

Systemová ochrana McAfee

středa, 5. května 2010



ePolicy Orchestrator: Investice do bezpečnosti pro dnešek i zítřek



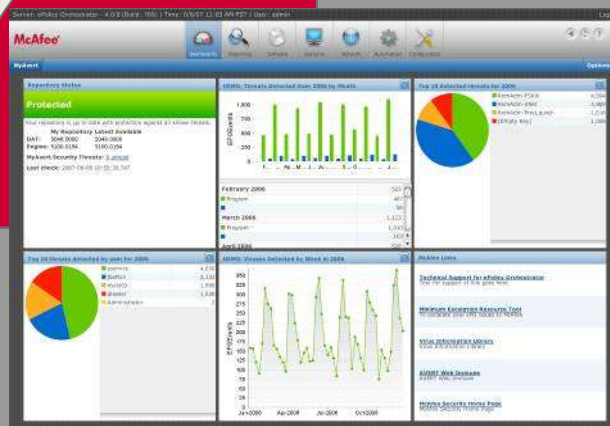
Total Protection for Endpoint

- AV/Anti-spyware
- Host IPS
- Desktop firewall
- Web security
- Network access control
- Policy auditing

IT Governance, Risk and Compliance

- Vulnerability scanning
- Remediation
- Policy auditing

Single Agent



Integrated Management

Total Protection for Data

- Endpoint encryption
- Device control
- Data loss prevention

Total Protection for Network

- Network IPS
- Content Security Blade

ePolicy Orchestrator: Investice do bezpečnosti pro dnešek i zítřek



Total Protection for Endpoint

- AV/Anti-spyware
- Host IPS
- Desktop firewall
- Web security
- Network access control
- Policy auditing

IT Governance, Risk and Compliance

- Vulnerability scanning
- Remediation
- Policy auditing

Single Agent



Integrated Management

Total Protection for Data

- Endpoint encryption
- Device control
- Data loss prevention

Total Protection for Network

- Network IPS
- Content Security Blade

ePolicy Orchestrator: Investice do bezpečnosti pro dnešek i zítřek



Total Protection for Endpoint

- AV/Anti-spyware
- Host IPS
- Desktop firewall
- Web security
- Network access control
- Policy auditing

IT Governance, Risk and Compliance

- Vulnerability scanning
- Remediation
- Policy auditing

Total Protection for Data

- Endpoint encryption
- Device control
- Data loss prevention

Total Protection for Network

- Network IPS
- Content Security Blade

Single Agent



Integrated Management

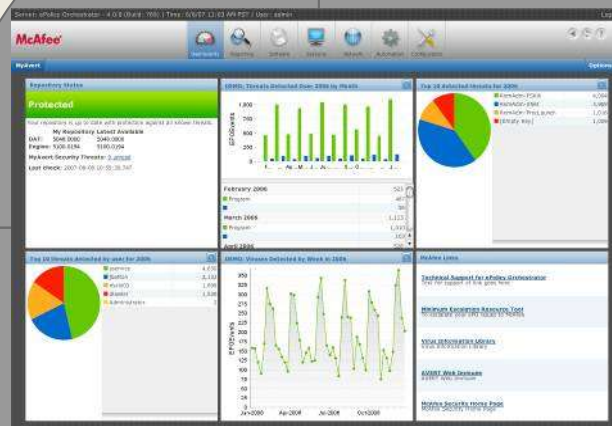
Total Protection for Endpoint

- AV/Anti-spyware
- Host IPS
- Desktop firewall
- Web security
- Network access control
- Policy auditing

IT Governance, Risk and Compliance

- Vulnerability scanning
- Remediation
- Policy auditing

Single Agent



Integrated Management

Total Protection for Data

- Endpoint encryption
- Device control
- Data loss prevention

Total Protection for Network

- Network IPS
- Content Security Blade

Vzájemné propojení se zabezpečeném koncového bodu (endpoint security)

McAfee

McAfee Total Protection

Endpoint

Antivirus

Anti-Spam/Anti-Spyware

Web Security

Host DLP

Endpoint Encryption

Desktop Firewall

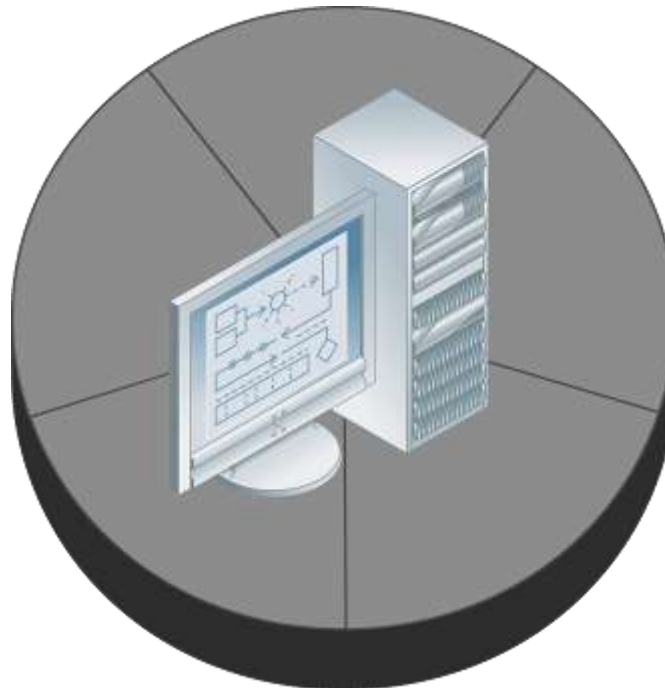
Host IPS

NAC

Device Control

Policy Auditing

McAfee Agent



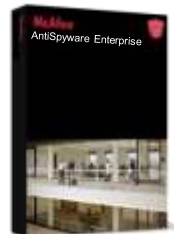
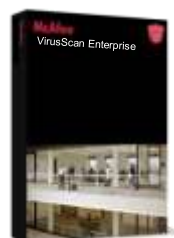
ePO



