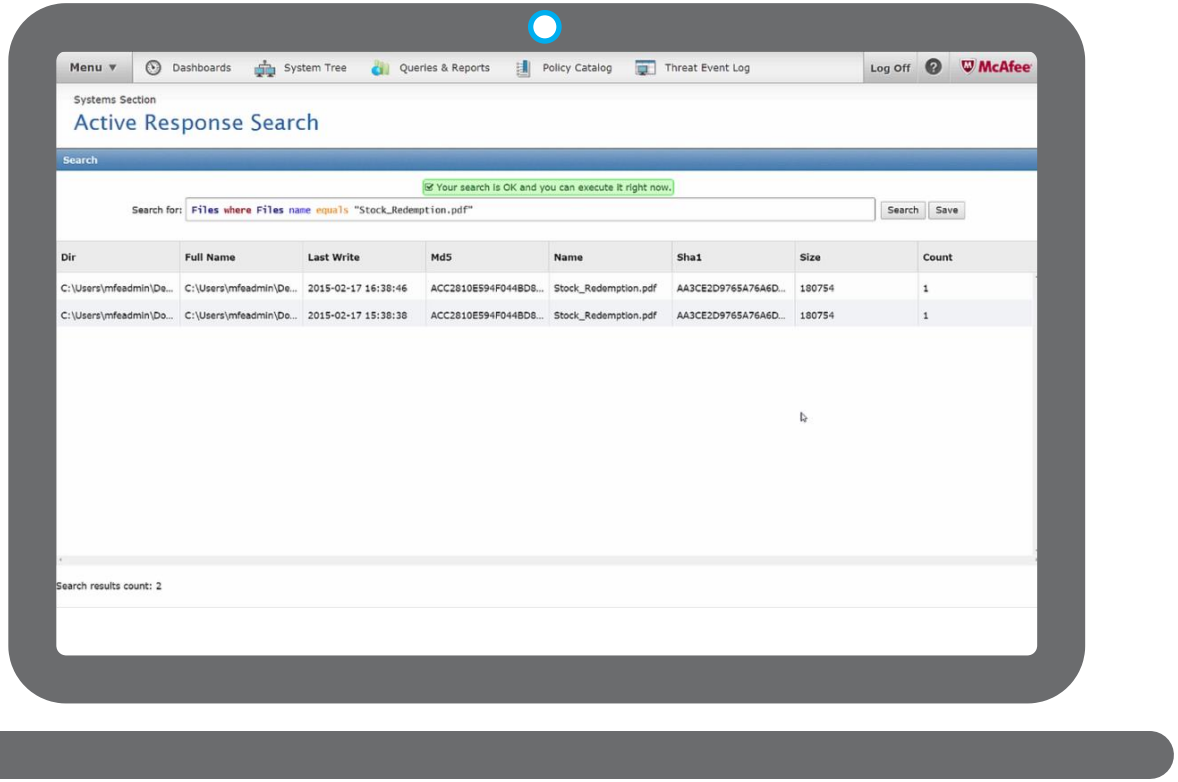
- MAR Server – virtuální image na VMware
- MAR Client
- DXL Fabric



Provázanost a správa pomocí McAfee ePolicy Orchestrator

Vyhledávání souborů, procesů, služeb nebo komunikace

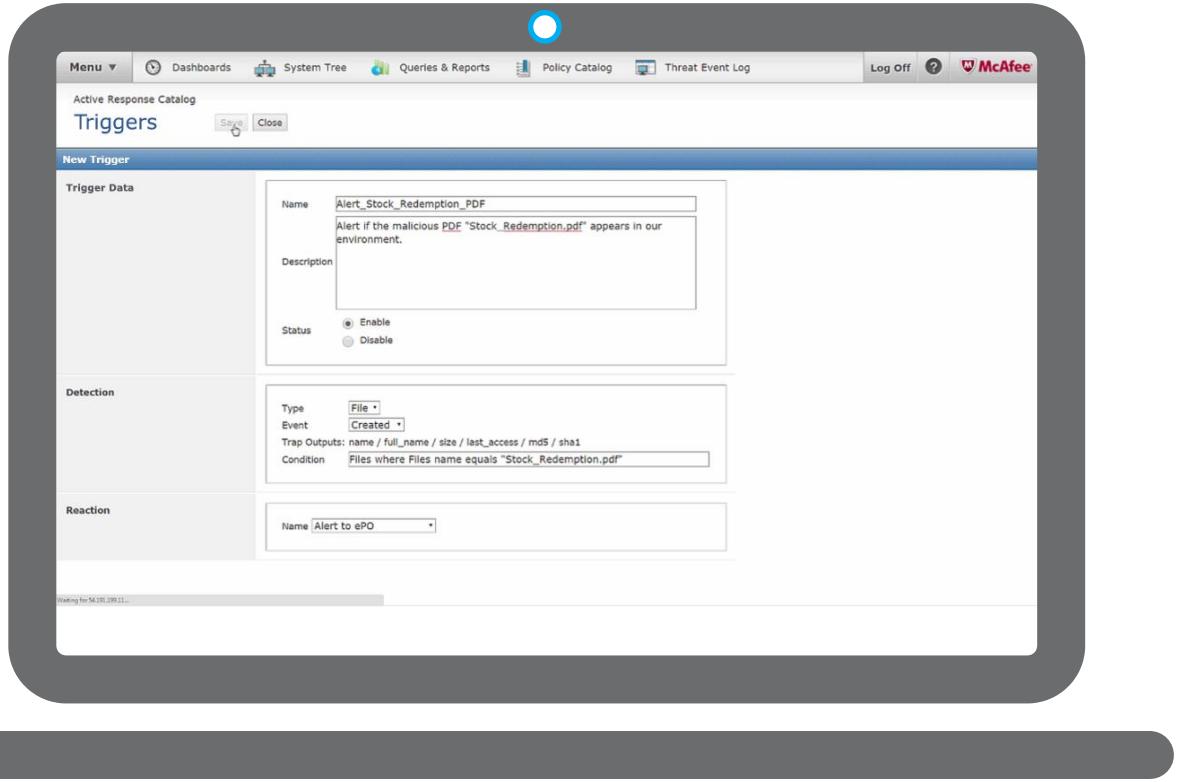
Spouštění přednastavených nebo manuálně vytvořených dotazů



Nepřetržitá ochrana s McAfee ePolicy Orchestrator

Nastavení automatických spouštěčů pro specifické události

Trigger vyvolá akci, která bude automaticky vykonána při detekci události



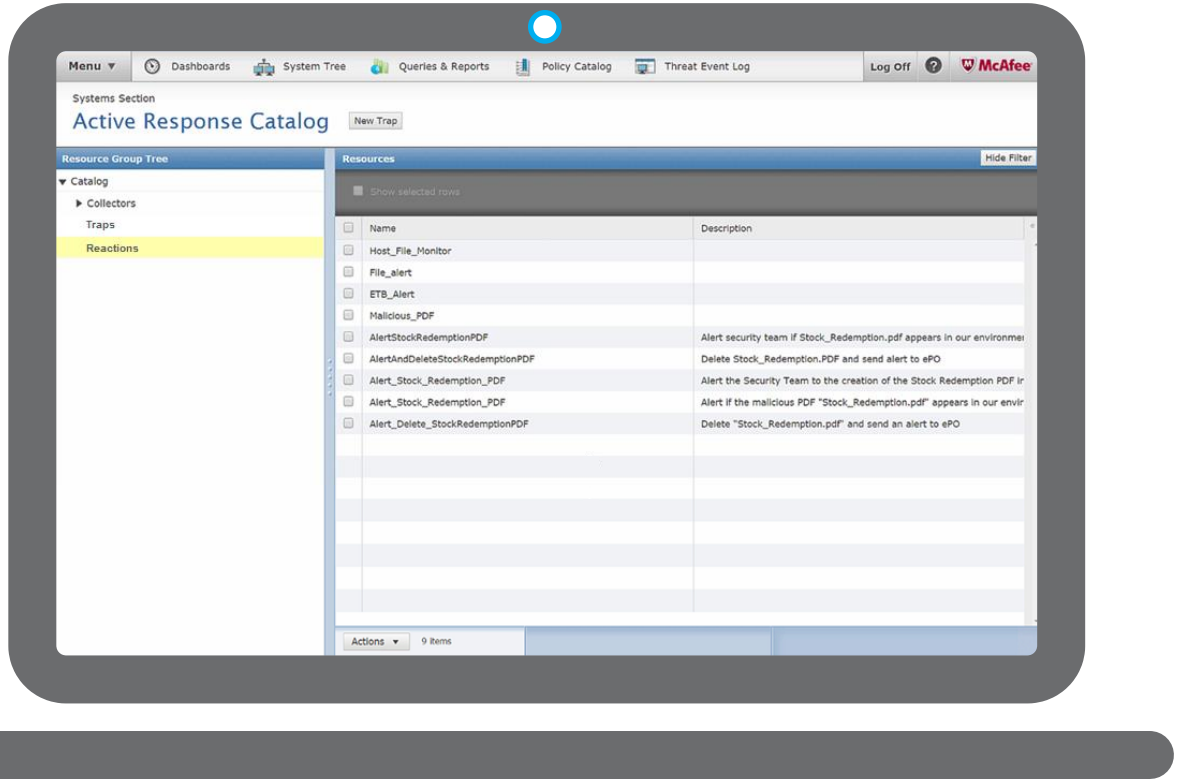
Automatizace s McAfee ePolicy Orchestrator

1.

