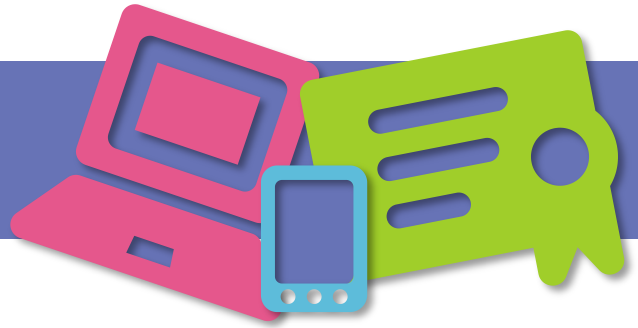
SECURITY 2014

22. ročník konference o bezpečnosti v ICT

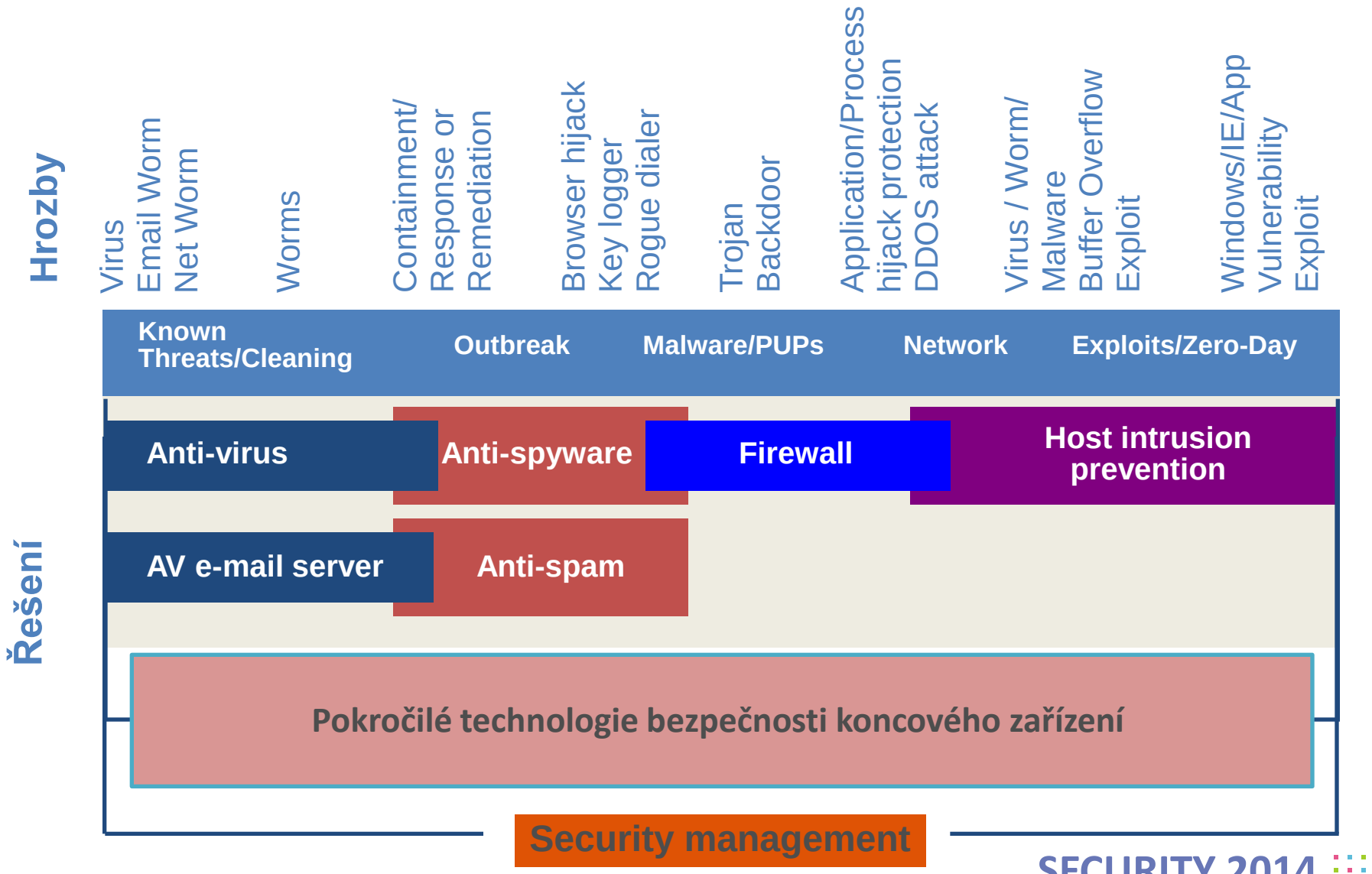


S vitamínem C nevystačíte, ale jeho nedostatek vás bude stát zdraví

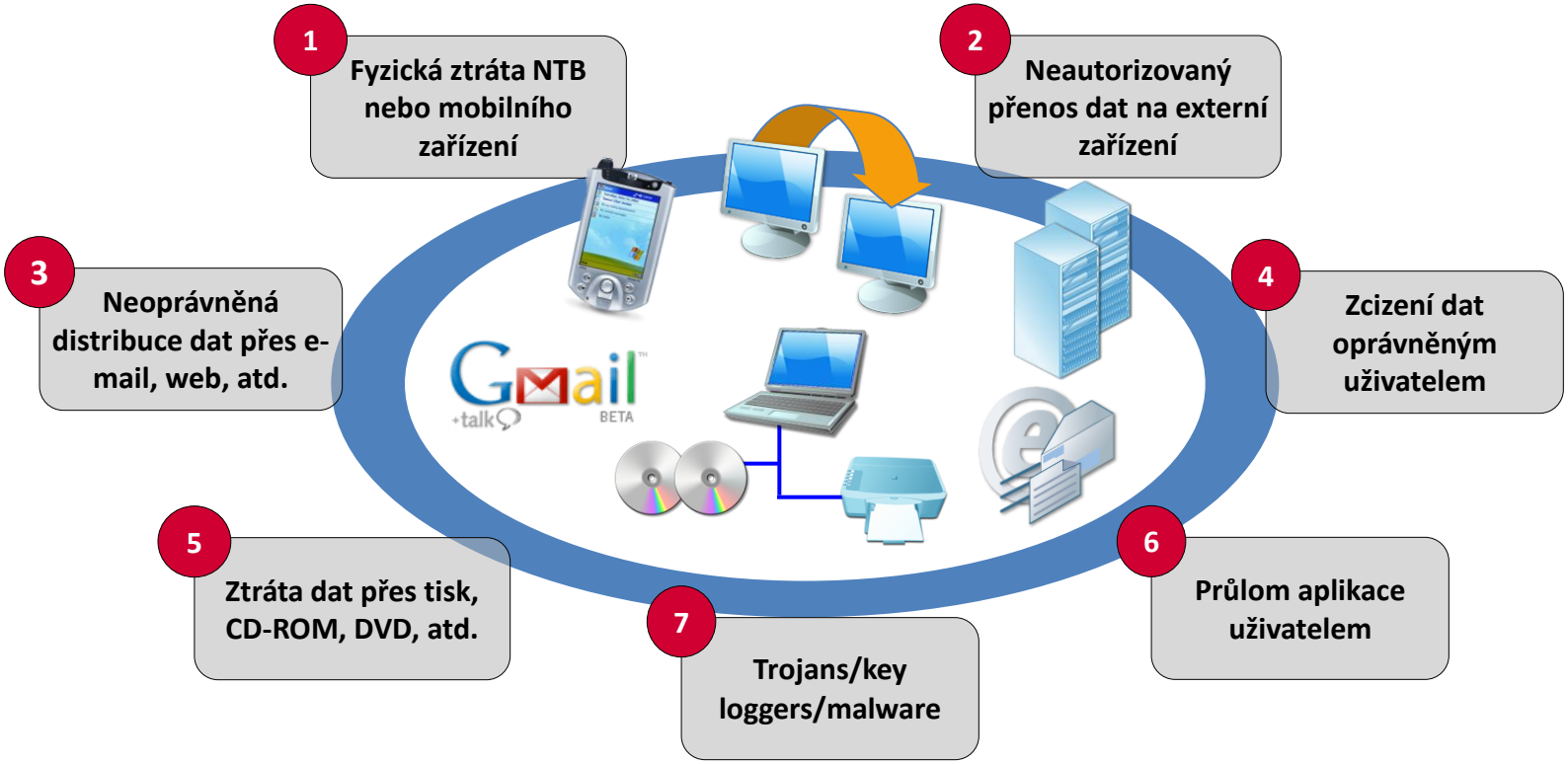
Jan Strnad

McAfee

Komplexní hrozby, které se neustále vyvíjí, vyžadují úplnou ochranu



Další hrozba na koncových zařízeních = uživatel



Centrální řízení bezpečnosti – od antiviru až k pokročilé bezpečnosti

Centrální správa

1 Antivirus

2 Antispyware

3 Desktop Firewall

4 Host Intrusion Prevention

5 Web Security

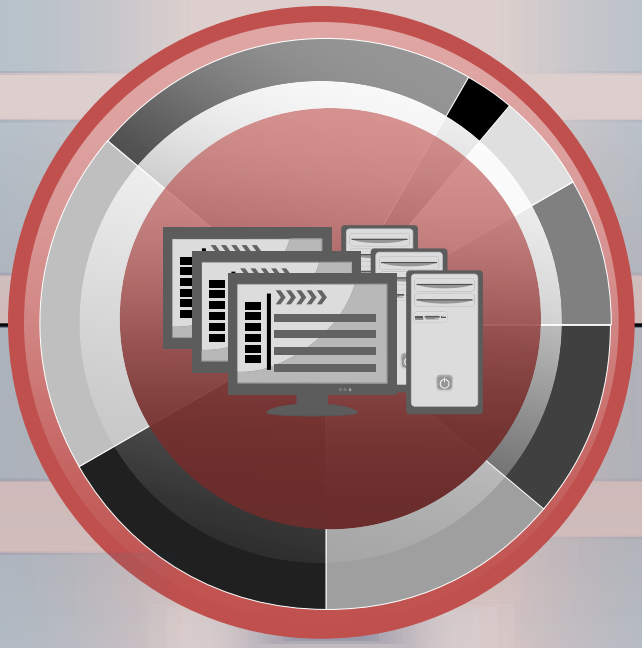
6 Data Protection
(DLP, Encryption)

7 Kontrola aplikací
Application whitelisting

8 MDM
Mobile Device Management

9 Databázová ochrana

10 SIEM



Základní ochrana

Antivir a antispywae

- Detekce známého malware hrozby - viry, červy, spyware, key loggery, rootkity, Trojany
- Heuristická analýza
- Access protection pravidla pro limitaci přístupu a blokaci systémů
