

COMGUARD
communication security



Security Workshop

Karim Ifrah

Channel Sales Manager, COMGUARD a.s.



Value Added Distribuce CZ+SK+UA

- **Specialista na bezpečnosti IT**

- **Komplexní portfolio pro zabezpečení** datových center i sítě organizace od perimetru, přes DMZ až na klientské stanice

- **Nadnárodní distribuční společnost**

- Certifikace ISO 27001 (ISMS)
- Certifikace ISO 9001 a ISO 14001
- Certifikace NBU
- **Náš tým = 13 let zkušeností v oblasti IT security**

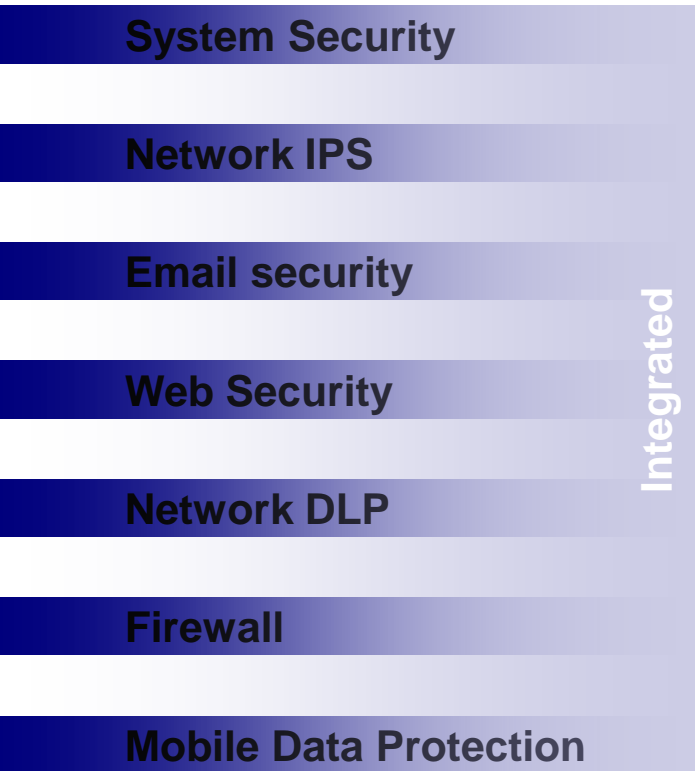
- **Akreditované školicí středisko**

- Support centrum pro distribuované řešení

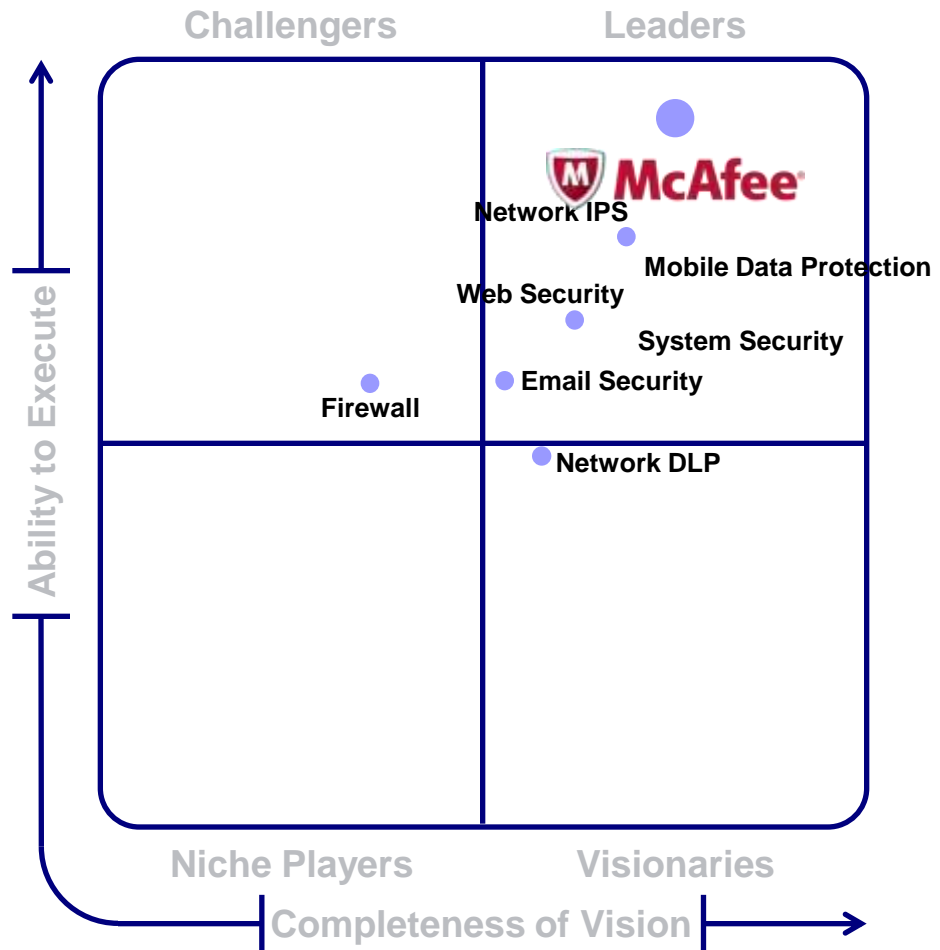
- **1st level a 2nd level** support
- **Expertní poradenství a služby** v oblasti bezpečnosti IT
- Hotline, HelpDesk, odborné konzultace
- Vzdálená správa a podpora administrace
- Outsourcing správy

