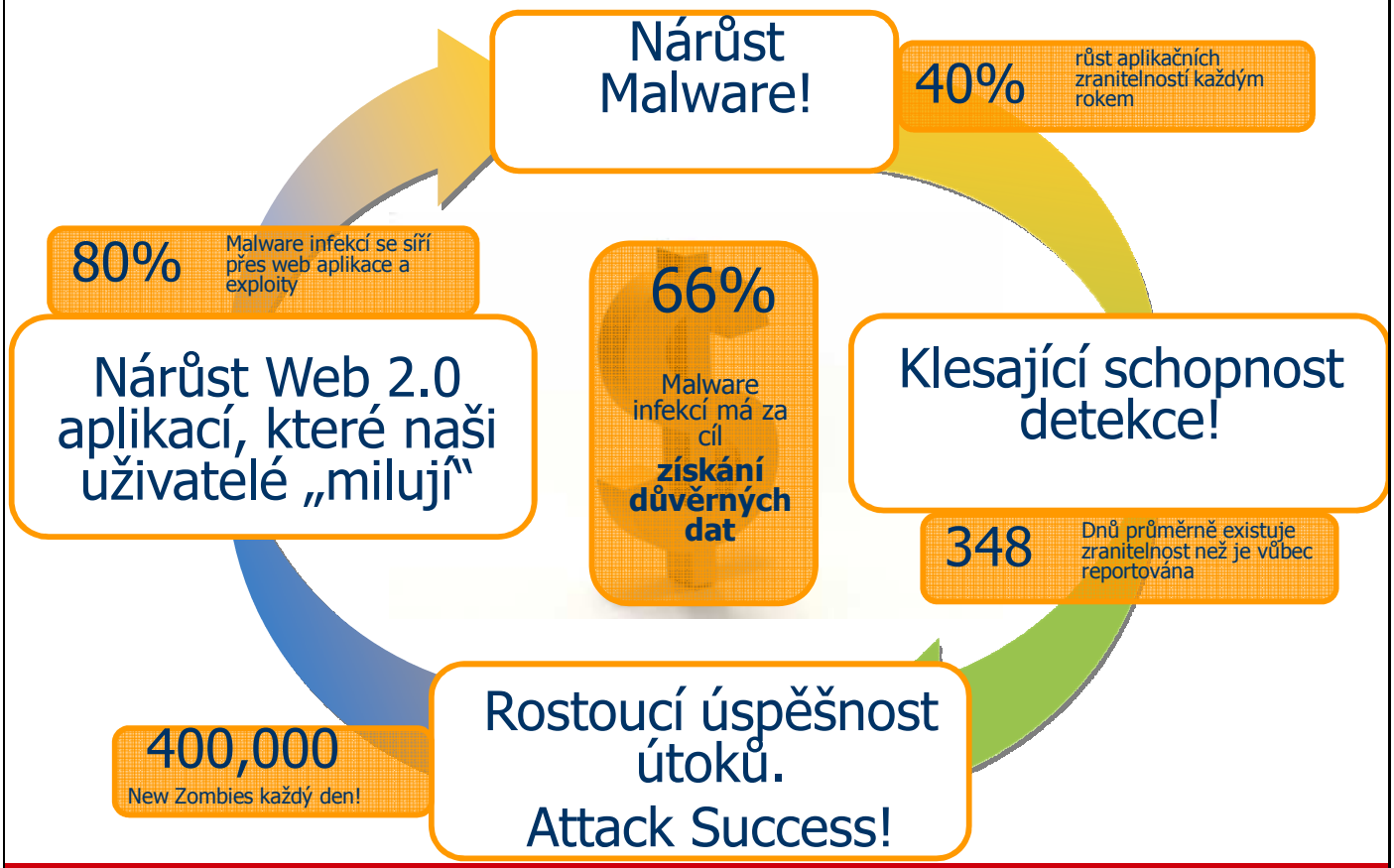
COMGUARD
communication security

BEZPEČNOST pro prostředí WEB 2.0

Ing. Jan Dymáček
Výkonný ředitel
COMGUARD a.s.

COMGUARD

Ohrožení pro naše peníze



COMGUARD

Jak tedy můžeme efektivně redukovat riziko?

- Jak se účinně chránit?

Implementace Gateway ochran WEB prostředí – nejlepší řešení ochrany uživatelů a sítí před hrozbami Web 2.0!

- Ne všechny bezpečnostní brány jsou ale rovnocenné – většina je doposud navržena pro Web 1.0 World
- Co je tedy EFEKTIVNÍ technologie pro bezpečnost Web 2.0 world!
  - **Reputation system** kteé sleduje škodlivé *servery* hostující záludné *kódy*
  - **Anti-Malware** technology that looks for *known* and *unknown* attacks
  - **Application Proxy** Gateways to *protect* Web-facing applications
  - **Příchozí i odchozí provoz**

Implementace jednorázových hesel

- Zabrání schopnosti odcizení hesel a prolomení přístupu pro web aplikace jako je OWA nebo LNWA

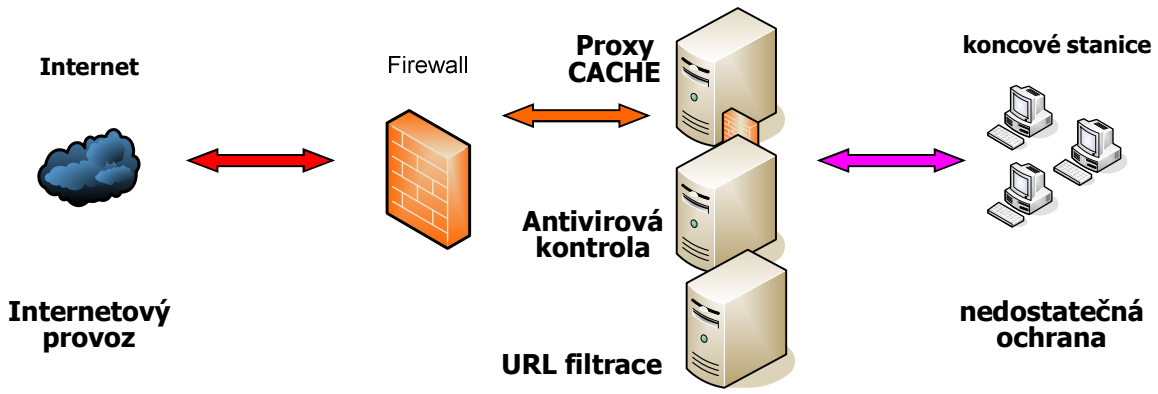
Implementace aplikačních proxy firewallů

- Dovnitř i vně sítě komunikuje vždy je důvěryhodná proxy firewallů, ždáná přímá spojení nejsou dovolena
- Proxy firewallu zkontroluje provoz a eliminuje nežádoucí kódy

COMGUARD

Typické enterprise řešení pro WEB 1.0.

Typické enterprise řešení pro web 1.0



Typická podniková síť:

- Firewall
- Web Proxy a Cache
- URL filtrace
- Antivirus pro http

- Paketový firewall
- Linux based (squid)
- Off box
- Off box

COMGUARD a.s., Vídeňská 119b Brno, Freyova 27 Praha, obchod@comguard.cz, www.comguard.cz

SECURE COMPUTING
Webwasher
Web Gateway Security

SECURE COMPUTING
TrustedSource
Global Intelligence

Moduly:

SECURE CACHE

ANTI-MALWARE

URL FILTER

ANTI-SPAM

SSL SCANNER

Potřebujete více?

