



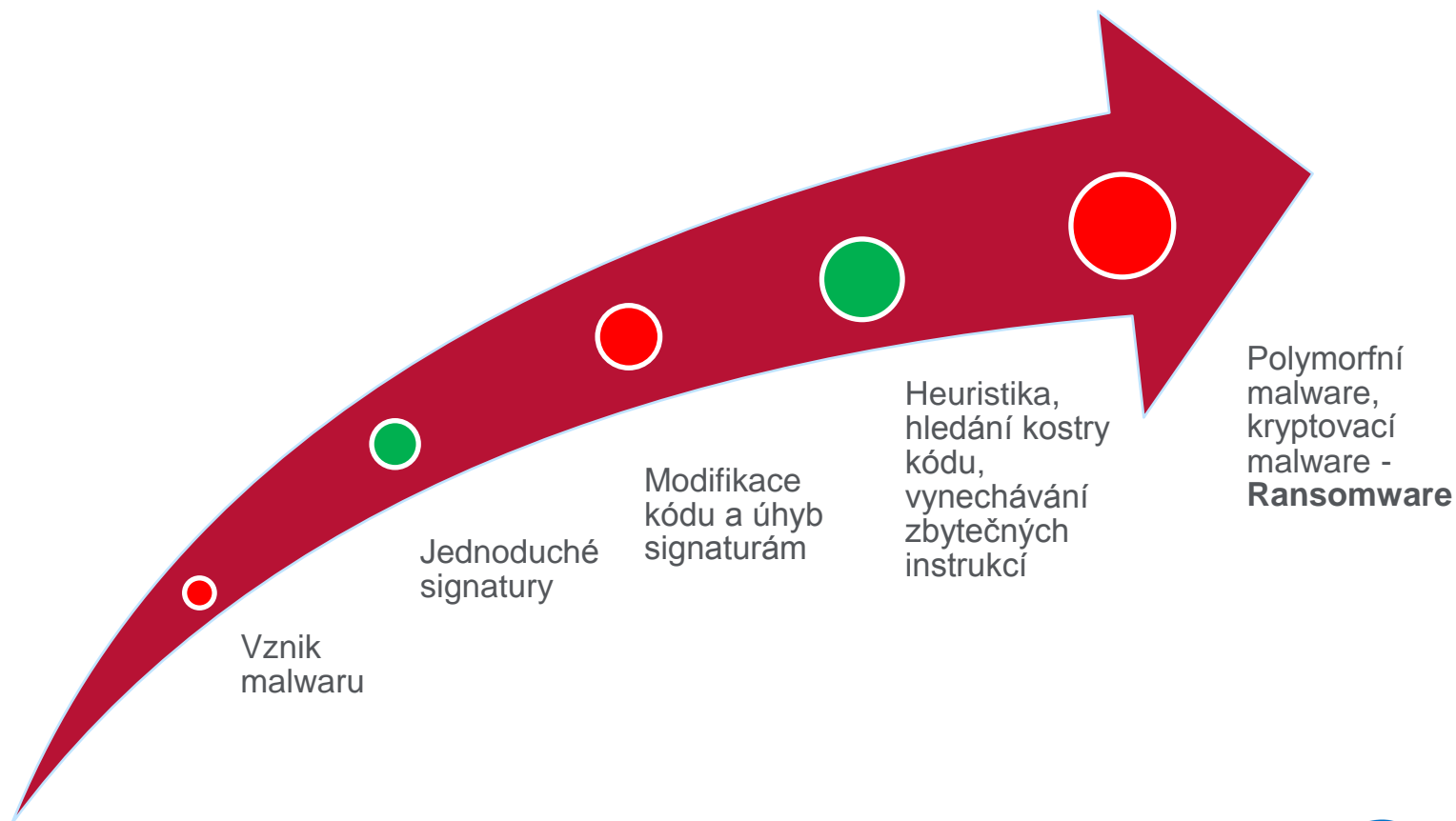
Kryptoviry a malware pod 100% kontrolou

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 ne zvítězí ani jedna strana, ale malware bude vždy o krok napřed, protože reaguje na aktuálně dostupné bezpečnostní technologie



Ransomware – predikce Intel Security 2016

Ransomware

Ransomware will remain a major and rapidly growing threat in 2016, fueled by anonymizing networks and payment methods.



257,357
New samples
detected in 1H 2014

Ransomware-as-a-service

Inexperienced cybercriminals will leverage ransomware-as-a-service, magnifying the growth in ransomware.



380,652
New samples
detected in 2H 2014



2,026,752
New samples
detected in 1H 2015

Remediation

Attackers will increasingly encrypt files before they are backed up, making remediation more difficult.

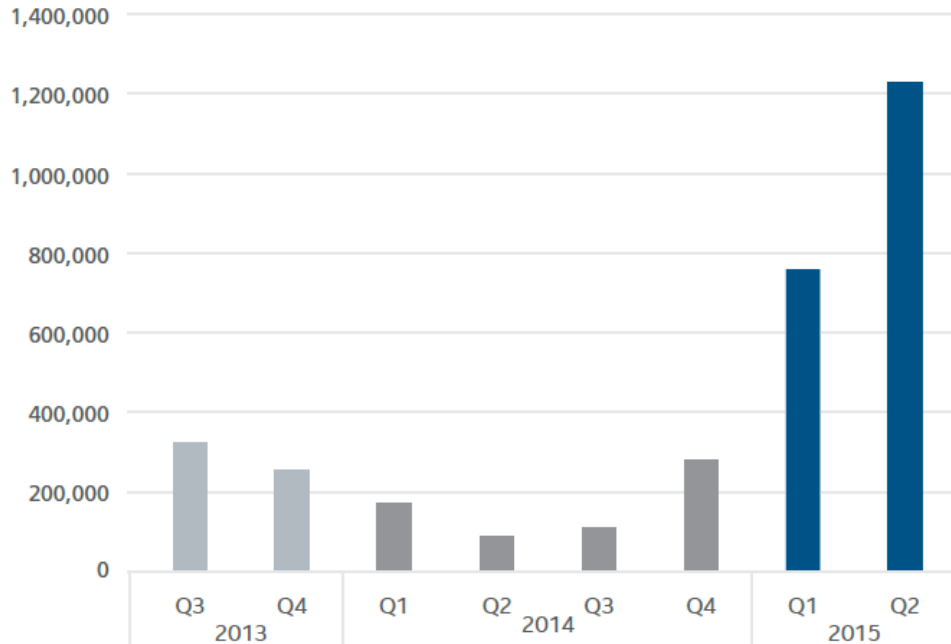
McAfee Labs 2016 Threats Predictions

Ransomware

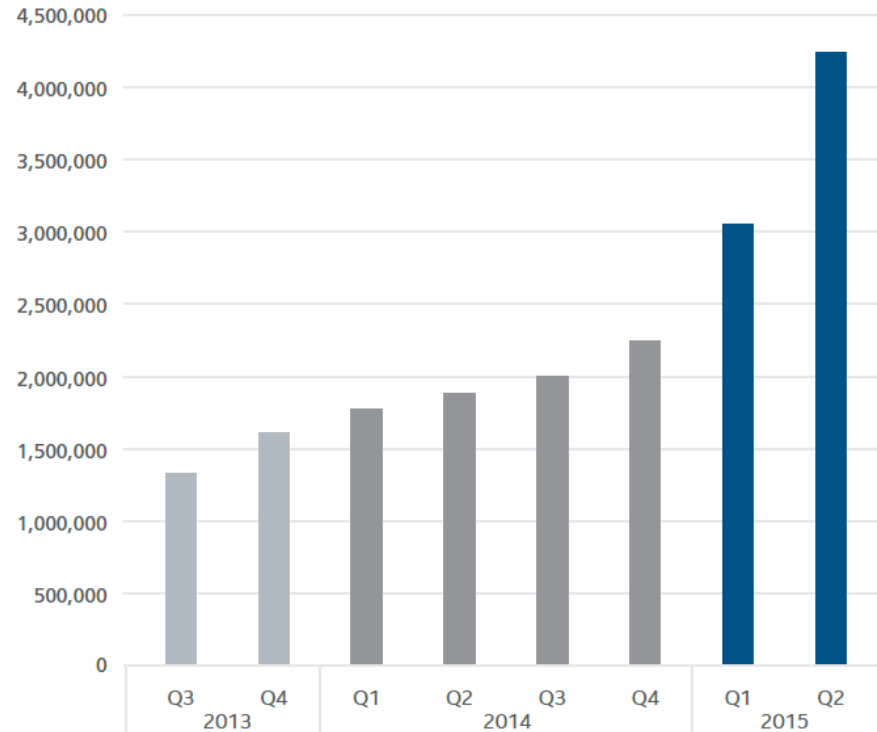
Ransomware zůstává hlavní a rychle rostoucí hrozbou v roce 2016, využívající anonymitu sítě a nových platebních metod – bitcoin.

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

New Ransomware



Total Ransomware



Problémy s Ransomware útoky ve světě



Home / Security

Ransomware authors streamline attacks, inf... rise

Ransomware authors continue improving file-encrypting programs for Windows and Android, making these nightmarish attacks harder to detect. The biggest ransomware threat for Windows users is CryptoWall, a malware program that encrypts a wide range of files and demands...



Insight into what to prepare for tomorrow
Learn more »



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

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 News & Commentary Authors Slideshows Video Radio Reports White Papers Events Black IS has been held hostage by ransomware that has apparently...

ATTACKS/BREACHES APP SEC CLOUD ENDPOINT MOBILE PERIMETER RISK OPER

ATTACKS/BREACHES

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.

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.

3/13/2015 06:00 PM



Jai Vijayan News

Connect Directly

BBC Sign in News Sport Weather iPla

NEWS

Home UK World Business Election 2015 Tech Science Hea

Technology

Gamers targeted by ransomware v

13 March 2015 | Technology



McAfee Confidential

NETWORKWORLD Most read:



Gartner Critical Capabilities

Ransomware: Pay it or fight it?



Cryptolocker – fáze nákazy a obrana



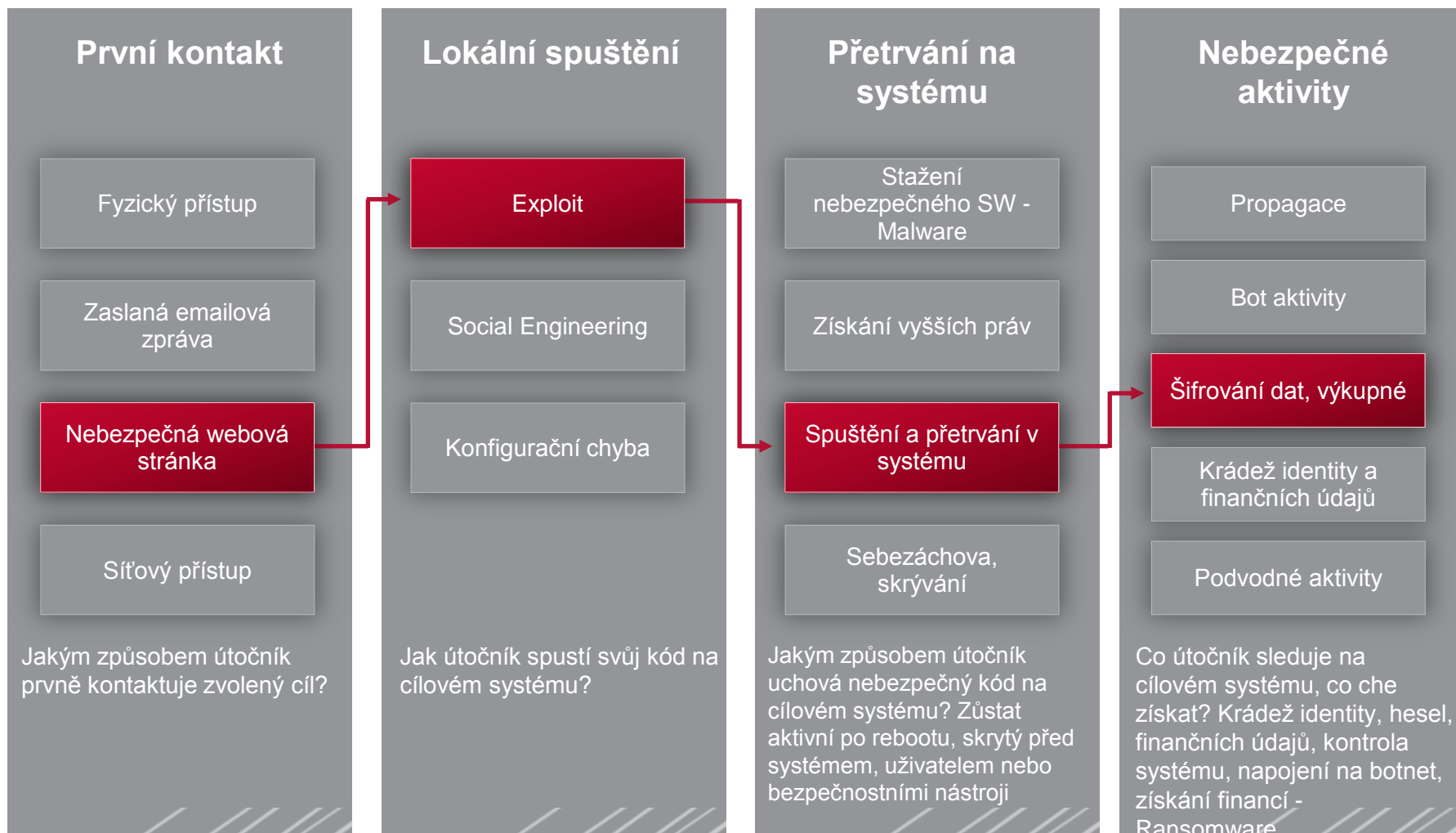
Jaký je další krok?

- 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 porovnáním 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 Intelligence 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

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

Lokální spuštění

On-Access Scanning

McAfee Database Activity Monitor

Database Vulnerability Blocking

McAfee Endpoint protection

Rootkit Prevention

McAfee Host Intrusion Prevention

Buffer Overflow Prevention

Behavioral Prevention

McAfee Application Control, Threat Intelligence Exchange

Install and Execution Prevention

Přetrvání na systému

McAfee Endpoint Protection

File Scanning

Nebezpečné aktivity

Write Blocking

Change Protection



McAfee Application control

TM

McAfee Application Control

Bezpečnostní nástroj využívající inteligentní whitelisting

Dynamický whitelisting



Ochrana před spuštěním neautorizované aplikace

Ochrana paměti



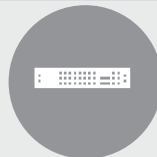
Ochrana operační paměti proti útokům a manipulacím s aplikacemi - buffer overflow útoky

Reputace souborů



Integrace s GTI a TIE pro klasifikaci aplikací jako Good, Bad a Unknown

Integrace



Napojení na ADT pro kontrolu souborů pomocí sandbox technologie, Desktop Firewall integrace

Princip funkce whitelistingu



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

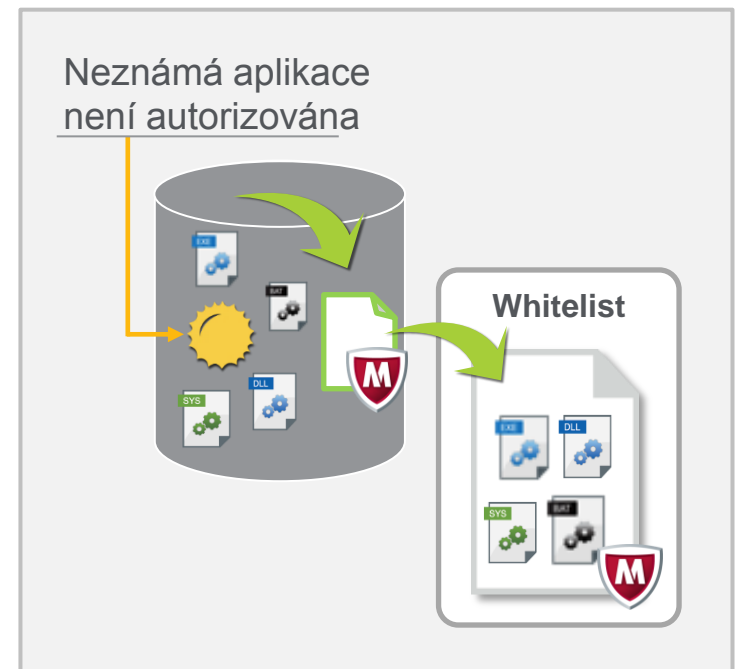
1. Pokus o spuštění programu

- Spustitelný soubor nebo komponenta OS

2. MAC porovnává binární kód s whitelitem

3. Pokud soubor není ve whitelistu, spuštění programu se zablokuje.

- Událost je logována, alertována nebo auditována



Dynamický model Application Controlu



Zamčeno
whitelistingem



Automatická aktualizace
whitelistu



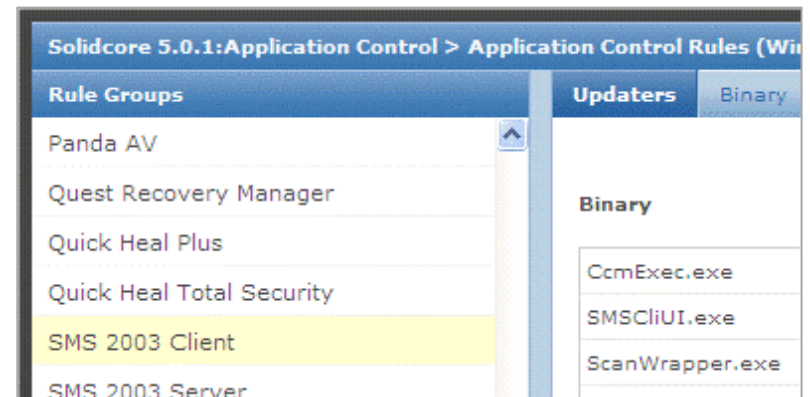
Návrat do zamčeného
stavu



Dynamický model whitelistingu

1. Důvěryhodné procesy

- Nově vytvořená nebo modifikovaná aplikace je přidána do whitelistu
- Podpora standardních updatů 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 populární metoda
 - Vytvoření vlastního certifikátu a podepsání autorizovaných aplikací

Issued To	Issued By	Expiration Date
Adobe Systems	VeriSign Class 3 Code Signing 2004 CA	11/5/09 3:59:51 America/Los_An