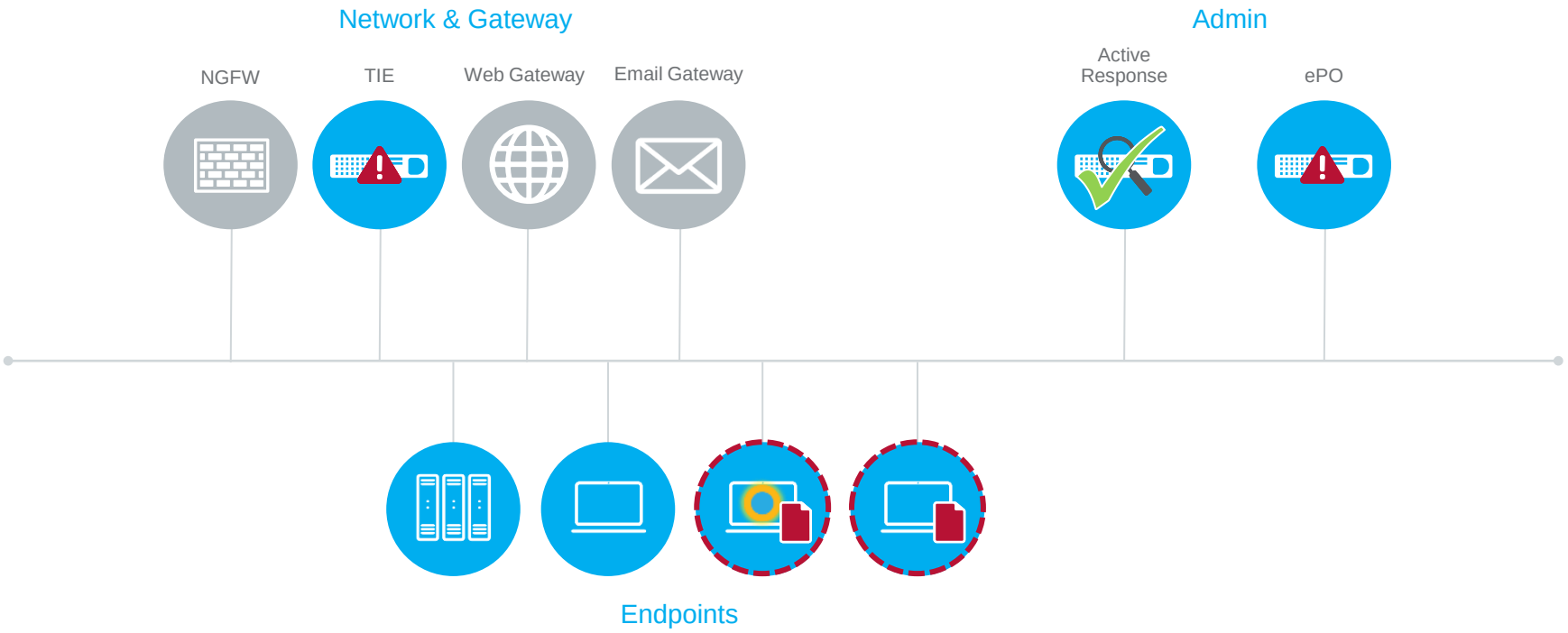
Stále běžící „collector“ sbírá relevantní informace

2.

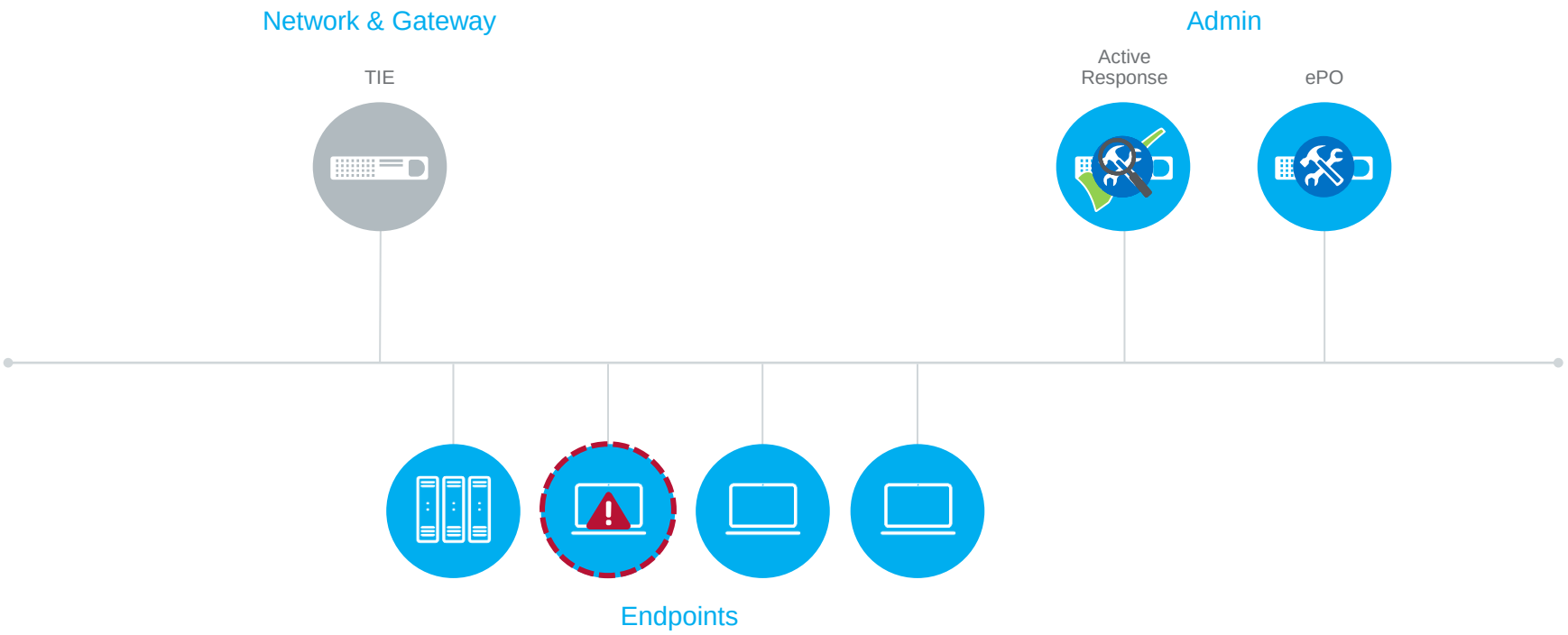
Pohled na události a vykonané akce



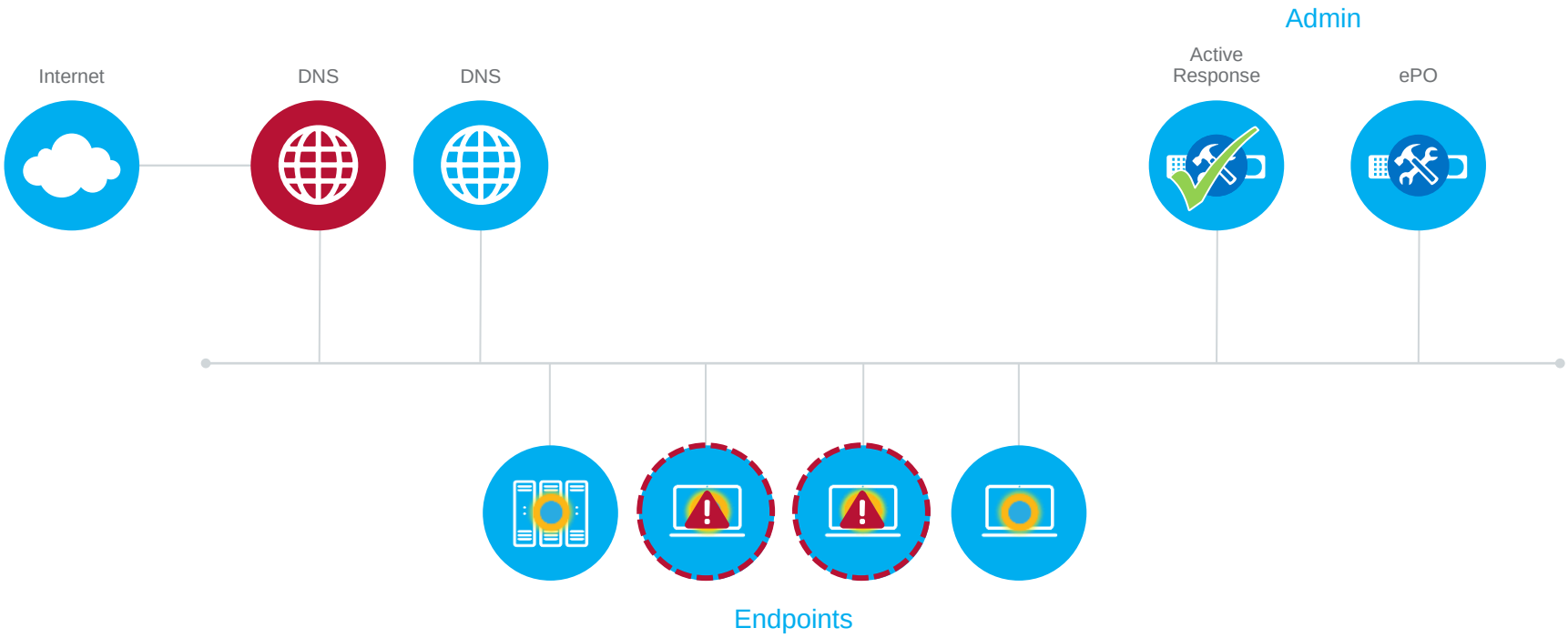
Proaktivní vyhledávání nebezpečných souborů