McAfee VirusScan® Enterprise

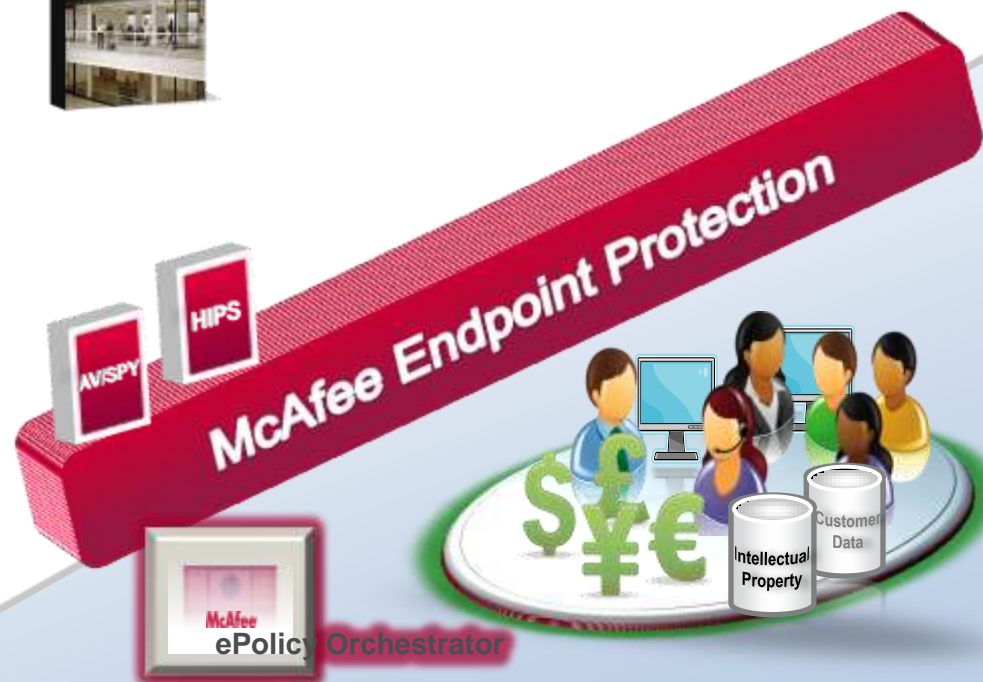
McAfee AntiSpyware® Enterprise

- Ochrana proti známému malware a hackerům
- Obrana proti exploitům, které využívají známě zranitelnosti
- Ochrana proti root-kitům, spyware, viruses, worms, key-loggerům a ostatnímu zlomyslnému kódu
- Největší instalace v oboru 5M+ koncových bodů



McAfee Host Intrusion Prevention for Desktop

- Chrání proti neznámému malwaru & zero-day zranitelnostem
- Eliminuje urgentnost záplatování a tím snižuje operační náklady na bezpečnost
- Umožňuje zero-day ochranu pro > 95% Microsoft zranitelností
- Důvěra a instalace US Department of Defense



McAfee Network Access Control

- Slouží k bezpečnému/ ve shodě s přístupem uživatelů k podnikové síti (zaměstnanci, hosté, kontraktori atd.) stejně jako zařízení (tiskárny, IP telefony atd.)
- Umožňuje dynamický health-check stejně jako vynucení podrobné politiky & shody
- Umožňuje bezpečný přístup bez nutnosti upgrade síťové infrastruktury



McAfee Host Data Loss Prevention (McAfee Total Protection for Data)

- Chrání proti náhodnému/chtěnému úniku dat & neautorizovanému použití zařízení
- Odhaluje a klasifikuje důvěrné informace
- Monitoruje a vynucuje pohyb dat na základě podrobné uživatelské politiky



McAfee Endpoint Encryption (formerly SafeBoot encryption)

- Šifrování všech důvěrných dat s možností volby celého disku, virtuálního disku, souborů a složek nebo mobilních zařízení
- Kompletní ochrana dat v případě ztráty zařízení v souladu s regulatorními předpisy
- Centrální politika a správa šifrovacích klíčů v heterogenním podnikovém prostředí
- Využíváno každou šestou státní správou v celosvětovém měřítku



McAfee Email Security

- Automatizované filtrování malwaru
- Policy-based ochrana příloh
- Výkonné anti spamové filtrování



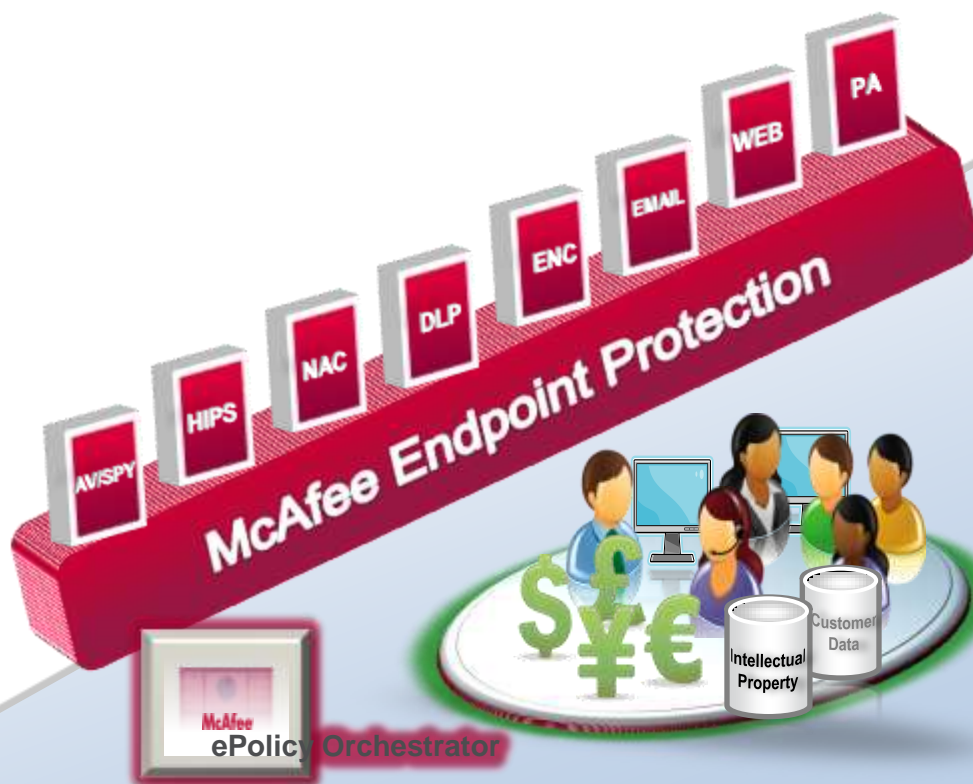
McAfee SiteAdvisor

- Varuje a chrání uživatele před návštěvou nebezpečných infikovaných web stránek např. vyvolaných spywarem
- Více jak 97% celosvětově nejvíce navštěvovaných stránek je analyzováno a katalogizováno
- Zajistí bezpečné surfování, vyhledávání a nakupování na webu



McAfee Policy Auditor

- Zjednodušuje správu
- Zajišťuje jistotu při externích auditech
- Trvalé potvrzení/vykazování shody
- Automatizace manuálních auditů
- Vynucení shody



ePolicy Orchestrator

McAfee

středa, 5. května 2010



Co je McAfee ePolicy Orchestrator



- Centrální management server pro McAfee produkty
- ePO odpovídá na 3 klíčové otázky
 - Jsem zabezpečený?
 - Jsem ve shodě?
 - Existuje nějaké riziko?
- ePO klíčové vlastnosti
 - Instaluje, spravuje a udržuje bezpečnostní produkty
 - Centrální konfigurace a vynucení systémové bezpečnostní politiky
 - Reporty o shodě a zaznamenaných událostech