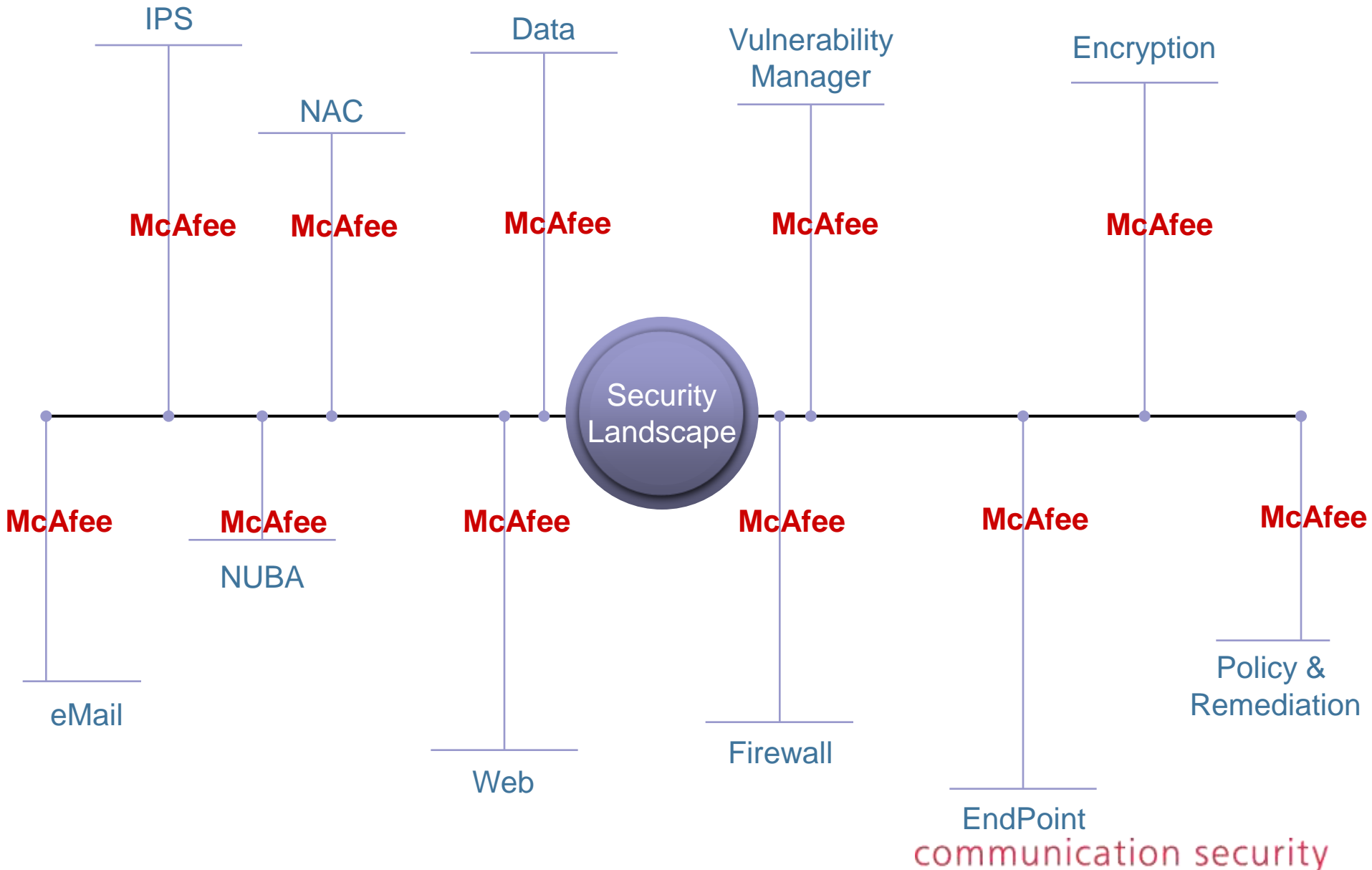
- **Audity v oblasti bezpečnosti IT dle ISO 27001**