Dynamický model whitelistingu

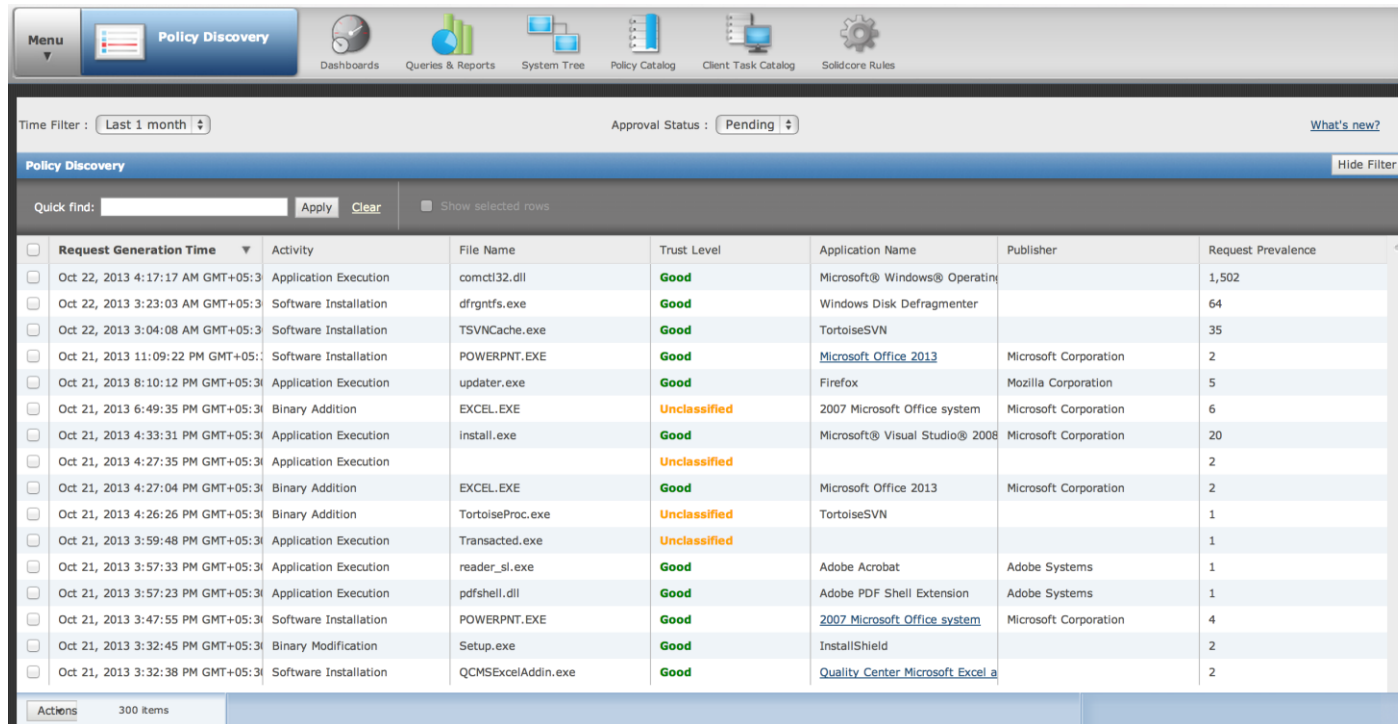
3. Důvěryhodný adresář

- Definuje sdílený adresář, který je důvěryhodný pro instalaci aplikace

Updaters	Binary	Trusted Users	Publishers	Installers	Trusted Directories
Path		Action			
\\fileserver.solidcore.local\startupscripts		Include			

Dynamický model whitelistingu

4. Důvěryhodný uživatel (IT Admins)



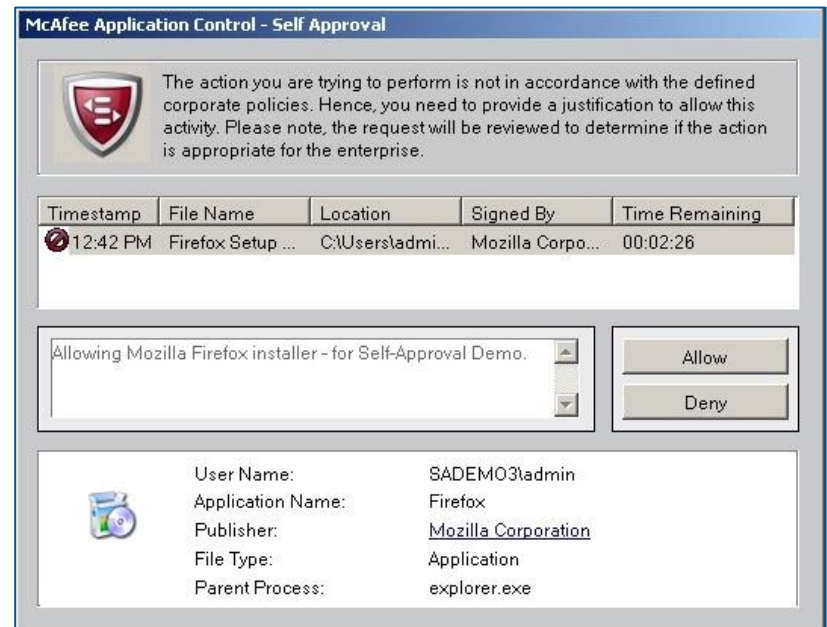
The screenshot displays the McAfee Policy Discovery interface. At the top, there is a navigation bar with icons for Menu, Policy Discovery, Dashboards, Queries & Reports, System Tree, Policy Catalog, Client Task Catalog, and Solidcore Rules. Below this, a filter bar shows 'Time Filter : Last 1 month' and 'Approval Status : Pending'. The main content area is titled 'Policy Discovery' and contains a table of application requests. The table has columns for Request Generation Time, Activity, File Name, Trust Level, Application Name, Publisher, and Request Prevalence. The data rows show various activities like Application Execution, Software Installation, and Binary Addition for files such as comctl32.dll, dfrgnfs.exe, TSVNCache.exe, POWERPNT.EXE, updater.exe, EXCEL.EXE, install.exe, EXCEL.EXE, TortoiseProc.exe, Transacted.exe, reader_sl.exe, pdfshell.dll, POWERPNT.EXE, Setup.exe, and QCMExcelAddin.exe. Trust levels are either 'Good' or 'Unclassified'. The interface also includes a 'Quick find' search bar and an 'Actions' button at the bottom left.

<input type="checkbox"/>	Request Generation Time	Activity	File Name	Trust Level	Application Name	Publisher	Request Prevalence
<input type="checkbox"/>	Oct 22, 2013 4:17:17 AM GMT+05:30	Application Execution	comctl32.dll	Good	Microsoft® Windows® Operating System		1,502
<input type="checkbox"/>	Oct 22, 2013 3:23:03 AM GMT+05:30	Software Installation	dfrgnfs.exe	Good	Windows Disk Defragmenter		64
<input type="checkbox"/>	Oct 22, 2013 3:04:08 AM GMT+05:30	Software Installation	TSVNCache.exe	Good	TortoiseSVN		35
<input type="checkbox"/>	Oct 21, 2013 11:09:22 PM GMT+05:30	Software Installation	POWERPNT.EXE	Good	Microsoft Office 2013	Microsoft Corporation	2
<input type="checkbox"/>	Oct 21, 2013 8:10:12 PM GMT+05:30	Application Execution	updater.exe	Good	Firefox	Mozilla Corporation	5
<input type="checkbox"/>	Oct 21, 2013 6:49:35 PM GMT+05:30	Binary Addition	EXCEL.EXE	Unclassified	2007 Microsoft Office system	Microsoft Corporation	6
<input type="checkbox"/>	Oct 21, 2013 4:33:31 PM GMT+05:30	Application Execution	install.exe	Good	Microsoft® Visual Studio® 2008	Microsoft Corporation	20
<input type="checkbox"/>	Oct 21, 2013 4:27:35 PM GMT+05:30	Application Execution		Unclassified			2
<input type="checkbox"/>	Oct 21, 2013 4:27:04 PM GMT+05:30	Binary Addition	EXCEL.EXE	Good	Microsoft Office 2013	Microsoft Corporation	2
<input type="checkbox"/>	Oct 21, 2013 4:26:26 PM GMT+05:30	Binary Addition	TortoiseProc.exe	Unclassified	TortoiseSVN		1
<input type="checkbox"/>	Oct 21, 2013 3:59:48 PM GMT+05:30	Application Execution	Transacted.exe	Unclassified			1
<input type="checkbox"/>	Oct 21, 2013 3:57:33 PM GMT+05:30	Application Execution	reader_sl.exe	Good	Adobe Acrobat	Adobe Systems	1
<input type="checkbox"/>	Oct 21, 2013 3:57:23 PM GMT+05:30	Application Execution	pdfshell.dll	Good	Adobe PDF Shell Extension	Adobe Systems	1
<input type="checkbox"/>	Oct 21, 2013 3:47:55 PM GMT+05:30	Software Installation	POWERPNT.EXE	Good	2007 Microsoft Office system	Microsoft Corporation	4
<input type="checkbox"/>	Oct 21, 2013 3:32:45 PM GMT+05:30	Binary Modification	Setup.exe	Good	InstallShield		2
<input type="checkbox"/>	Oct 21, 2013 3:32:38 PM GMT+05:30	Software Installation	QCMExcelAddin.exe	Good	Quality Center Microsoft Excel a		2

Dynamický model whitelistingu

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

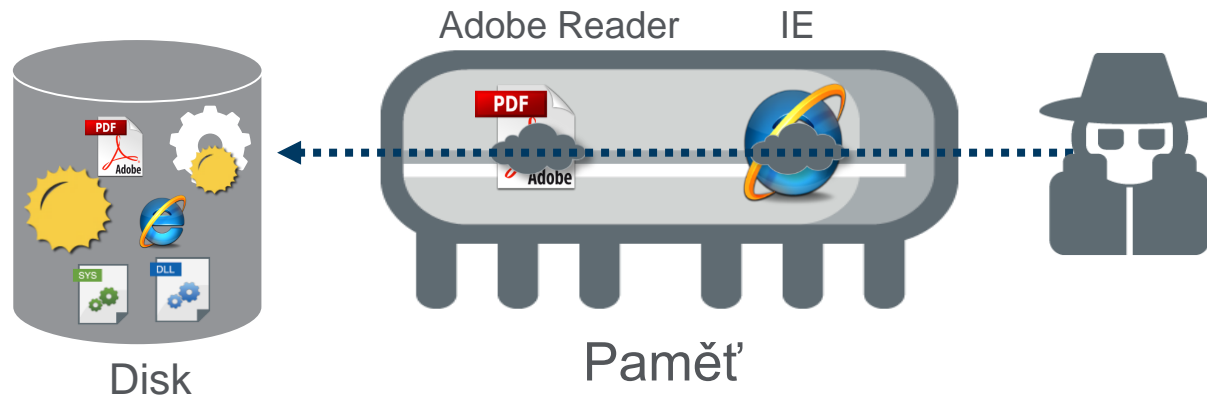
- Aplikace, která není ve whitelistu, může být **schválena** uživatelem
- Tento model je vhodný pro uživatele/systémy, kde se dějí časté změny (není doporučený pro všechny uživatele)
- Administrátor má možnost auditovat tyto uživatelsky schválené aplikace a může provést změny - povolit/zalázat



Ochrana paměti počítače – proč je nutná?



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



Ochrana paměti – Co dělá Application Control



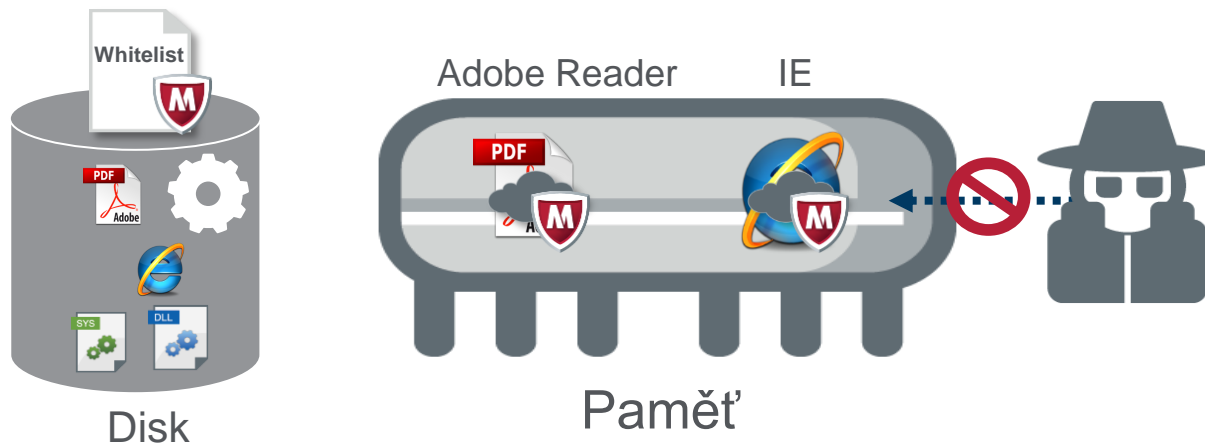
Ochrana aplikace whitelistem

- 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



Inventorizace aplikací

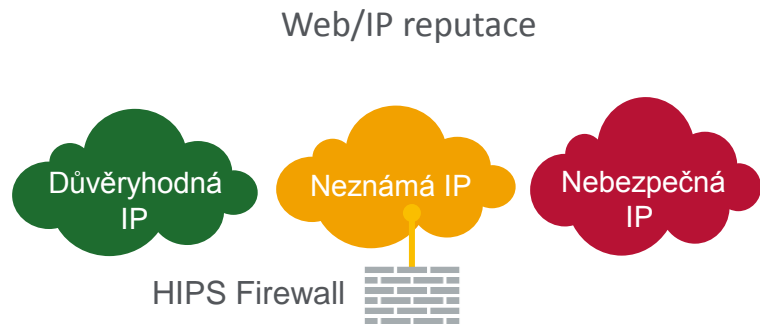


- Ucelený přehled o všech aplikacích na koncových bodech – seznam whitelistů v jedné konzoli
- Kontrola aplikací s Globálním reputčním systémem GTI – ohodnocení bezpečnosti aplikací
- Seznam aplikací s neznámou reputací – možnost okamžité nápravy – povolit/zakázat
- Seznam zastaralých verzí běžících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

Binary Name	Version
ati2dvaq.dll	6.13.10.6153
ati2mtaq.sys	6.13.10.6153

Spolupráce s firewallem pro neznámé aplikace

Reputace souborů + IP reputace

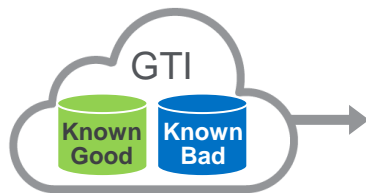


- **Neznámá aplikace** komunikuje na **neznámou IP** => podezřelá aktivita!
- Aplikace může být Botnet/APT komunikující na Command & Control Server
- **Síťová aktivita je blokována firewallem**

Inventory By Applications		Inventory By Systems	
Application		Search	
Applications Collapse All		Binaries	
▼ All Applications		Quick find: <input type="text"/>	
▶ Good Apps (566)		<input type="checkbox"/> Binary Name ▲ Version	
Bad Apps (0)		<input type="checkbox"/> mediaplayer.exe 2.102.0.0	
▼ Unclassified Apps (1)			
InstallIQ Installation Utility (2.102.0.0) (W3i, LLC)			

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) blokována komunikace

Jaké řešení vybrat do prostředí společnosti?

	Jednoúčelové systémy	Servery	COE stanice/notebooky	Dynamické stanice/notebooky
	 <p>Kiosk POS ATM</p>			
	← STATICKE		DYNAMICKÉ →	
Primární Antimalware				 
Sekundární Antimalware				



TIE / DXL

Threat Intelligence Exchange Data Exchange Layer

TM

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

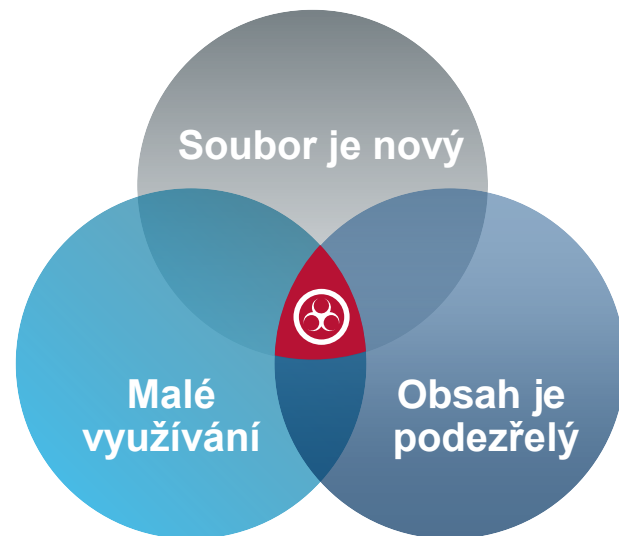
- Okamžité reakce na detekované hrozby oproti rychlosti aktualizaci DAT
- Centrální bod který agreguje požadavky na GTI z interní sítě

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)