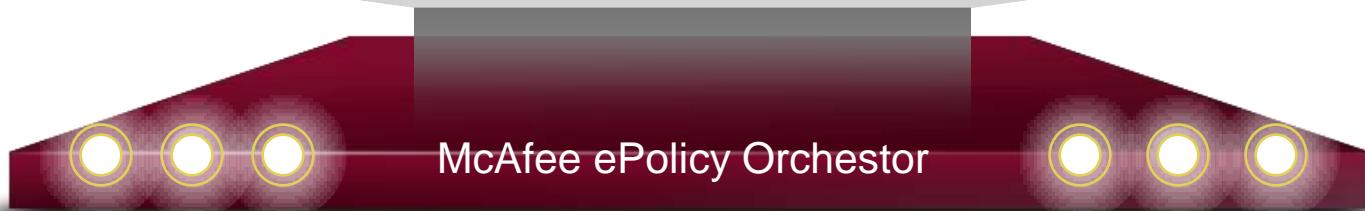


McAfee ePolicy Orchestrator

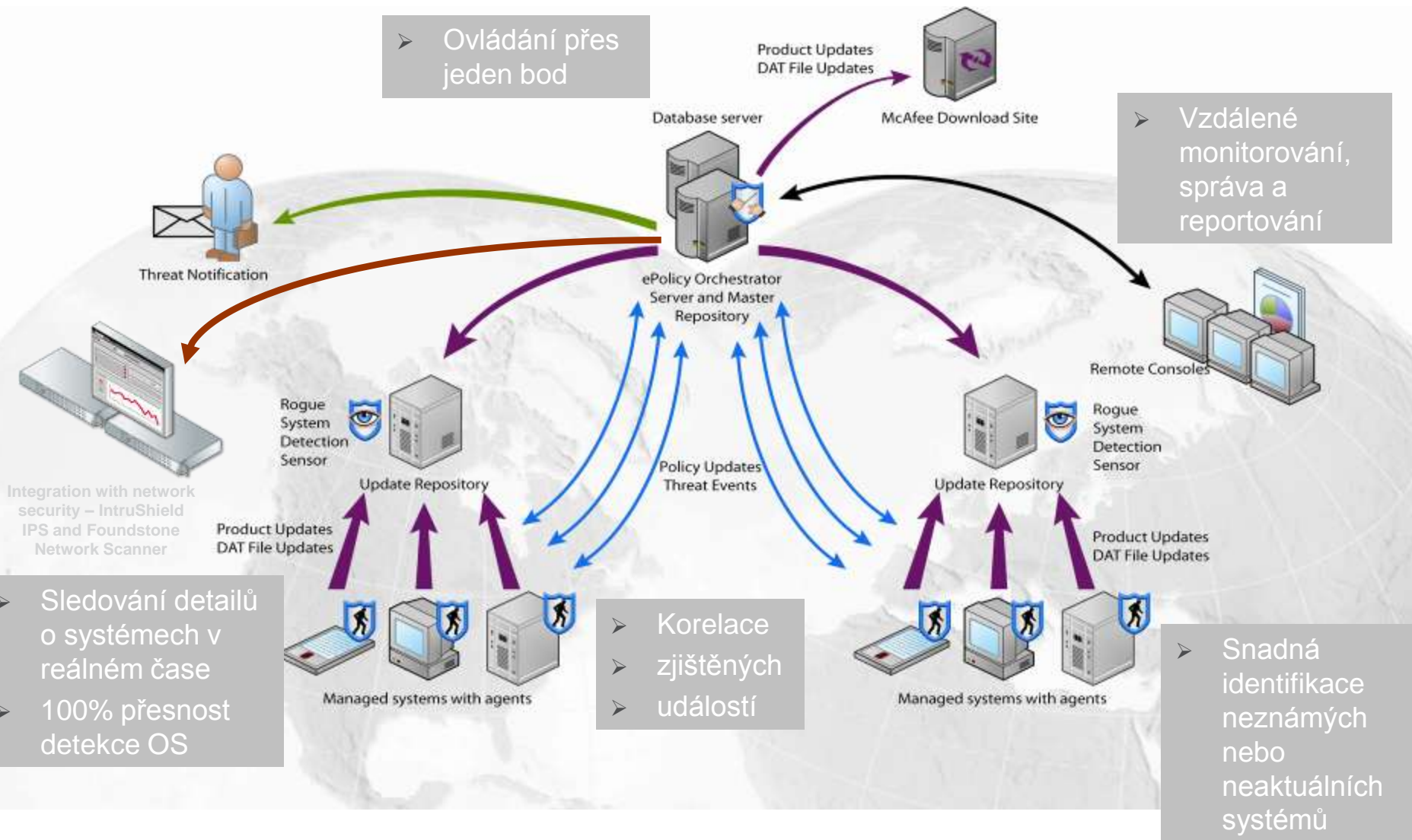
Nejdůležitější vlastnosti

McAfee®

- **Viditelnost až na koncový bod**
 - Jednotný pohled na systémy napříč celou sítí
- **Uživatelsky nastavitelné rozhraní**
 - Uživatelsky nastavitelné rozhraní pro více administrátorů
- **Dynamický dashboard a reporty**
 - Pohled na stav v reálném čase s možností automatických nebo manuálních akcí
- **Definice přístupových práv pro správu**
- **Rogue System Detection**
 - Detekuje a identifikuje zařízení na síti s možností notifikace nebo následné akce
- **Automatizace správy**
 - Automatizované úlohy na základě detekovaných událostí
- **Robustní architektura pro velké i malé podniky**
 - Robustní architektura pro správu více jak 150 tis. systémů, podpora HA
- **Detailní informace**
 - Sbírá detailní informace o jednotlivých systémech na síti, událostech, možnost optimalizace dle těchto parametrů