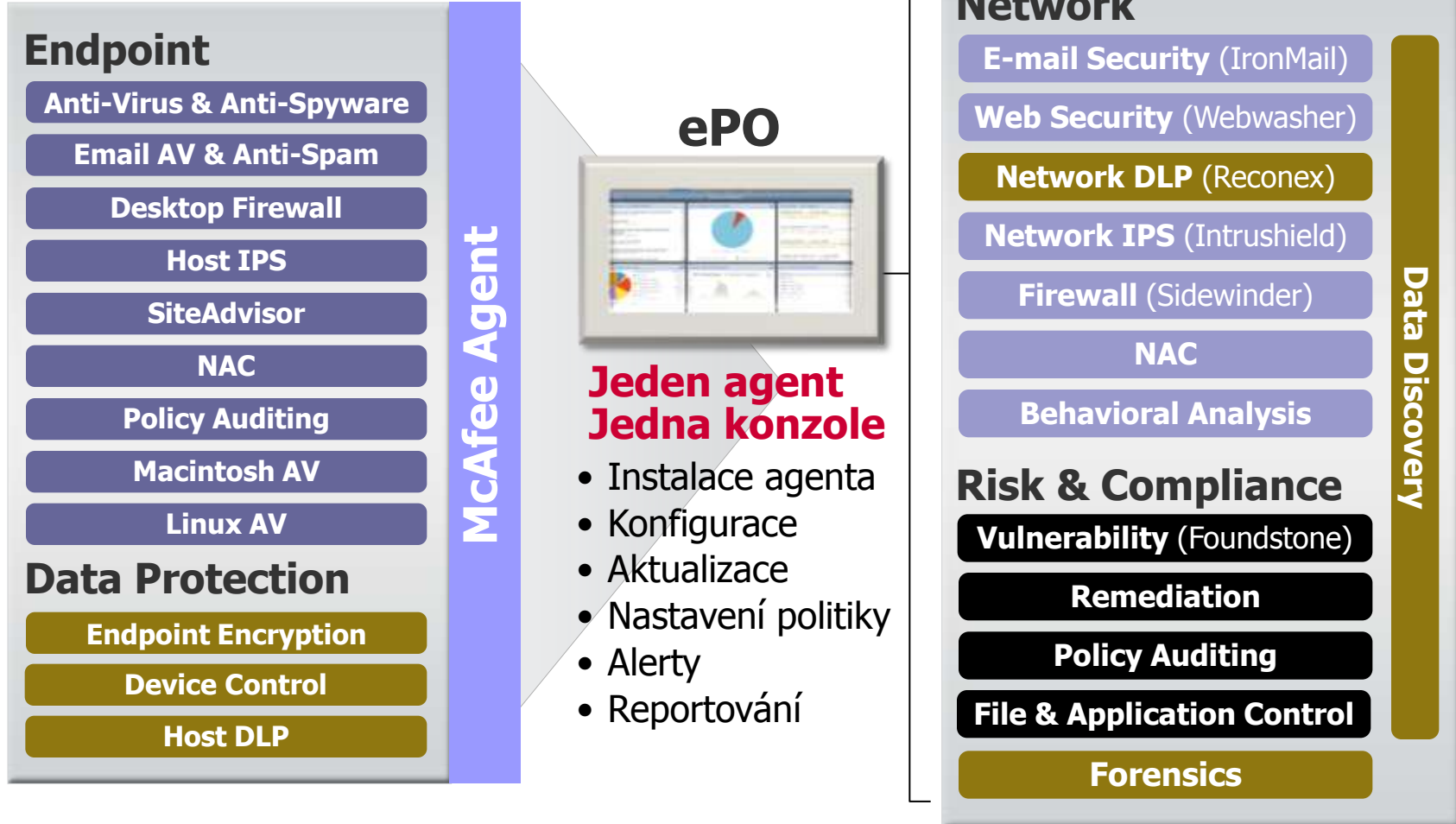




Source: Gartner







Konkurence

Compliance Management

- Data Loss Prevention
- Auditovací řešení



Desktop řešení

- Anti-virus
- Anti-spyware
- Desktop Firewall
- Desktop IPS



**Mnoho produktů
=
Složitá správa**

IPS řešení

- IPS a IDS řešení
- Email a web ochrana



Risk Management

- Vulnerability Management



McAfee



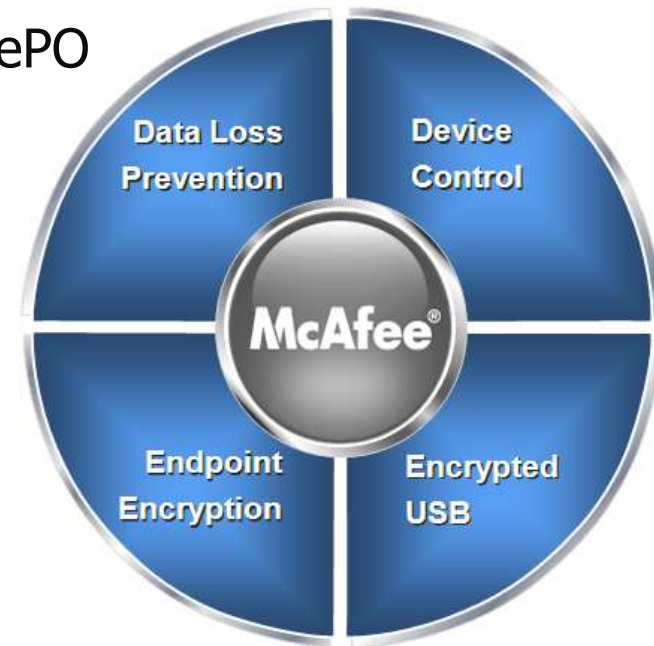
**Komplexní imunitní
systém**

**=
Jednotná správa**

- **Prevence úniku citlivých dat (DLP)**
 - McAfee Host Data Loss Prevention with ePO
 - Ochrana na koncových zařízeních
 - McAfee Network DLP Appliances
 - Ochrana na síťové úrovni
 - McAfee Device Control
 - Zabraňuje neoprávněnému používání připojitelných zařízení do firemní sítě

- **Šifrování dat**

- McAfee Endpoint Encryption for PCs
 - Šifrování celých disků
- McAfee Endpoint Encryption for Files and Folders
 - Šifrování souborů a adresářů
- McAfee Endpoint Encryption for Virtual Disk Windows / MAC
 - Šifrované virtuální disky
- McAfee Encrypted USB
 - Šifrované USB flash disky a HDD



- McAfee Host Data Loss Prevention with ePO
 - Softwarový agent instalovaný na koncová zařízení napříč organizací
 - Server pro logování a analýzy
 - Centrální řízení politik a nasazení
 - Monitorování událostí v reálném čase
 - Generování reportů

- McAfee Total Protection for Data
 - Balíček obsahuje:
 - McAfee Host Data Loss Prevention
 - McAfee Device Control
 - McAfee Endpoint Encryption for PCs
 - McAfee Endpoint Encryption for Files and Folders

- McAfee Network DLP
 - Dodáváno jako hardware appliance + software licencovaný per user



Network DLP Discover

Napomáhá nalézt, vyhodnotit a klasifikovat citlivé informace.