4 výkonnostní modely včetně SecureCache WW500/1100/1900/2900 Anti-Malware, AntiVirus (McAfee, Sophos), URL Filtrace, SSL Scanner, Content Reporter

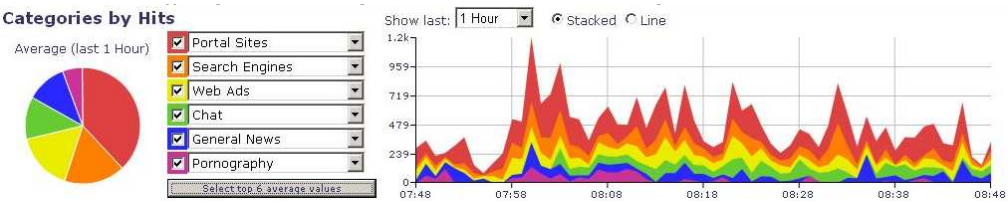
Secure Web - **Webwasher® SME250**

elegantní, rychlé a účinné řešení ochrany internetového provozu

Webwasher SME250 je ekonomické snadno nasaditelné bezpečnostní řešení umožňující efektivně řídit a kontrolovat obsah hlavních typů internetového provozu. Je určen pro společnosti do 1000 uživatelů, které chrání na vstupu do sítě (typicky za firewallem). Je postaven na kvalitním hardwaru, zabezpečném operačním systému a 4 softwarových modulech, kterými jsou: **URL filtrace, Anti-Malware** (viry, červy, spyware, trojské koně…), **Anti-Spam a SSL Scanner**. Díky synergii těchto nástrojů představuje tu nejúčinnější ochranu před známými i neznámými typy útoků a hrozeb (ověřeno nezávislými testy viz 2. strana), kterou doplňuje napojení na systém globální inteligence **TrustedSource** spravující nejrozsáhlejší databázi subjektů na internetu a jejich reputace!

Hlavní přínosy Webwasher® SME250:

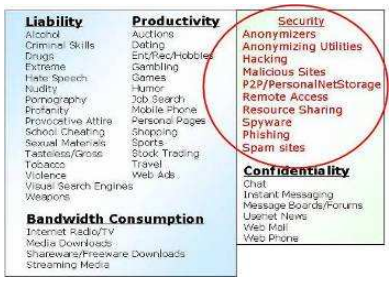
- ✓ Řízení využívání Internetu zaměstnanci automatizovanou URL filtrací
- ✓ Ochrana HTTP, HTTPS, SMTP, FTP
- ✓ **SecureCache a DNS Cache** - zabezpečená cache s optimalizací pro vysoký výkon
- ✓ Lokální analýzy doplňuje nejnověji technologie založená na reputaci - **propojení se systémem globální inteligence TrustedSource**
- ✓ **Ekonomicky výhodné řešení**: „balíček" zahrnuje hardware,



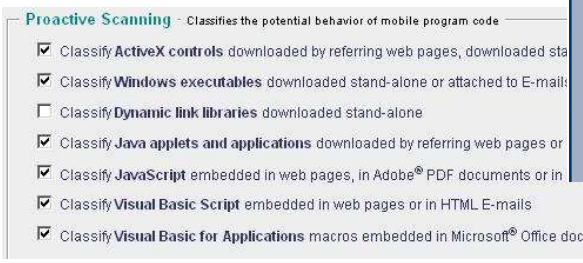
Specifikace modulů a jejich funkcí:

WEB Cache	▪ Unikátní řešení web cache s ohledem na bezpečnost v dnešním Web 2.0 prostředí. SecureCache™ využívá revoluční technologie podrobující skladované objekty proaktivní kontrole a testům reputace z hlediska bezpečnosti dříve, než jsou doručeny koncovým uživatelům.
URL Filtering	▪ Nejnovější generace URL filtrace je napojená na inteligentní globální reputační databázi TrustedSource ▪ Denně aktualizovaná databáze kategorizovaných stránek SmartFilter® ▪ **Zvyšuje produktivitu, snižuje spotřebu konektivity, zabezpečuje před zneužitím dat uživatelů**. Přehledný reporting v ceně řešení.
Anti-Malware (viry, červy, spyware a jiné škodlivé kódy)	▪ Okamžitá ochrana proti všem druhům škodlivých kódů pro web a email provoz (Vítěz testů – viz. 2. strana) ▪ Proaktivní filtrační metody poskytují ochranu i před neznámými hrozbami zahrnující kombinované útoky, spyware, trojské koně, viry, červy či útoky v čase nula ▪ Přesná detekce založená na signaturách odhalující známé typy útoků
Únik citlivých dat	▪ Komplexní vynucení bezpečnostní politiky organizace ▪ Naplňuje cíle bezpečnostní politiky ochrany citlivých dat
Anti-Spam	▪ Napojení na globální inteligenci TrustedSource přinášející nejúčinnější ochranu proti spammerským zombie PC ▪ Prevence v boji proti infiltraci škodlivých kódů ▪ Odstranění čas konzumující nevyžádané pošty
SSL Scanning	▪ Dočasně dešifruje SSL provoz a umožňuje tak uplatnění kontroly obsahu na přítomnost nežádoucích kódů ▪ Uplatnitelné na odchozí i příchozí provoz ▪ Centrální správa certifikátů ▪ Provoz je po dešifraci a kontrole opět šifrován a odeslán na cílovou destinaci

Webwasher® URL Filter je tvořen důmyslnými nástroji opírající se o databázi kategorizovaných URL SmartFilter a reputačního systému TrustedSource. Účinně chrání uživatele před vstupem na nebezpečné webové stránky a tím se stává preventivním nástrojem v boji proti malware. Jako nástroj personálního řízení umožňuje omezit plýtvání časem a produktivitou zaměstnanců, chrání před vstupem nelegálních dat do vnitřní sítě a napomáhá šetřit internetovou konektivitu. Vše je podporováno sofistikovaným reportovacím nástrojem SmartReporter, který poskytuje detailní a přitom snadno dosažitelné informace o využívání webu.



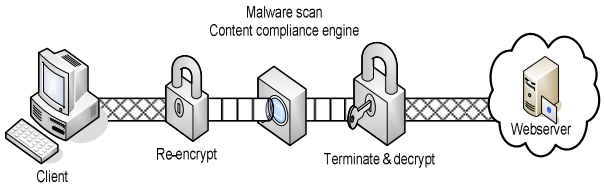
Webwasher® Anti Malware Protection je modul využívající signatury spolu s proaktivní ochranou, který dokáže chránit příchozí i odchozí provoz před všemi druhy známých i neznámých útoků a malware. Kombinuje v sobě přínosy globální inteligence TrustedSource a analytické nástroje schopné vyhodnocovat nestandardní a nebezpečné chování způsobené útočícími kódy. Ochrany jsou doplněny o pravidelné aktualizace databáze pravidel reprezentujících nejčastější postupy hackerů vzhledem ke zveřejněným zranitelnostem. Tímto způsobem umí ochránit všechny důležité typy provozu jako jsou http, smtp, ftp a dokonce i https, jelikož je v součinnosti s modulem Webwasher® SSL Scanner. Navíc obsahuje nástroje schopné bránit ztrátě informací zapříčiněné vlastními uživateli.



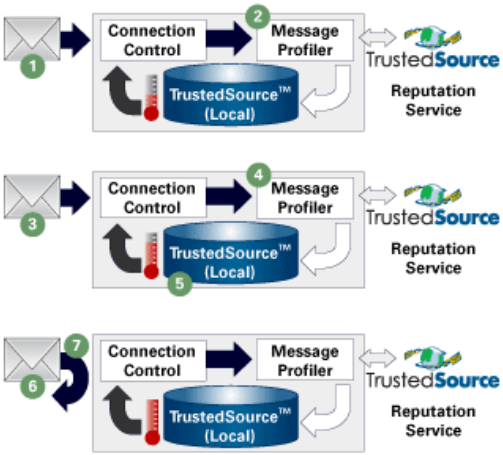
RANKED RESULTS		
#1	Webwasher	99.97%
#2	AntiVir	99.95%
#3	AVK 2007	99.95%
#4	AVK 2006	99.89%
#5	Symantec	99.04%
#6	Kaspersky	98.86%
#7	F-Secure	98.24%
#8	BitDefender	96.51%
#9	Norman	96.34%
#10	Nod32	95.80%
#11	Avast!	95.17%
#12	AVG	94.78%
#13	Fortinet	94.65%

AV-Test Labs 10/06 300 tis. vzorků

Webwasher® SSL Scanner vyplňuje vážný nedostatek v IT obraně společností tak, že kontroluje šifrovaný komunikační přístup do vnitřní sítě a zabraňuje tak průniku hackerům, virům a dalšímu škodlivému obsahu skrytému v SSL. Webwasher SSL Scanner umožňuje společnostem aplikaci jejich stávajících bezpečnostních postupů a pravidel o užívání Internetu na všechny klíčové webové protokoly: HTTP, FTP a HTTPS.