- Proaktivní komunikace se systémy výrobce pro detekci neznámých kódů

Firewall a Host IPS

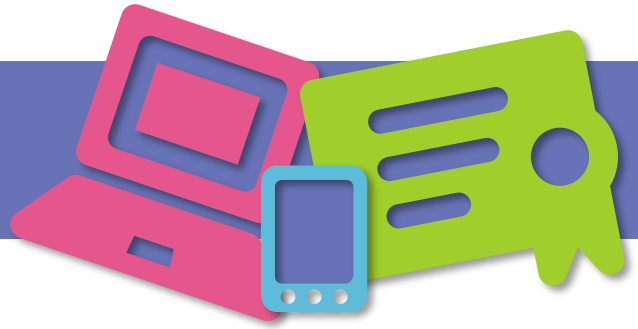
- Desktop Firewall
  - Chrání proti nechtěné komunikaci hrozeb, vynucuje bezpečnostní politiku pro příchozí i odchozí komunikaci
- Host IPS – detekční schopnosti
  - Signatury – přesná detekce známých hrozeb
  - Pravidla chování – detekce neznámých hrozeb s náchylností k false positive alarmům

Ochrana webové komunikace

- Snadná detekce bezpečných Web serverů
  - Zajistit bezpečné prohlížení webových stránek s jednoduchou odezvou – například zelená, žlutá nebo červené ikona informuje o nebezpečnosti navštívené stránky
- URL filtrace
  - Možnost definovat URL kategorie webových serverů, na které bude smět uživatel přistupovat a které mu budou zakázány.

SECURITY 2014

22. ročník konference o bezpečnosti v ICT



Ochrana DAT

Ochrana dat vyžaduje jiné myšlení

Snadná ztráta

Snadný přenos

Lákavé k odcizení

$490 $147 $147 $98

Cybercrime “Black Market” Value

Data musí být chráněna v těchto oblastech:

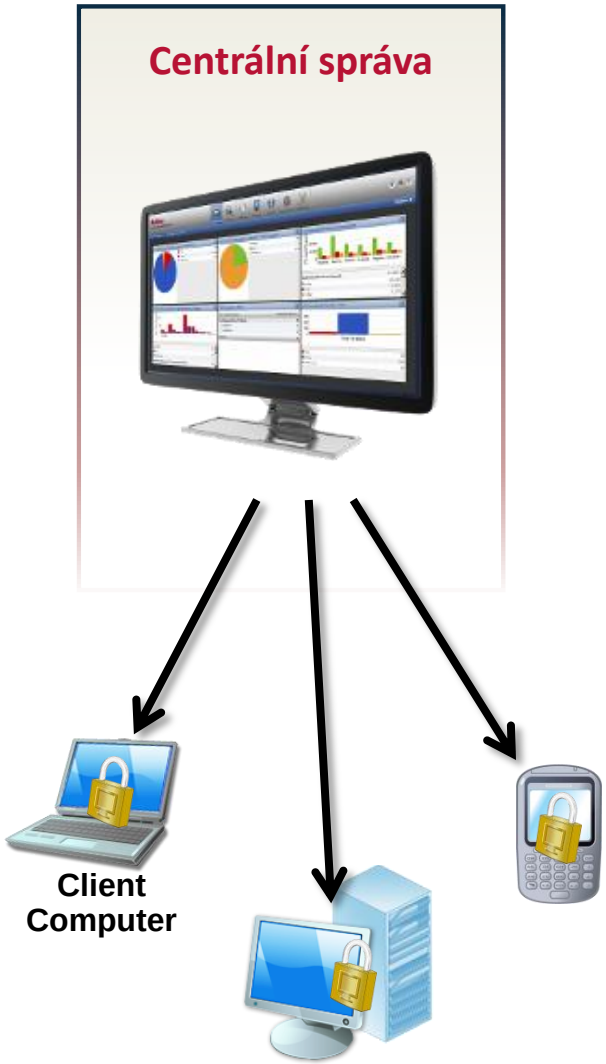
Použití

Lokalita

Zařízení

Přístup

Šifrování celých disků

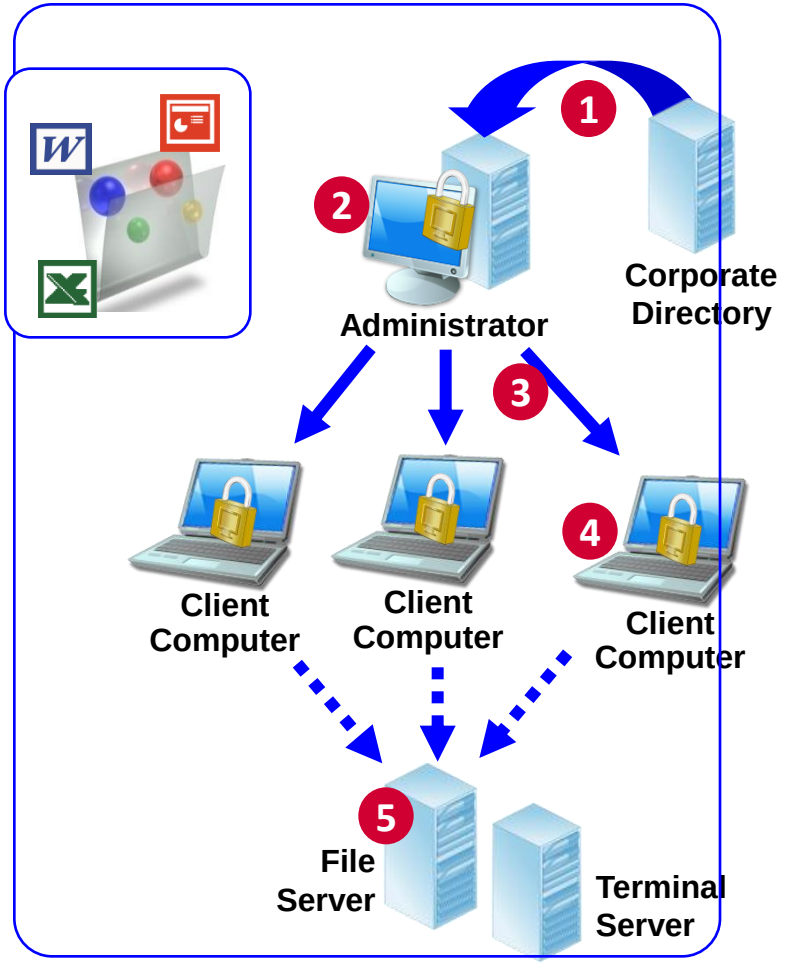


- **Potřeby zákazníků:**
  - Šifrování laptopů, desktopů, a mobilních zařízení včetně boot sektoru, systému nebo swap souborů.
  - Ochrana citlivých dat při ztrátě nebo odcizení zařízení
  - Safe Harbor protection – Ztráta šifrovaných dat = nevyžaduje veřejné vysvětlování

- **Doporučené vlastnosti:**
  - Šifrovací algoritmus AES 256
  - Podpora instrukcí AES-NI, které akcelerující operace nad algoritmem AES
  - Podpora SSD disků
  - Podpora pro laptopy, desktopy a mobilní zařízení
  - Centrální správa
  - Certifikace: například FIPS 140-2, Common Criteria Level 4, BITS, CSIA, apod.