Network DLP Monitor

Pasivně monitoruje veškerý síťový provoz, analyzuje jeho obsah a reportuje události, které mohou způsobit ztrátu dat.

Network DLP Prevent

Na síťové úrovni blokuje aktivity, které mohou vést ke ztrátě důvěrných informací.

Network DLP Manager

Nástroj pro řízení politik, konfiguraci a administrativu.

- McAfee Encrypted USB



Typ	SanDisk	Standard	Bio	Hard Disk
Podporované OS	<ul style="list-style-type: none"> Windows 2000, XP, Vista 	<ul style="list-style-type: none"> MS Windows 2000, XP, Vista, 7 Apple Mac OS X (standalone usage only) 	<ul style="list-style-type: none"> Windows 2000, XP, Vista, 7 Mac OS X (standalone usage only) Linux (biometric mode only) 	<ul style="list-style-type: none"> Windows 2000, XP, Vista, 7 Mac OS X (standalone usage only) Linux (biometric mode only)
Kapacita	1, 2, 4, 8 GB	1, 2, 4, 8,16, 32 GB	1, 2, 4, 8,16, 32 GB	250, 320, 500 GB
Autentizace heslem	ano	ano	ano	ano
Biometrická autentizace	-	-	ano	ano
256-Bit AES Hardware Encryption	ano	ano	ano	ano
Virtualizace (PC-on-a-Stick)	volitelně, je třeba další software	volitelně, je třeba další software	volitelně, je třeba další software	volitelně, je třeba další software
FIPS 140-2 certifikace	ano	ano	ano	ano
Digital Identity & Crypto Services	-	-	volitelně	volitelně
Centrální správa přes McAfee ePO	ano	ano	ano	ano
McAfee Anti-Malware	ano	volitelně	volitelně	volitelně

COMGUARD
communication security



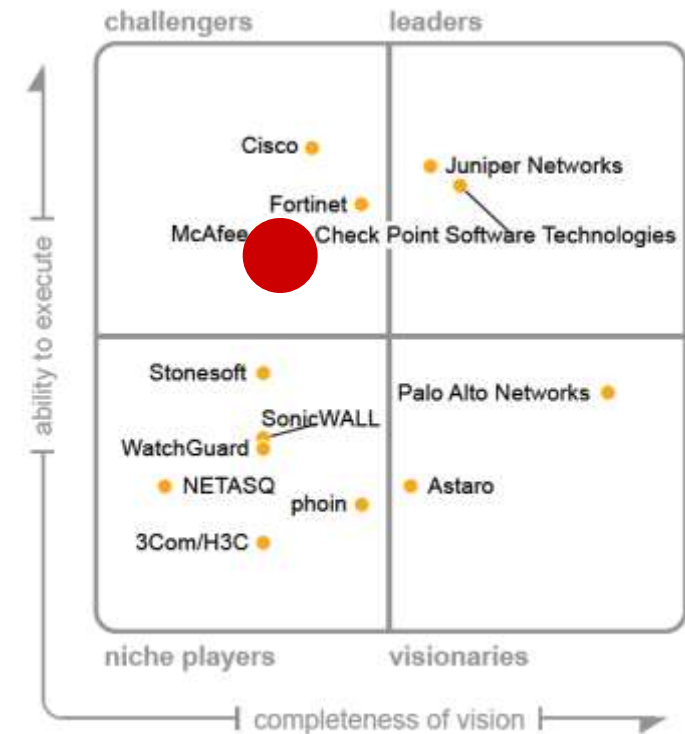
Security Workshop



- McAfee Firewall Enterprise (Sidewinder)
 - Stále nepřekonaný aplikační proxy firewall s mnoha integrovanými bezpečnostními moduly (UTM)
- McAfee Network Security Threat Behavior Analysis (NTBA) Appliance
 - Monitorování a reportování neobvyklého chování aplikací a hostů
 - Informace sbírá z routerů a switchů (NetFlow)
 - Chrání síť před červi, botnety, zero-day útoky, spamem či průzkum. útoky
 - Integrace s McAfee Network IPS (IntruShield)



- Firewall Ent. (Sidewinder)