Webwasher® AntiSpam je založen na unikátní technologii MethodMix™ slučující v sobě četné identifikační metody, které odhalují nevyžádanou poštu s téměř 100% přesností a minimální chybovostí. Velkou předností je spolupráce **s TrustedSource**, díky které je schopen identifikovat maily odeslané spammerskými zombie PC a URL databází SmartFilter. Umožňuje administrátorům vytvářet vícero „front“, díky kterým jsou legitimní maily odbavovány přednostně takřka bez prodlení a teprve poté jsou uplatněny všechny metody hodnocení zpráv na podezřelou poštu.



Connection Control - využití databáze TrustedSource™

1. zpráva přichází z IP “bob.spammer.net”
2. Message Profiler skenuje zprávu a rozhodne o blokaci. TrustedSource™ (lokální i globální databáze) se aktualizuje.
3. další zprávy přichází z “bob.spammer.net”
4. Message Profiler skenuje zprávu a rozhodne o blokaci.
5. TrustedSource™ (lokální i globální databáze) se aktualizuje a je dosažena prahová hodnota pro odmítnutí spojení.
6. další zprávy přichází “bob.spammer.net”
7. Connection Control odmítá spojení. Mail server není zatěžován analýzou, zpráva není vůbec přijata.

Po předem definované době je proveden reset blokace a proces se opakuje

INFORMUJTE SE NA ENTERPRISE MODELOVÉ ŘADY PRO AŽ 40.000 UŽIVATELŮ S INTEGROVANOU WEB CACHE

Secure Firewall - **Sidewinder**

kompaktní, výkonné a nejbezpečnější řešení na trhu!

SECURE COMPUTING
Sidewinder
Network Gateway Security

SECURE COMPUTING
TrustedSource
Global Intelligence

REFERENCE:

USA: US Bank, Federal Reserve Bank, Goldman Sachs, Amgen, Anheuser-Busch, Bank of Missouri, New York Stock Exchange, Securities Exchange Commission, Solomon Smith Barney, Lockhead Martin, Aetna Insurance, Fortis Insurance, United Airlines,…

USA Government: GAO, DFAS, CIA, NSA, FBI, USAF, US Army, US Navy, SPAWAR,…

International: Credit-Suisse-First-Boston, Deutsche Bank, National bank of Slovakia, Sanwa Bank, Safra Bank, Banamex, Redbank, Australian DoD, China Ministry, NEC, Japan government, Schröders, France Telecom, Alcatel, Cap Gemini E&Y, World Health Organization, Q8 Petroleum, Parker Hannifin,

Společnost Secure Computing se specializuje na bezpečnost sítí více než 20 let. UTM Firewall Sidewinder® konsoliduje do jednoho systému všechny hlavní funkce pro zabezpečení internetového provozu. V současnosti patří vůbec k nejbezpečnějším řešením na trhu díky unikátnímu souboru technologií „Zero-hour Attack Protections (ZAP™)". Chrání sítě i aplikace před známými i neznámými hrozbami díky integrovaným ochranám proti narušení (IPS), virům, spywaru, spamu, phishingu a jiným zákeřným kódům. Sidewinder také chrání organizace před riziky spojenými s využíváním internetu zaměstnanci a bezpečně rozšiřuje možnosti vzdáleného přístupu pro zaměstnance, partnery a zákazníky přes VPN služby a řízený přístup. Součástí je i napojení na globální inteligenci TrustedSource.

Hlavní přednosti **UTM** řešení **Sidewinder®** Security Appliance:

- ✓ **Split server ochrany** přímo na firewallu: Secure MAIL, DNS, aj.
- ✓ **TrustedSource antispam ochrany v ceně řešení!**
- ✓ **Volitelný antivirus a antispyware modul** (http, ftp i smtp)*
- ✓ **URL filtrace SmartFilter** - automatické řízení web přístupů zaměstnanců
- ✓ Integrované plnohodnotné **IPS** s reakcemi Strikeback®

- ✓ **Ochrana VoIP** provozu aplikačními proxy pro SIP a H.323
- ✓ **47x Aplikační proxy** i stavová inspekce – filtrování od 3. do 7. vrstvy OSI
- ✓ Zero-hour Attack Protections (ZAP™) včetně detekce anomálií a událostí
- ✓ QoS a filtrování internetového spojení (URL, IM, P2P, ActiveX, Java)
- ✓ IPSec VPN s NAT-T a autentizací pomocí jednorázových hesel

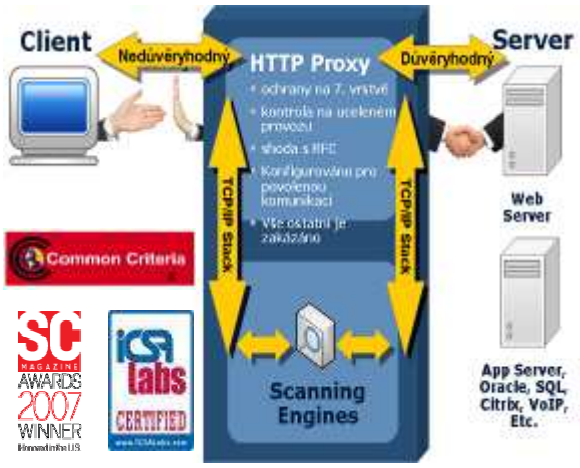
- ✓ Virtuální „black hole" technologie odrazující útočníky
- ✓ Skrytí vnitřní sítě (network cloaking)
- ✓ Jediný firewall na trhu bez „emergency security patch"

- ✓ Cluster management (active/active nebo active/standby)
- ✓ Centrální řízení stovek appliancí pomocí Command Centre™
- ✓ Propustnost až 2,25 Gbps pro aplikační kontroly, podpora VLAN
- ✓ Jednotná hardwarová platforma s 3 letou zárukou a servisem u zákazníka

** žádný z modulů není postaven na open source, garance vysoké kvality*

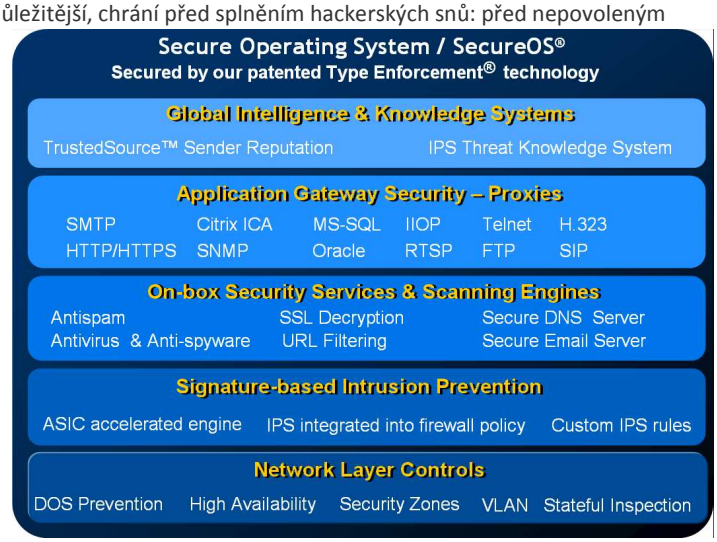
Obrany aplikačními proxy a zabezpečenými split servery

Při použití aplikační proxy brány neexistuje žádné přímé spojení mezi interní (chráněnou) sítí a Internetem. Aplikační proxy na straně do interní sítě vystupují jako server. Převezmou požadavek, na aplikační úrovni jej překontrolují a (nyní jako klient) zahájí komunikaci se skutečným serverem na Internetu. To umožňuje nejen ochranu IP stacku chráněných zařízení, ale zejména jemnější řízení datového provozu – možnosti zadávání specifických pravidel. Navíc je možné přímo na firewallu provozovat serverové služby typu SMTP (sendmail), DNS a to navíc ve split módu a zajistit tak maximální ochranu serverů ve vnitřní síti / DMZ.