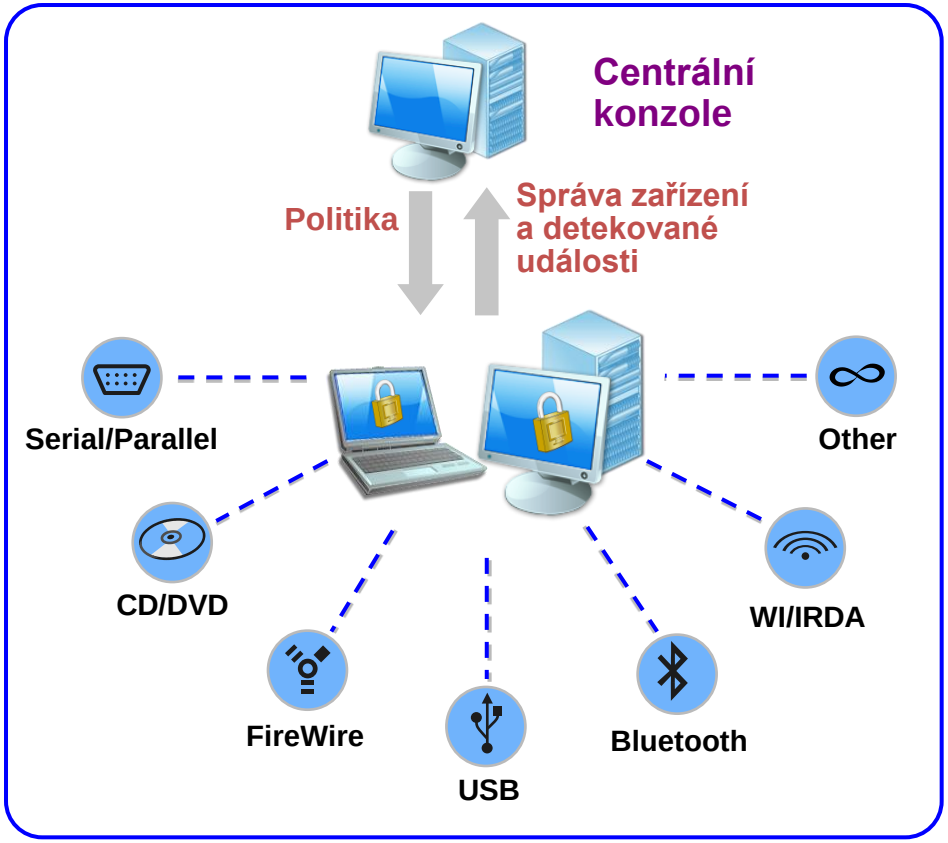
Šifrování souborů a složek

- Možnost šifrovat lokální i sdílená data
  - Pomocí jednoho klíče, který je dostupný pro jednoho nebo více uživatelů
  - Pomocí lokálního klíče pro osobní ochranu dat
- Šifrování externích datových úložišť přes USB rozhraní
  - USB disky,
  - Flash disky
- Centrální definice politiky umožňuje detailnější nastavení i ve velké společnost
- Automatické šifrování a dešifrování bez ztráty výkonu a plně transparentní pro uživatele – AES 256
- Ochrana souborů a složek na stanicích, laptopech a serverech



Device Control

- Možnost nastavení politiky pro připojení nebo blokování zařízení:
  - USB zařízení
  - CD, DVD
  - Bluetooth
  - FireWire.....
- Možnost nastavení politiky pro zápis nebo Read-only pro jednotlivá zařízení
- Centrální správa a definice politik pro skupiny uživatelů
- Logování o připojení zařízení nebo kopírování dat
- Podpora jak paměťových médií – CD, DVD, USB disk, SD karta, tak Plug and Play zařízení – modem...

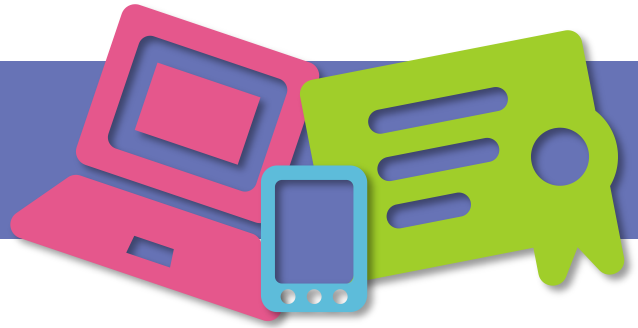


Data Loss Prevention

- **Potřeby zákazníků:**
  - Zabránit uživatelům, kteří mají přístup k citlivým datům společnosti, zneužít nebo odnést tyto data
  - Plná kontrola a audit zneužití citlivých dat
- **Doporučené vlastnosti:**
  - Ochrana dat proti zneužití, jako například Email , Web, tisk, poslámí emailem, copy/paste, kopírování na I/O zařízení
  - Široké spektrum ochrany a monitoringu citlivých dat jako:
    - Detailní logování & forenzní evidence
    - Real-time ochrana & blokování
    - Notifikace uživatele a administrátora
    - Karanténa citlivých dat

SECURITY 2014

22. ročník konference o bezpečnosti v ICT



Aplikační kontrola – dynamický whitelisting aplikací

Aplikační Whitelisting

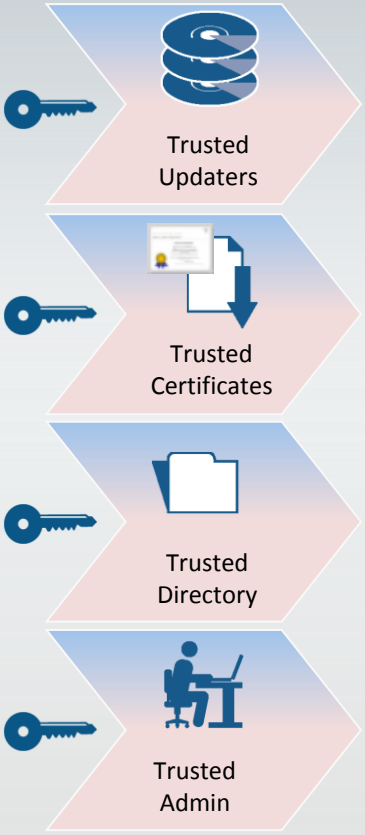
- Whitelist je vytvářen během instalace produktu skenováním systému – aplikací, knihoven, ovladačů a skriptů

1. Pokus o spuštění programu
   - Spustitelný soubor nebo komponenta OS
2. AW porovnává binární kód s whitelistem
3. Pokud není ve Whitelistu, spuštění programu se zablokuje.
   - Událost je logována, alertována nebo auditována

Dynamická aktualizace aplikací

Aktivní Whitelisting

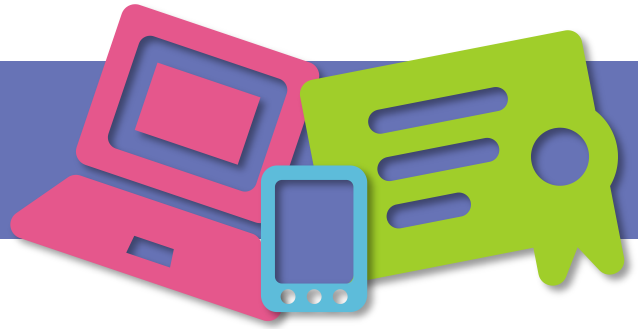
Automatická aktualizace Whitelistu



Návrat do aktivního Whitelistingu

SECURITY 2014

22. ročník konference o bezpečnosti v ICT



Správa mobilních zařízení - MDM

Výzvy pro správu a řízení mobilních zařízení

Obrovský rozvoj mobilních zařízení

- Smartphony, netbooky, tablety
- Využívané k práci, zábavě, hrám..
- Nezávislé, připojitelné kdekoliv

Využívání soukromých zařízení v podniku

- Kontrola a správa jak podnikových, tak soukromých mobilních zařízení

Nové aplikace a potřeby

- Doručení podnikových dat v případě potřeby
- Veřejné obchody s aplikacemi versus lokální aplikace

Správa mobilních zařízení

Plná kontrola pro :

- **Správu a bezpečné používání**
- **Nižší cena za podporu**
- **Ochrana podnikových dat a síťového přístupu**

Zabezpečení mobilních zařízení

Zařízení

Data

Aplikace

Zabezpečení mobilních zařízení

Ochrana mobilních zařízení

- Správa zařízení (MDM) – hesla, správa modulů
- Anti-malware
- Ochrana Webové komunikace