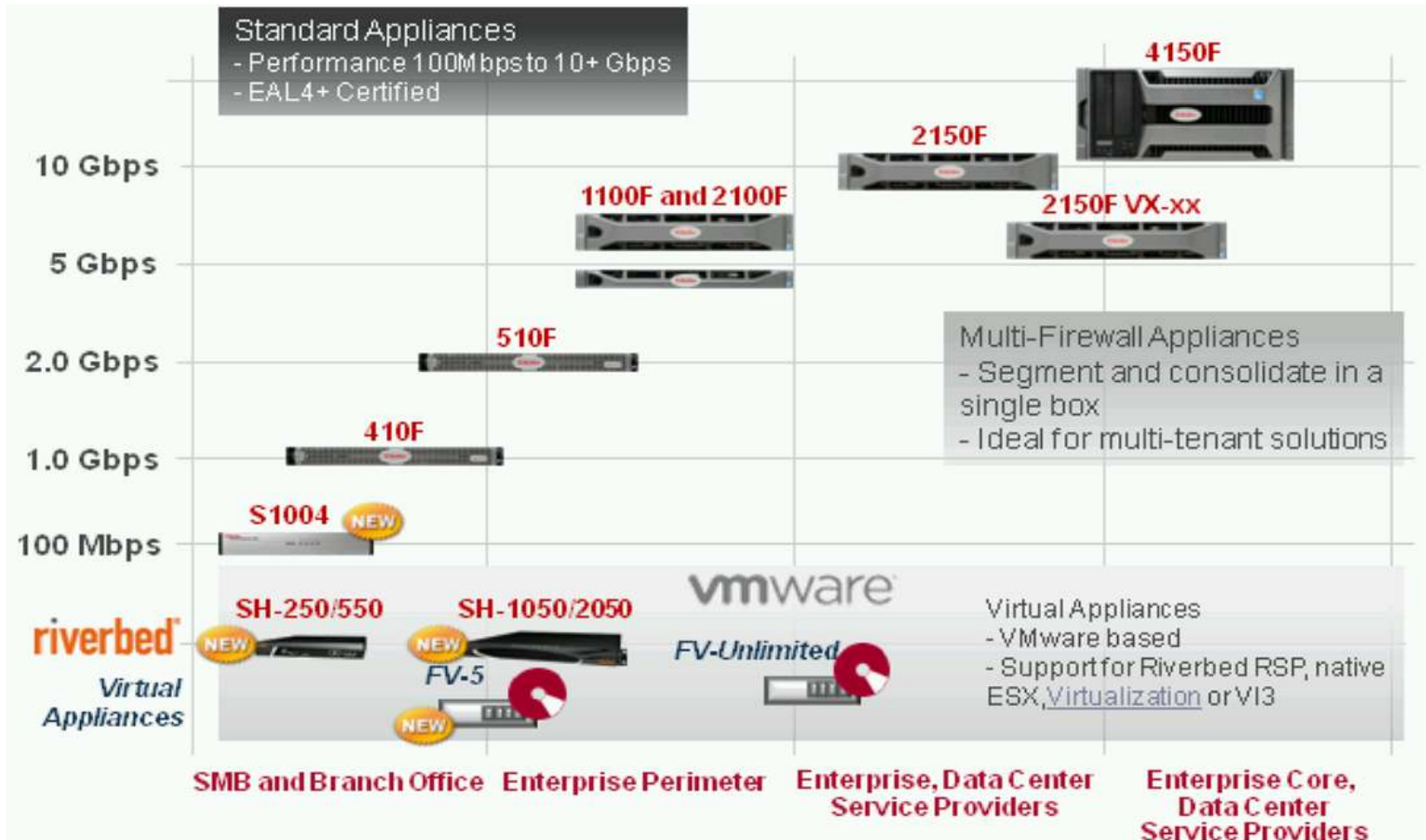
Source: Gartner (March 2010)

As of March 2010

- Gartner believes that if McAfee maintains the road map then it could become the next significant firewall market disrupter and potential market leader.

- McAfee Firewall Enterprise (Sidewinder)
 - Nová verze 8
(integrace identity uživatelů, řízení provozu dle aplikací, ...)
 - Moduly ZDARMA na firewallu:
 - McAfee Firewall Reporter
 - McAfee TrustedSource + Geo-Location
 - McAfee Firewall Enterprise Anti-Virus
 - McAfee SmartFilter
 - McAfee Firewall Enterprise Intrusion Prevention
 - McAfee Firewall Enterprise Encrypted Filtering
 - Samostatný produkt pro analýzu a simulace pravidel – McAfee Firewall Enterprise Profiler
 - „Klasická“ appliance / kontejner pro VMware ESX / 2150VX / verze pro Riverbed
 - Nový model S1004 pro menší organizace od cca 40.000,- Kč

- McAfee Firewall Enterprise (Sidewinder)