Centralizovaná správa bezpečnosti



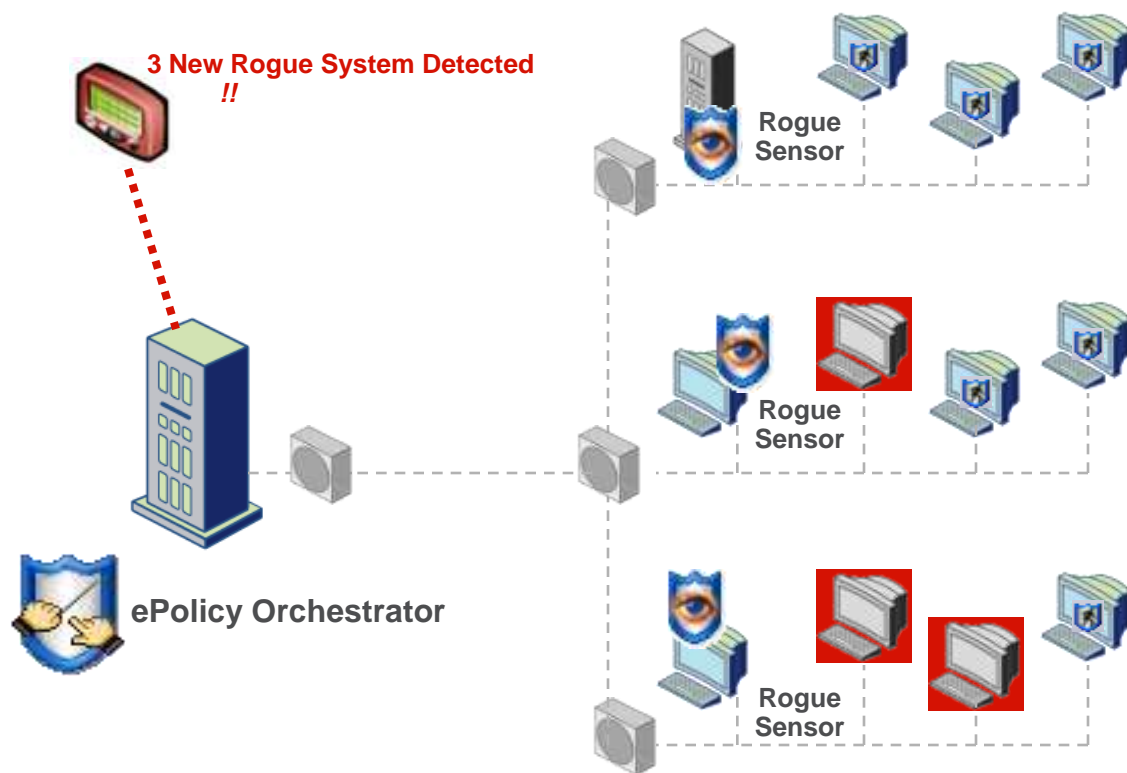
Dramaticky zvyšuje rychlost odezvy

- Dashboards poskytuje srozumitelný a rychlý pohled na stav bezpečnosti ve společnosti
 - Dashboardy zobrazují komplexní informace o bezpečnosti v reálném čase
 - Korelační inteligence poskytuje informace o riziku
 - Dynamické prokliknutí na detaily
 - Možnost sdílení s více administrátory
- Akce na základě zobrazené informace
 - Možnost spuštění úloh a reportů přímo z dashboardu (např. update now úloha)
 - Možnost okamžité reakce na události z přednastavených prahových hodnot
- Generování reportů na vyžádání, plánování reportů, při detekované události
 - Plánovač automatizovaných reportů a export do různých formátů - email html, xml, csv, nebo pdf



Rogue System Detection

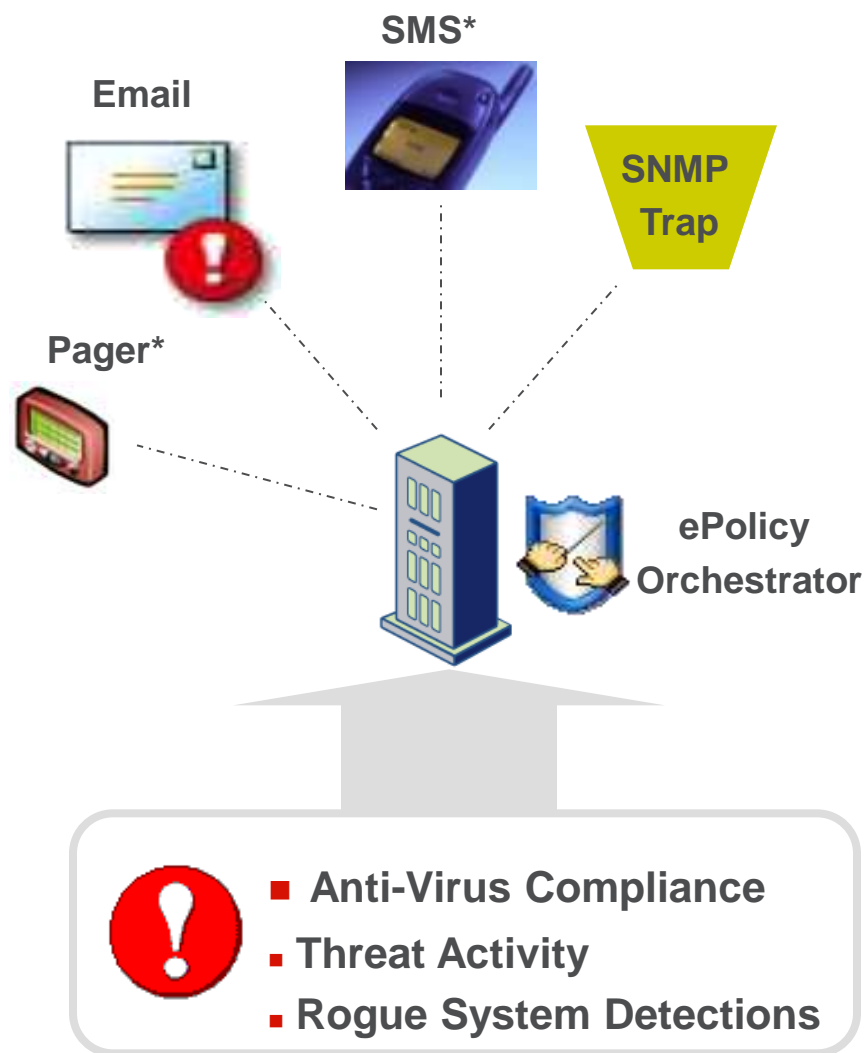
Detekuje zařízení připojené do sítě – PC, routery, tiskárny, Access pointy.....



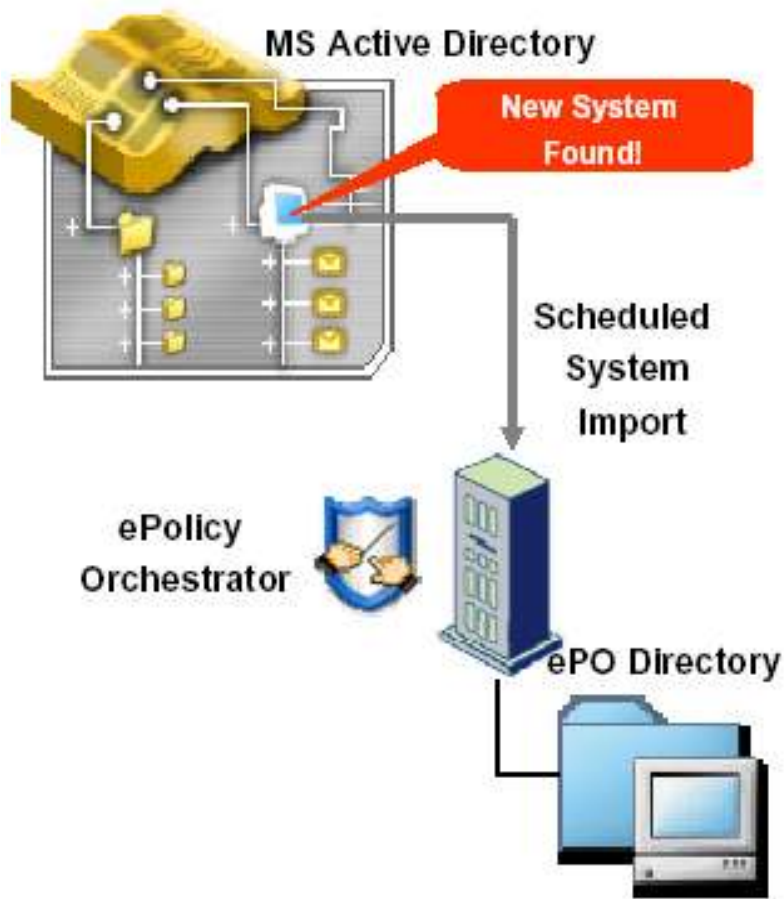
- Umisťuje jeden sensor na subnet
- Sensors pasivně poslouchá na síti broadcasty (Layer2: ARP, DHCP)
- Sensor upozorňuje ePO server na nové systémy pracující na síti
- ePO server zjišťuje, zda se jedná o známý nebo neznámý systém porovnáním s ePO databází.
- ePO posílá alert nebo automaticky instaluje patřičnou ochranu.