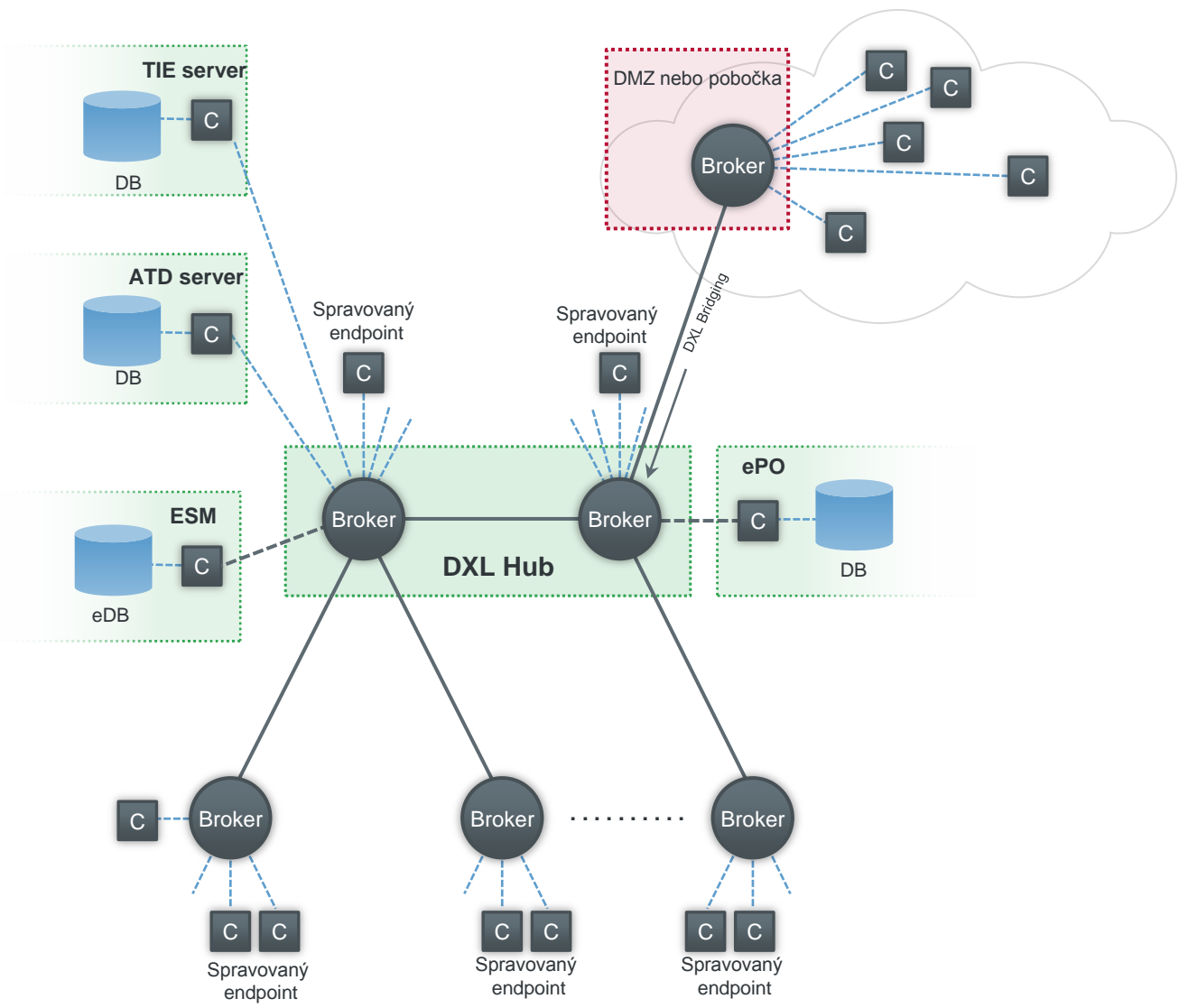
Navržen pro optimalizaci komunikace zařízení na sítích s malou šířkou pásma, vysokou latencí nebo nespolehlivé sítě

Šifrovaná komunikace pomocí TLS 1.2 na portu 8883

Server iniciuje komunikaci na dříve nedostupného klienta

DXL je plně spravován pomocí ePO serveru



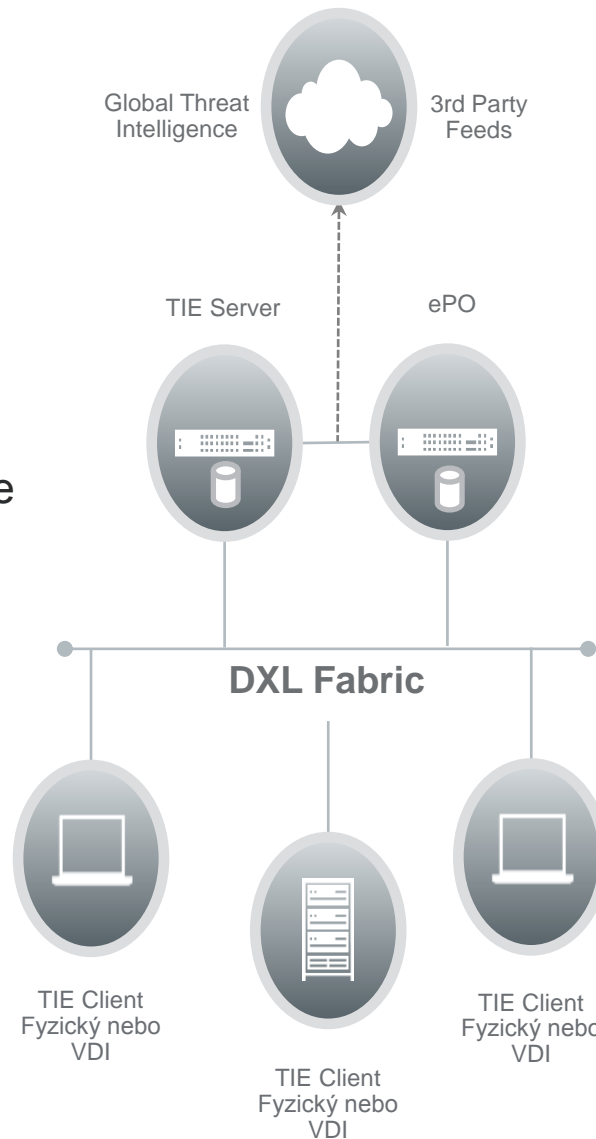


TIE/DXL architektura

McAfee Threat Intelligence Exchange

Komponenty řešení

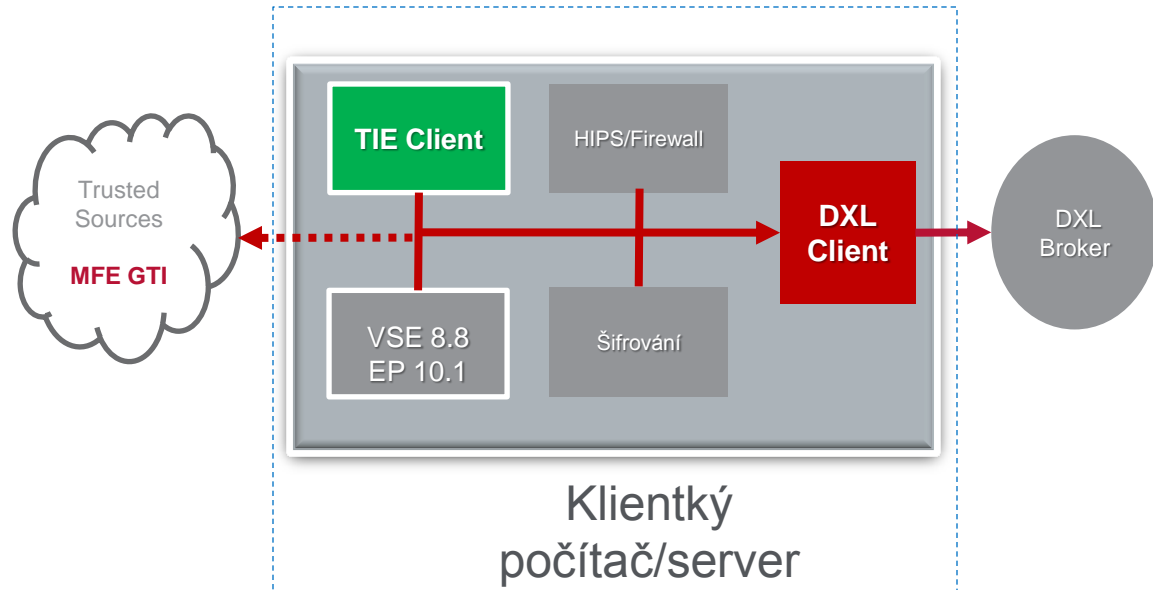
- TIE Server – virtuální image na VMware
- TIE Client
- DXL Fabric



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

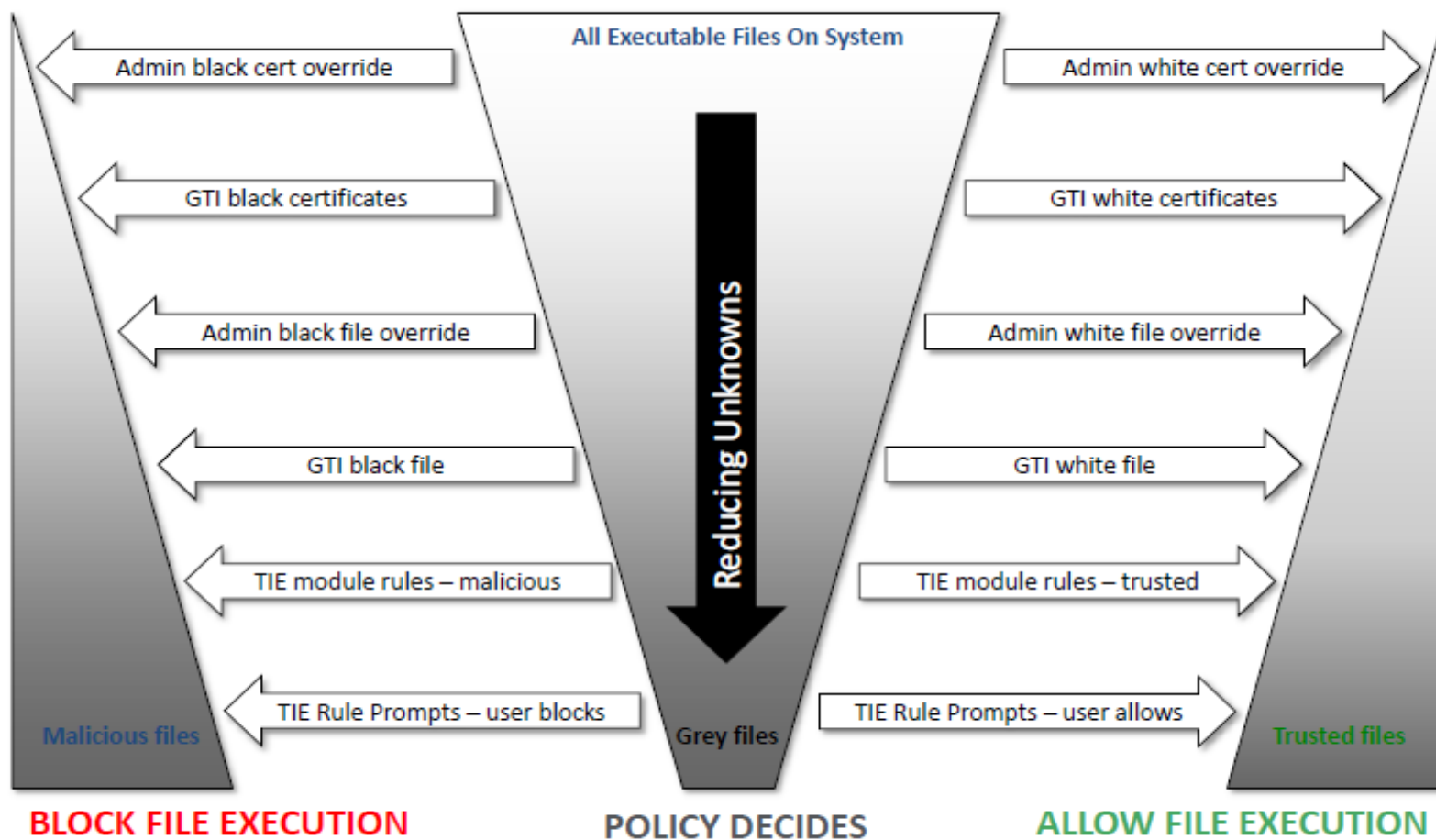
- Cesta k souboru, instalace služby, spouštění klíčů
- Soustění souboru z lokální sítě, počítače, z Internetu
- Počet spuštění soubor v rámci lokální sítě

✓ Data o certifikátech

- Seznam certifikátů a jejich řetězení
- Soubor podepsaný platným/revokovaným certifikátem

TIE logika klienta – filtr pro určení reputace souboru


A layered approach that systemically narrows the 'unknown files'



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 .NET 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**

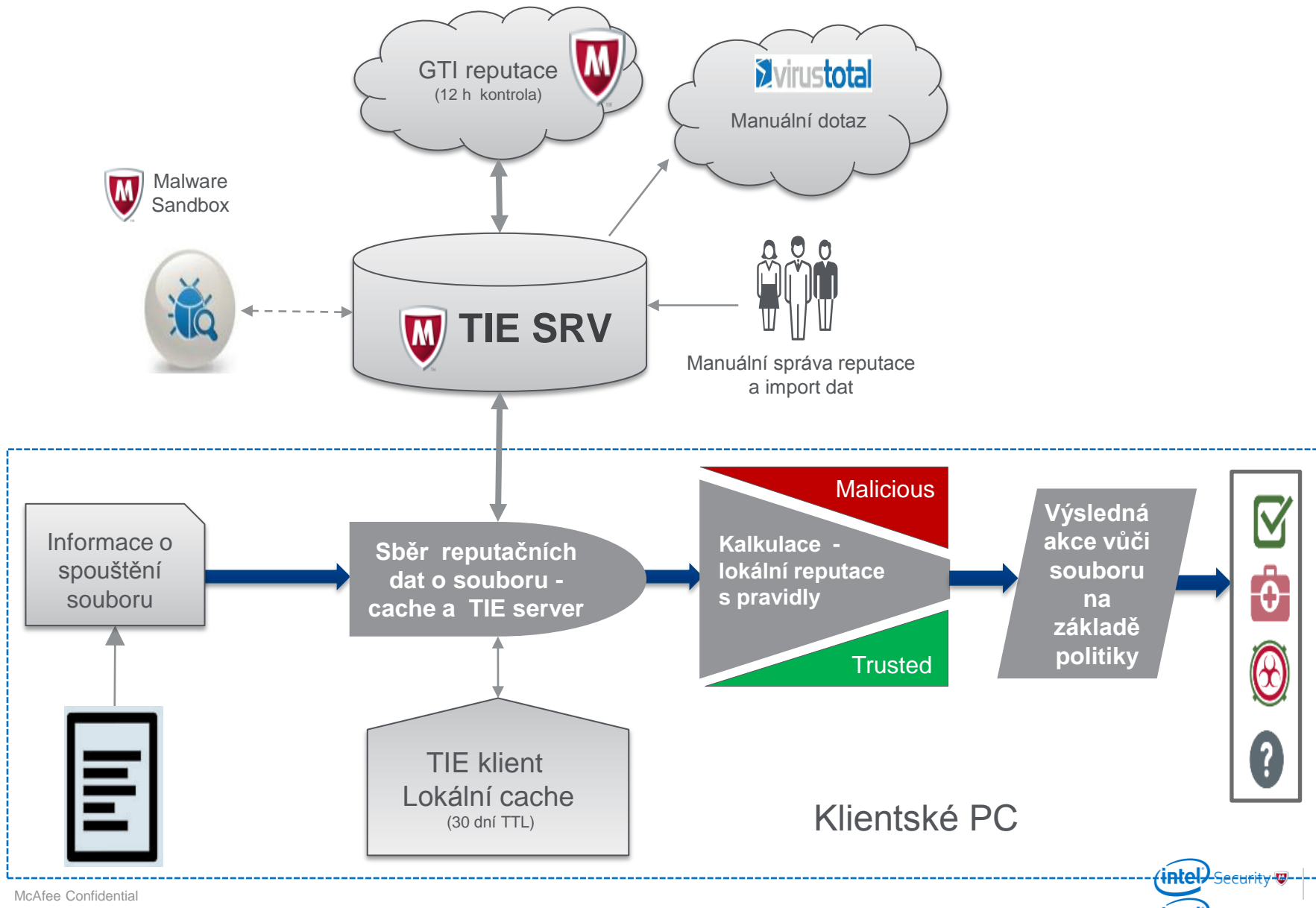


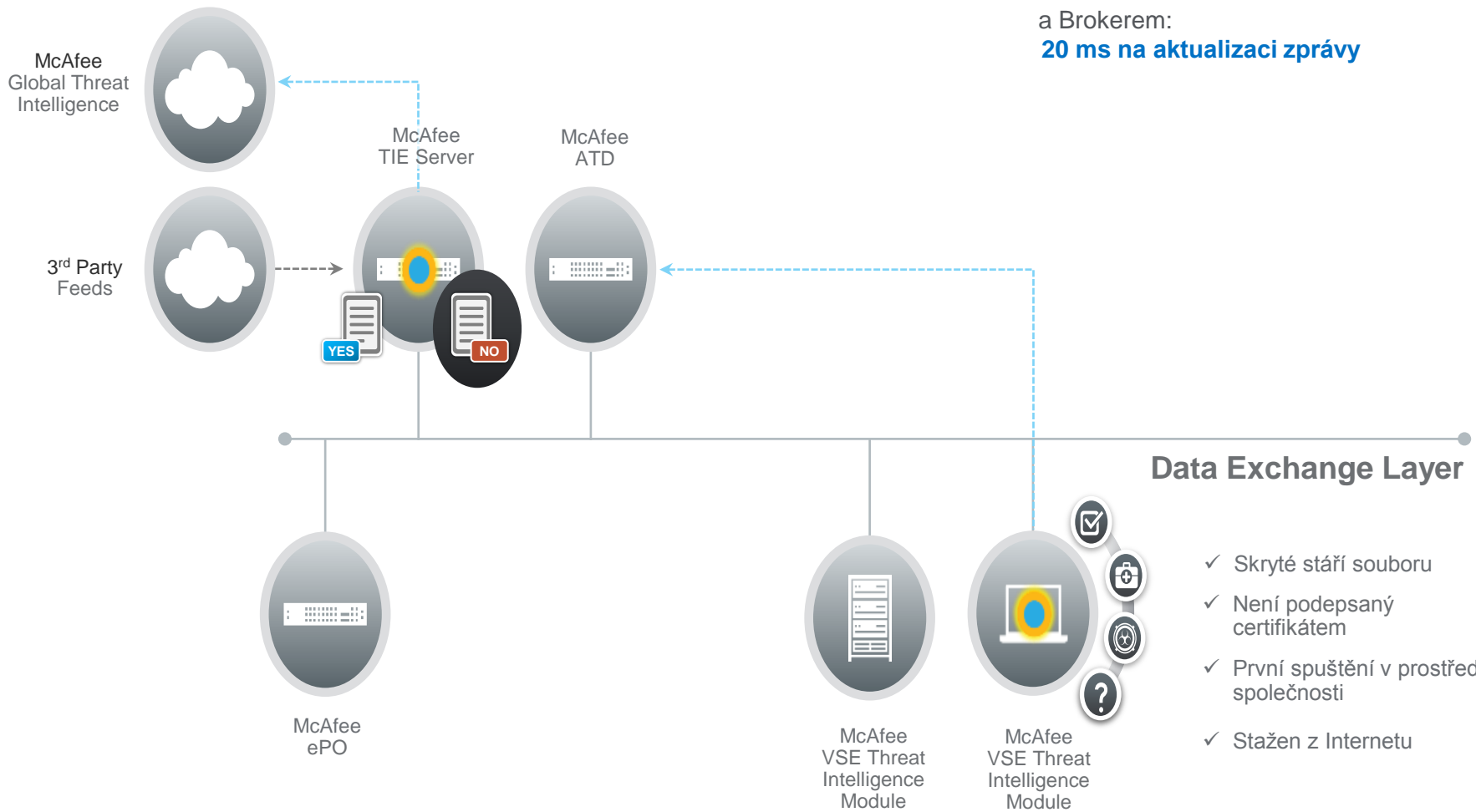
Neznámý soubor - malware

- 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

TM

McAfee Advanced Threat Defense

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

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

Engine

Zákaznický definovatelné Sandbox image

Admin VM
Linux 64bit:

Administration
Scheduler
Task manager
File input / Server
Results output

Communication
HTTP/HTTPS
FTP/SFTP
Restful API
Socket

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

Windows XP
SP2/SP3



Server 2003
SP1/SP2



Server 2008
64bit



Windows 7
32bit/64bit



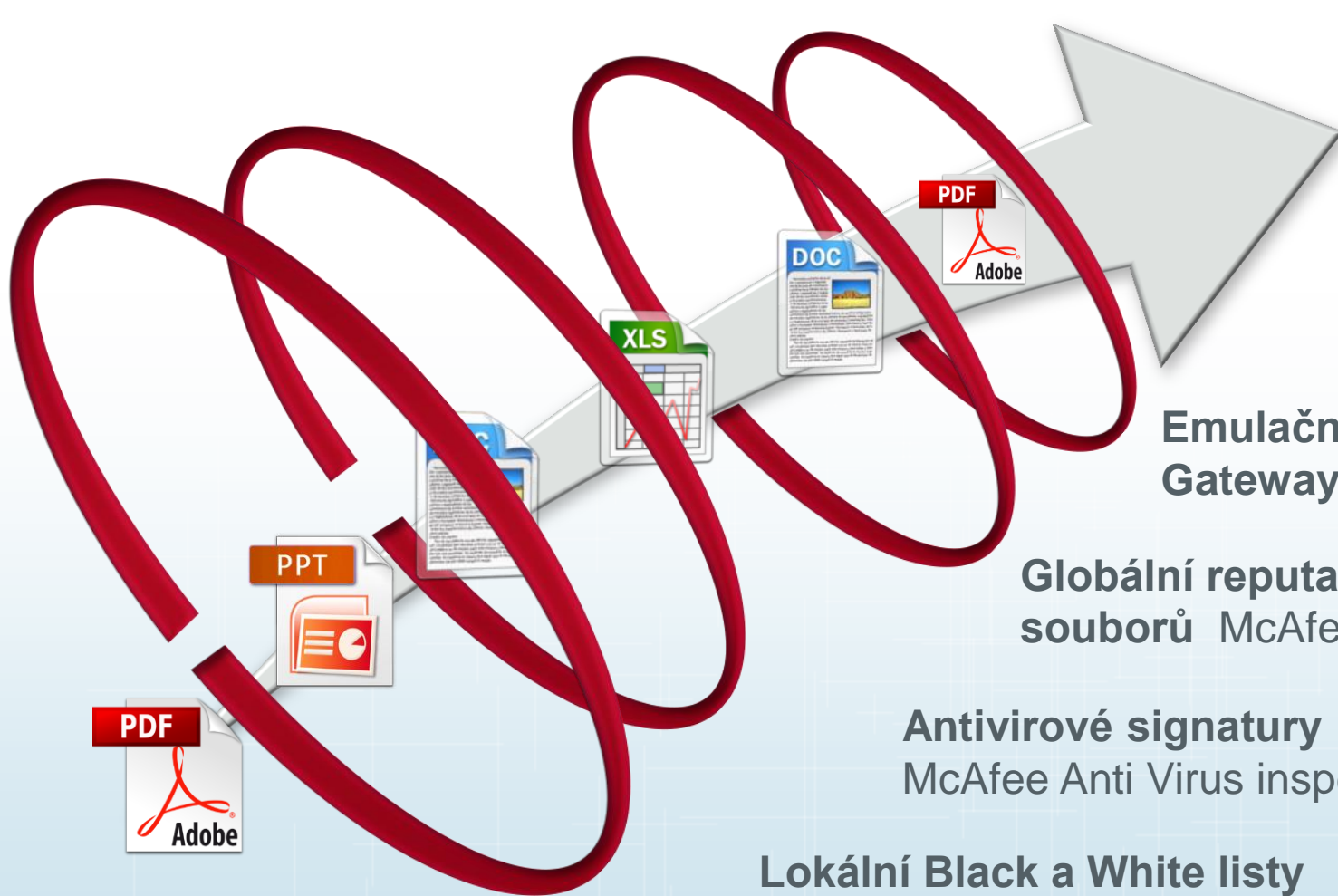
Android



Type-I Hypervisor



Intel-based Hardware Platform



Sandboxing
Statická a
dynamická
analýza

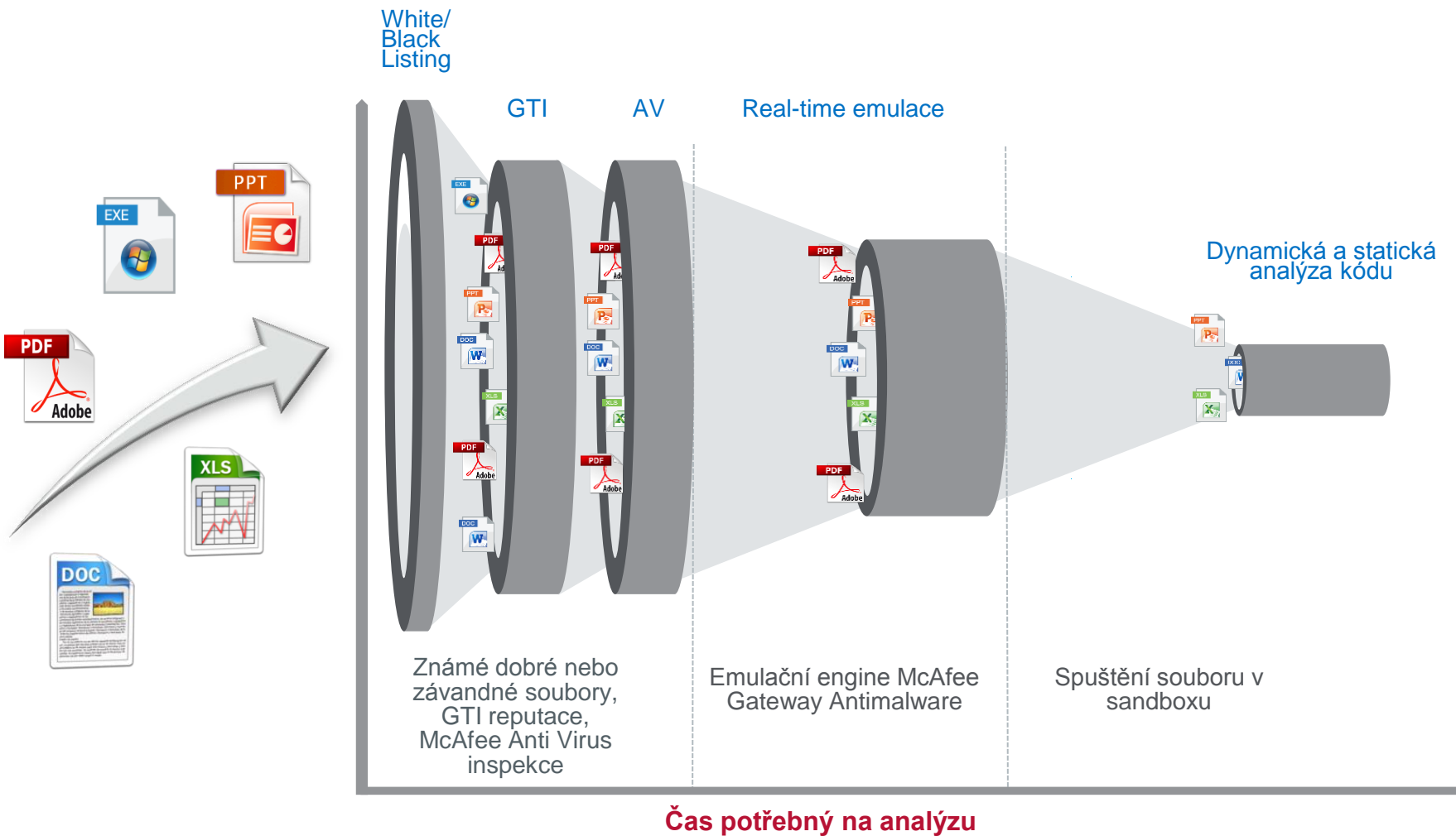
**Emulační engine –
Gateway Anti- Malware**

**Globální reputace
souborů McAfee GTI**

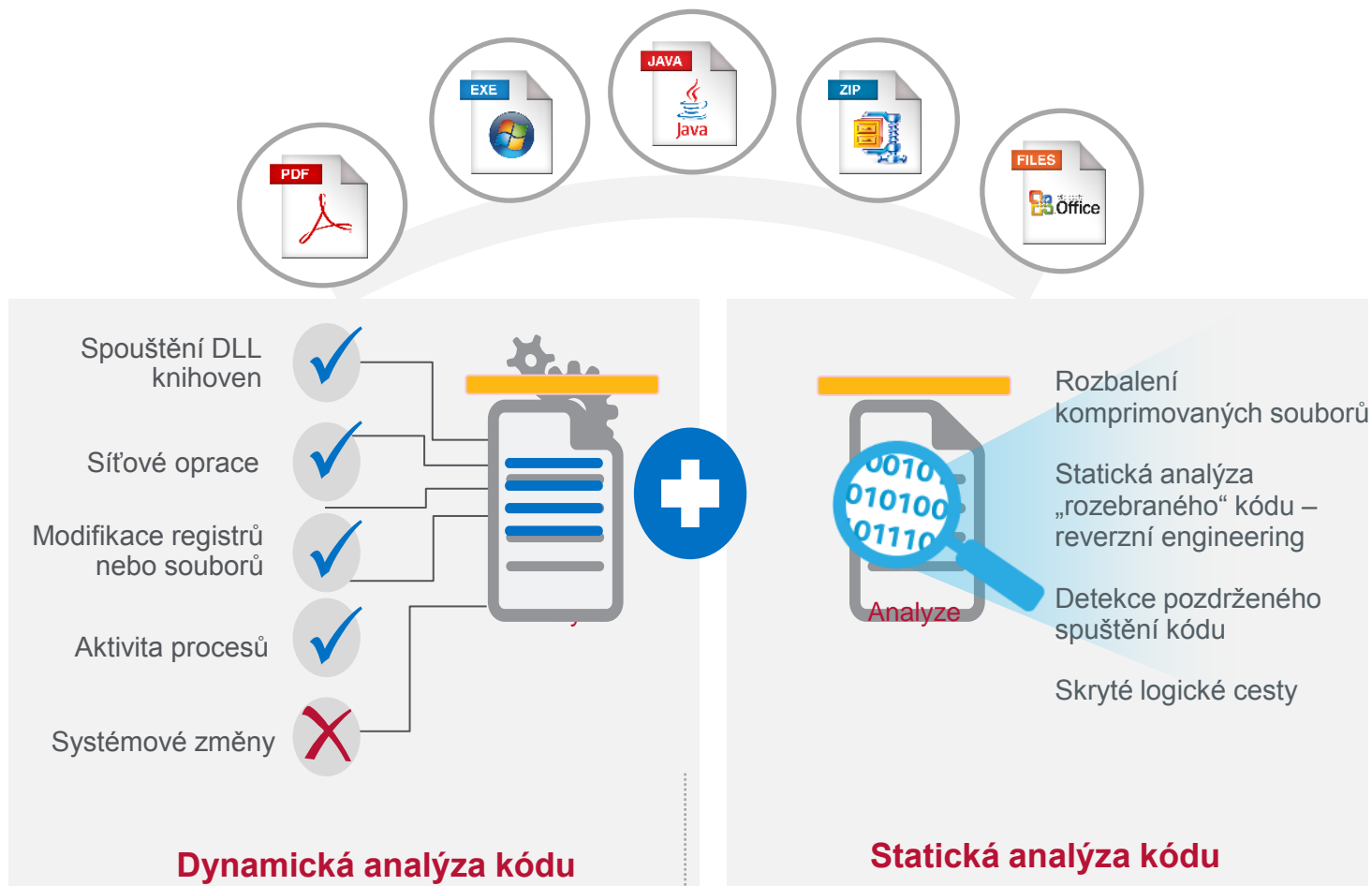
Antivirové signatury
McAfee Anti Virus inspekce

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

Analyzer Profile

***Name:**

Description:

VM Profile:

Automatically Select OS

Enable Windows 32-bits VM Profile: Windows 64-bits VM Profile:

Runtime Parameters

Archive Password: **Confirm Password:**

Minimum Run Time (sec): **Maximum Run Time (sec):**

Reports, Logs, and Artifacts

<input checked="" type="checkbox"/> Analysis Summary	<input type="checkbox"/> Packet Captures
<input type="checkbox"/> Dropped Files	<input type="checkbox"/> Disassembly Results
<input type="checkbox"/> Logic Path Graph	<input type="checkbox"/> User API Log

Analyze Options

<input checked="" type="checkbox"/> Local Black List	<input type="checkbox"/> Anti-Malware
<input type="checkbox"/> GTI File Reputation	<input checked="" type="checkbox"/> Gateway Anti-Malware
<input checked="" type="checkbox"/> Sandbox	<input checked="" type="checkbox"/> Run All Selected

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

The screenshot displays the McAfee ATD Analysis Results interface. At the top, there is a table titled 'Samples' with columns for 'Reports', 'Submitted Time', 'Severity', and 'File Name'. A context menu is open over the table, listing options: Analysis Summary (HTML), Analysis Summary (PDF), Dropped Files, Disassembly Results, Logic Path Graph, and Advanced Threat Defense Engine Results. The 'Advanced Threat Defense Engine Results' window is open, showing detailed information for a file. The file summary includes File ID, File Size, MD5, and SHA1 hashes. The malware confidence is 'Very High'. The malware indicators list various actions performed by the malware, such as identifying itself, enumerating WinSock settings, creating content under Windows system directories, and deleting registry keys. Below this, the 'Individual Engine Results' table shows the detection status of various engines: Gateway Anti-Malware, GTI File Reputation, and Anti-Malware are all 'Inconclusive', while the Sandbox engine is 'Very High' and identifies the malware as 'Malware.Dynamic'. The 'Sandbox Analysis Results' section shows the analysis environment as 'Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601), 64-bit'. At the bottom, there are buttons for 'Download Full Analysis Report', 'Open ATD Console', and 'Close'.

Reports	Submitted Time	Severity	File Name
	2014-11-24 22:03:37 CST	Very High	VirusShare_07b8368be91b54dabaa2...
		Very High	VirusShare_1952133061179fce1b5d3...
		Very High	VirusShare_b2e47584f7385ecf9f1a73...
		Very High	VirusShare_2815962f0bffd288d3a806...
		Very High	VirusShare_3ef5decc426a844091514...

Engine	Malware Confidence	Malware Name
Gateway Anti-Malware	Inconclusive	---
GTI File Reputation	Inconclusive	---
Anti-Malware	Inconclusive	---
Sandbox	Very High	Malware.Dynamic

Integrace McAfee ATD

Přímá integrace na úrovni konfigurace

- **McAfee TIE/DXL technologie**

- TIE client přeposílá podezřelé spustitelné soubory na hloubkovou analýzu

- **McAfee Web Gateway**

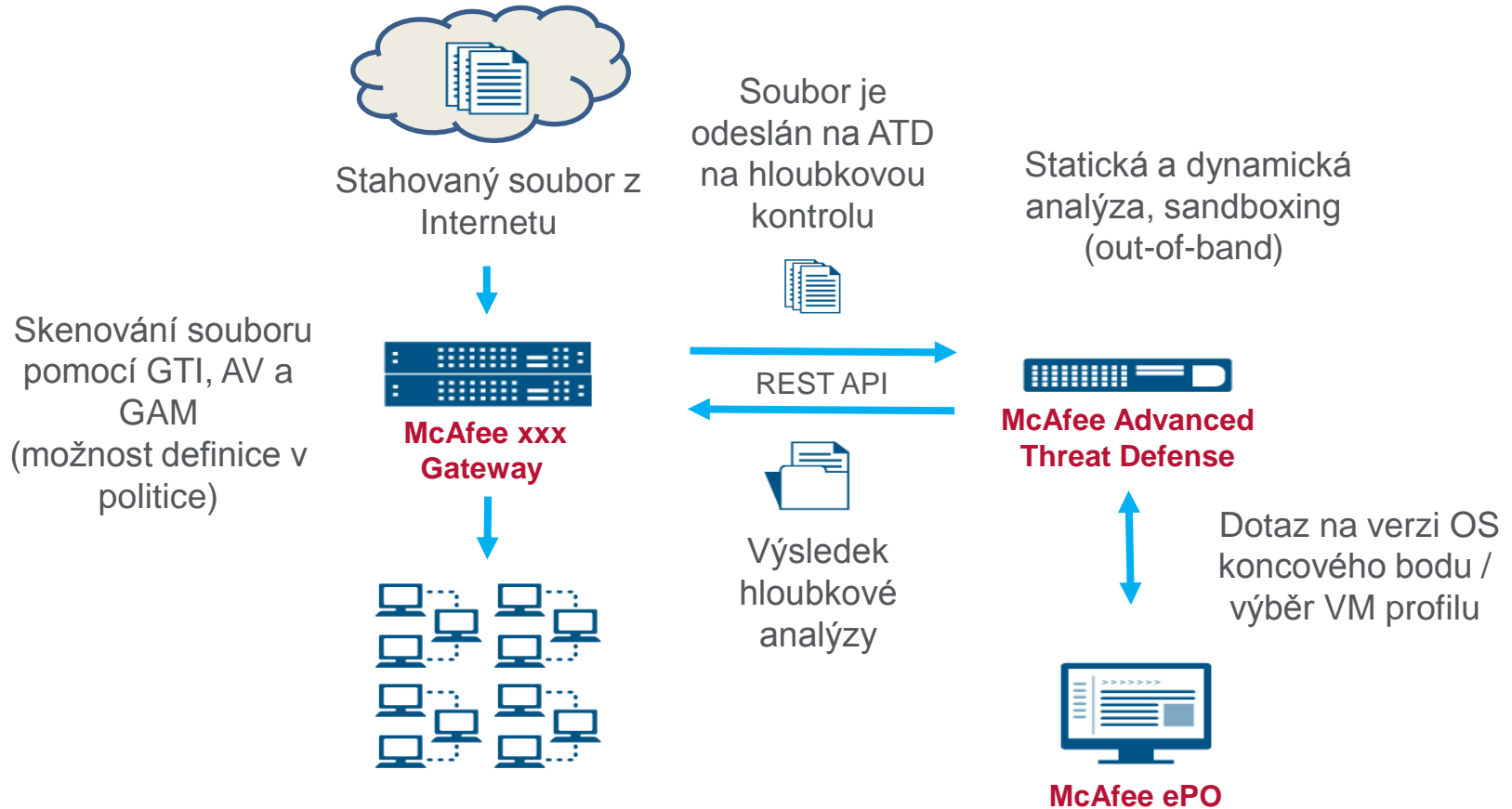
- Přeposílá pouze podezřelé soubory, typicky to budou applety, dokumenty, programy, apod.