Náprava a odstranění škodlivém kódu



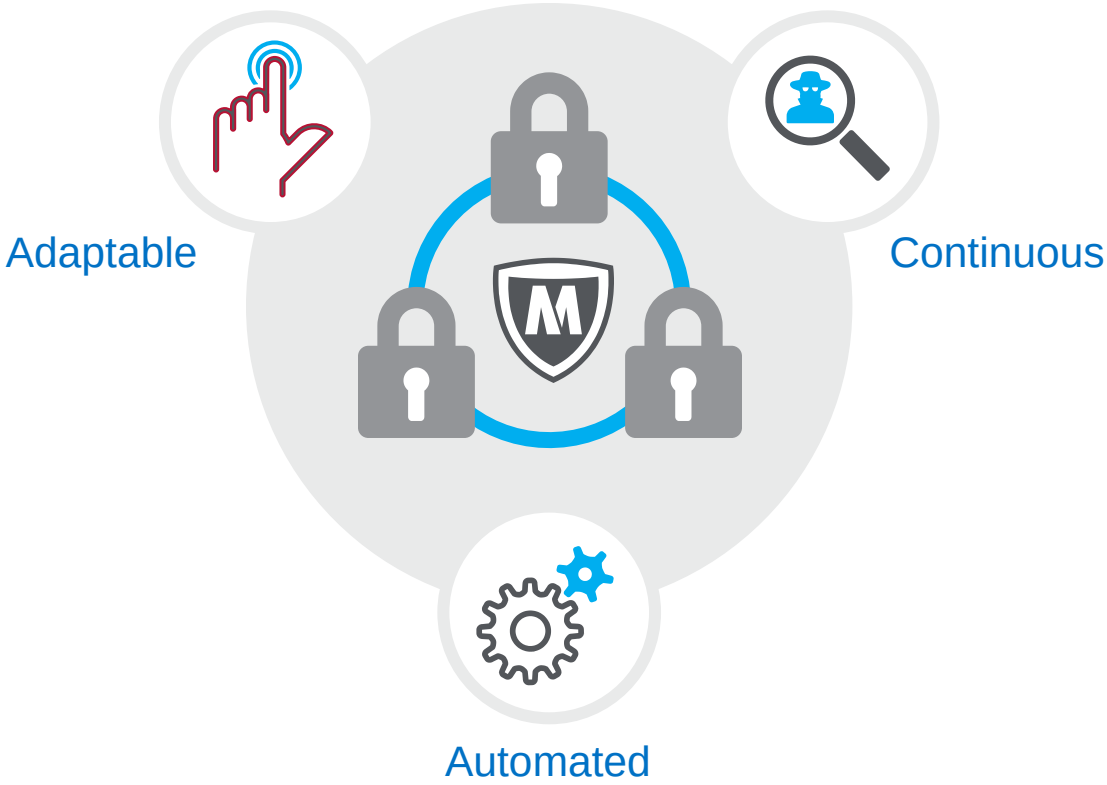
Monitorování síťové aktivity



McAfee Active Response

Shrnutí

- Hloubkové a nepřetržité monitorování systémů
- Adaptivní a snadno nastavitelný nástroj
- Jedna unifikovaná správcovská konzole – ePO server
- Detekce a náprava problémů mnohem rychleji!



McAfee Security Connected

Adaptivní, organizovaná a automatizovaná detekce a reakce na hrozbu rychleji, než se tato hrozba stačí dále rozvíjet.

Útočník Proniká obranou

Application Control nebo TIE klient detekuje spouštění souboru

McAfee TIE server poskytuje informace z lokálních/globálních zdrojů

McAfee Active Response vypátrá, zlikviduje, a oznámí informaci o hrozbě

McAfee ePolicy Orchestrator (ePO) poskytuje jednotnou konzoli pro správu všech technologií

Security information & Event Management

McAfee SIEM

Co je SIEM?

SIEM je evolucí a integrací dvou rozdílných technologií

- Security Event Management (SEM)
  - Primárně zaměřen na shromažďování bezpečnostních událostí
- Security Information Management (SIM)
  - Primárně zaměřen na normalizaci a korelaci bezpečnostních událostí

Security Information & Event Management (SIEM) je sada technologií pro:

- Sběr logů
- Normalizaci logů
- Parsování logů
- Agregaci logů
- Shromažďování nativních logů
- Korelaci logů
- Analýzu

Tři hlavní faktory ovlivňující většinu SIEM implementací

1. Viditelnost hrozeb v reálném čase
2. Efektivnost správy bezpečnosti
3. Požadavky na shodu a správu logů

SIEM se stále vyvýjí …

- SIEM Content Awareness (Next Generation SIEM)
  - Systém, který je schopen analyzovat události ze všech vrstev až k aplikačním datům

IM, Chat

WebMail
Email

Web Access
(HTTP)

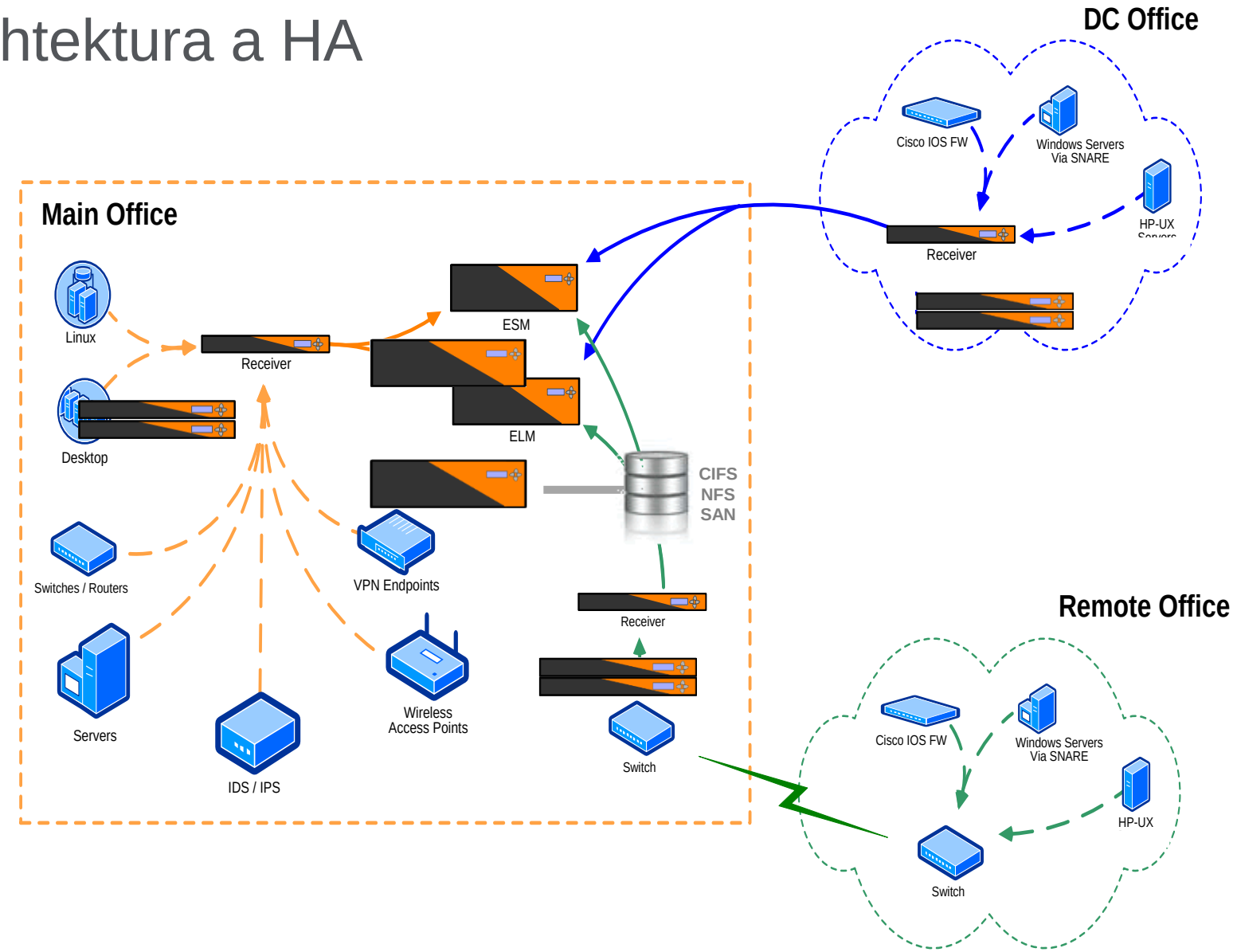
P2P File
Sharing

Protocol
Anomalies

Škálovatelná architektura

Inteligence a provozní efektivita	GTI/TIE	ePO	NSP	MVM	ATD
Adaptivní analýza rizik & Historické korelace	McAfee Advanced Correlation Engine 				
Integrovaný SIEM & Log Management	Mcafee Enterprise Security Manager 		McAfee Enterprise Log Manager 		
Monitoring aplikací a DB komunikace	McAfee Application Data Monitor 		McAfee Database Event Monitor 		
Sběr logů & Distribuovaná korelace logů	McAfee Receivers 				Big Security Data DB