Ochrana dat

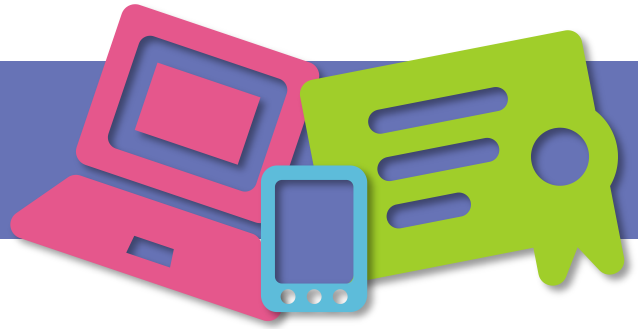
- Data Protection (Lokalizace, Lock, Wipe, Delete)
- Detekce Jailbroken a Rooted zařízení a jejich blokace
- Šifrování

Ochrana aplikací

- Konrola a ochrana aplikací
- Bezpečné úložiště - bezpečný kontejner
- Blokování aplikací

SECURITY 2014

22. ročník konference o bezpečnosti v ICT



Ochrana databází

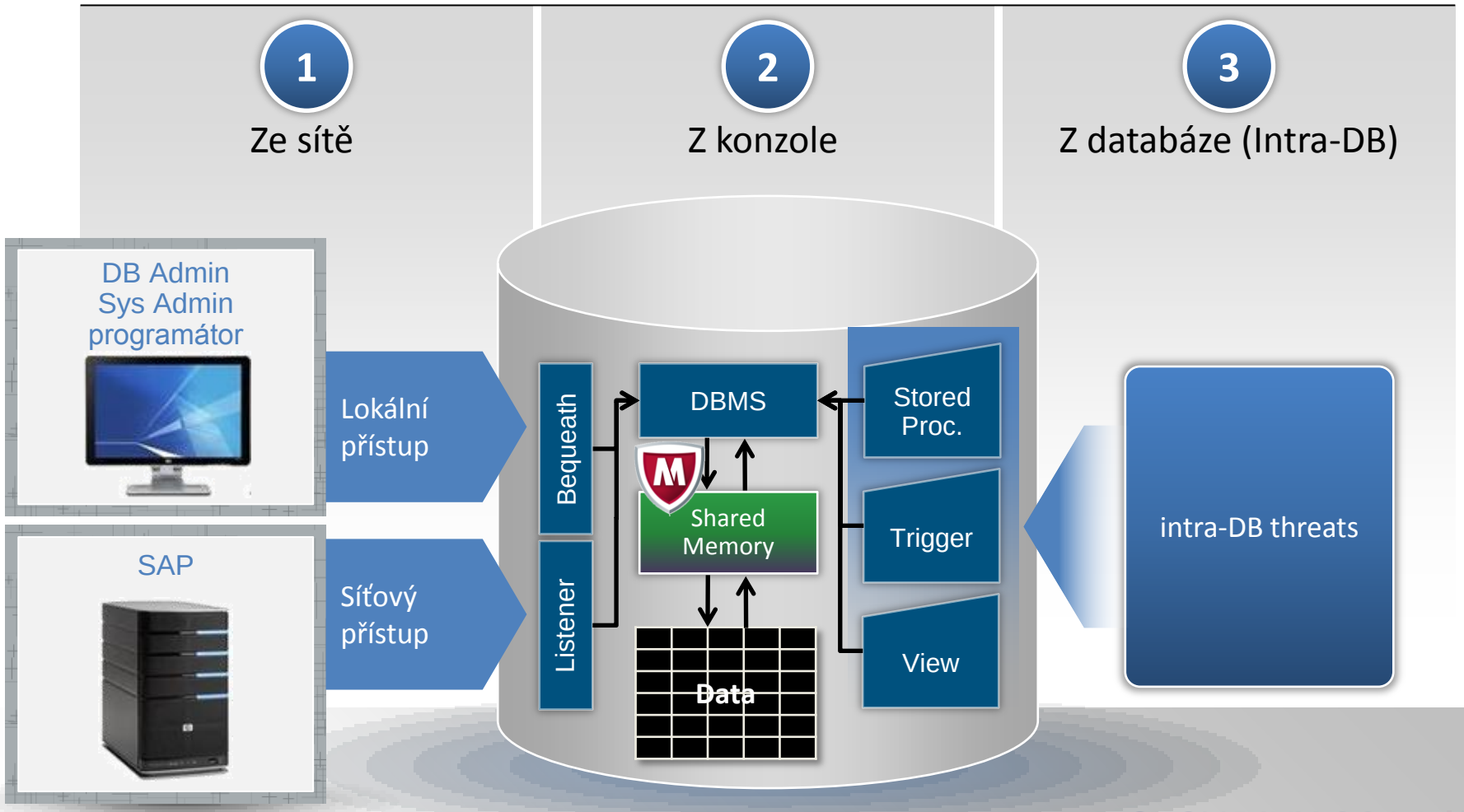
Proč chránit databáze před hrozbami?

- Databáze udržují velké množství citlivých informací
  - Čísla kreditních karet a bankovní záznamy
  - Finanční a účetní informace
  - Intelektuální vlastnictví
  - Informace o zákaznících
  - Osobní data
  - Průměrná cena DB záznamu je 300$
- Ale
  - **Databáze nejsou monitorované**
  - **Zřídka prováděný upgrade**
  - **Minimální nebo žádné záplaty**

- Toto dělá z databází snadný cíl útoku, kdy 75% útoků míří na databáze

Ochrana databáze napříč všemi vektory

Databáze může být přístupná ze třech různých bodů:

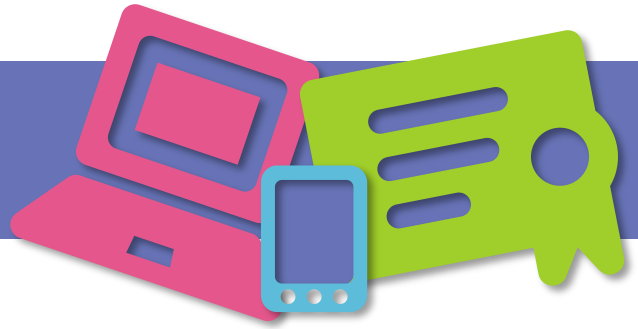


Virtuální záplatování

- **Instalace bezpečnostních záplat bývá bolestivá:**
  - Vyžaduje intenzivní testování
  - Má často za následek výpadky provozu
- **Někdy je to téměř nemožné:**
  - Provoz 24/7/365 (jedno okno pro údržbu za rok)
  - Vysoce customizovaná aplikace
  - DBMS verze, která již není dlouho podporovaná výrobcem
  - Limitované lidské zdroje
- **Řešení: Virtual Patching**
  - Ochrana proti známým a zero-day zranitelnostem bez výpadku nebo změny kódu **do doby, než je možné záplatovat**