Shoda & notifikace o událostech

McAfee



- Proaktivní informace
 - Shoda antivirové politiky
 - Aktivita hrozeb
 - Sledování spamu a filtrovaných událostí
 - Rogue systém
- Více forem notifikace
 - Email, SMS, Text Pager
 - Integrace do vyšších managementů přes SNMP

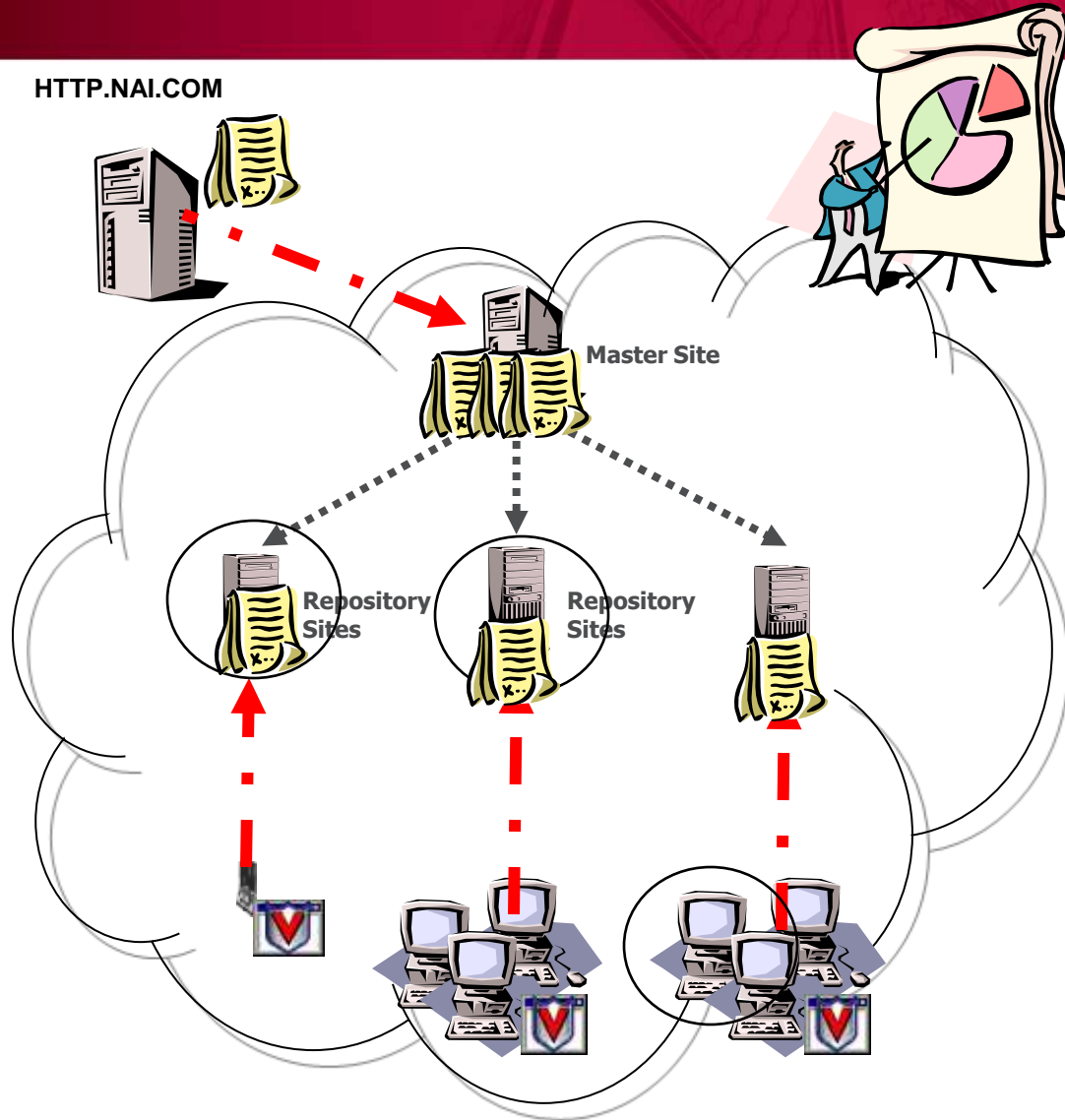


- Plánovaná synchronizace informací z Active Directory
- Možnost definovat více úloh pro více kontejnerů
- Automatické odmazávání počítačů z ePO struktury po odstranění z AD
- Automatické sortování synchronizovaných počítačů z AD do skupin ePO serveru

Globální aktualizace

McAfee®

HTTP.NAI.COM



- Kontrola DAT v Master repository
- Ruční nebo plánované úlohy pro aktualizaci
- Instalace do Repository
- Poslání Superagent Wake-up
- Superagents kontaktuje ostatní agenty a pošle Catalog
- Klient stáhne nový DAT a spustí instalaci
- Klient reportuje na ePO o provedené akci