Jádro systému, integrovaný SecureOS®

Technologie Type Enforcement (TE) je mechanismus povinné kontroly přístupu. V zásadě jde o striktní uplatnění **mandatory access control**, tedy aplikace běžící v systému mají striktně definovaný přístup ke konkrétním zdrojům v systému, bez ohledu na běžná unixová oprávnění a bez ohledu na to, zda je vlastníkem superuživatel (root) či nikoliv. TE chrání řízení periferních jednotek, jádro operačního systému, operační systém jako takový a co je nejdůležitější, chrání před splněním hackerských snů: před nepovoleným přístupem ke zdrojům (root access). Technologie znemožňuje útočníkovi zneužít jedné služby k tomu, aby se dostal k další, zabraňuje instalaci zlomyslného softwaru, spustit jakýkoliv úspěšný útok, jehož výsledkem je přeplnění vyrovnávací paměti (Buffer overflow) nebo převzetí a vyřazení systému díky vniknutí do základního přístupu (root access).



Díky technologii Type Enforcement® implementované přímo do jádra OS nemůže žádný hacker Sidewinder využít k tomu, co dělají hackeři nejčastěji, tedy:

- spustit útok na jiné služby,
- změnit bezpečnostní politiku,
- spustit permanentní útok importem nástrojů do firewallu Sidewinder,
- oklamat proxy a servery na firewallu tím, že uživatel vně firemní sítě je na vnitřní straně firewallu.

TrustedSource® - globální bezpečnostní inteligence ve Vašich službách

TrustedSource je engin korelující v celosvětovém měřítku hrozby v prostředí internetu. V rámci své inteligentní databáze zpracovává informace o globálním vývoji emailové komunikace, webového provozu a obecně škodlivých kódech. Zaznamenává komunikační chování jednotlivých subjektů (přiřazuje jim reputaci), objem odeslaných zpráv, trendy v komunikaci apod. Informace pak zpětně využívají bezpečnostní brány Secure Computingu, které mohou odmítat spojení se zombie PC/spammary (subjekty se špatnou reputací) bez využití vlastního výpočetního výkonu! (www.trustedsource.org.)

Modelová řada „D“ verze 7:

modely 4150 a RM700 na vyžádání

						
Model	**110D** mini 1U	**210D** mini 1U	**410D** small 1U	**510D** small 1U	**1100D** enterprise 1U	**2150D** 2U
Ethernet rozhraní základ/max/ (opt)	4 -10/100	4 -10/100	4/6 - 10/100 (4)	4/6 Gigabit (4)	8/14 Gigabit (4)	8/20 Gigabit (6)
Počet uživatelů	Neomezen	Neomezen	Neomezen	Neomezen	Neomezen	Neomezen
Doporučený počet uživatelů	Menší firma do 75 uživatelů	Menší firma do 150 uživatelů	Střední firma do 300 uživatelů	Střední firma do 600 uživatelů	Střední/velká společnost	Velká společnost
Maximum odchozích IP adres	100	200	400	700	Unlimited	Unlimited
Počet modulů aplikačních ochran	1 (max 3)	2 (max 3)	1 (max 3)	2 (max 3)	2 (max 4)	2 (max 4)
HW upgrady	2 možnosti	1 možnost	2 možnosti	1 možnost	1 možnost	1 možnost
RAID	N/A	N/A	N/A	N/A	RAID 1	RAID 5
Napájecí zdroj	jeden	jeden	jeden	jeden	jeden/volitelně i redundantní	redundantní
Propustnost pro paketovou filtraci (TCP)	150 Mbps	180 Mbps	275 Mbps	650 Mbps	1.6 Gbps	2.6 Gbps
Současná spojení	10,000 +	50,000	100,000	500,000	1,000,000	1,600,000
Propustnost při aplikační kontrole	100 Mbps	140 Mbps	230 Mbps	250 Mbps	1.2 Gbps	1.8 Gbps
IPSec AES propustnost/ spojení	60 Mbps/75	80 Mbps/125	160 Mbps/200	160 Mbps/250	240 Mbps/350	350 Mbps/500

SECURE COMPUTING
SafeWord
Identity and Access Management

PODPOROVANÉ TOKENY, USB KLÍČE A SMARTCARTS:
Safeword Silver, Gold, Platinum a Alpine Token Enterprise Solution Pack navíc: SoftToken a MobilPass; Aladdin eToken R2 a Pro: Datakey SignaSure Models 320 a 330, Gemplus: GPK 8000, IBM Embedded Security Subsystem na ThinkPad, Rainbow iKey 1000, 2000, Rockey (Feitian) ePass1000, Axalto: Cryptoflex a Cyberflex, Sony: FIU-710 Fingerprint Identification Unit ("Puppy")

REFERENCE:
Citibank (600.000 už.) **Boeing** (80.000 uživatelů) **American Express** (60.000) **Sun Microsystems** (30.000) **CISCO Systems** (40.000) **Sony**, **Sharp**, **BNP Paribas**, **Alcatel** a další

SC MAGAZINE AWARDS

Secure **SafeWord**

flexibilní systém řízení identity a přístupu uživatelů

„AAA" (Authentication + Authorization + Accounting) systém **SafeWord 2008** od společnosti Secure Computing chrání a centrálně řídí přístup uživatelů k informačním aktivům a aplikacím organizace. Uživatelé jsou zbaveni frustrace způsobené pamatováním si složitých hesel a jejich častou obměnou, jelikož jim bezpečná (silná) jednorázová hesla pro přihlášení do všech důležitých aplikací a systémů generuje např. token pověšený na klíčence, nebo aplikace na mobilním telefonu. Systém je vytvořen pro snadnou integraci do prostředí Microsoft a poskytuje dvoufaktorovou autentizaci pro různé VPN, Citrix, Web aplikace, Webmail a Outlook Web Access.

Hlavní přínosy:

- ✓ **Správa uživatelů** přes Active Directory nebo vlastní integrovaná databáze
- ✓ Autentizace pro **Windows Login ***
- ✓ Autentizace pro **terminálové služby a remote desktop ***
- ✓ **Podpora autentizace do všech IPSec VPN kompatibilních s RADIUS autentizací** (VPN brány Sidewinder, SnapGear, Alcatel, CISCO, CheckPoint, aj.**)**
- ✓ Autentizace do SSL VPN a **vlastní SSL VPN gateway SecureWire**
- ✓ Autentizace do **CITRIX** aplikací a **Outlook Web Access**
- ✓ Autentizace do **Wireless LAN**
- ✓ **Universal Web Agent pro Web based aplikace ***
- ✓ **SDK** pro propojení se specifickými systémy *****
- ✓ Generování jednorázových hesel **neexpirujícími tokeny** s Life Time Warranty
- ✓ Generování jednorázových hesel na mobilním telefonu - **MobilPass ***

* Škálovatelné řešení na míru Vašich potřeb.

SafeWord 2008 je možné pořídit ve dvou funkčně odlišných verzích. Základ tvoří systém pro zabezpečení přístupu vzdálených uživatelů přes VPN, který je možné rozšířit o komplexní „AAA" řešení, tzv. Enterprise Solution Pack (ESP). *Další informace naleznete na druhé straně.*

SafeWord 2008 - nejlepší řešení pro prostředí Microsoft

SafeWord 2008 je vytvořen pro **Windows 2008**, nicméně umožňuje využít jak 32-bitové, tak 64-bitové Windows operační systémy, vč. Vista, Windows 2008 Server, Windows 2003 a XP. Dvoufaktorová autentizace SafeWord 2008 je do tohoto prostředí plně integrována (Active Directory) a připravena řídit identitu, bezpečnost přístupů a efektivní fungování organizace.