SECURITY 2014

22. ročník konference o bezpečnosti v ICT



Bezpečnostní nástroje pod OS

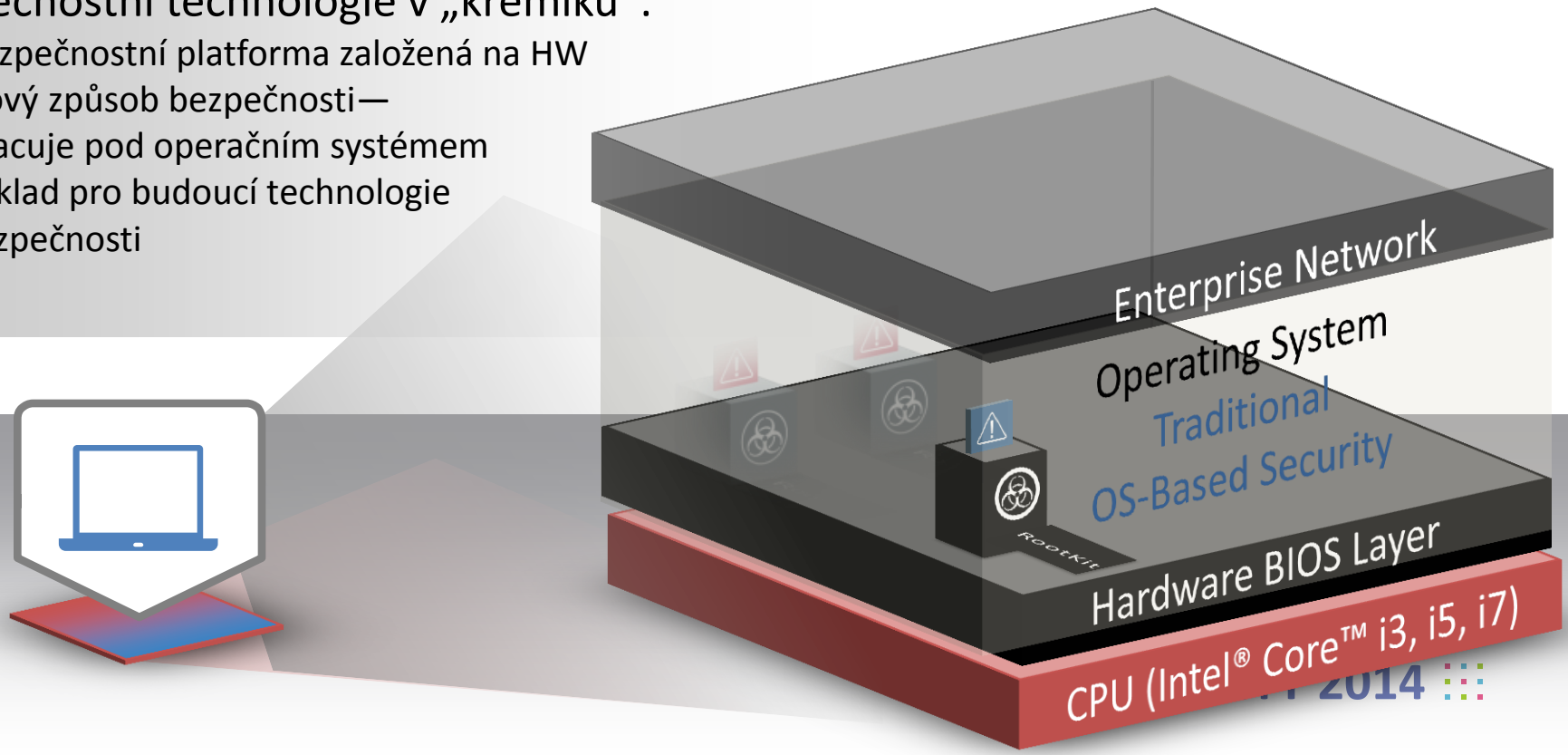
Ochrana pod operačním systémem

Tradiční ochrana

- Pracuje nad operačním systémem
- Není schopna detekovat skryté techniky útoků – APT hrozby, Rootkity
- Úspěšnost detekce se snižuje

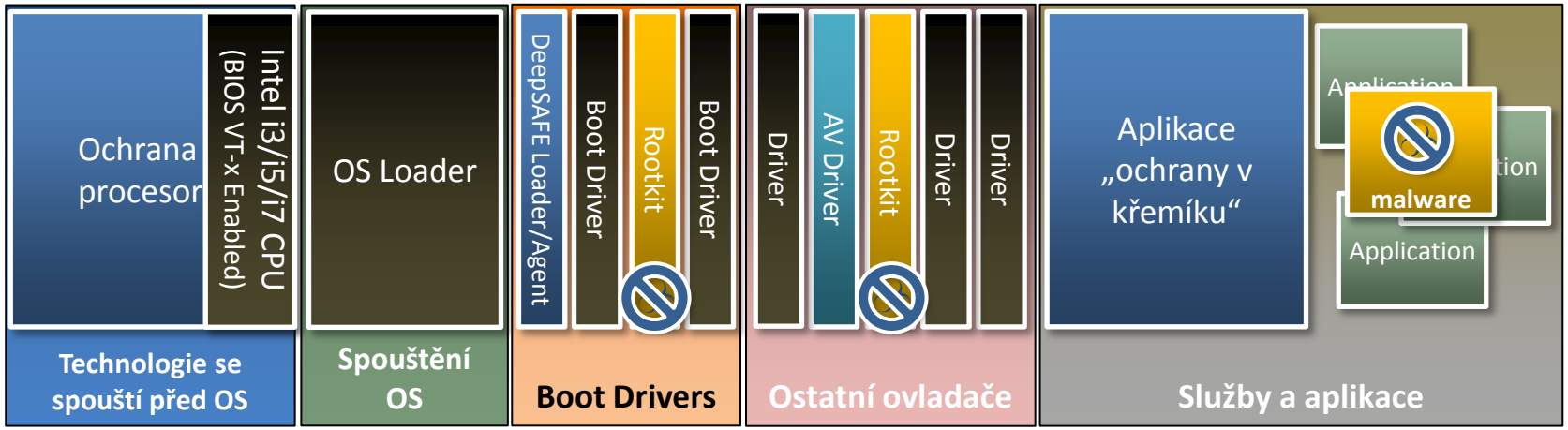
Bezpečnostní technologie v „křemíku“:

- Bezpečnostní platforma založená na HW
- Nový způsob bezpečnosti—
  pracuje pod operačním systémem
- Základ pro budoucí technologie
  bezpečnosti