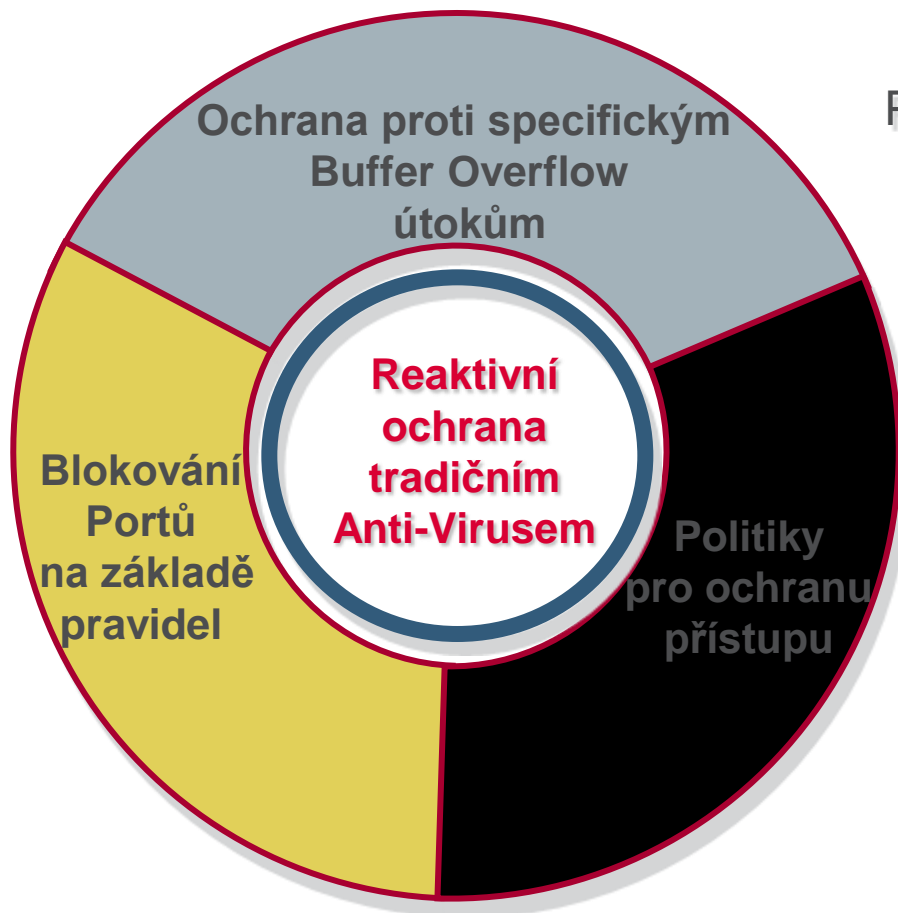
VirusScan Enterprise & Anti-Spyware

McAfee

středa, 5. května 2010



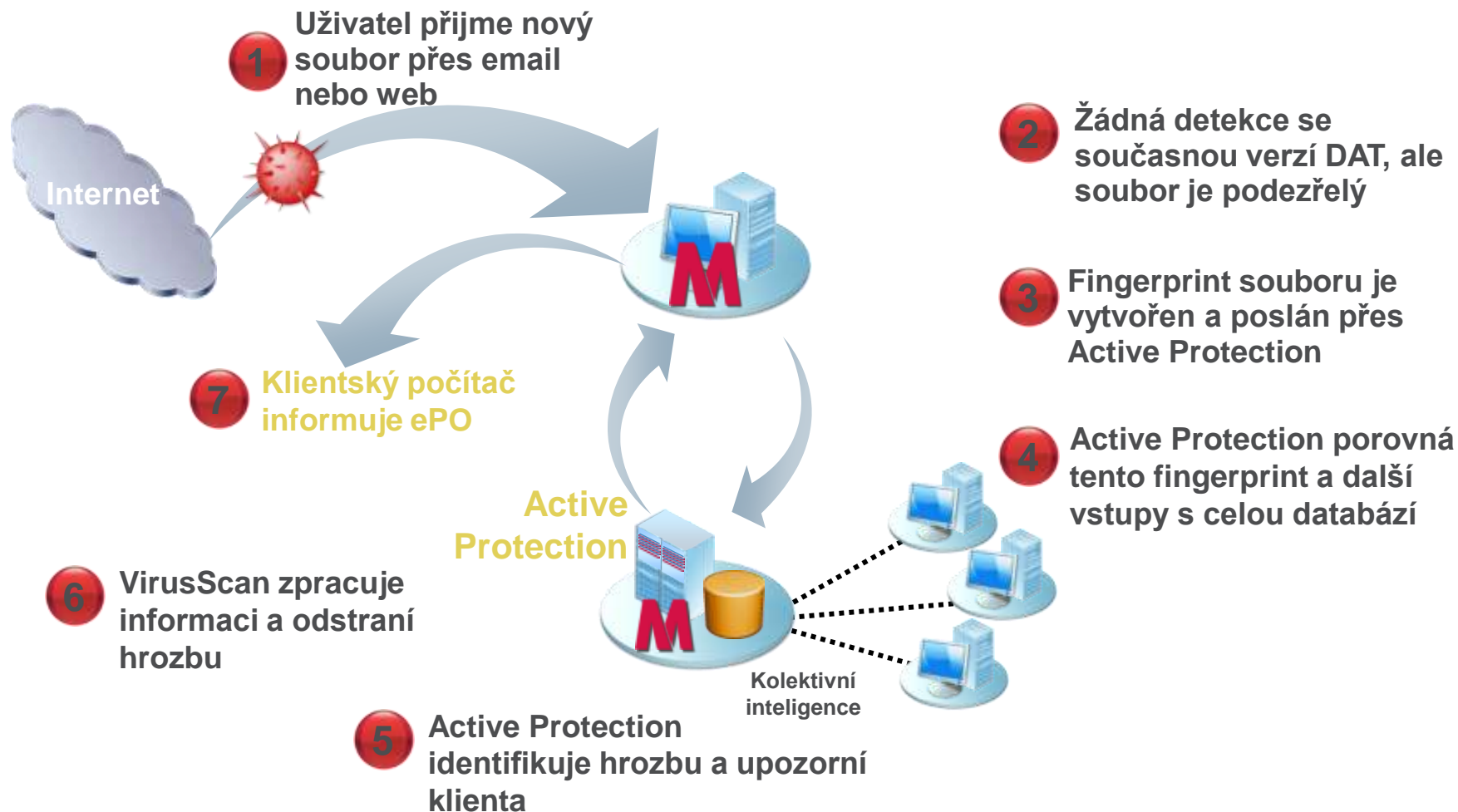
Proaktivní ochrana proti hrozbám *bez aktualizace*



Poskytuje ochranu proti „Zero Day“ útokům!