- **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

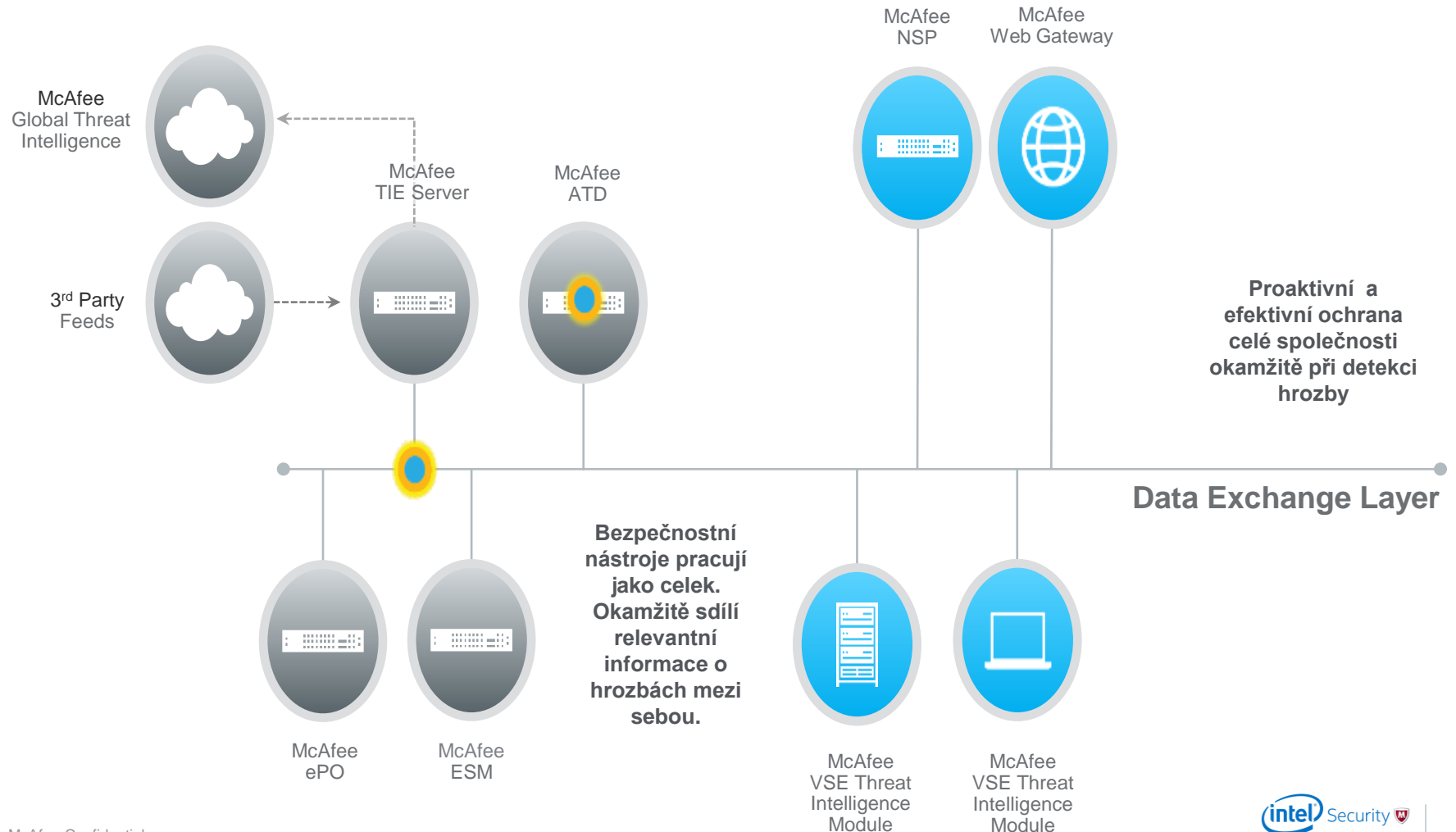
Architektura MWG, IPS a ATD



Threat Intelligence Exchange

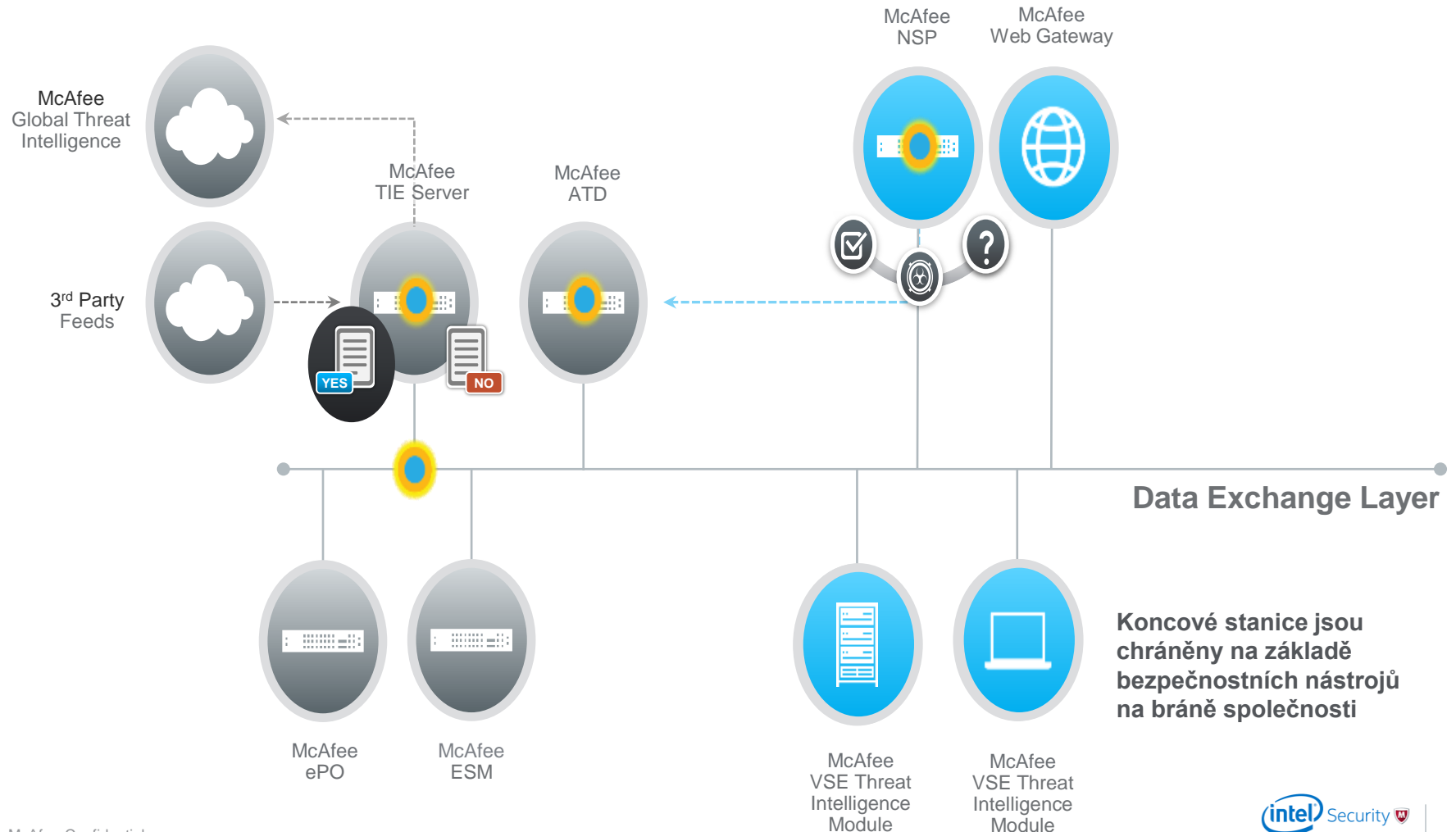
Integrace s branovým řešením bezpečnosti

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



Threat Intelligence Exchange

Integrace s branovým řešením bezpečnosti



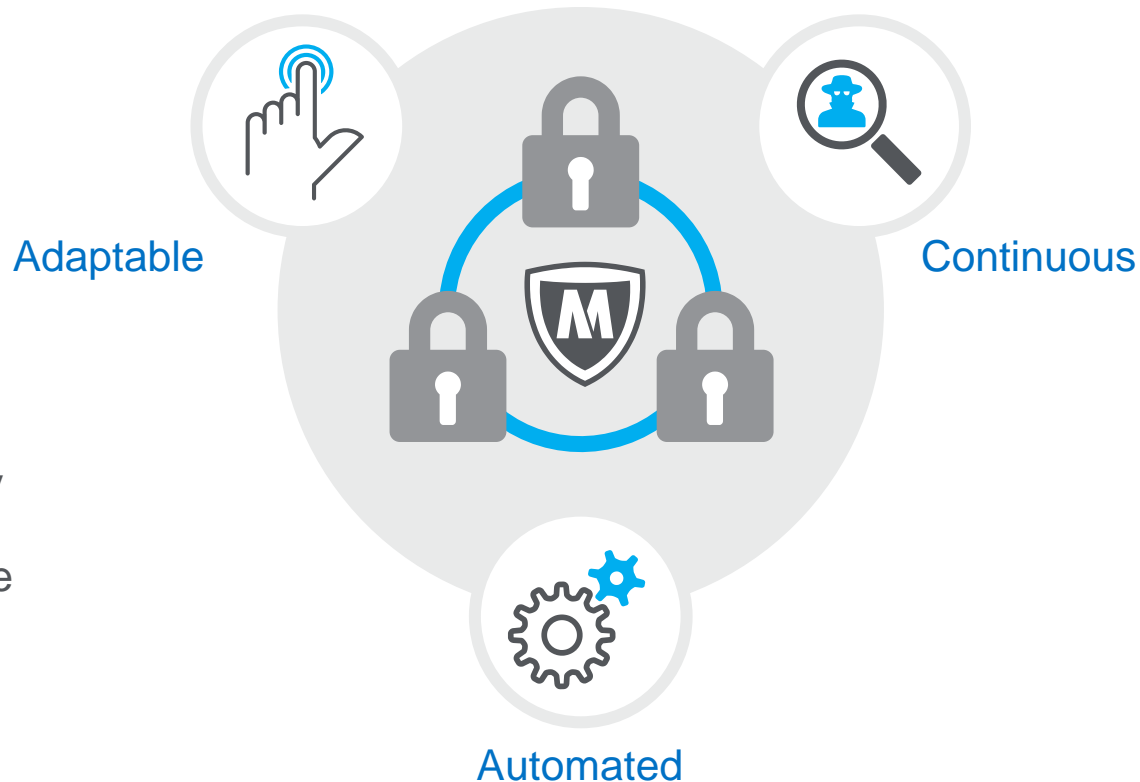


McAfee Active Response



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

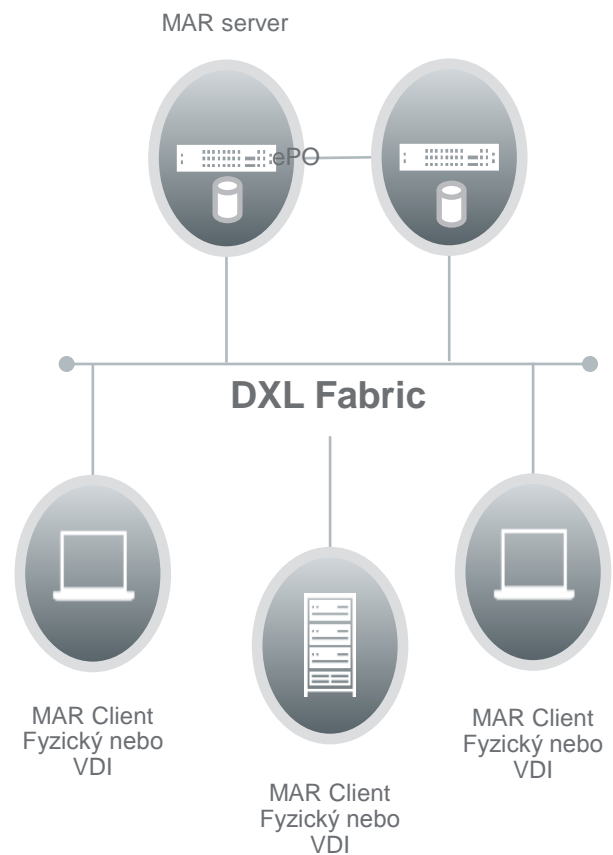


MAR/DXL architektura

McAfee Active Esponse

Komponenty řešení

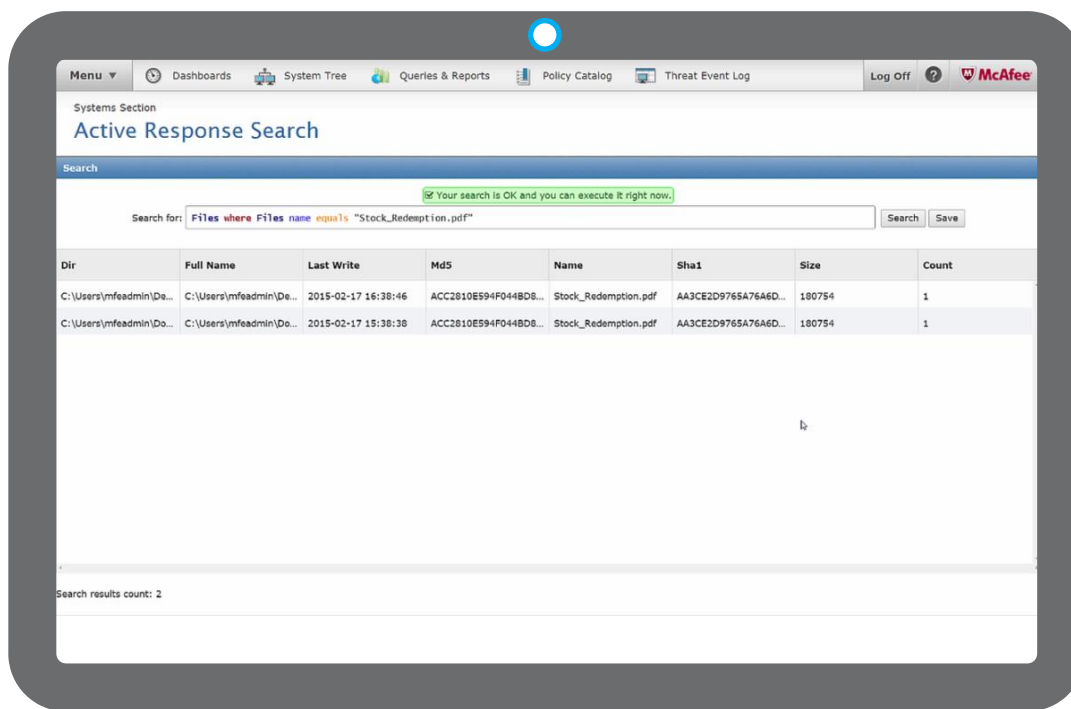
- MAR Server – virtuální image na VMware
- MAR Client
- DXL Fabric



Provázanost a správa pomocí McAfee ePolicy Orchestrator

Vyhledávání souborů, procesů, služeb nebo komunikace

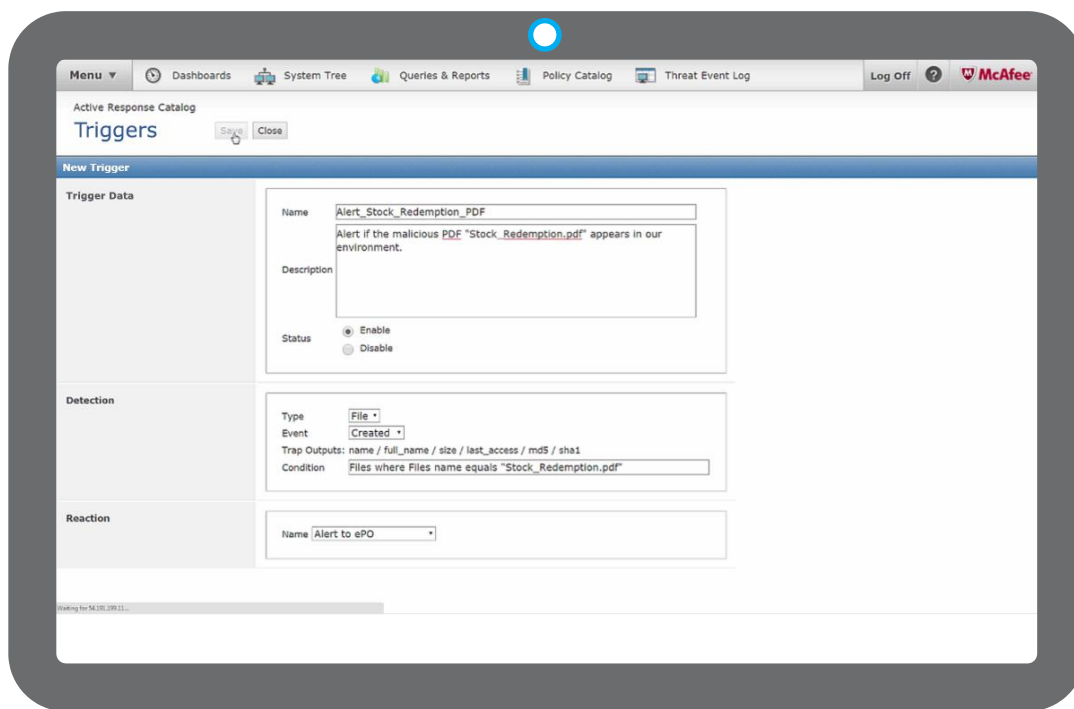
Spouštění přednastavených nebo manuálně vytvořených dotazů