SIEM architektura – distribuovaná archtektura a HA

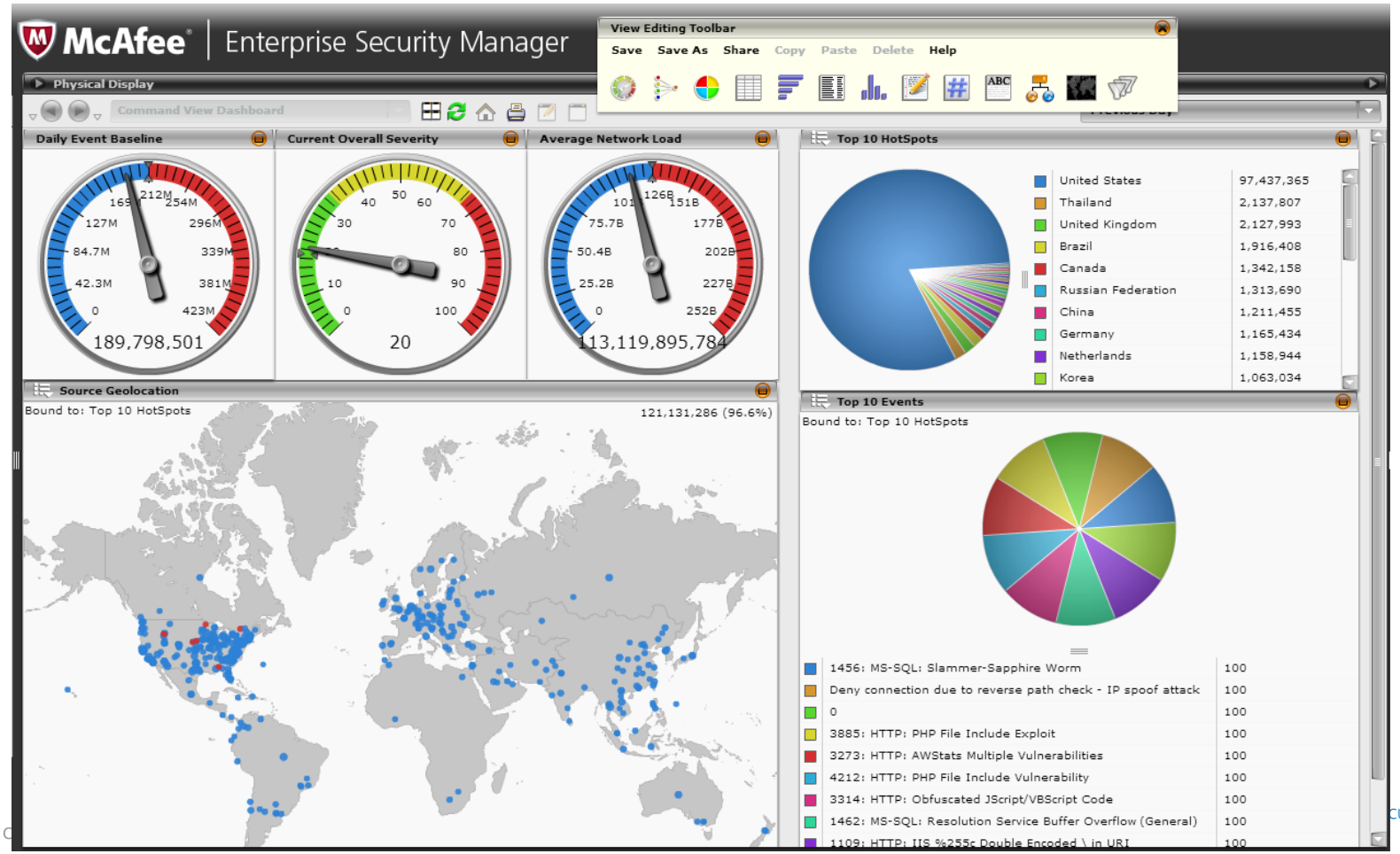



https://esm.ams.mcafeeebc.com/Application.html
McAfee | Enterprise Security Manager
NGCP | options | help | logout
Local ESM
Default Summary EBC
Current Day
Filters
Physical Display
Type here to search for a device
Physical Display
Local ESM
(Local ESM)
Advanced Correlation Engine (Historica
Advanced Correlation Engine (Real-Tin
AMS McAfee ePO (172.18.161.3)
AMS McAfee MVM (172.18.161.41)
AMS McAfee NSP (172.18.161.4)
McAfee Application Data Monitor
McAfee Database Security Monitor
McAfee Enterprise Log Manager
McAfee Event Receiver
(McAfee Event Receiver)
AMS Apache
AMS Appsecinc DBprotect (ASP)
AMS Arbor Peakflow
Alarms
Cases
Traffic to Suspicious Geo
Traffic to Suspicious Geo
Traffic to Suspicious Geo
Traffic to Suspicious Geo
Virus detected
Virus detected
Traffic to Suspicious Geo
Traffic to Suspicious Geo
Traffic to Suspicious Geo
Virus detected
Virus detected
0
15
0
Event Device Type
2,118,041 (100%)
Network Security Manager (ASP) 1,368,039
McAfee Application Data Monitor 671,501
PostgreSQL 22,176
WMI Event Log 17,253
McAfee Firewall Enterprise (ASP) 15,166
Correlation Engine 11,513
MSSQL 5,853
MySQL 4,225
ePolicy Orchestrator (ASP) 1,437
VirusScan (ePO) 364
Host Data Loss Prevention (ePO) 186
McAfee Web Gateway (ASP) 170
Host Intrusion Prevention (ePO) 109
McAfee Enterprise Security Manag 29
McAfee ACE Risk Manager 14
Page 1
Event Source IPs
Bound to: Event Device Type
172.18.163.5 1,370,393
172.18.162... 381,008
172.18.161.1 52,617
172.18.161... 51,013
172.18.161... 41,830
172.25.109.2 35,257
172.18.161.3 23,539
172.18.161... 16,654
Page 1
Event Destination IPs
Bound to: Event Source Users
172.18.161... 1,368,497
172.18.162.6 252,723
172.18.162.5 119,456
172.18.161.1 112,997
172.18.161.3 33,094
172.18.161.6 27,510
172.18.161... 22,623
192.175.48.6 18,804
Page 1
Total Flow Collection Rate Per Second
5
Rate: -None-
Total Collection Rate Per Second
25
Rate: -None-
Event Distribution
2,118,041 (100%)
Events
Bound to: Event Distribution
Severity
Rule Message
Ever
161775 McAfee_FW_Ent Server traffic - enc 215
18000 McAfee_FW_Ent Monitord informati 720
Hints
Source User
Sensor_Name
Direction
Interface
NTP_Opcode
NTP_Request
NTP_Server_Mo...
NTP_Client_Mode
SNMP_Error_Code
SNMP_Version
SNMP_Item_Type
SNMP_Operation
Authoritative_A...
Query_Response
DNS_Class

Uživatelský dashboard

Výkonný, drag-and-drop dashboard editor

Možnost okamžité modifikace pohledů a sledování výsledků



Centrální správa logů - Log Management

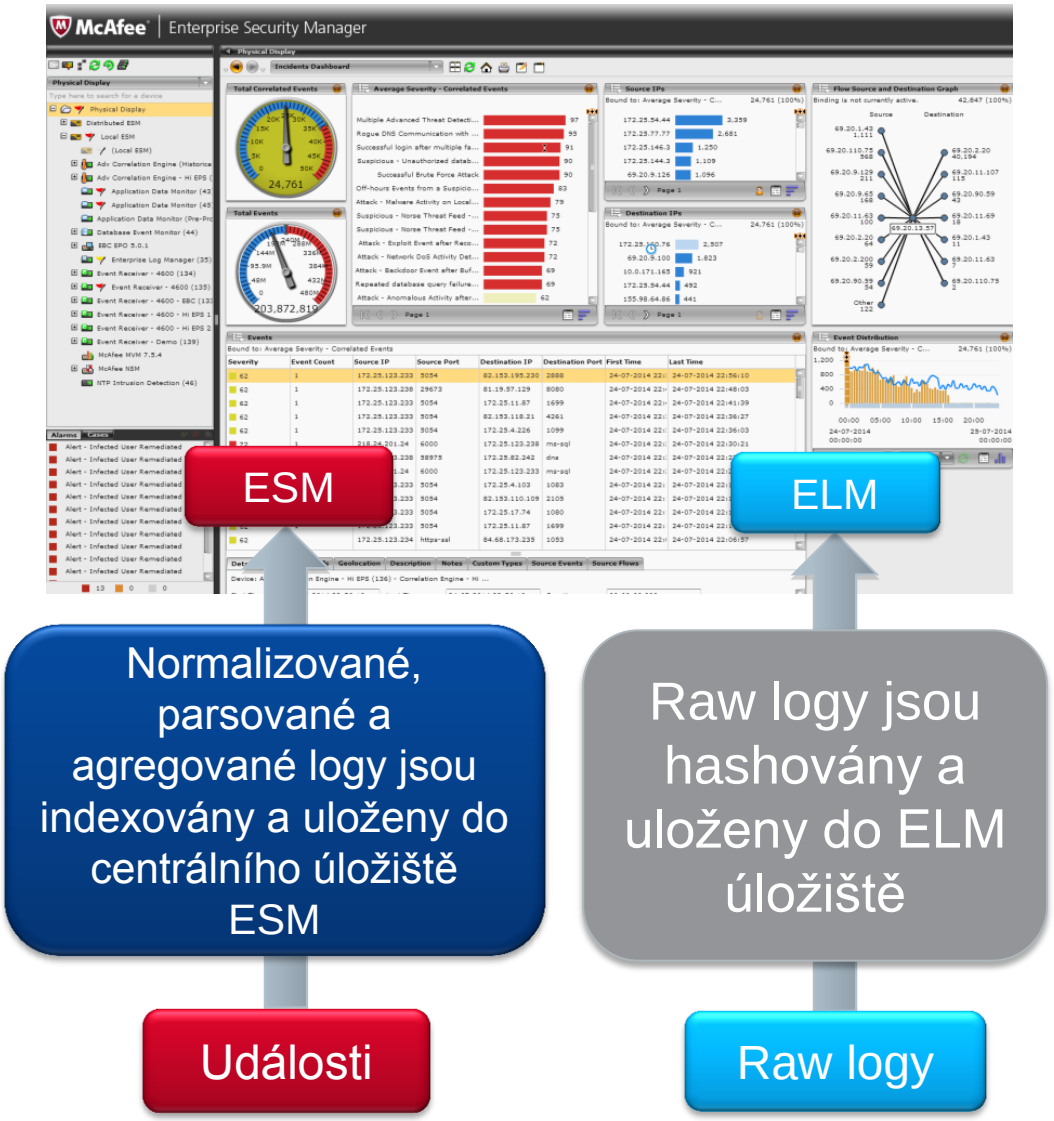
Jedna centrální správa pro agregované on-line události a nativní RAW logy