Token nebo mobilní telefon – volba je na Vás

SafeWord neexpirující token s doživotní zárukou generuje po zmačknutí tlačítka jednorázové unikátní heslo, které nemůže být za žádných okolností znovu použito. Odpadá tedy hrozba jeho kompromitace, či zneužití hackery. Dvoufaktorová autentizace zároveň zabraňuje zneužití tokenu samotného, jelikož výsledné „heslo“ se vždy skládá z krátkého řetězce, který si uživatel pamatuje a z části, kterou generuje token. Využití mobilního tokenu je naprosto identické, přičemž má uživatel o jednu starost s nošením tokenu míň. Podporovány jsou BlackBerry, Windows Mobile, Palm, nebo telefony podporující J2ME.

Nadstavbové řešení ESP navíc mimo jiné obsahuje:

- ✓ Volitelná správa uživatelů přes Active Directory nebo **vlastní SafeWord databázi**
- ✓ Universal web agent pro autentizaci přístupů na web servery
- ✓ Agenty pro Oracle, UNIX a další systémy
- ✓ MobilePass – podpora generování hesel na mobilních telefonech
- ✓ Generováni X.509 certifikátů
- ✓ Role-based autentizace a řízení přístupových práv (autorizace)
- ✓ Rozšířené reportovaní nástroje
- ✓ SafeWord RADIUS server
- ✓ Dostupné SDK pro propojení se specifickými systémy

SECURE COMPUTING SafeWord Identity and Access Management	Základní verze	Rozšíření o „Enterprise Solution Pack“
Identifikuje uživatele pro tyto přístupové metody	VPN (IPSec/SSL) Citrix rozhraní webové aplikace RADIUS kompatibilní systémy Outlook Web Access	VPN (IPSec/SSL), Citrix rozhraní webové aplikace, RADIUS kompatibilní systémy, Outlook Web Access, Windows login, terminálové služby/Citrix, všechny webové servery, všechny webové aplikace, UNIX login, vlastní aplikace, SafeWord SecureWire
Podporované autentikátory	SafeWord Alpine token	SafeWord Alpine token SofToken II MobilePass – mobilní telefony BlackBerry, Palm, Win Mobile, J2ME enabled, Windows Desktop) Digitální certifikáty
Podporované autentikátory třetích stran	Žádný	Digitální certifikáty USB tokeny Smart cards
Úložiště uživatelských účtů	Active Directory	Active Directory nebo integrovaná vlastní databáze uživatelů (ESP pack)
Správa uživatelů	Skrze Active Directory plug-in	Skrze Active Directory plug-in nebo v rámci vlastní konsole SafeWord
Reportování	Vlastní nástroje AD/ MS Windows	Vlastní nástroje AD/ MS Windows + pokročilé reportovací nástroje SafeWord (uživatelské i administrační)
Autorizace založená na rolích	Skrze vlastní Active Directory mechanizmy	Skrze vlastní Active Directory mechanizmy nebo integrované SafeWord role a ACL
Automatické přihlášení uživatele	Integrováno, jednoduché uživatelské centrum	Integrováno, jednoduché uživatelské centrum, nebo pokročilý server pro správu uživatelů
SDK-Softwarové nástroje pro vlastní aplikace	Žádný	Autentizace Administrace SofToken

Secure Mail - **IronMail**

moderní bezpečnostní brána pro poštovní provoz

IronMail
Messaging Gateway Security

SECURE COMPUTING
TrustedSource
Global Intelligence

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

„BEST BUY“
http://www.scmagazineus.com/Secure-Computing-IronMail/Review/532/

Common Criteria Certified

Několikaúrovňová DETEKCE **SPAMU:**

- **Whitelisty**
- **Blacklisty**
- **Analýza obsahu**
- **Spam signatury**
- **Adaptivní analýza obsahu**
- **Spam URL detekce**
- **Analýza hlaviček**
- **Detekce falzifikátů**
- **Detekce hromadných zpráv**
- **Engin pro detekci**

Společnost Secure Computing již více než 20 let ochraňuje ty nejcitlivější sítě (FBI, CIA, NSA, …) a řeší bezpečnostní problémy mnoha významných společností a institucí po celém světě. IronMail, chránící poštovní provoz, užívá více než 40 % společností z Fortune 500, přičemž toto sofistikované řešení ve formě appliance je nyní dostupné jak pro velké, tak i menší společnosti.

Hlavní přínosy:

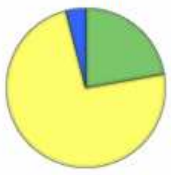
- ✓ **Email anti-spam & phishing / anti-virus & spyware / IPS / firewall**
- ✓ **TrustedSource** - globální inteligence - blokování Zombie PC a spammerů
- ✓ **Dynamická karanténa** pro podezřelé zprávy napojená na TrustedSource
- ✓ **Proaktivní i reaktivní ochrana pošty** před viry, trojany, červy, DoS útoky, directory harvests útoky, phishingem, spamem, botnety (**Zombie PC**), spyware a nevhodným obsahem v jednom řešení!
- ✓ **Chrání a řídí příchozí i odchozí provoz**
- ✓ **Blokuje útoky** dříve, než mohou zasáhnout emailové servery
- ✓ **DLP – ochrana před únikem informací**
- ✓ **Šifrování zpráv -** gateway to gateway bez příplatku
- ✓ **Škálovatelné řešení** / vysoký výkon / připraveno pro růst potřeb společnosti
- ✓ **Řešení na klíč** - forma appliance - HW & SW v jednom - SW není třeba instalovat.

TrustedSource® - globální bezpečnostní inteligence

IronMail je založen na mnoha navzájem provázaných technologiích, které navazují na globální inteligenci TrustedSource Reputation Service. Jedná se o řešení korelující v celosvětovém měřítku hrozby v prostředí internetu. V rámci své inteligentní databáze zpracovává informace o globálním vývoji emailové komunikace, webového provozu a obecně škodlivých kódech. Zaznamenává komunikační chování jednotlivých subjektů (přiřazuje jim reputaci), objem odeslaných zpráv, trendy v komunikaci apod. Informace pak zpětně využívají bezpečnostní brány Secure Computingu, které mohou odmítat spojení se zombie PC / spammery (subjekty se špatnou reputací) bez využití vlastního výpočetního výkonu! (www.trustedsource.org.)

Executive Summary

Inbound



	Good	Spam	Virus	Policy	Total
Count	3,366	10,923	6	598	14,893
Percent	22.6%	73.3%	0.0%	4.0%	100.0%
Count	1,226	0	0	17	1,243
Percent	98.6%	0.0%	0.0%	1.4%	100.0%

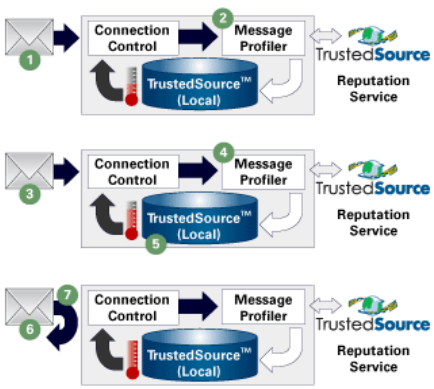
Outbound

Queue Status Current

Queue Name	Enabled	Running	In Queue	No Action Taken	Action Taken
Internal Queue - MIME Ripper	✓	●	8	16137	35
Internal Queue - Content Extraction	✓	●	8	16129	0
Super Queue	✓	●	0	N/A	N/A
Queue - Virus Scan	✓	●	0 (0%)	16120 (100%)	6 (0%)
Queue - Mail Monitoring	✓	●	0 (0%)	15542 (100%)	13 (0%)
Queue - Content Filtering	✓	●	0 (0%)	13823 (89%)	1723 (11%)
Queue - Anti-Spam	✓	●	0 (0%)	3390 (22%)	12133 (78%)
Queue - Corporate Compliance	!	N/A	0 (0%)	0 (0%)	0 (0%)
Internal Queue - MIME Joining	✓	●	1	4623	0

Connection Control - využití databáze TrustedSource™

1. zpráva přichází z IP “bob.spammer.net”
2. Message Profiler skenuje zprávu a rozhodne o blokaci. TrustedSource™ (lokální i globální databáze) se aktualizuje.
3. další zprávy přichází z “bob.spammer.net”
4. Message Profiler skenuje zprávu a rozhodne o blokaci.
5. TrustedSource™ (lokální i globální databáze) se aktualizuje a je dosažena prahová hodnota pro odmítnutí spojení.
6. další zprávy přichází “bob.spammer.net”
7. Connection Control odmítá spojení. Mail server není zatěžován analýzou, zpráva není vůbec přijata.