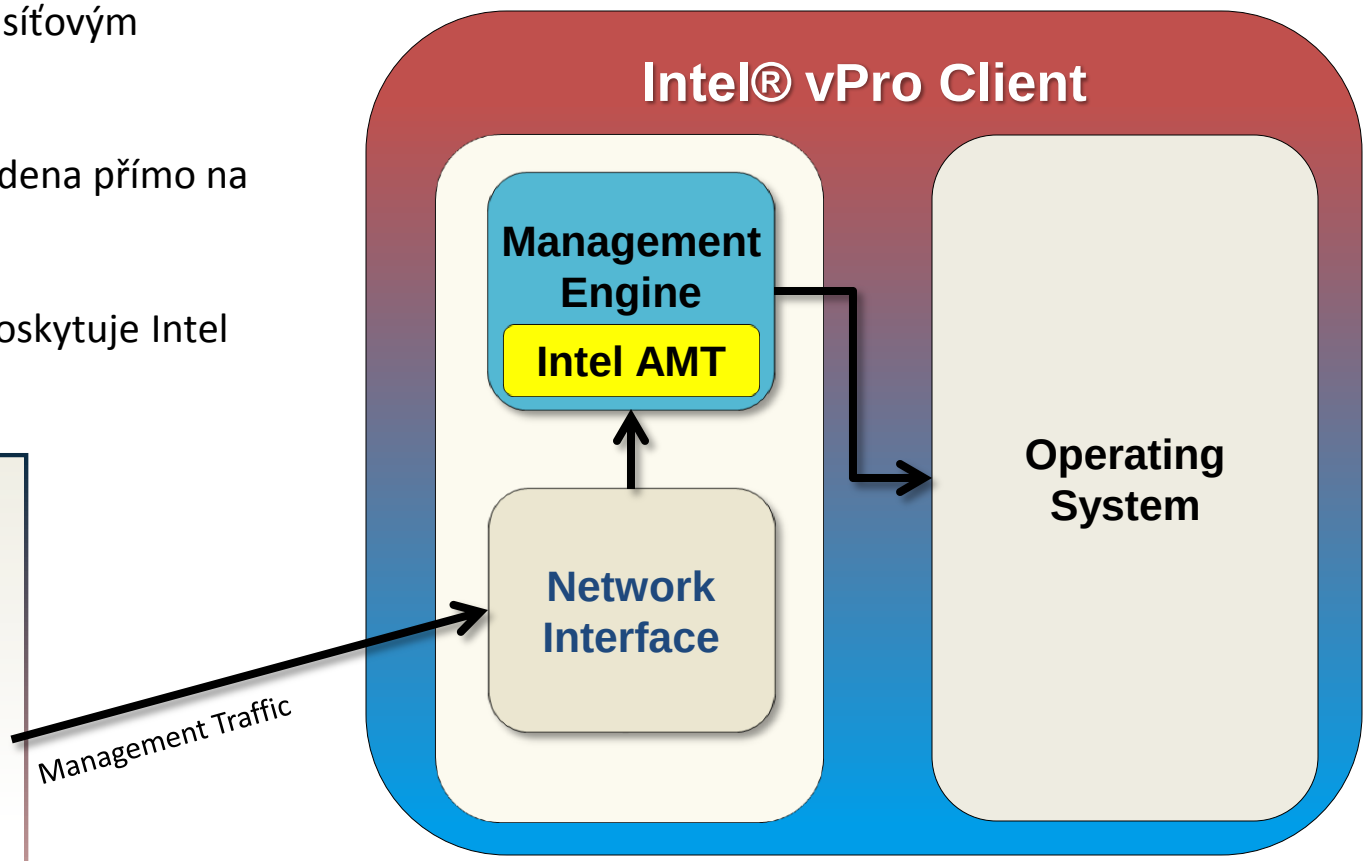
Ochrana pod OS - zastavuje skryté hrozby

- Real-time monitoring operační paměti
- Identifikuje kernel-mode rootkity v reálném čase
- Blokuje loudování ovladačů
- Technologie startuje před OS
- Informuje o podezřelém chování



Centrální správa pomocí Intel AMT

- AMT je umístěn mezi síťovým rozhraním a OS
- Vzdálená správa je vedena přímo na Intel AMT
- Síťovou konektivitu poskytuje Intel firmware, ne OS



Možnosti správy pod OS

Centrální konzole pro správu

Intel AMT vzbudí počítač a Agent provede komunikaci na centrální MCM server

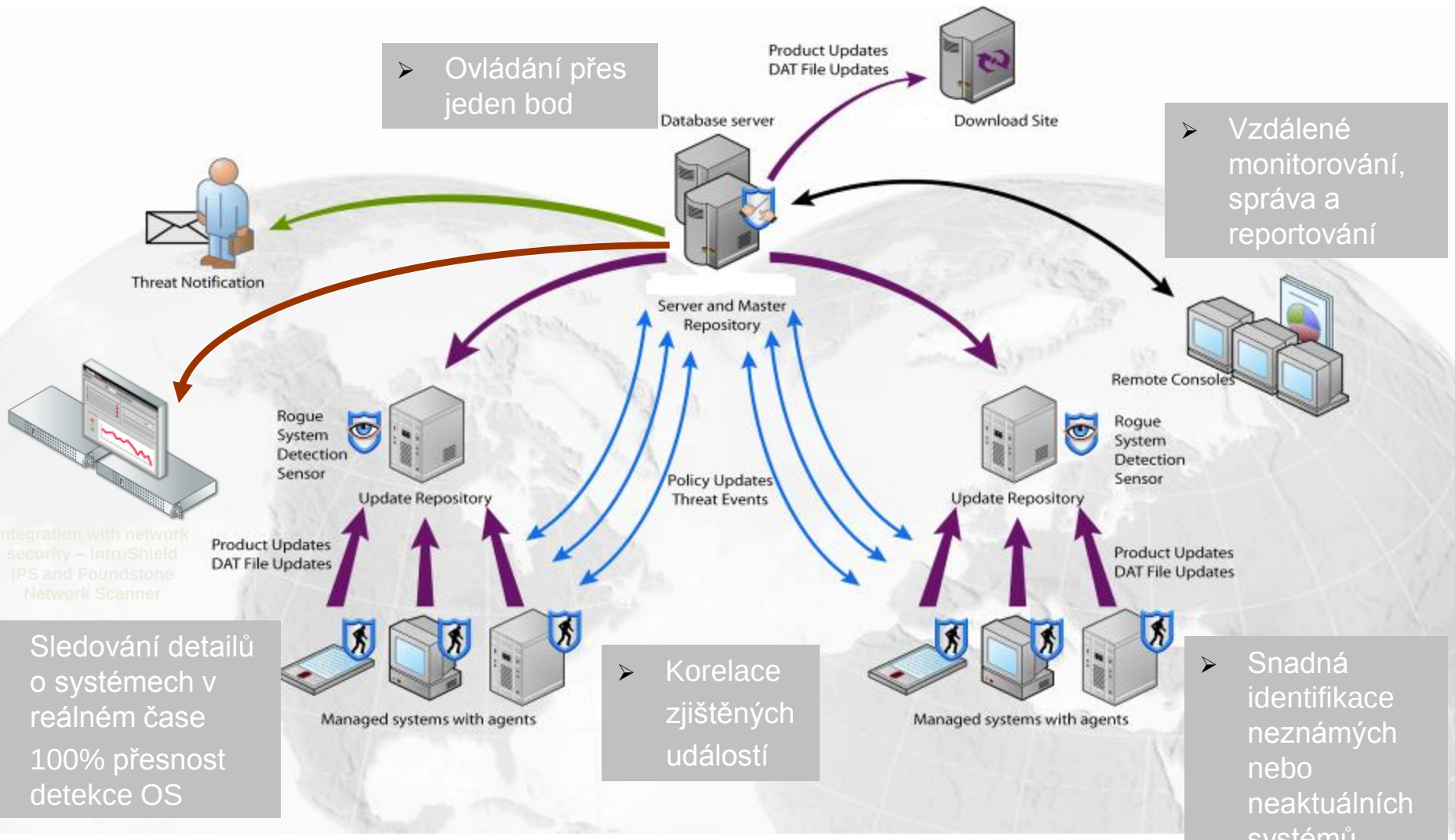
Centrální MBSM server odešle úlohu na lokálního agenta:

- Aktualizace bezpečnostních nástrojů
- Spuštění ODS
- Odeslání událostí
- Dešifrace disku
- Boot systému z externího image
- Spuštění procesu
- Shutdown

Wake Up počítače
AMT Alarm nebo Power-on

Centralizovaná správa bezpečnosti

- Ovládání přes jeden bod



- Vzdálené monitorování, správa a reportování

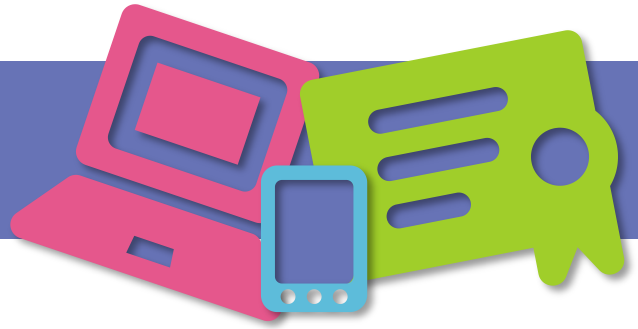
- Sledování detailů o systémech v reálném čase
- 100% přesnost detekce OS

- Korelace zjištěných událostí

- Snadná identifikace neznámých nebo neaktuálních systémů

SECURITY 2014

22. ročník konference o bezpečnosti v ICT



SIEM technologie

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
- Korelaci
- Agregaci
- Normalizaci
- Shromažďování
- Analýzu

Tři hlavní faktory ovlivňující většinu SIEM implementací

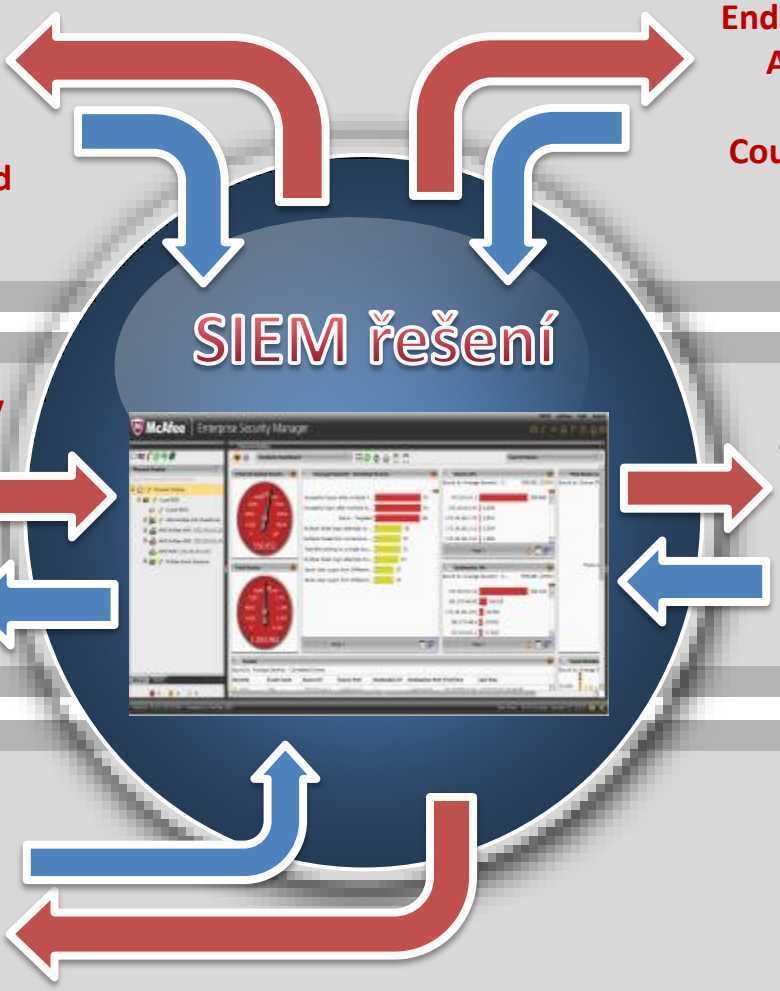
1. Viditelnost hrozeb v reálném čase
2. Efektivnost správy bezpečnosti
3. Požadavky na shodu a správu logů

Nové možnosti SIEM řešení

Threat Intelligence Feed

Network Security Assessment & Countermeasure Response

3rd Party Technology Feeds



Endpoint Security Assessment & Countermeasure Response

Asset Discovery & Vulnerability Assessment

Shrnutí

- Pouze s antivirem na dnešní hrozby nevystačíte (neznámý malware, APT, Rootkity), nicméně tvoří základ počítačové bezpečnosti
- Rozšířená bezpečnost vyžaduje další nástroje, jako HIPS, DLP, šifrování, aplikační kontrolu, ochranu databází a virtuálního světa...
- Důležité je zaměřit se i na ochranu mobilních zařízení, na kterých jsou také citlivá data
- Centrální správa všech bezpečnostních komponent snižuje cenu a lidské zdroje
- Napojení na SIEM technologie dává komplexní obraz o chování sítě a detekci hrozeb

SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Jan Strnad

Intel Security (McAfee)

jan_strnad@mcafee.com