Flexibilní možnost uložení logů

- Direct Attached Storage
- SAN
- NAS
- iSCSI
- NFS

Konfigurovatelné nastavení udržování a vymazávání logů

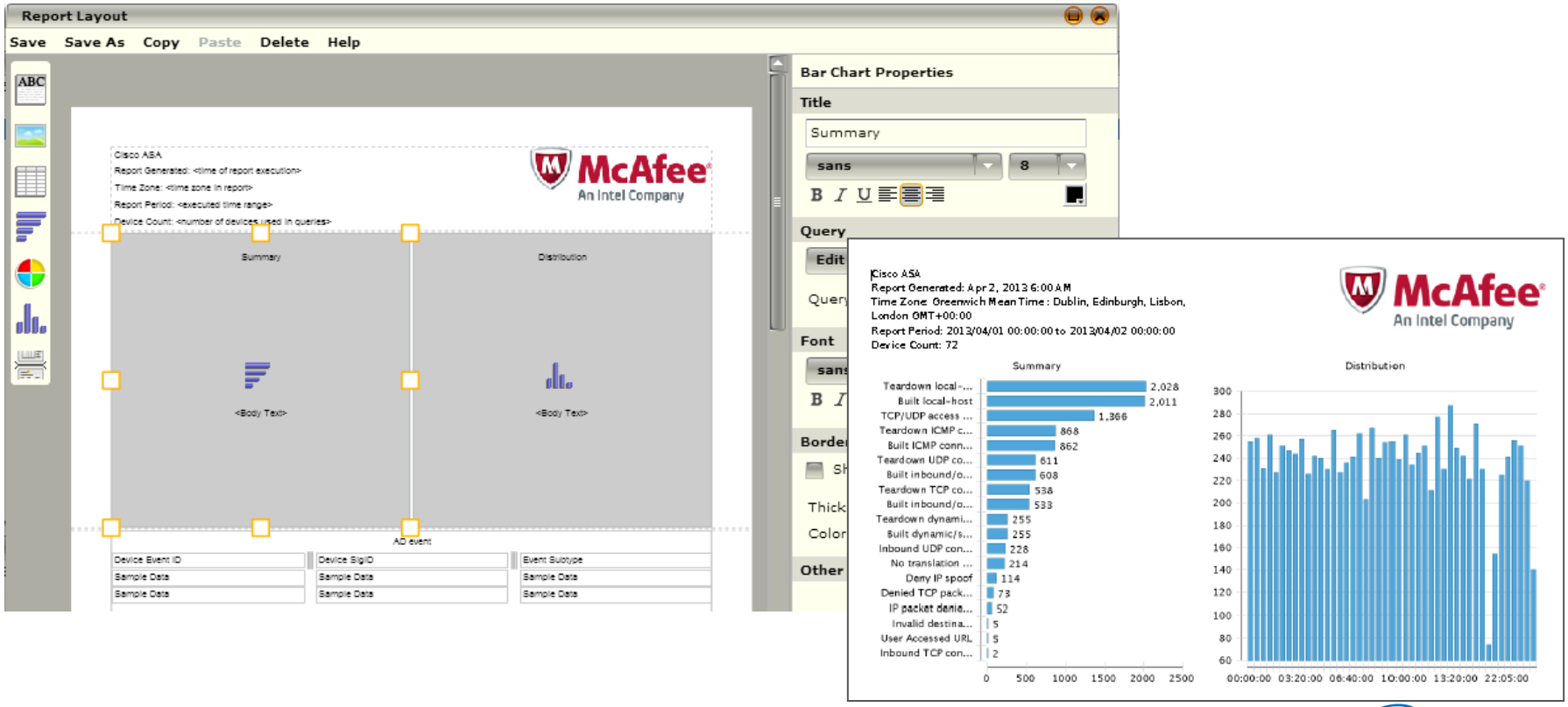
Logy jsou šifrované a hashované



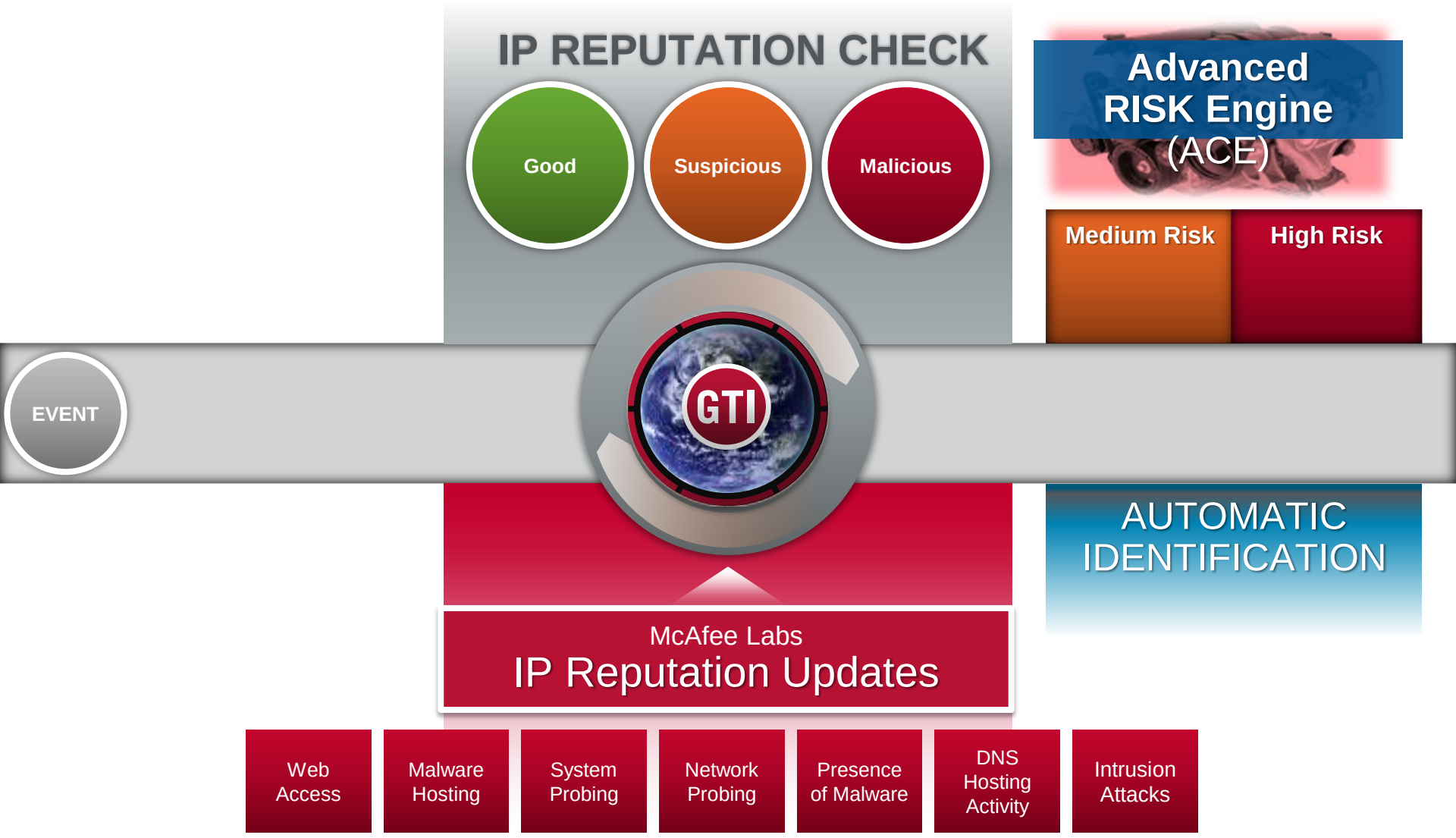
Reporting

Více jak 100 přednastavených reportů

Výkonný, grafický reportovací editor

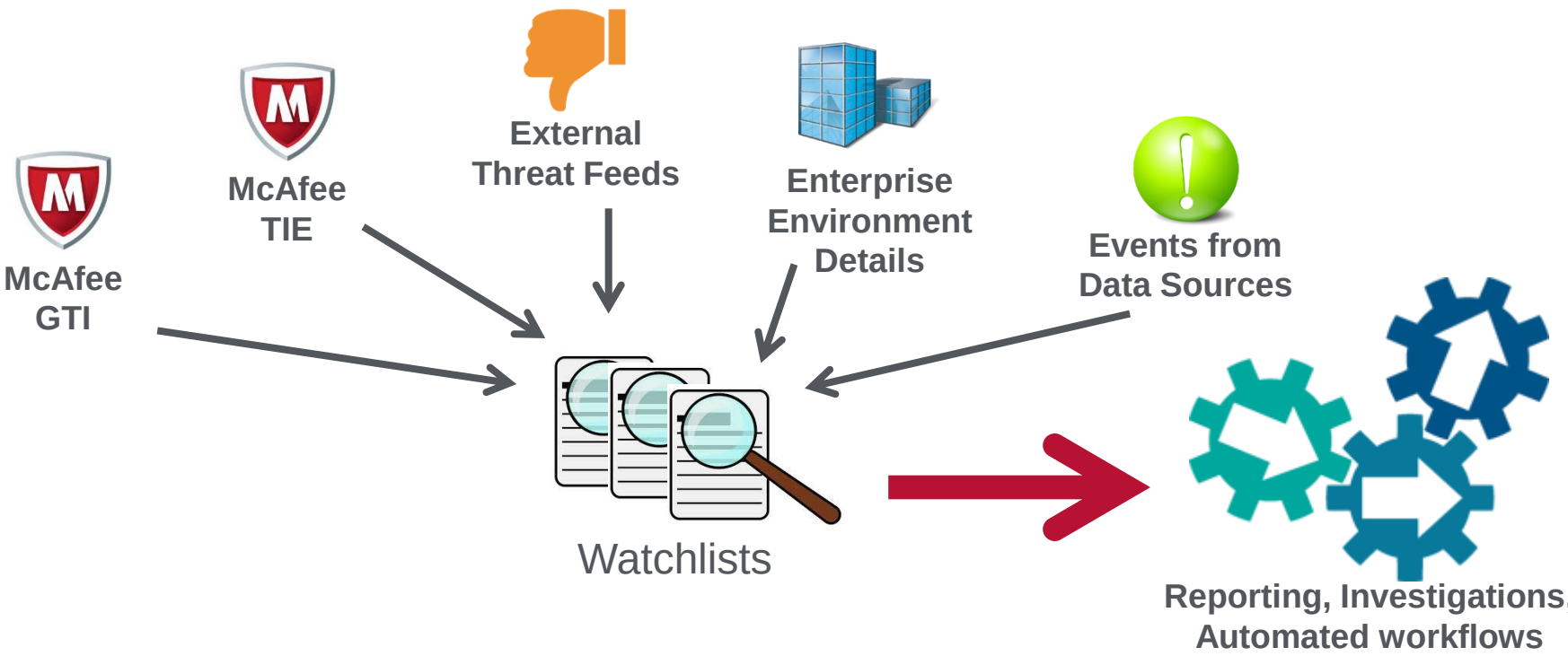


Global Threat Intelligence (GTI)