Po předem definované době je proveden reset blokace a proces se opakuje.

Outbreak Defender™ - rozšiřuje schopnost reakce antiviru na základě signatur a filtrování příloh o ochranu tzv. okna zranitelnosti. Řeší tak bezpečnost i v období od vzniku nového útoku po aktualizaci virové databáze o jeho signaturu. K tomu využívá informace z TrustedSource a vlastní proaktivní mechanizmy. Zároveň chrání reputaci firmy tím, že nepropustí vně útoky vzniklé ve vlastní LAN.

Email Firewall & IPS - IronMail je účelové zařízení se zabezpečeným OS schopným reagovat na útoky typu buffer overflow, denial-of-service, directory harvest, protocol attacks či port scans. Chrání před zlomyslnými kódy a neautorizovanými spojeními využitím znalosti chování, vynucováním dodržení protokolu a **nepřetržitými aktualizacemi signatur** známých útoků.

Secure Web mail - přístup pro mobilní uživatele - Modul Secure Web mail dovoluje bezpečně přistupovat mobilním uživatelům na poštu odkudkoli z jakéhokoli prohlížeče a to bez omezení, jaké skýtá klasické spojení formou VPN. Spolupracuje s Microsoft Outlook Web Access, Lotus Domino Web Access a Novell GroupWise Web Access.

Transparentní šifrování založené na pravidlech - IronMail nabízí díky integraci kryptografie několik možností, jak chránit poštu šifrováním. Zároveň je díky principu přednastavených pravidel vůči koncovým uživatelům zcela transparentní.

⇒ Business-to-Business: IronMail šifruje zprávy mezi branami užitím standardu TLS, S/MIME a OpenPGP.

⇒ Business-to-Consumer: IronMail dovoluje příjemcům bez šifrovacích nástrojů přijímat poštu přes zabezpečené webové rozhraní.

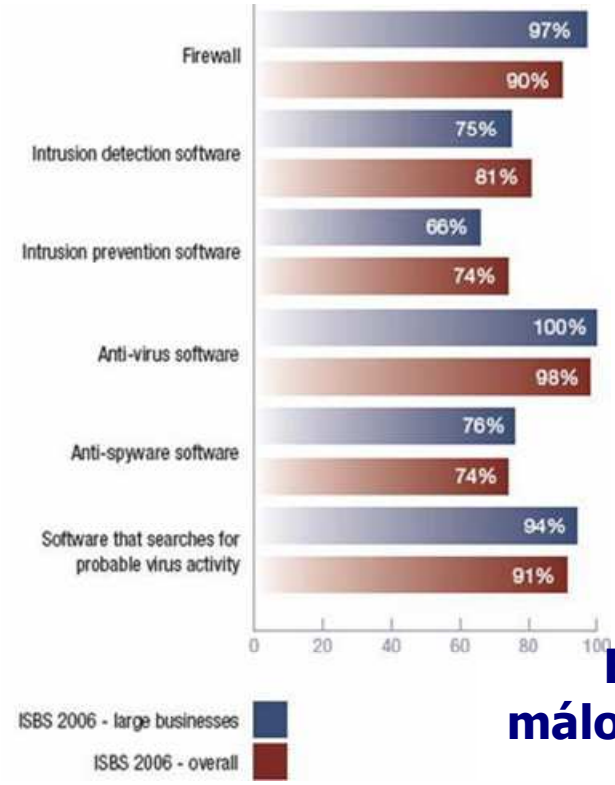
Bezpečnostní standardy a ochrana citlivých dat - Užitím nástrojů pro detekci citlivých dat a obsahu je zajištěna shoda se standardy (HIPAA, SOX, GLBA, …) a tím i bezpečnost firemní komunikace. K tomu, aby se vně firmy nedostaly důvěrné informace se zprávy filtrují dle obsahu, opatřují se „otisky“, jsou zkoumány statistickými metodami určujícími jejich význam dle podobnosti s dokumenty v databázi apod.

Obrázkový spam - Důležité také je, aby se společnost chránila před šířením nevhodných dokumentů a obrázků ve vlastní síti. Funkce **„Image analysis“** dokáže na základě precizně vyvíjených metod detekce kompozice (ne pouze dle procentuálních analýz) **rozpoznávat obrázky** v přílohách emailů. Odpadá tak obava o šíření nemravných obrázků zabírajících cenné místo na pevných discích.

		E-Class		S-Class	
IronMail	**Model**	**E5200**	**E2200**	**S120**	**S10**
Základní specifikace	**Předpokládaný počet uživatelů**	Neomezeno	Neomezeno	< 1000	< 100
	Počet procesorů	2x Quad Core Xeon	Quad Core Xeon	Dual Core Pentium	1
	Dostupné moduly v ceně Email protection	TrustedSource, Anti-Spam, Basic Compliance, Gateway-to-Gateway encryption (TLS, S/MIME and PGP Open), Webmail Protection a Image Analysis.			TrustedSource, Anti-Spam, Basic Compliance
Hardwarové specifikace	**RAID**	Level 5 + Hot spare	Level 1	Level 1	None
	Redundantní el. zdroj	Ano	Ano	Ne	Ne
	Redundantní větrák	Ano	Ano	Ne	Ne
	NIC (Mbps)	10/100/1000 x 4	10/100/1000 x 2	10/100 x 2	10/100 x 2

COMGUARD

Hrozby rostou a jsou více mířeny na aktiva!



97% podniků má firewall
100% podniků má antivirus

ALE hrozby se dnes šíří přes web a ZEJMÉNA prostřednictvím MALWARE

JEN MÁLO organizací má dnes implementovánu proaktivní antimalware ochranu a navíc s kontrolou SSL

Běžná ochrana je dnes jen málo dostačující – web hrozby jsou podceňovány!

COMGUARD

Web 2.0 – je evolucí

Definice z Wikipedie....

Termín **„Web 2.0"** označuje to, co někteří lidé považují za další fázi vývoje webu, včetně jeho architektury a aplikací. Tato další fáze rozvoje webu se vyznačuje následujícími rysy:

změnou hypertextových stránek z izolovaných úložišť informací na zdroje obsahující informace i funkcionalitu – stávají se tak platformou poskytující webové aplikace koncovému uživateli.

sociální fenomén - tvorba a distribuce webového obsahu je dostupná komukoliv, otevřená komunikace, decentralizace autorit, sdílení a znovuvyužití, a „trh jako konverzace"

více organizovaný a roztříděný obsah s propracovanější hyperlinkovou strukturou

zvýšení ekonomické hodnoty webu tak, že přesáhne internetovou horečku na konci devadesátých let

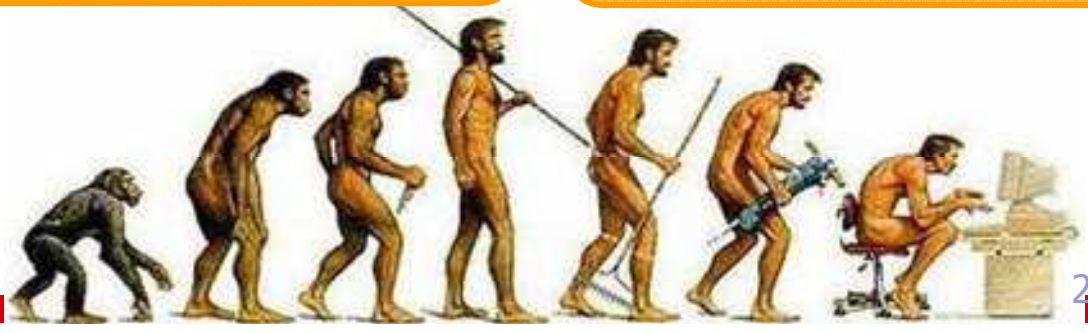
Wikipedia (Defining Web 2.0)