COMGUARD
communication security



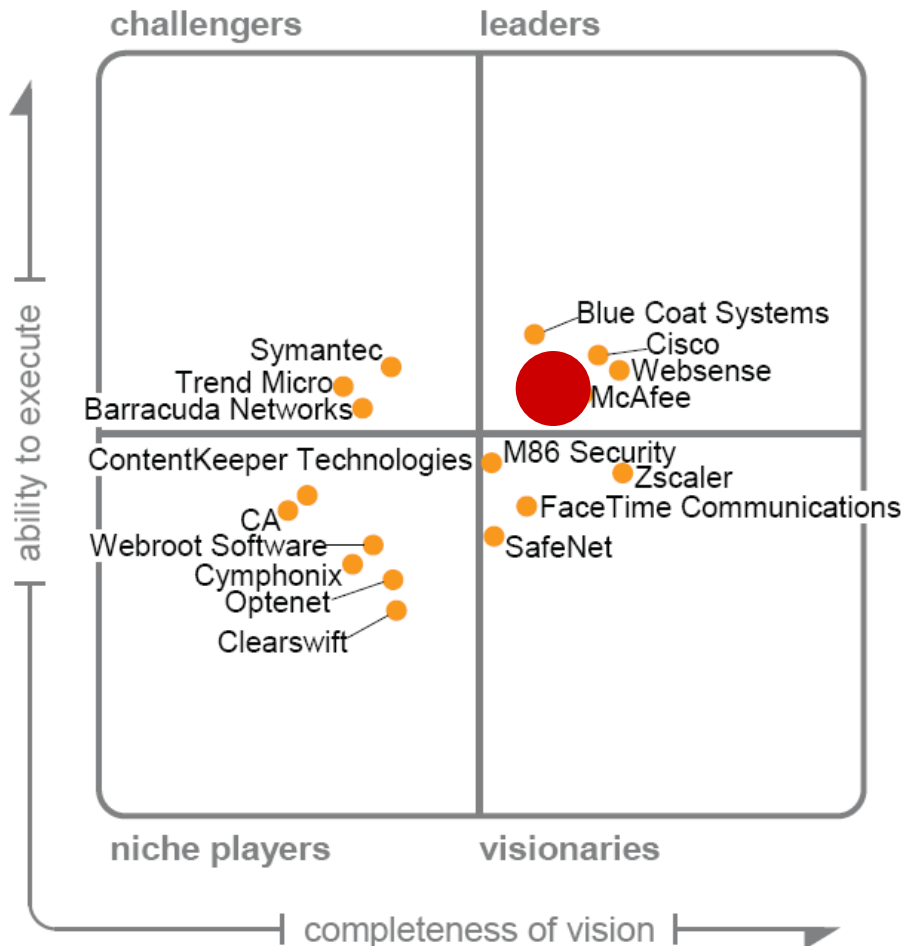
Security Workshop



- Web Gateway Appliance
 - McAfee Web Gateway (Webwasher)
- McAfee Smartfilter
- Email Gateway Appliance
 - McAfee Email Gateway (IronMail)
- Network Security Suites
 - McAfee Total Protection for Internet Gateways
 - McAfee Total Protection for Email Gateways
- Email and Web Security
 - McAfee Email and Web Security Appliance (EWS)
 - McAfee Content Security Blade Server



- McAfee Web Gateway (Webwasher)



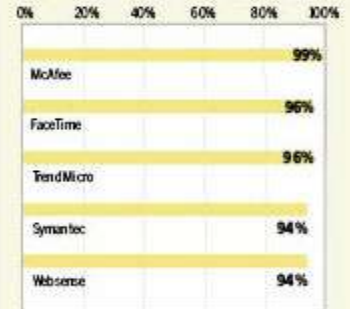
Network World Lab Alliance,
Network World December
07, 2009 12:04 AM ET

McAfee's appliance thwarted more malware – with lower latency – than the other gateways.

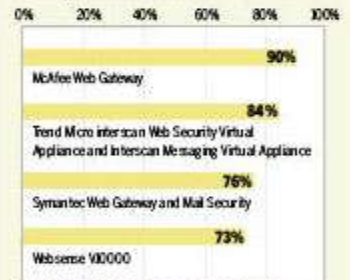
McAfee's Web Gateway appliance is our **Clear Choice winner**. It does an excellent job of keeping malware (both Web site-based and e-mail-borne) at bay, is responsive, has an intuitive, customizable user interface and scales well.

Malware blocking success rate

How well the products blocked 100 malware attacks



Phishing detection success rate



BASED ON 1,000 MESSAGES, 500 PHISHES, 500 LEGITIMATE





Latency while inspecting executable files for malware







Source: Gartner (January 2010)

As of January 2010

- McAfee Web Gateway (Webwasher)
 - Category-based and reputation-based web filtering, McAfee anti-virus, proxy, cache, SSL scanning, Content control filters, McAfee Web Reporter Basic.

Modelová řada				
	WW500 (1U)	WW1100 (1U)	WG5000 (1U)	WG5500 (2U)
Procesor	Single	Dual Core	1 Quad Core	2 Quad Core
Paměť	2 GB	2 GB	6 GB (až 64GB)	12 GB (až 64GB)
Rozhraní	2 x Gb NIC	4 x Gb NIC	4 x Gb NIC	4 x Gb NIC
RAID	N/A	RAID 1	RAID 1	RAID 1/RAID 5
HDD	160 GB SATA	2x160 GB SATA	2 x 300 GB SAS	6 x 300 GB SAS
Napájecí zdroj	jeden	jeden	redundantní	redundantní
Podp.ICAP/IFP	ano/ano	ano/ano	ano/ano	ano/ano

- McAfee Email Gateway (IronMail)