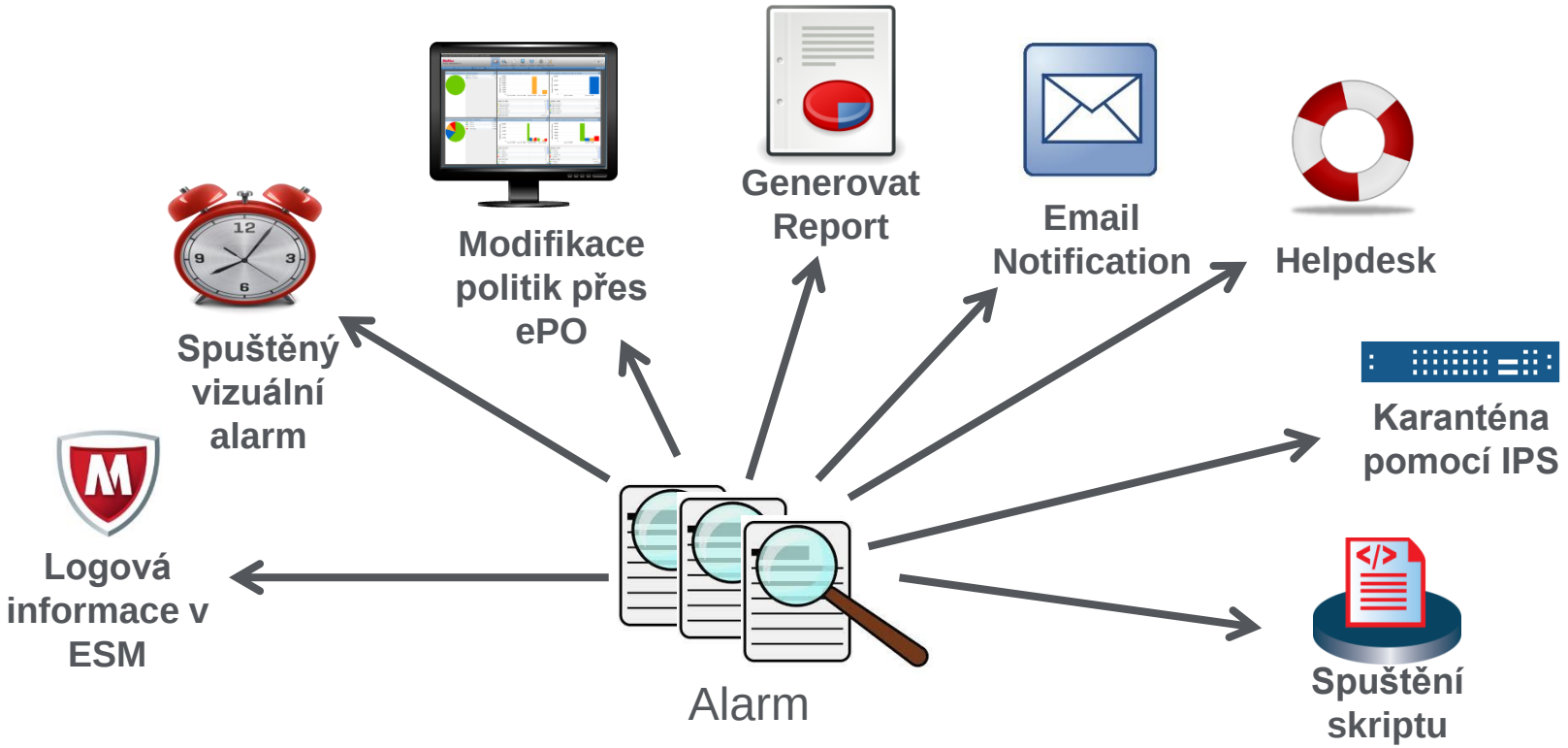
Watchlists

- Watchlists umožňuje filtrovat události, které se následné využijí pro spuštění alarmu nebo jako vstup do korelačního pravidla
- Podporuje manuální nebo automatickou aktualizaci watchlistu



Alarm

- Alarm je vlastnost SIEM systému, která umožňuje spustit alarm na základě definovaných podmínek, které nastanou při on-line sledování prostředí



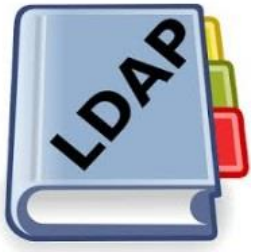
Enrichment

Enrichment přidává další informace do logu. Pomáhá obohacovat logové informace.