CO Web 2.0 JE:

- Evoluce Internetu, na co dnes používáme web, která je výsledkem dramaticky rostoucích zkušeností uživatelů
- Změna rovnováhy v bezpečnosti: ze serverů na web browsery

CO TO NENÍ:

- Nová verze software web browseru nebo web serveru
- Urychlení pro Internet ☺



1998 2008

Charakteristické vlastnosti prostředí web 2.0

- dynamicky generovaný obsah, spolupráce, sdílení, IM, blogy, mobilita,... (Ajax, Atom, CSS, RSS, XHTML, XML,...)
- na stovkách webů může publikovat kdokoliv, cokoliv
- automatická napadení aktivním obsahem webových stránek, e-mailů,...
  - využívá se sociální inženýrství (odkazy z Wikipedie na malware)
  - neschopnost rychlé reakce uživatelů na nové bezpečnostní hrozby
- aktualizace antivirových programů jsou nedostačující (např.: projekt metasploit)
- podniky jsou ohrožovány nejen riziky plynoucími z úniků firemního „know-how", ale i finančními náklady spojenými s likvidací malware nákaz
- Test AV.TEST lab: 2006 – 300tis vzorků malware, 2008 – 1mil vzorků malware

COMGUARD

The World of Web 1.0

- To co vidíte je to co jste získali!
- příklad Web 1.0 stránek ..

COMGUARD a.s., Vídeňská 119b Brno, Freyova 27 Praha, obchod@comguard.cz, www.comguard.cz

- Ne vždy ***vidíte*** co dostáváte **a** často dostanete o co jste **NEŽÁDALI!**
- Často ***odesíláte*** informace, instalujete aktivní skripty, software bez vaší interakce
- Obsah je „natlačen" uživateli
  - RSS čtečky
  - Personalizované stránky (Seznam.cz, Amazon.com
- Obsah je automatizovaný
  - Javascripts
- Obsah je seskupovaný z více zdrojů
  - Mapy, předpovědi počasí
- Obsah může být „Vytvořen" a „Umístěn"
  - Wikipedia
  - Blogy & Socialní sítě, YouTube, FaceBook
- Další Web Server-Side technologie
  - Nesprávně napsané webové aplikace jsou napadeny malware
  - 1 z 10 legitimních Web site jsou dnes napadeny m

COMGUARD a.s., Vídeňská 119b Brno, Freyova

COMGUARD

Web 2.0 zvyšuje riziko pro váš business

Web 2.0 **Server-Side** technologie umožňují cyber zločincům

- 'Umístit' linky na škodlivý obsah nebo grafické odkazy
- 'Umístit' škodlivý obsah na zranitelné Web stránky

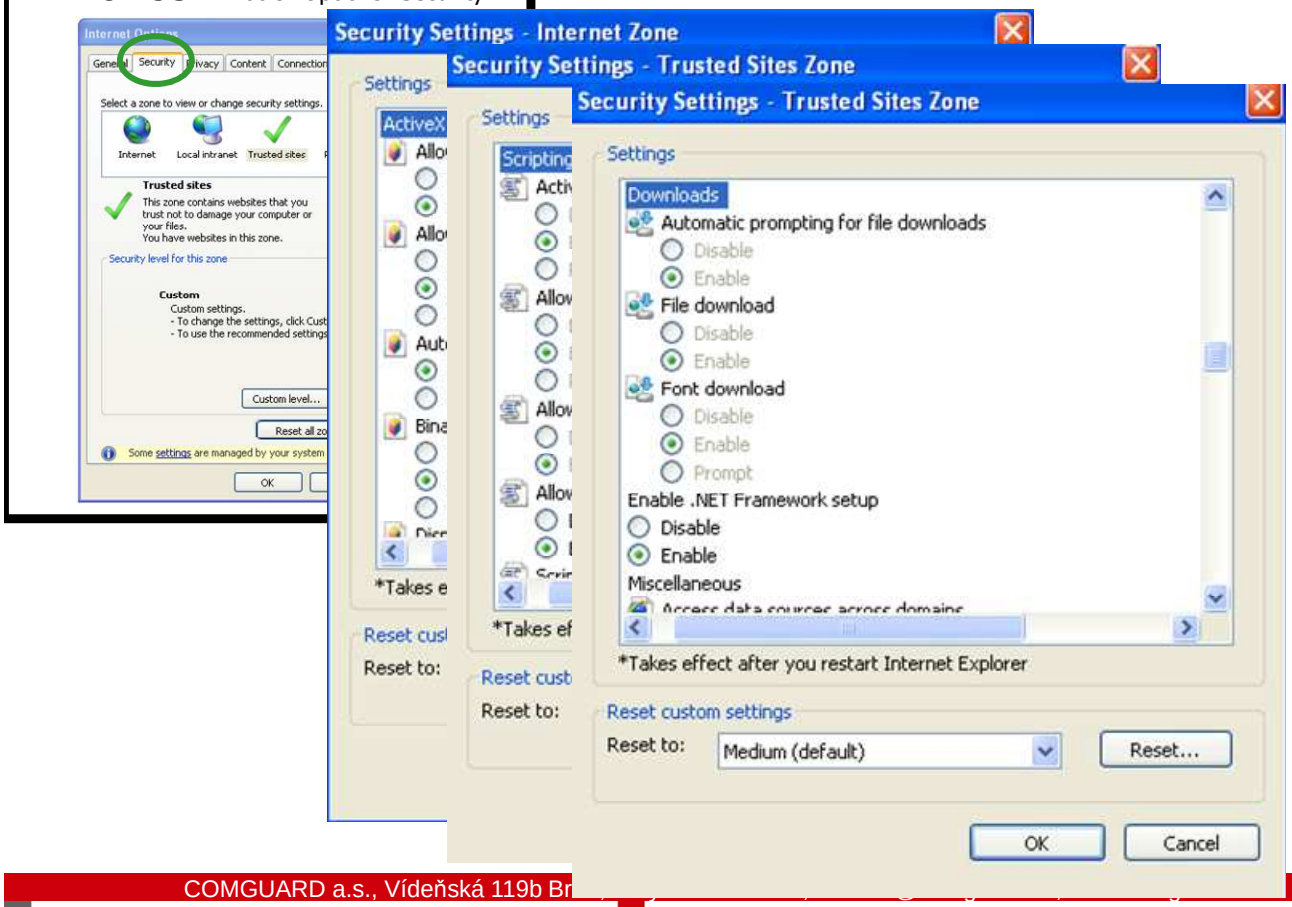
Web 2.0 **Browser** technologie umožňují cyber zločincům

- 'Doručit' škodlivý obsah díky povolení Web 2.0 Push technologií
- 'Automatizovat' doručení škodlivého obsahu díky používání scriptů. (uživatelé dokonce nemusí na nic kliknout)
- Zasílat SPAM/Phishing na soukromé Webmail účty (a obejít tak podnikové antispamy)