Nepřetržitá ochrana s McAfee ePolicy Orchestrator

Nastavení automatických spouštěčů pro specifické události

Trigger vyvolá akci, která bude automaticky vykonána při detekci události



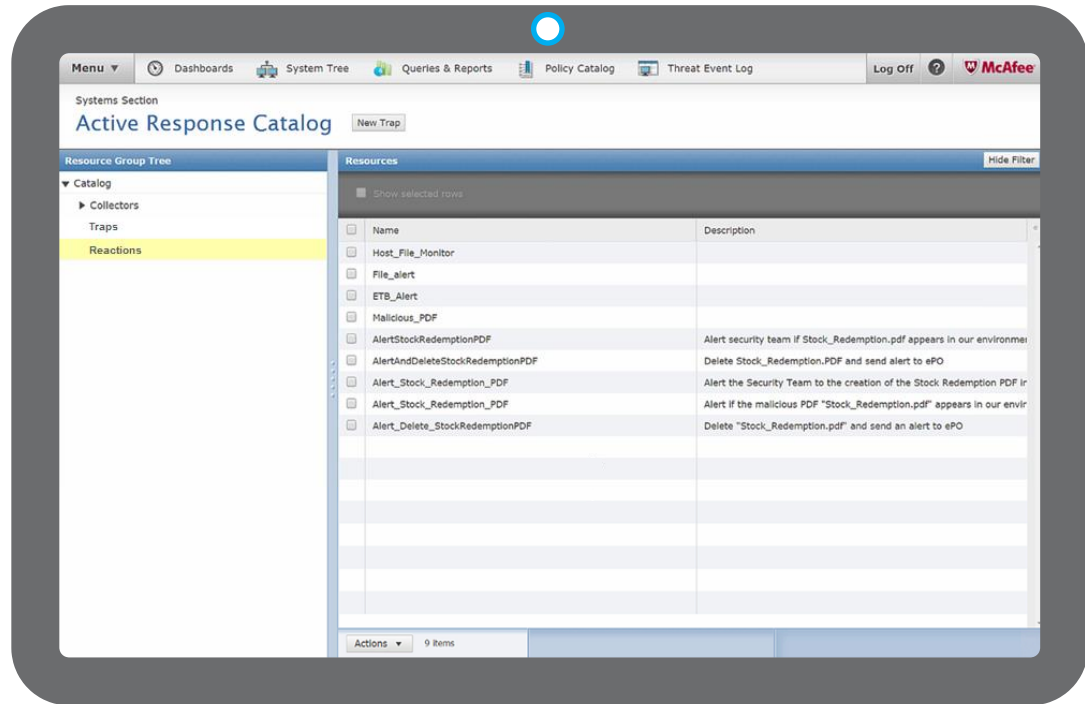
Automatizace s McAfee ePolicy Orchestrator

1.

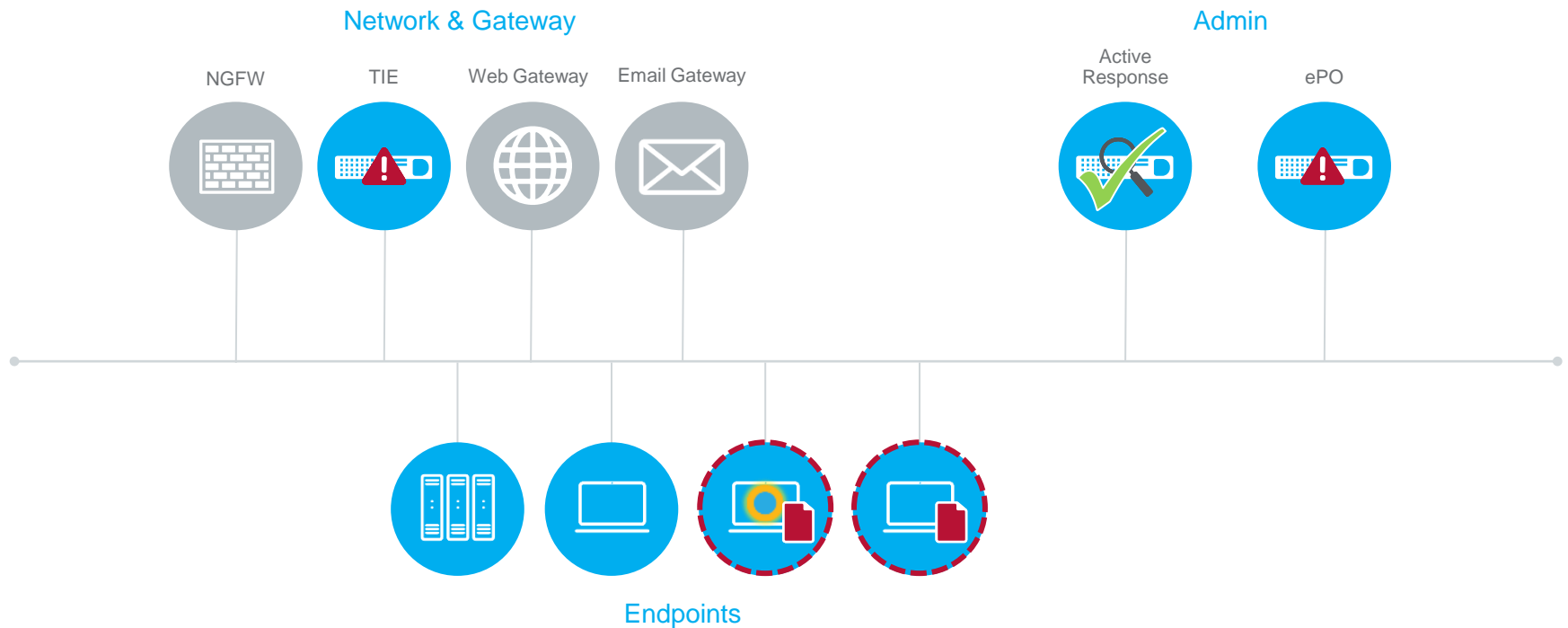
Stále běžící „collector“ sbírá relevantní informace

2.

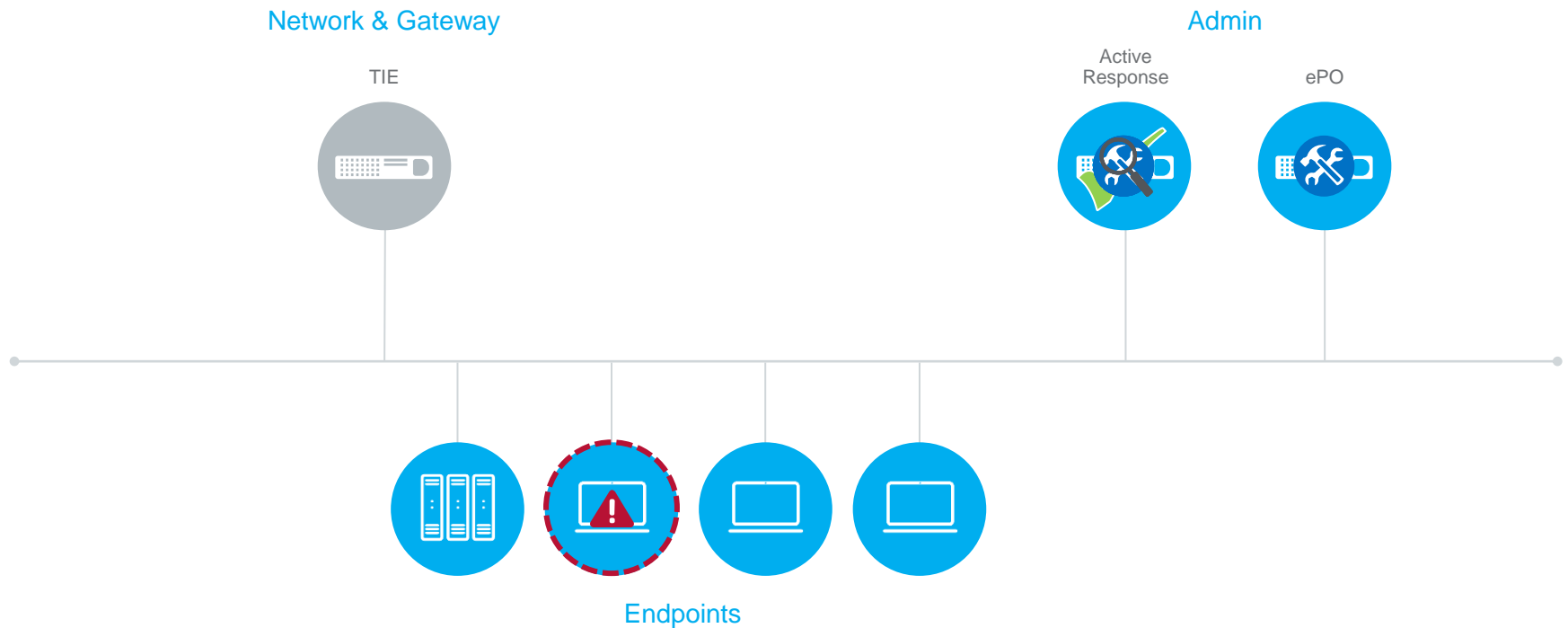
Pohled na události a vykonané akce



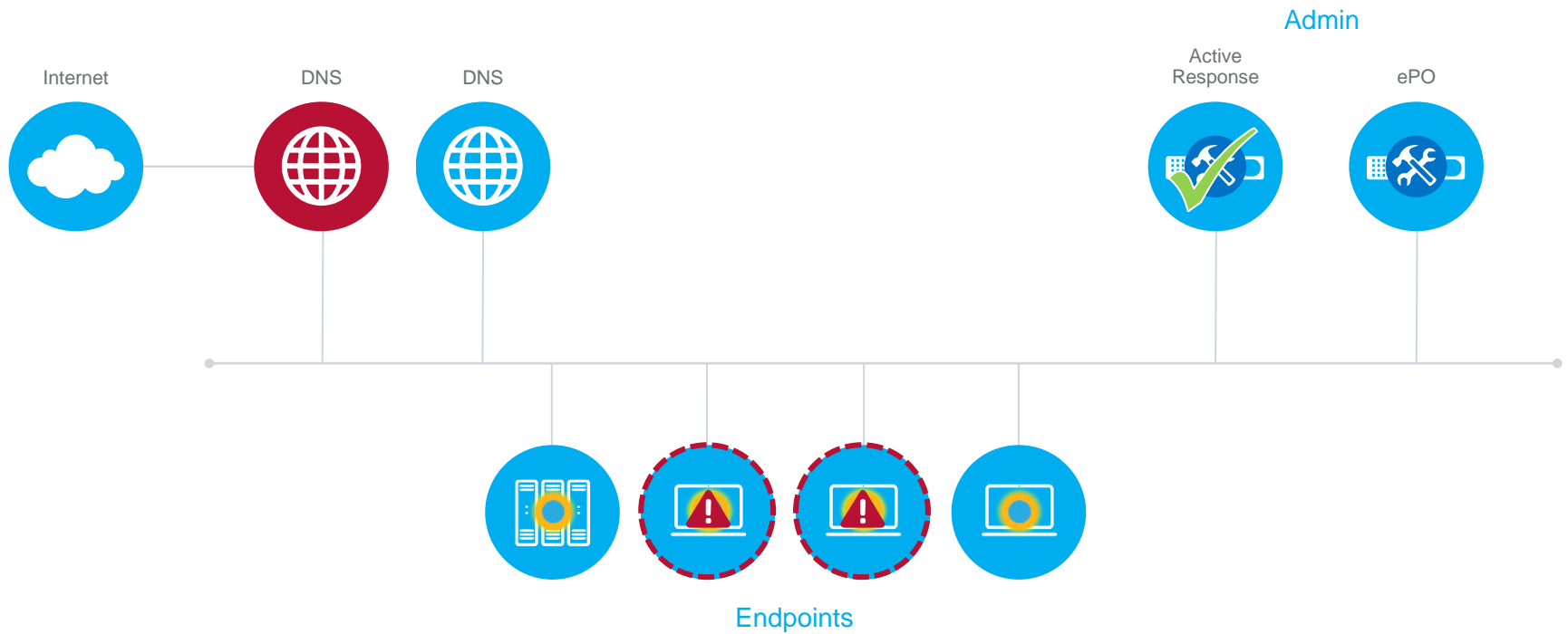
Proaktivní vyhledávání nebezpečných souborů



Náprava a odstranění škodlivém kódu



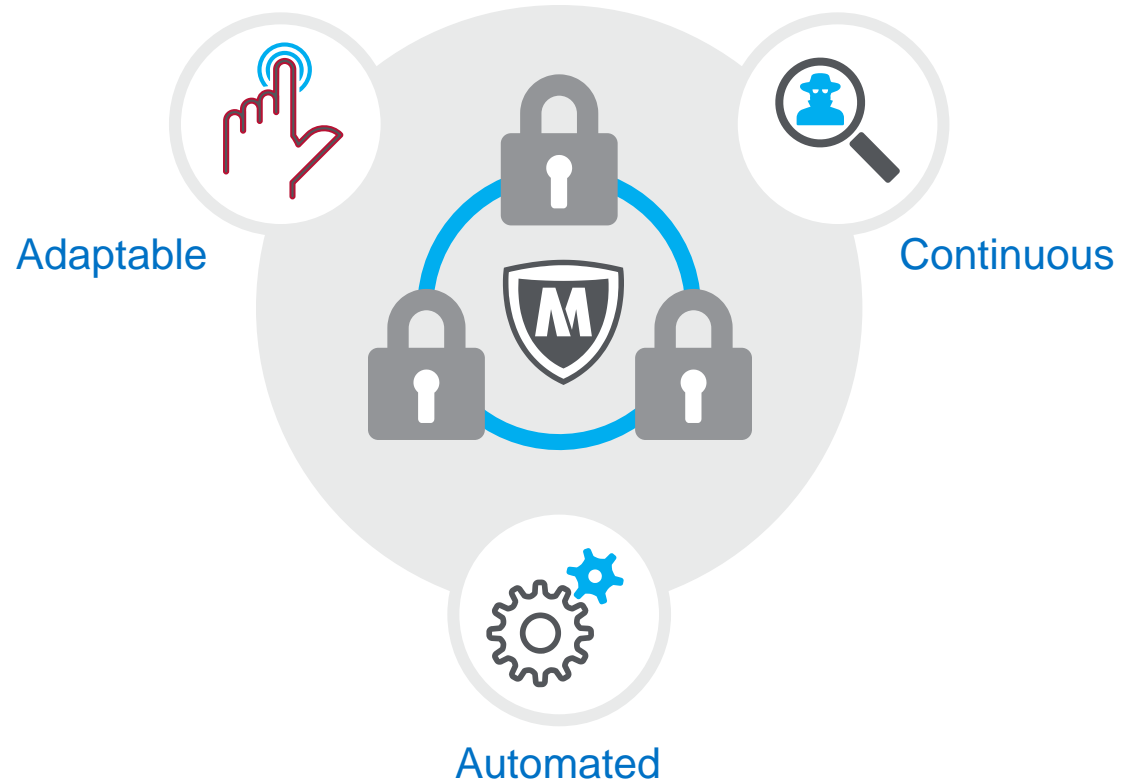
Monitorování síťové aktivity



McAfee Active Response

Shrnutí

- Hlubkové 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

TM

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 vyvíjí ...