Geolocation

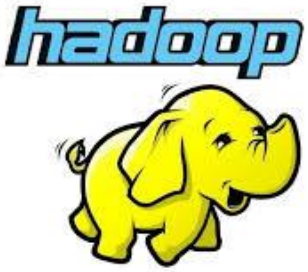
Network Zone

Event Category



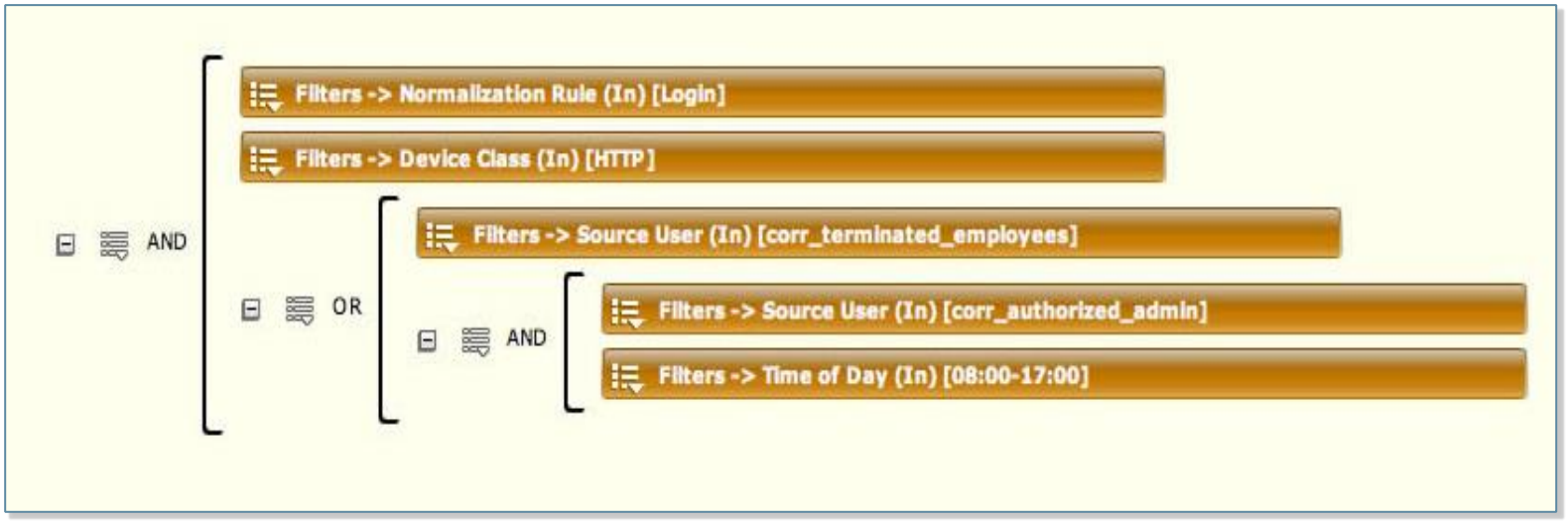
Databases

File Import

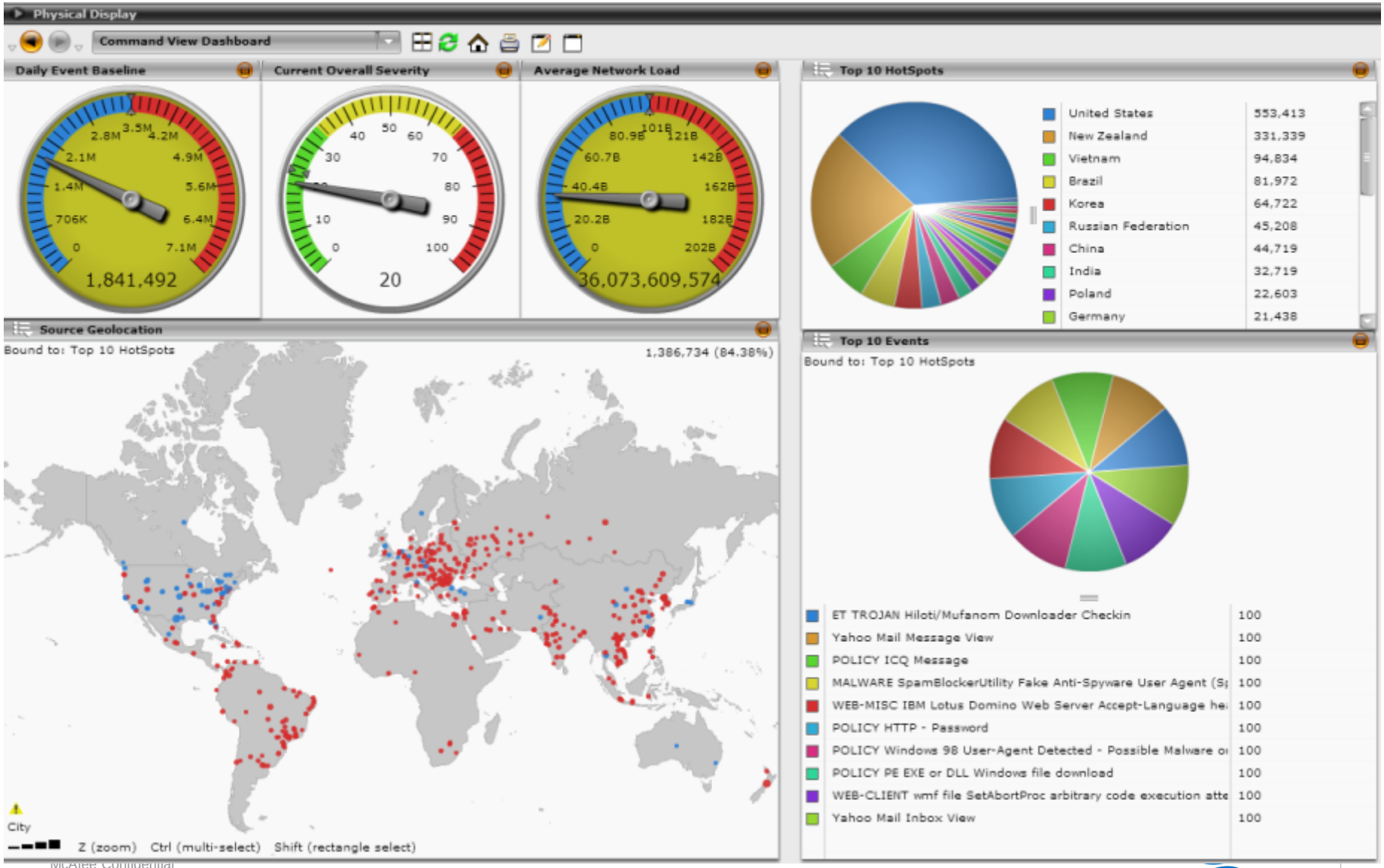


Correlation

- Více jak 175 přednastavených korelačních pravidel v politice
- Možnost vytváření vlastních korelačních pravidel pomocí přehledného grafického rozhraní
- Dedikovaná ACE appliance zajišťuje vyšší výkon a více funkcí oproti korelacím na Receiveru:
- • Real-Time Rules-based Correlation for both Events, Flows & deviation
- • Risk (Event Scoring) Correlation
- • Historical Correlation
  - Receiver zajišťuje pouze Real-Time Rules-based Correlation for Events.

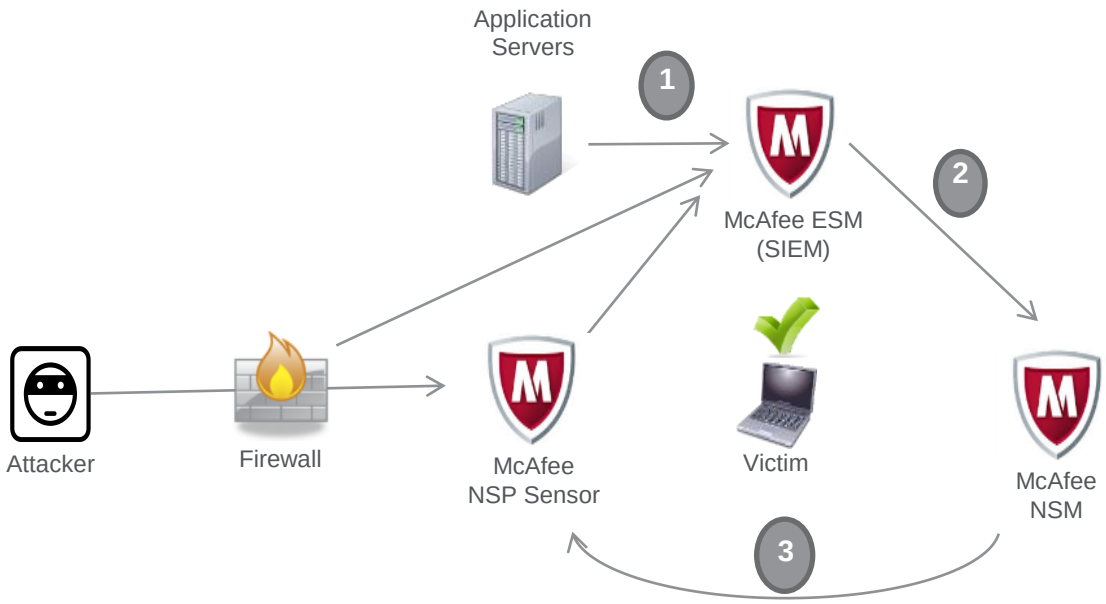


Geo-location Indicators



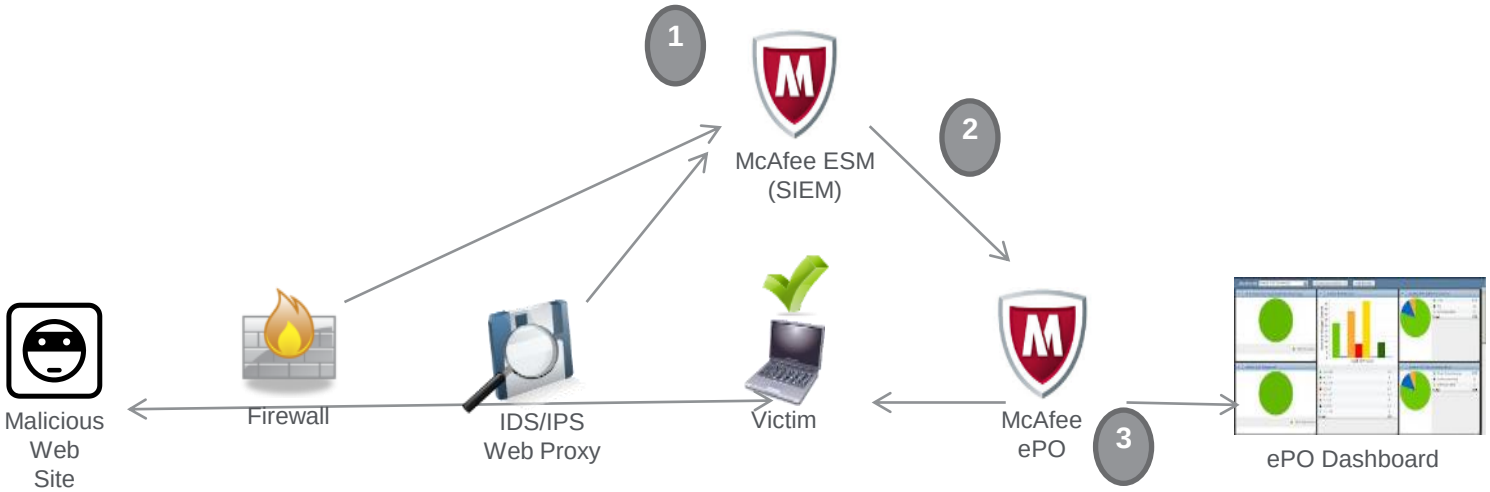
Orchestrace:
McAfee Network Security Platform

3. Na základě informace od ESM, NSM vynucuje karanténu útočného systému na NSP senzoru. Další komunikace z nebezpečného systému je blokována, útok je zastaven ve velice brzkém stádiu.



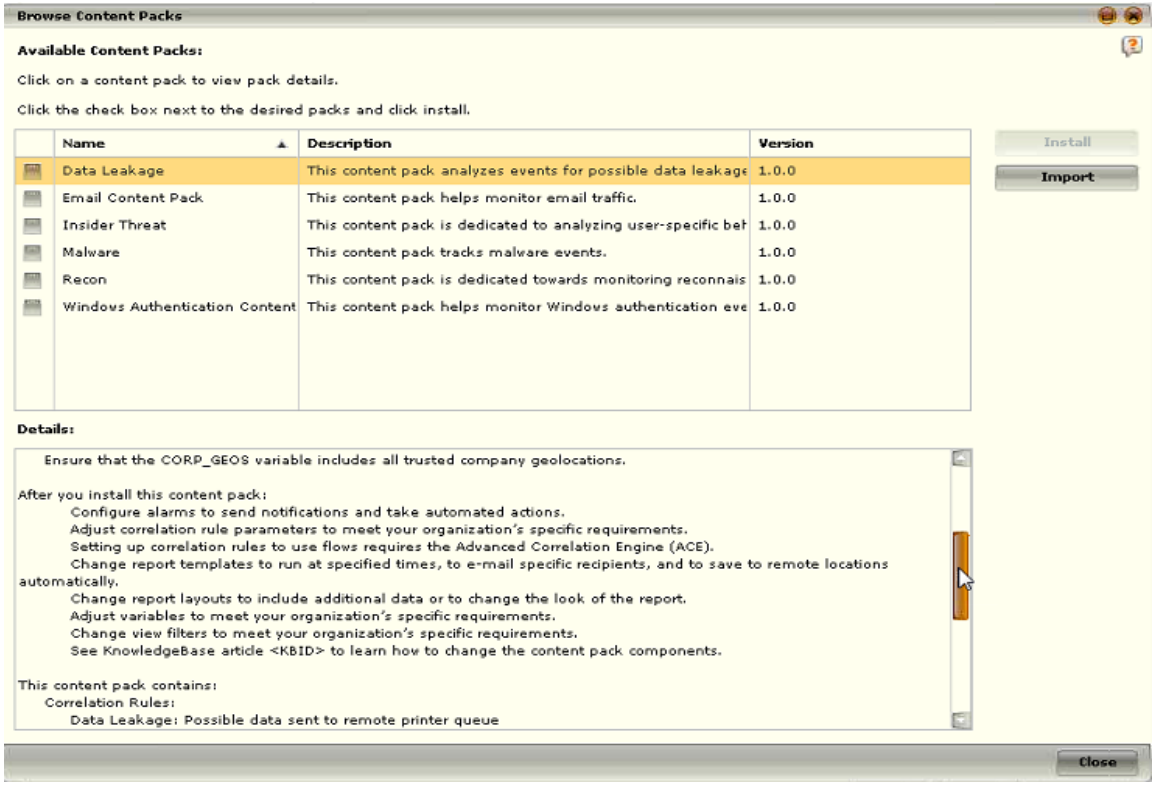
Orchestrace:
McAfee ePolicy Orchestrator