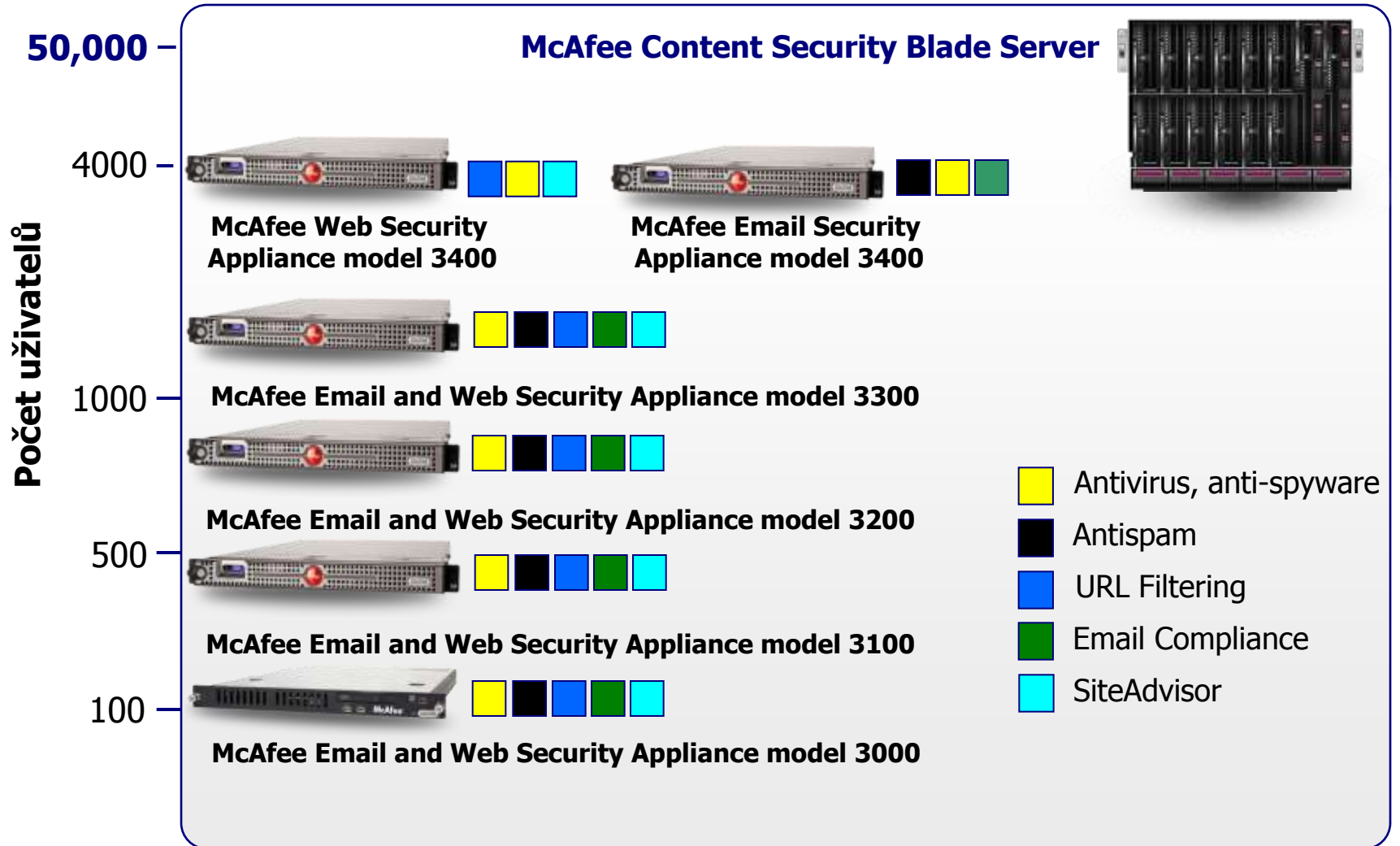
Modelová řada				
	EG-5500	EG-5000	S120	S10
Počet uživatelů	neomezen	neomezen	neomezen	neomezen
Počet portů	4	4	2	2
Procesor	2x Quad Core	Quad Core	Core2Duo	Single Core
RAID	Level 5 + Hot spare	Level 1	Level 1	---
HDD	800 GB	300 GB	160 GB	160 GB
Redund. zdroj/větrák	Ano	Ano	Ne	Ne
Dostupné moduly	Antispam & Antiphishing, McAfee Anti-Virus, Dynamická karanténa, DLP – pokročilá ochrana před únikem informací, Šifrování zpráv, Ochrana web mail serverů (OWA, Lotus, Novell), Analýza obrázků a TrustedSource			Antispam & Antiphishing , McAfee Anti-Virus, DLP – základní ochrana před únikem informací, Trusted-Source,

- McAfee Total Protection for Internet Gateways
 - Cenově velmi výhodné řešení
 - Balíček obsahuje tyto licence:
 - McAfee Web Security (Webwasher)
 - McAfee Web Anti-Malware (proaktivní ochrana pro web 2.0)
 - McAfee Email Security (IronMail)
 - McAfee Network DLP Prevent
 - Zákazník aktivuje licence hardwarem

- McAfee Total Protection for Email Gateways
 - Balíček obsahuje tyto licence:
 - McAfee Email Security (IronMail)
 - McAfee Network DLP Prevent
 - Zákazník aktivuje licence hardwarem

- McAfee Email and Web Security Appliance (EWS)
 - Určeno pro **SMB**, včetně hw a licencí od 40 tis. Kč
 - Předinstalované řešení s **neomezenou licencí** obsahuje:
 - McAfee Email and Web Security Appliance software
 - Anti-Spam and Email Compliance
 - McAfee Web Filtering (SmartFilter)
 - Verze pro VMware (VMware Server or ESX), 100 uživ cca 27 tis. Kč

- Content Security Blade Server
 - McAfee Content Security Blade Server Chassis pro 6 nebo 14 blades
 - McAfee Content Security Management Blade
 - McAfee Content Security Scanning Blade
 - **Neomezená licence**: McAfee Email and Web Security, McAfee Web Security a McAfee Web Anti-Malware, Gateway Edition.



- Konkurenční upgrade EWS 3000 s neomezenou licenci
 - 31.500,- Kč (hw, sw, licence, support)
 - Uplatnitelné pro Barracuda Networks, Symantec, ronPort, Proofpoint, TrendMicro a Websense
 - Není omezen počet
- McAfee Security as a Service
 - McAfee SaaS Web & Email Protection Suite
 - McAfee SaaS Email Protection & Continuity
 - McAfee SaaS Email Protection
 - McAfee SaaS Web Protection
 - McAfee SaaS Email Inbound Filtering
 - McAfee SaaS Email Outbound Filtering Option
 - McAfee SaaS Email Inbound Filtering & Continuity - Appliance Option