- SIEM Content Awareness (Next Generation SIEM)

- Systém, který je schopen analyzovat události ze všech vrstev až k aplikačním datům



Škálovatelná architektura

Intelligence 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



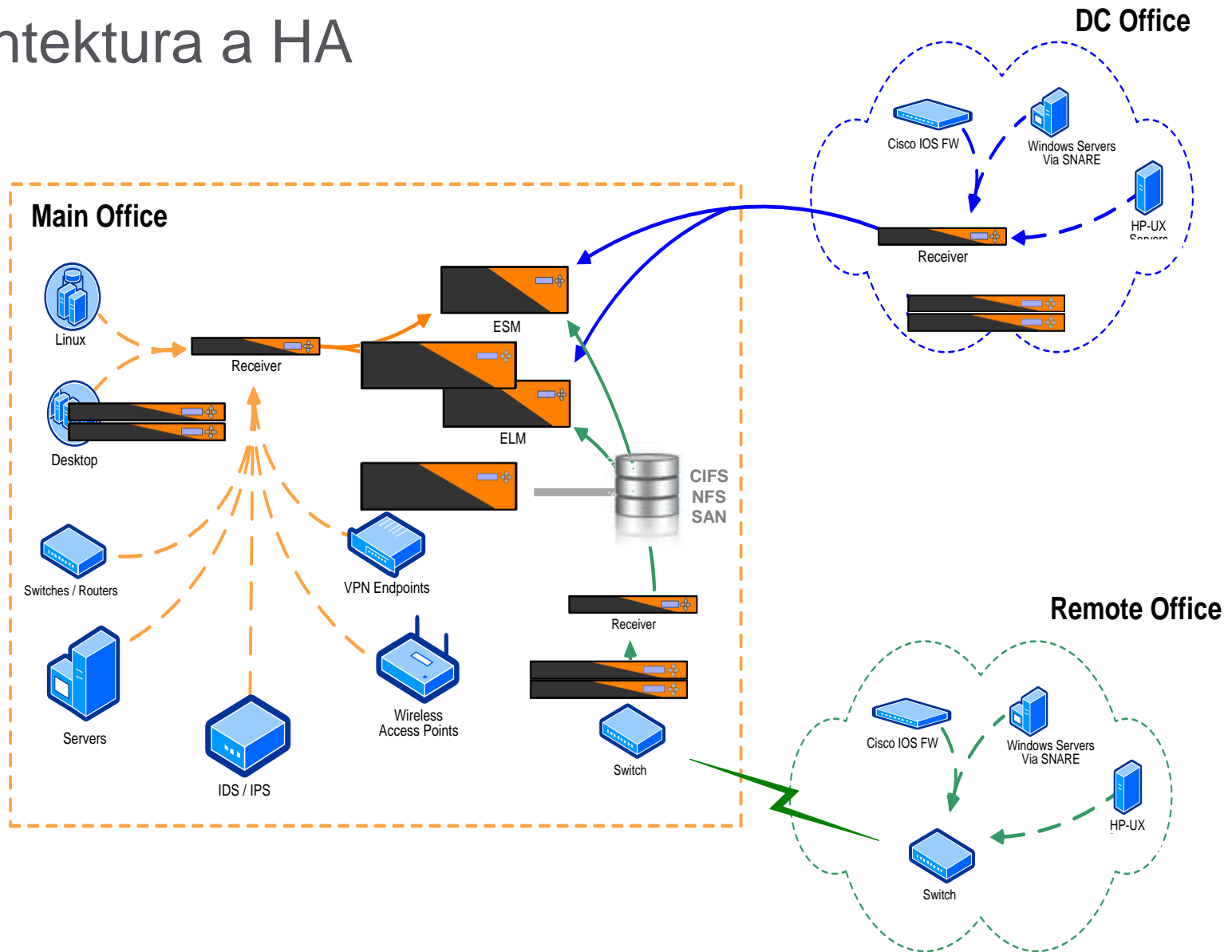
Sběr logů &
Distribuovaná korelace logů

McAfee Receivers



Big
Security
Data DB

SIEM architektura – distribuovaná architektura a HA



McAfee Enterprise Security Manager



Physical Display

Type here to search for a device

- Physical Display
 - Local ESM
 - (Local ESM)
 - Advanced Correlation Engine (Historical)
 - Advanced Correlation Engine (Real-Time)
 - 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
- Traffic to Suspicious Geo
- Virus detected
- Virus detected
- Traffic to Suspicious Geo
- Traffic to Suspicious Geo
- Traffic to Suspicious Geo
- Traffic to Suspicious Geo
- Virus detected
- Virus detected
- Virus detected
- Virus detected

0 15 0

Local ESM

Default Summary EBC

Current Day

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

Total Flow Collection Rate Per Second

Rate: -None-

Total Collection Rate Per Second

Rate: -None-

Event Distribution

2,118,041 (100%)

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

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

Events

Bound to: Event Distribution

Severity	Rule Message	Ever
161775	McAfee_FW_Ent Server traffic - enc	215
18000	McAfee_FW_Ent Monitor informati	720

Filters

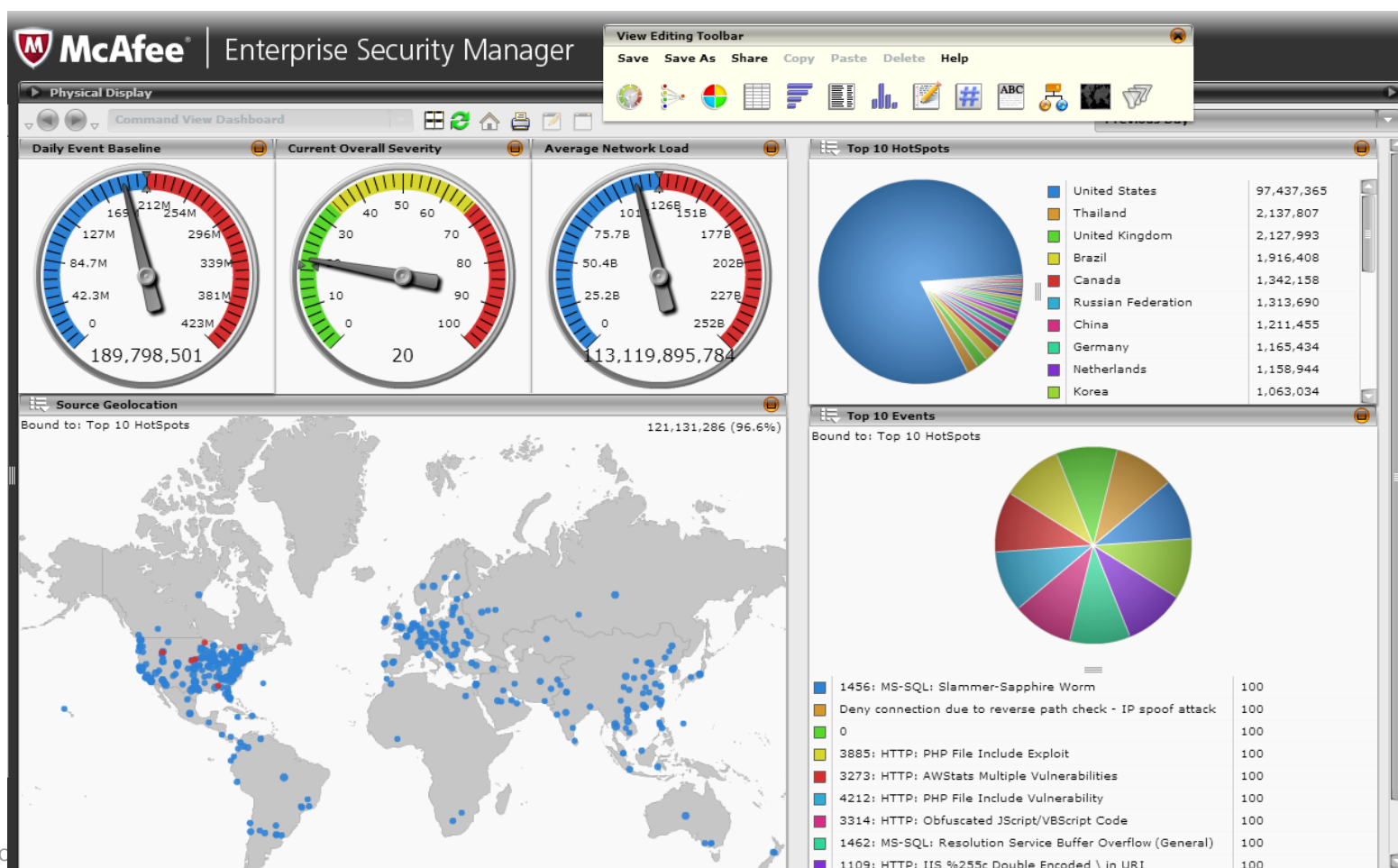
Hints

- 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



ESM

ELM

Normalizované, parsované a agregované logy jsou indexovány a uloženy do centrálního úložiště ESM

Raw logy jsou hashovány a uloženy do ELM úložiště

Události

Raw logy

Reporting

Více jak 100 přednastavených reportů
Výkonný, grafický reportovací editor

The screenshot displays the McAfee Report Layout editor interface. The main window shows a report design with a header containing the McAfee logo and report metadata. The body of the report is divided into sections for 'Summary' and 'Distribution'. A 'Bar Chart Properties' panel is visible on the right, showing settings for the 'Summary' chart, including font (sans, size 8) and query options. Below the editor, the rendered report is shown, featuring a horizontal bar chart for the 'Summary' section and a vertical bar chart for the 'Distribution' section.

Report Metadata:

- Device: Cisco ASA
- Report Generated: Apr 2, 2013 6:00 AM
- Time Zone: Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London OMT+00:00
- Report Period: 2013/04/01 00:00:00 to 2013/04/02 00:00:00
- Device Count: 72

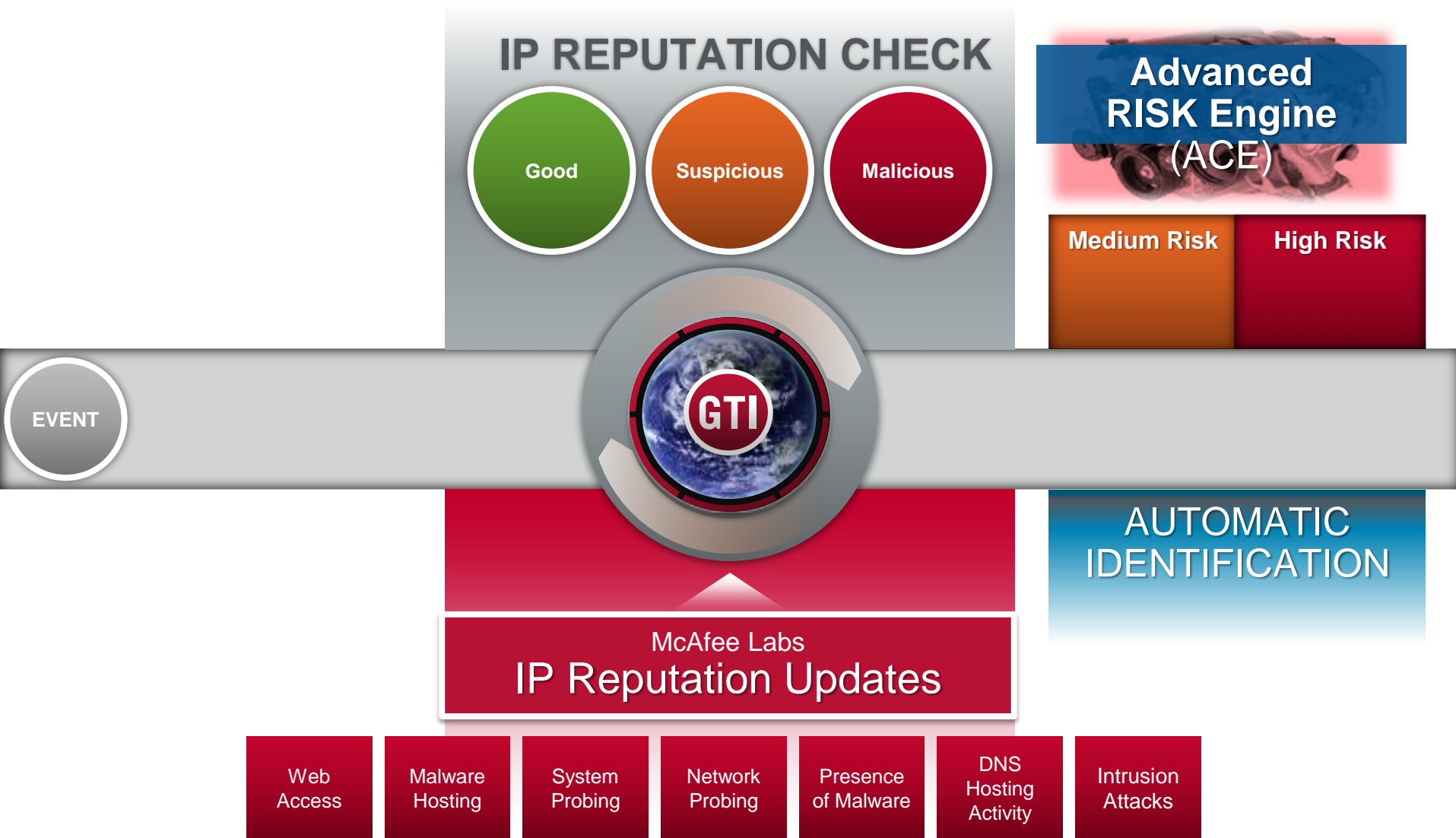
Summary Chart Data:

Category	Count
Teardown local-host	2,028
Built local-host	2,011
TCP/UDP access...	1,366
Teardown ICMP c...	868
Built ICMP con...	862
Teardown UDP co...	611
Built inbound/o...	608
Teardown TCP co...	538
Built inbound/o...	533
Teardown dynami...	255
Built dynamic/s...	255
Inbound UDP con...	228
No translation ...	214
Deny IP spoof	114
Denied TCP pack...	73
IP packet denie...	52
Invalid destina...	5
User Accessed URL	5
Inbound TCP con...	2

Distribution Chart Data:

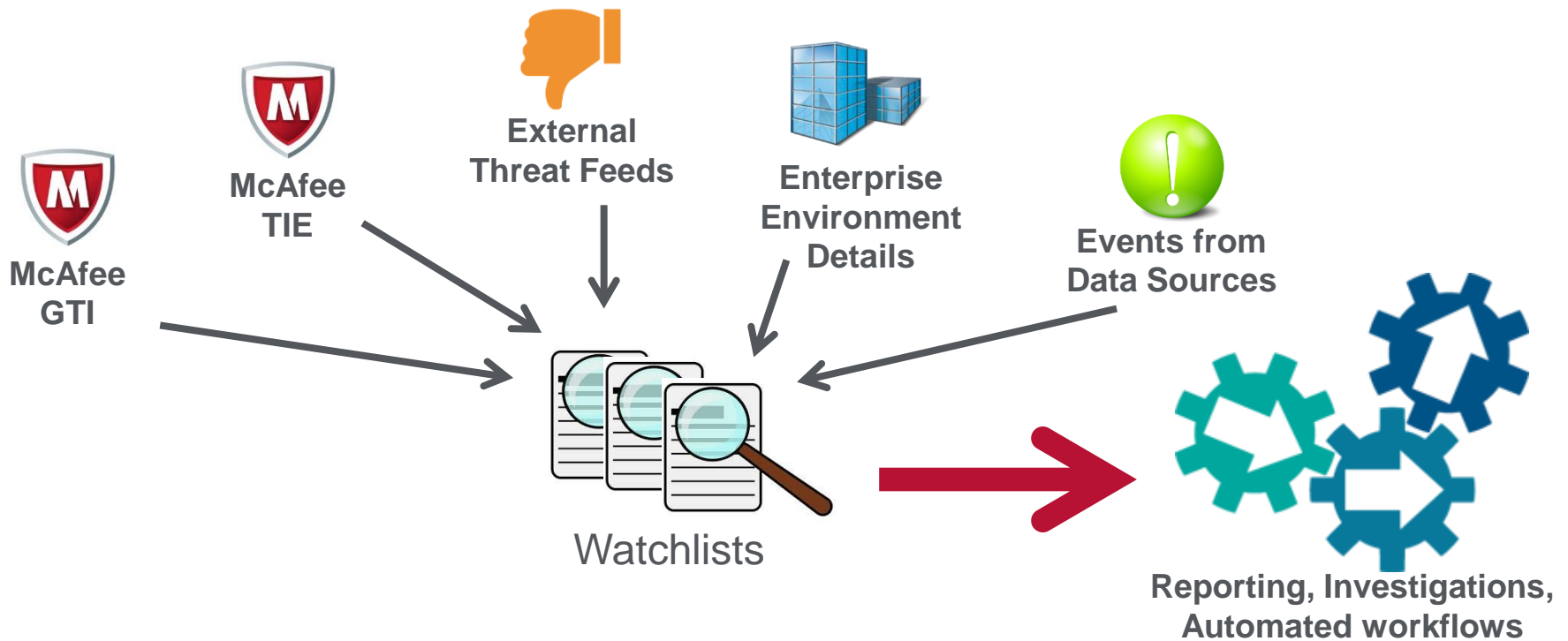
Time	Count
00:00:00	250
03:20:00	240
06:40:00	250
10:00:00	260
13:20:00	280
22:05:00	140

Global Threat Intelligence (GTI)



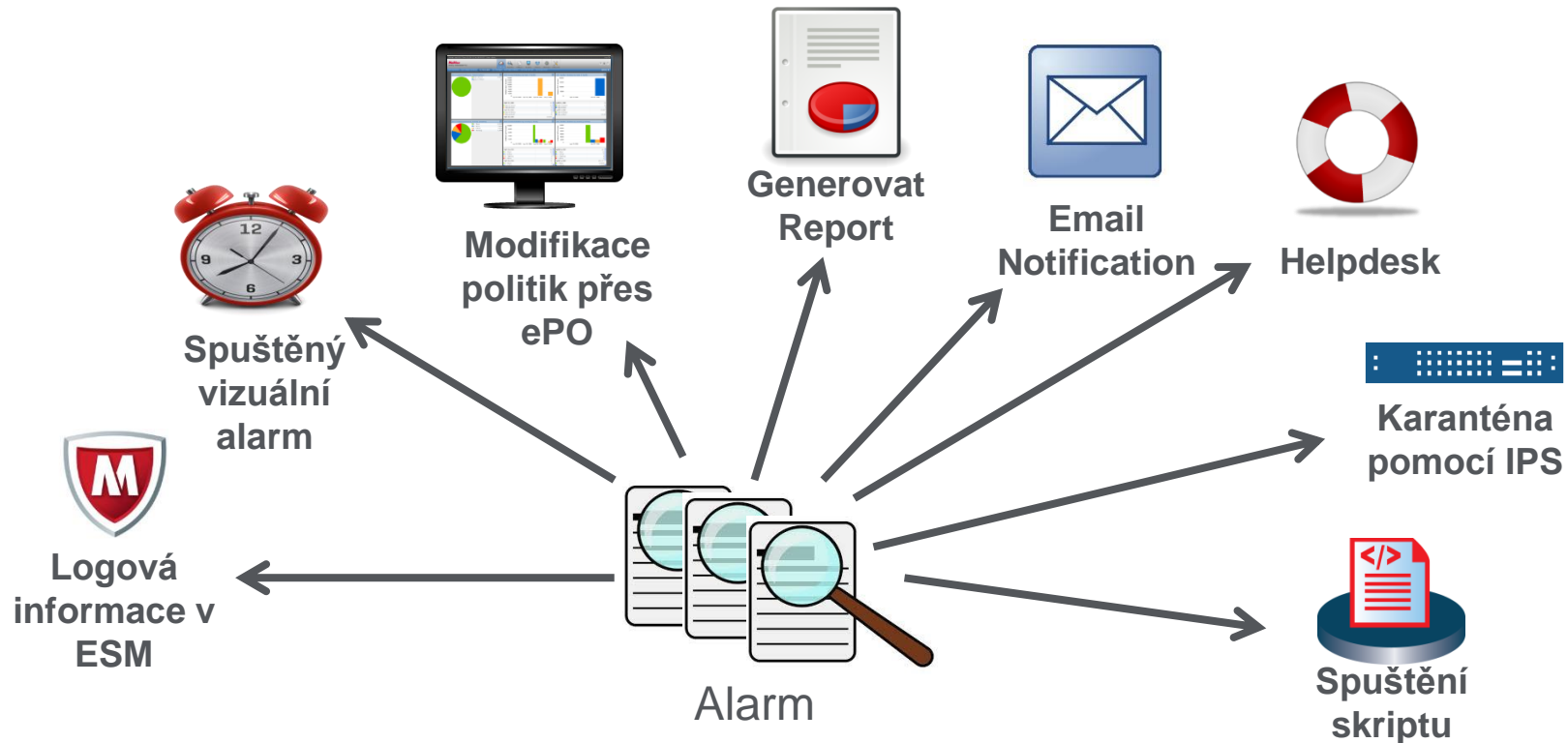
Watchlists

- Watchlists umožňuje filtrovat události, které se následně 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