3. Na základě odpovědi od ESM, ePO uplatňuje restriktivní politiku na systémy, na které se útočí, efektivní k zastavení útoku v prvotní fázi.



Content packs

Content Packs – přednastavené šablony pro rychlé nastavení SIEM pro různé oblasti bezpečnosti
Content Pack obsahuje dashboardy, korelační pravidla a alerty
Content Pack je možné manuálně upravovat – úpravy nebudou přepsány novou aktualizací
McAfee plánuje 12 Content Packů, systém se automaticky aktualizuje

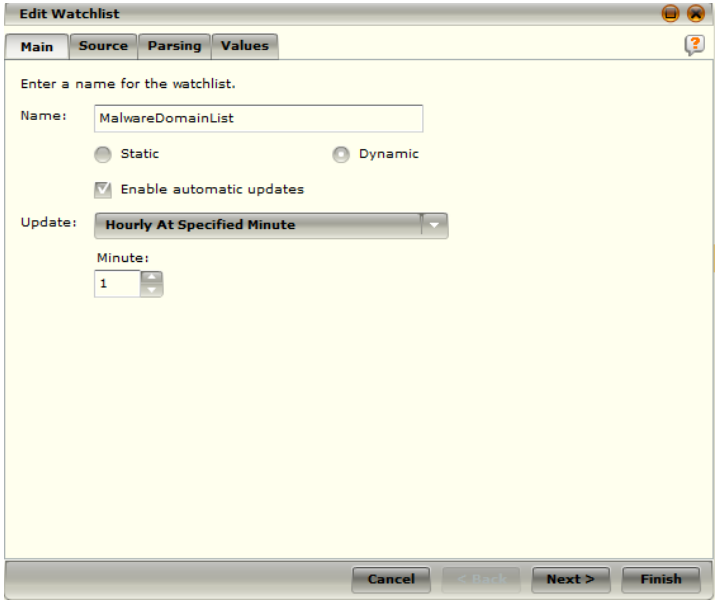


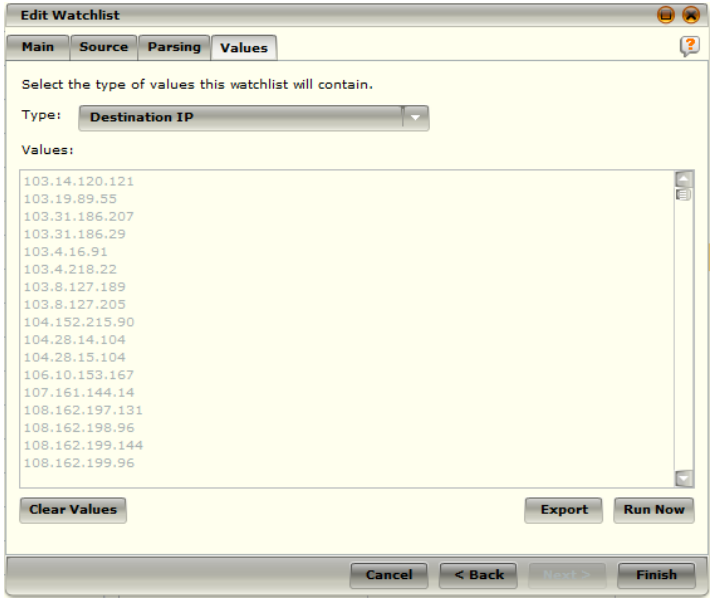
Dynamické watchlisty a Threat Awereness

Další zdroj informací do Watchlistu z HTTP/HTTPS stránek – Indicators of Compromise

Automatické stahování textových blacklistů URL, IP adres, hashů apod.

Jejich využití v alarmech, korelacích, filtrech





Threat awareness - Indicators of Compromise (IoC)

Manuální nebo automatizovaný import podezřelých IP, hashů, URL, názvů souborů z volně dostupných nebo placených služeb

Podporuje zpracování v různých formách včetně Cybox a STIX

Porovnává nové IoC s historickými událostmi v SIEMu

Jedním ze zdrojů může být i McAfee ATD

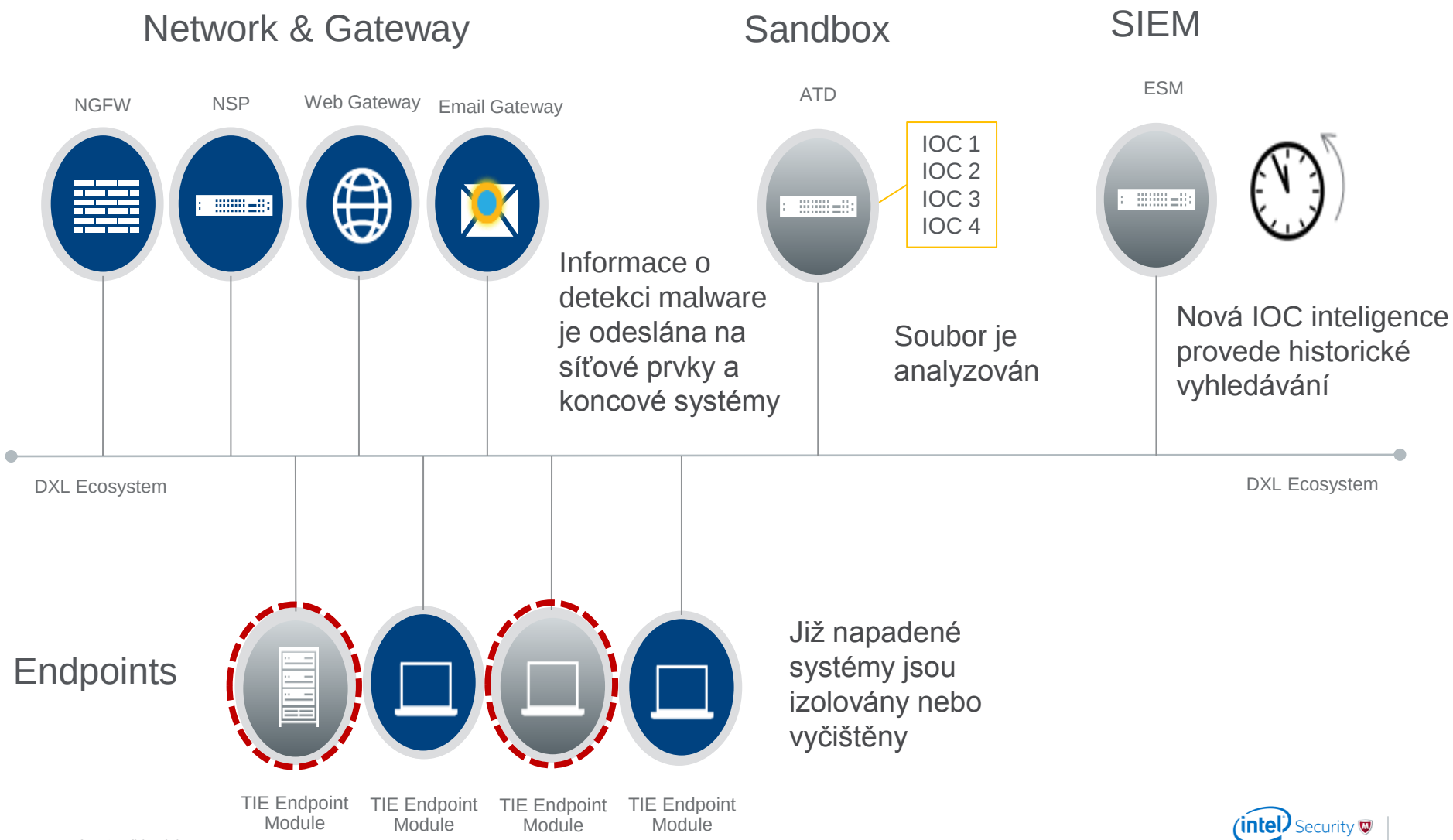
Threat awareness – historické porovnání

SIEM použije klíčové indikátory z IoC a prohledá logy – včetně informací z McAfee ATD

Pohledem zpět přes veškeré zaznamenané události zjistí, zda byl nějaký systém kompromitován

Pokud najde shodu – může vykonat akci podobně jako Alarm

Adaptive Threat Prevention and Detection
Integrace se SEIM



Jan Strnad, jan_strnad@mcafee.com, +420 602280387