Proaktivní ochrana s VirusScan Enterprise 8.7i

McAfee Active Protection – Artemis technologie



McAfee Site Advisor Enterprise



středa, 5. května 2010





Features	Benefits
Snadná detekce bezpečných Web serverů	<ul style="list-style-type: none">• Proaktivní browser ochrana zajišťuje bezpečné prohlížení webových stránek s jednoduchou odezvou – zelená, žlutá nebo červené ikona informuje o nebezpečnosti navštívené stránky
Snadná instalace	<ul style="list-style-type: none">• Instalace pluginu do browseru vzdáleně z ePO serveru šetří čas zajišťuje ochranu na všech koncových bodech ve společnosti
Rozsáhlá databáze testovaných Web serverů	<ul style="list-style-type: none">• Testováno více než 8.5 milionů webových serverů a stránek, což představuje více než 90% web provozu• Testuje zlomyslné kódy, stránky s PUP programy, excessive spam, webové linky a informuje o uživatelích a vlastnících

SiteAdvisor Enterprise Enables Safe Surfing

McAfee®



- Pokud prohledáváte pomocí Google, Yahoo! nebo MSN, SiteAdvisor's označuje každý nalezený odkaz



- Při prohledávání, ikona SiteAdvisoru změní barvu podle nebezpečnosti otevřené stránky



- Upozornění informuje uživatele o nebezpečnosti stránky



- Detailní popis výsledku detekce stránky přes jediné kliknutí

McAfee Host IPS

McAfee

středa, 5. května 2010



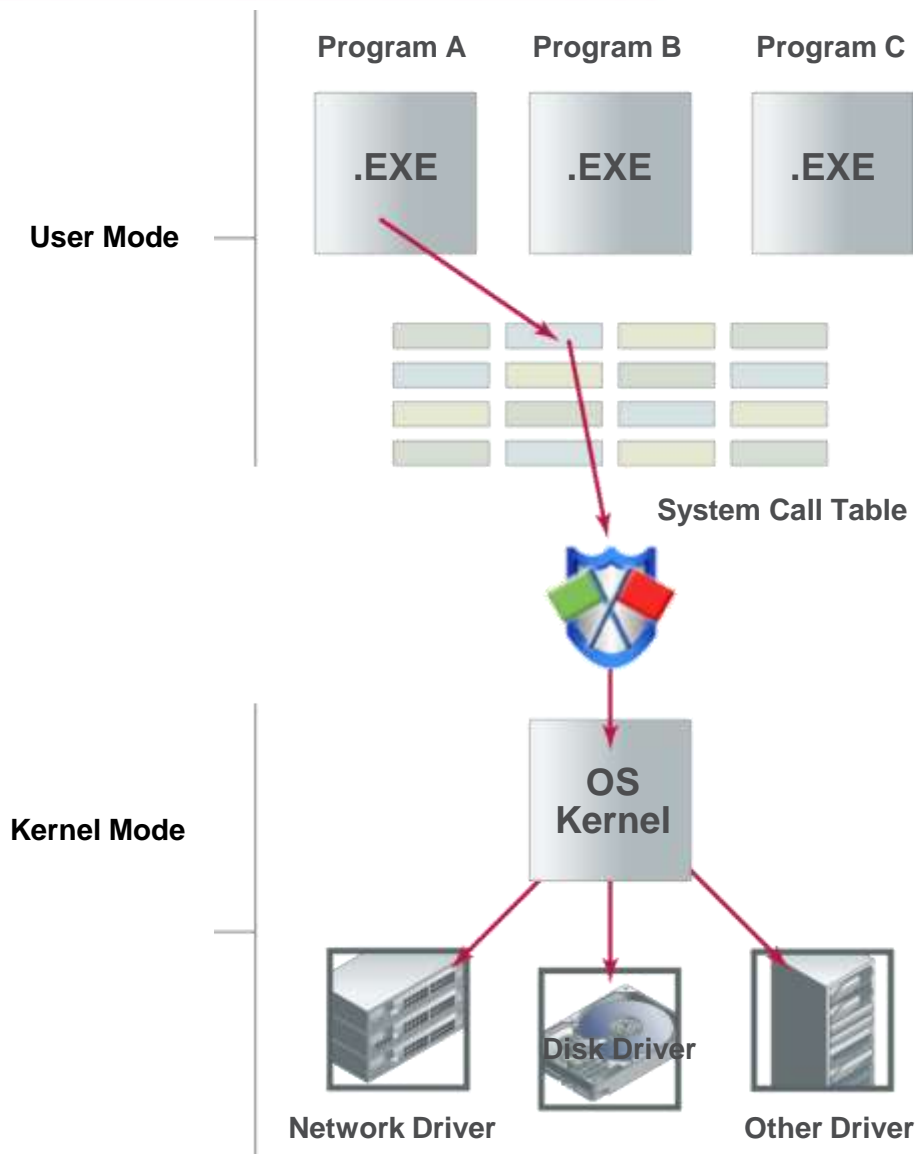
- **IPS s pravidly chování a signaturami**
 - Chrání systémy proti zero-day útokům a přesně detekuje známé hrozby
- **Integrovaný systémový firewall**
 - Další ochrana proti nechtěné komunikaci hrozeb, vynucuje bezpečnostní politiku pro příchozí i odchozí komunikaci
- **Aplikační kontrola**
 - Chrání aplikace před útoky nebo jejich zneužití k útoku
 - Definiuje, jaká aplikace smí být spuštěna
- **Centrální správa**
 - Snadná instalace/odinstalace, správa a reporting
 - Snižuje cenu za správu z jedné management konzole



Princip detekce – kontrola systémových volání

McAfee®

- McAfee Host IPS kontroluje systémová volání do jádra operačního systému
- Volání jsou kontrolována pravidelně aktualizovanými specifickými a generickými signaturami a pravidly chování
- Pokud je detekován útok, je spuštěna definovaná akce podle bezpečnostní politiky – záznam události do logu a zablokování útoku.
- Veškeré aktivity jsou v této fázi „viditelné“ a nešifrované. Je tedy možné přesně určit, zda se jedná o standardní aplikaci nebo o útok.