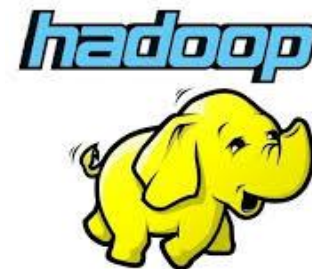
```
Mar 20 08:44:35 pcx02 sshd[263]: Accepted password for root from 216.101.197.234 port 56946 ssh2
```



Databases

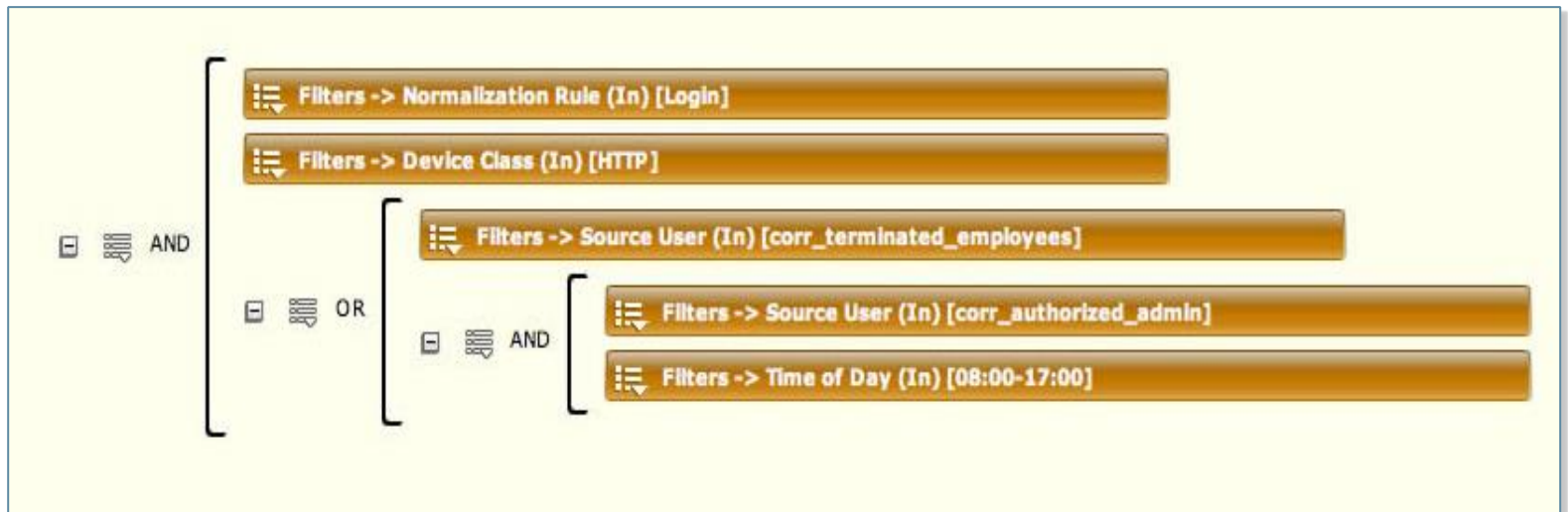


File Import

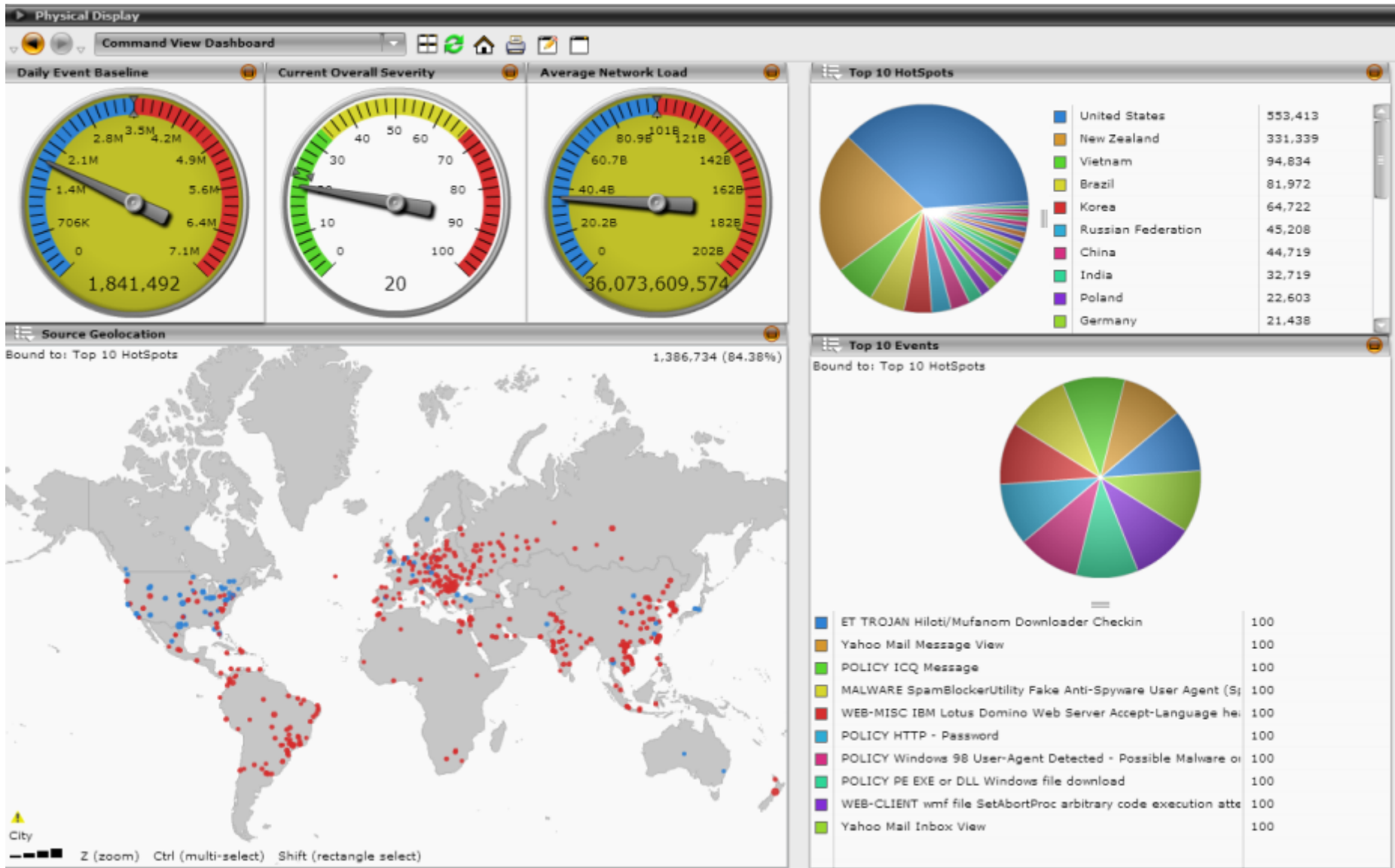


Correlation

- 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.

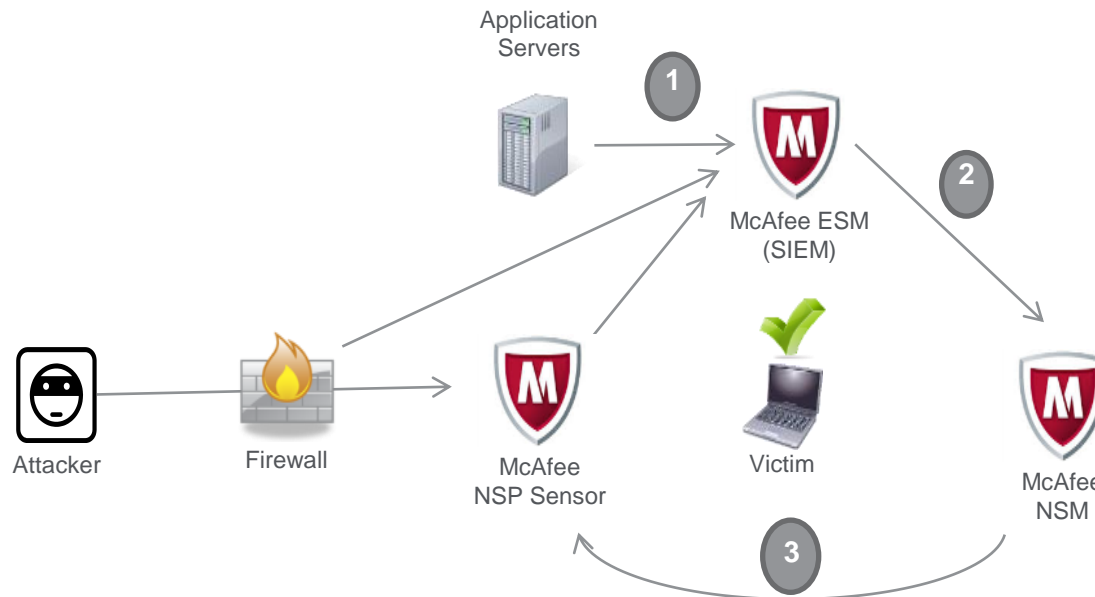


Geo-location Indicators



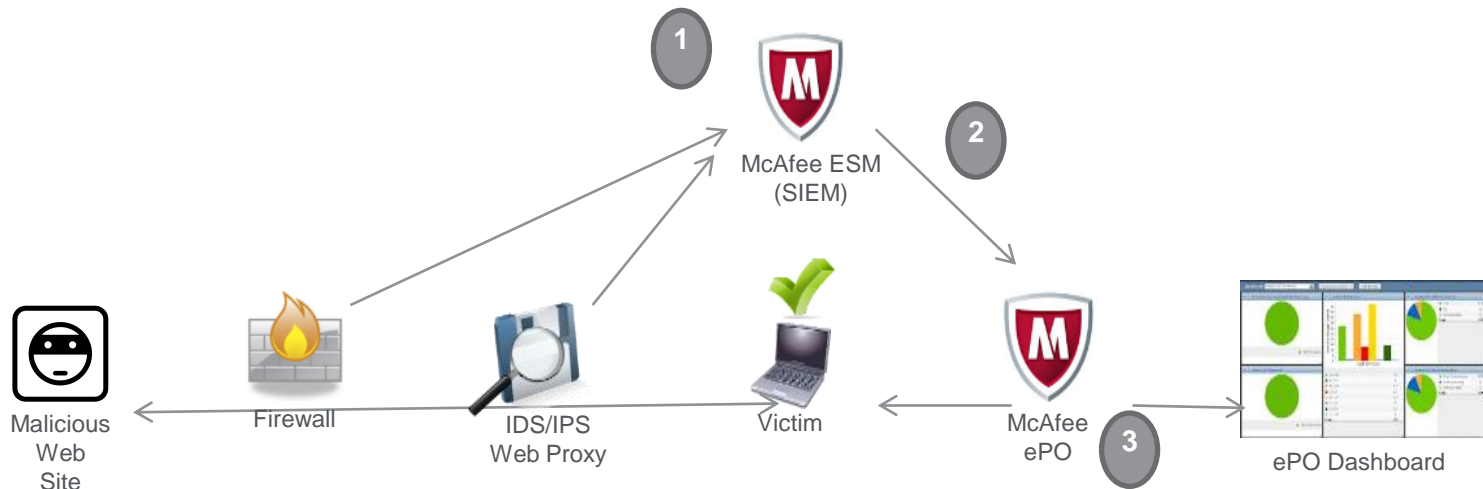
Orchestrace: McAfee Network Security Platform

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.



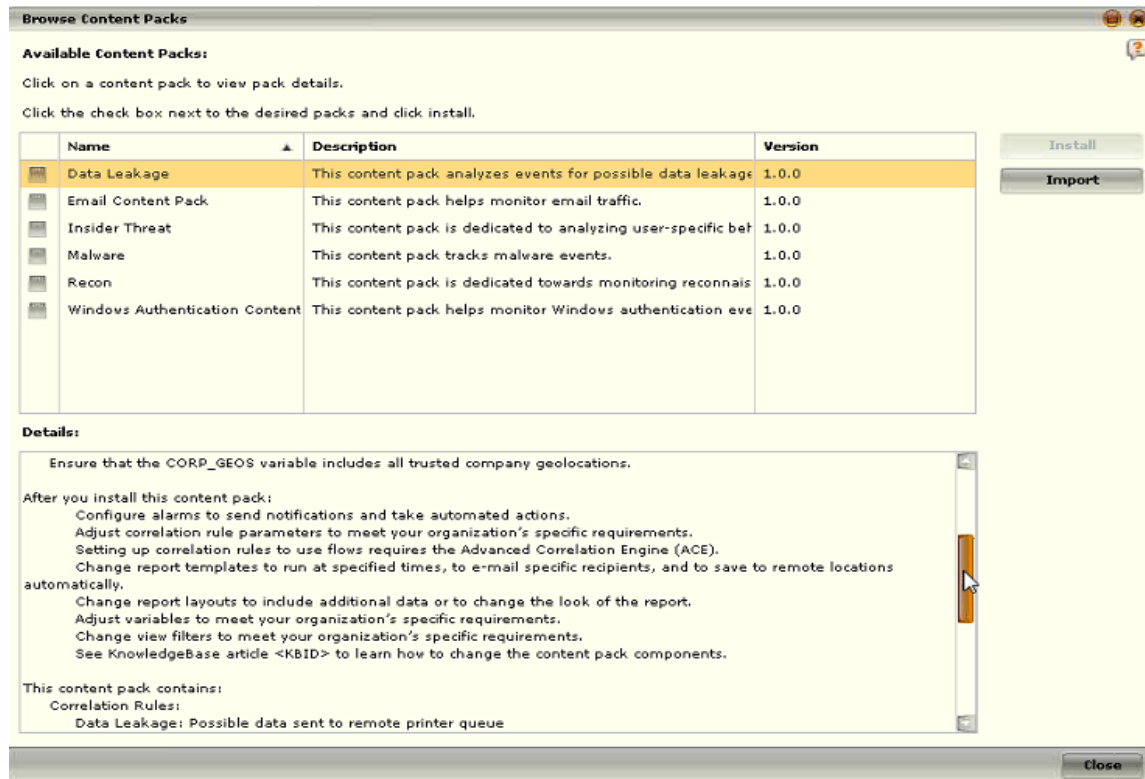
Content packs

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



Browse Content Packs

Available Content Packs:

Click on a content pack to view pack details.

Click the check box next to the desired packs and click install.

Name	Description	Version
<input checked="" type="checkbox"/> Data Leakage	This content pack analyzes events for possible data leakage	1.0.0
<input type="checkbox"/> Email Content Pack	This content pack helps monitor email traffic.	1.0.0
<input type="checkbox"/> Insider Threat	This content pack is dedicated to analyzing user-specific beh	1.0.0
<input type="checkbox"/> Malware	This content pack tracks malware events.	1.0.0
<input type="checkbox"/> Recon	This content pack is dedicated towards monitoring reconnais	1.0.0
<input type="checkbox"/> Windows Authentication Content	This content pack helps monitor Windows authentication eve	1.0.0

Details:

Ensure that the CORP_GEOS variable includes all trusted company geolocations.

After you install this content pack:

- Configure alarms to send notifications and take automated actions.
- Adjust correlation rule parameters to meet your organization's specific requirements.
- Setting up correlation rules to use flows requires the Advanced Correlation Engine (ACE).
- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.
- Change report layouts to include additional data or to change the look of the report.
- Adjust variables to meet your organization's specific requirements.
- Change view filters to meet your organization's specific requirements.
- See KnowledgeBase article <KBID> to learn how to change the content pack components.

This content pack contains:

- Correlation Rules:
 - Data Leakage: Possible data sent to remote printer queue

Buttons: Install, Import, Close

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

Edit Watchlist

Main Source Parsing Values

Enter a name for the watchlist.

Name:

Static Dynamic

Enable automatic updates

Update:

Minute:

Cancel < Back Next > Finish

Edit Watchlist

Main Source Parsing Values

Select the type of values this watchlist will contain.

Type:

Values:

- 103.14.120.121
- 103.19.89.55
- 103.31.186.207
- 103.31.186.29
- 103.4.16.91
- 103.4.218.22
- 103.8.127.189
- 103.8.127.205
- 104.152.215.90
- 104.28.14.104
- 104.28.15.104
- 106.10.153.167
- 107.161.144.14
- 108.162.197.131
- 108.162.198.96
- 108.162.199.144
- 108.162.199.96

Clear Values Export Run Now

Cancel < Back Next > Finish

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

The screenshot displays the 'Cyber Threat Feed Wizard' interface, specifically the 'Backtrace' tab. The wizard is designed to perform a backtrace analysis on indicators from a feed. Key configuration options include:

- Time Frame:** Last 7 days
- Assignee:** NGCP
- Severity:** 50
- Analysis Options:** Events, Flows
- Action Options:** Log event (checked), Auto-acknowledge Alarm, Visual Alert, Create Case, Update Watchlist, Send Message, Generate Reports, Execute remote command, Send to Remedy, Assign Tag with ePO, Blacklist, Custom alarm summary.

The background window shows a list of indicators with a 'Source Events' tab highlighted by a red arrow. The bottom of the wizard features 'Cancel', '< Back', and 'Finish' buttons.

Adaptive Threat Prevention and Detection

Integrace se SEIM

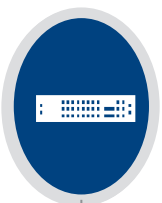
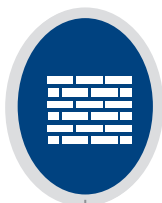
Network & Gateway

NGFW

NSP

Web Gateway

Email Gateway



Informace o detekci malware je odeslána na síťové prvky a koncové systémy

Sandbox

ATD



IOC 1
IOC 2
IOC 3
IOC 4

Soubor je analyzován

SIEM

ESM



Nová IOC inteligence provede historické vyhledávání

DXL Ecosystem

DXL Ecosystem

Endpoints



Již napadené systémy jsou izolovány nebo vyčištěny

TIE Endpoint Module

TIE Endpoint Module

TIE Endpoint Module

TIE Endpoint Module



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