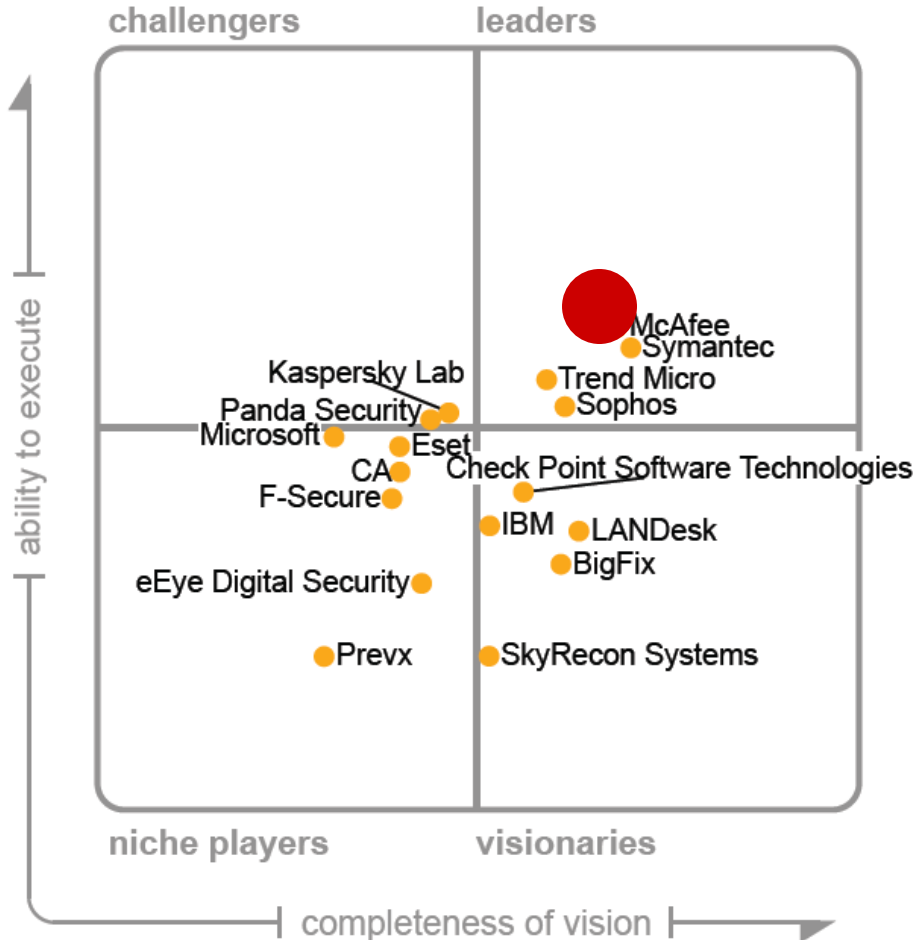
COMGUARD
communication security



Security Workshop



- McAfee System Security Suites



Source: Gartner (April 2009)

As of April 2009

- Porovnání starých a nových balíčků McAfee System Security

	SAV	EPS	AVD	TEE	TEN	TEA	EPA	TEB	TPE
ePO	OLD	NEW	OLD	OLD	OLD	OLD	NEW	NEW	NEW
Anti-virus	OLD	NEW	OLD	OLD	OLD	OLD	NEW	NEW	NEW
Email server (AV+ASpam)	OLD	NEW	OLD	OLD	OLD	OLD	NEW	NEW	NEW
Desktop firewall	OLD	OLD	OLD	OLD	OLD	OLD	NEW	NEW	NEW
SiteAdvisor Ent Plus	OLD	NEW	OLD	OLD	OLD	OLD	NEW	NEW	NEW
Anti-spyware	OLD	NEW	OLD	OLD	OLD	OLD	NEW	NEW	NEW
Host IPS	OLD	OLD	OLD	OLD	OLD	OLD	NEW	NEW	NEW
NAC	OLD	OLD	OLD	OLD	OLD	OLD	NEW	OLD	NEW
Policy Auditor	OLD	OLD	OLD	OLD	OLD	OLD	NEW	OLD	NEW
Device control	OLD	NEW	OLD	OLD	OLD	OLD	NEW	NEW	NEW
Web filtering	OLD	OLD	OLD	OLD	OLD	OLD	NEW	NEW	NEW
Endpoint Encryption	OLD	OLD	OLD	OLD	OLD	OLD	OLD	NEW	NEW
Mixed-platform	OLD	OLD	OLD	OLD	OLD	OLD	OLD	OLD	NEW

OLD NEW

- McAfee Total Protection for Virtualization
 - Obsah balíčku:
 - VirusScan Enterprise
 - VirusScan Enterprise for Linux
 - VirusScan Enterprise for **Offline Virtual Images**
 - (VMware ESX, Citrix, MS Hyper-V)
 - Anti-Spyware Enterprise
 - Host Intrusion Prevention for Server
 - Management: McAfee ePolicy Orchestrator

- Host IPS
 - = IPS + desktop firewall
 - McAfee Host Intrusion Prevention for Desktops with ePO
 - McAfee Host Intrusion Prevention for Servers with ePO

- McAfee Total Protection for Server Suite
 - Obsah balíčku:
 - VirusScan Enterprise
 - VirusScan for Linux
 - Application Control for Servers
 - Change Control for Servers
 - Policy Auditor for Servers
 - ePolicy Orchestrator

- McAfee Security as a Service
 - McAfee SaaS Total Protection
 - McAfee SaaS Endpoint & Email Protection Suite
 - McAfee SaaS Endpoint Protection Advanced
 - McAfee SaaS Endpoint Protection
 - McAfee Vulnerability Assessment Service Module

COMGUARD
communication security



Security Workshop