„Vulnerability Shielding“ – řešení problémů s aktualizací systémů

McAfee

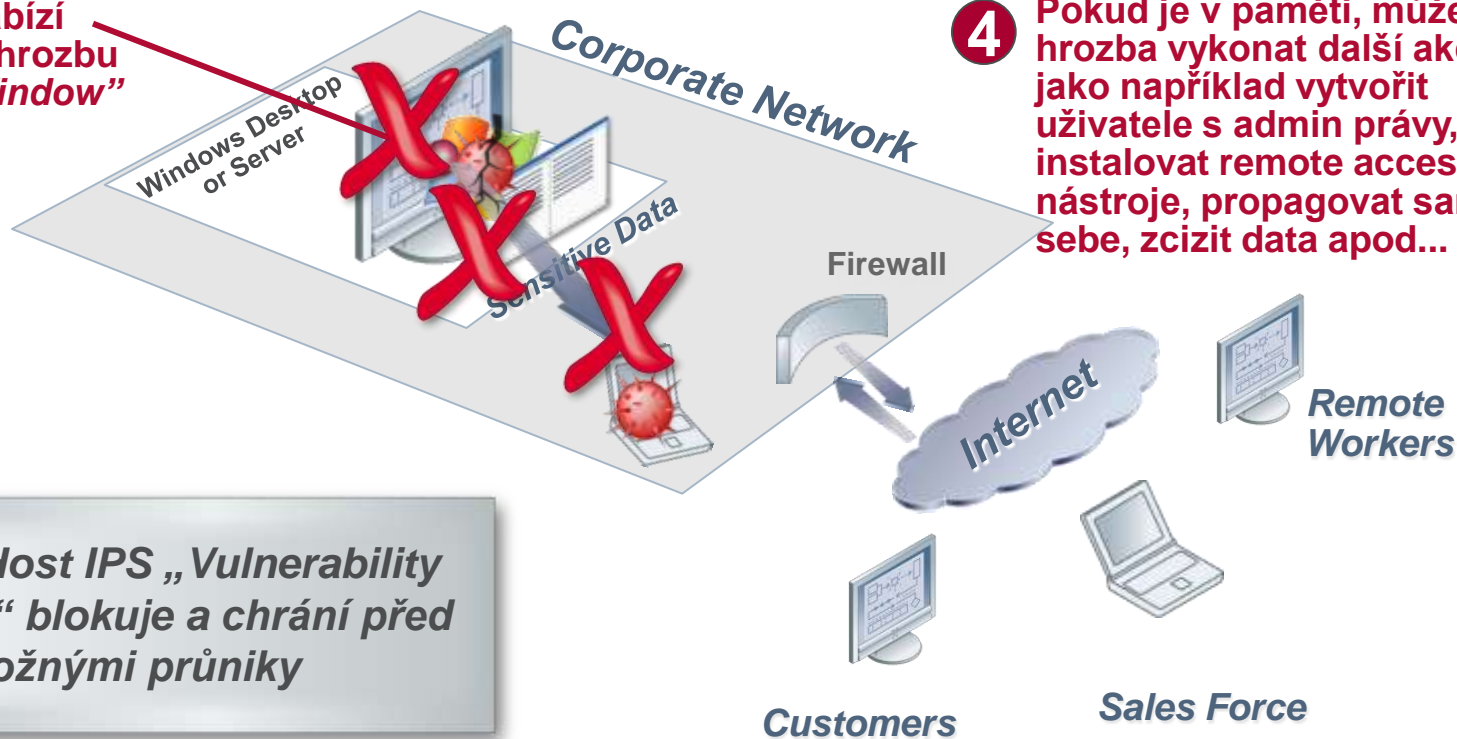
1 Hrozba je napsána tak, aby využila Windows zranitelnosti

2 Hrozba provede bufferoverflow

3 ...a zapisuje kód do paměti

4 Pokud je v paměti, může hrozba vykonat další akce jako například vytvořit uživatele s admin právy, instalovat remote access nástroje, propagovat sama sebe, zcizit data apod...

Existující Windows zranitelnost nabízí možnost vytvořit hrozbu „A Crack in the Window“



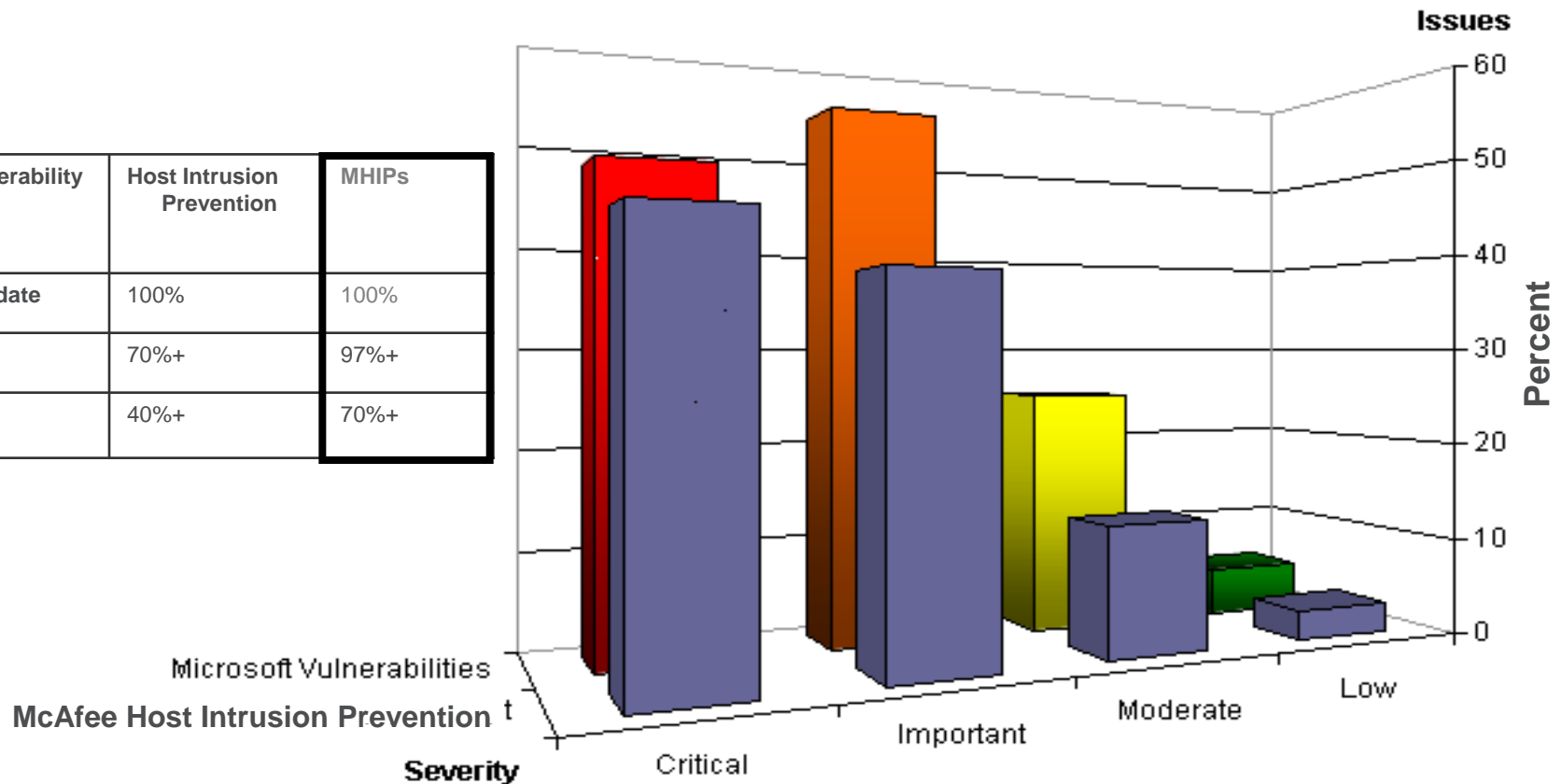
McAfee Host IPS „Vulnerability Shielding“ blokuje a chrání před možnými průniky

McAfee Host IPS w/ Vulnerability Shielding Coverage



**Projected Protection
(Both Signature and Zero Day Protection)**

Type of Vulnerability	Host Intrusion Prevention	MHIPs
Worm Candidate	100%	100%
Critical	70%+	97%+
Important	40%+	70%+



Děkuji za pozornost

McAfee

Jan Strnad
Sales Engineer for Czech Republic and Slovakia
jan_strnad@mcafee.com
+420 602 280 387

May 5, 2010