COMGUARD

Aplikace zabezpečení Web 2.0 na úrovni browseru

Browser >Tools>Options>Security



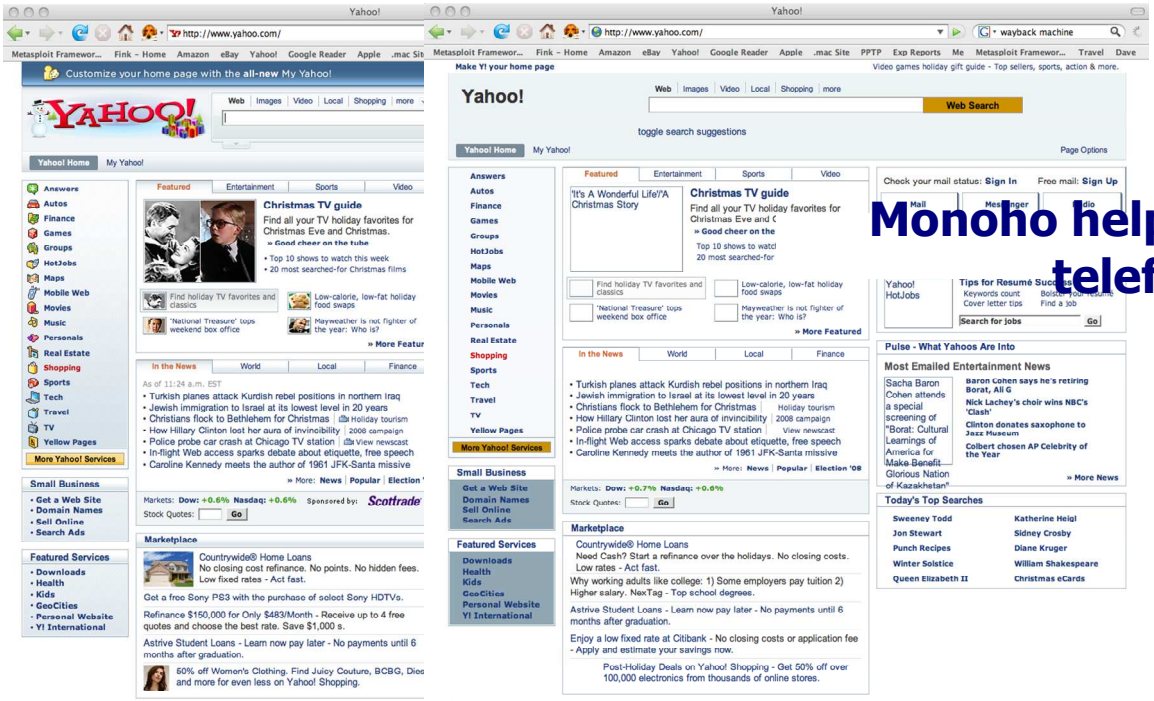
COMGUARD

Jak můžeme redukovat riziko?

- Na straně **Serveru ?**
  - Často zodpovědnost poskytovatele služeb - ne vlastníka webu
  - Ne každý zadavatel či vlastník webu skutečně zkontroluje jak je jeho web zapezpečen nebo bezpečně vytvořen
  - Weby cyber zločinců se nestarají o bezpečnost, sami kontrolují mnoho 'Zombie' Websites nebo email serverů!
  - **Výsledek**: Spoléhat se na to, že web servery aplikují dostatečnou bezpečnost není praktické!
    1 z 10 Webů je dnes infikován a situace se zhoršuje
- Na straně **Browseru ?**
  - ANO, je možné vypnout mnoho Web 2.0 vlastností (např. scripty)
  - ALE to způsobí moderní Web 2.0 Internet nepoužitelným ….

Jaký je výsledek?

- Před a po aplikaci „zabezpečení" na browseru



Monoho help desk telefonátů

SECURE COMPUTING®

Webwasher®

Web Gateway Security

od výrobce secure computing

- **AntiMalware**
- **skenování SSL**
- **Vlastní URL filtr**
- integrace technologie globální inteligence **TrustedSource** založené na reputaci
- **SecureCache** Webwasher Gateway zabezpečená cache

Gartner

Leader kvadrantu

COMGUARD

SECURE WEB – WEBWASHER!
Unikátní modulární systém

WEB PROXY
Secure Cache

Cache pro web provoz a DNS cache.
Unikátní zabezpečená cache - při aktu
opět zkontrolován a není

DOSTUPNÉ JAKO
APPLIANCE/SOFTWAROVÁ VERZE

Trusted Source

Powered By TrustedSource

ntruje až 40%
provozu BEZ ZATÍŽENÍ HW!

Anti Malware

Klasické antivirové signatury obohacené o pokročilé nástroje proaktivních kontrol.
Funkce v aktivním kódu, skriptu jsou analyzovány na nežádoucí aktivity
Odhaluje ve skriptech kódy zneu
Od roku 2006 nenašel přemožitele v

URL-Filter

Denně aktualizovaná on box datab
předdefinované (91+) a vlastní
level reporting.

SSL-Scanner

Dekóduje šifrovaný provoz, pro
firemní bezpečnostní politiky.

Anti Virus

Ultra-rychlá antivirová kontro
scanningu až **2 AV systémy (S**

Anti-Spam

Světová špička v oblasti filtrace
MethodMix™ (7 úrovní).

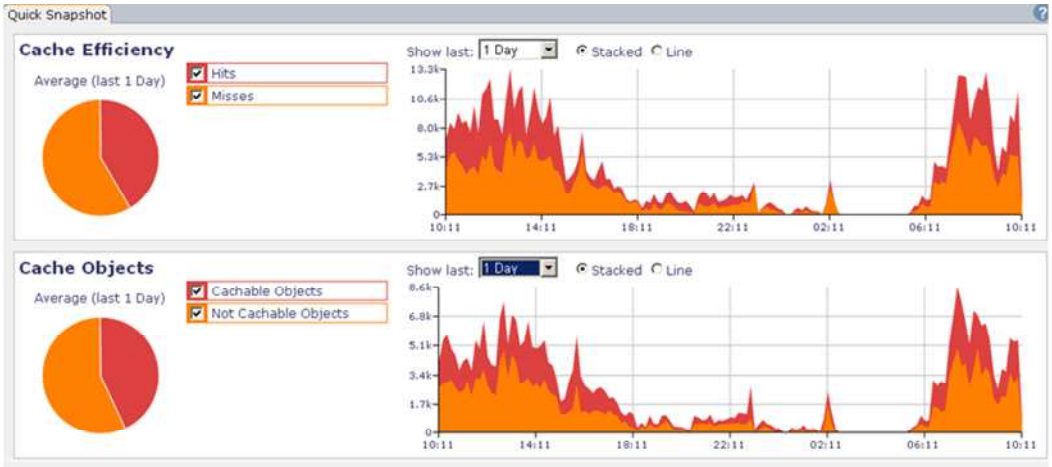
Reportovací nástroj

Enterprise-level reportování W

COMGUARD

Webwasher
Secure Cache

- Webová cache a DNS cache
  - zlepšuje využití pásma a bezpečnost
  - nestahujte obrázky, videa a další multimediální soubory několikanásobně!
  - **Umožňuje provázat politiky proxy s AntiMalware kontrolami a SSL kontrolou.**
  - podporuje podrobné black listy a white listy
  - Nastavení cachování dle politik (on/off, max velikost objektu)



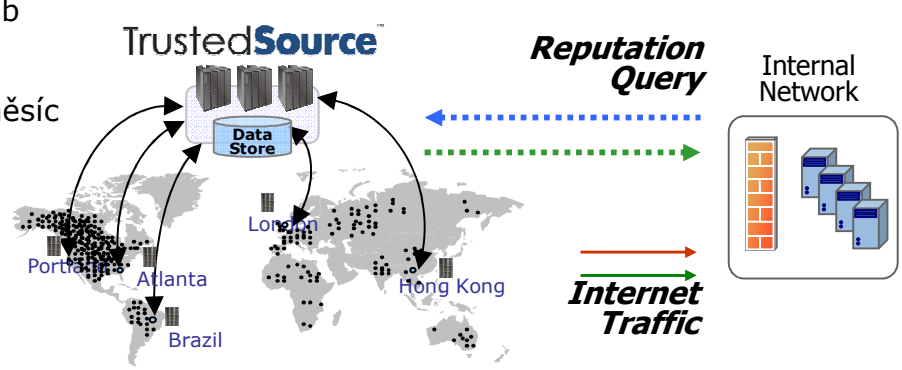
COMGUARD

Globální ochrany na základě reputací systémů

Největší síť globální reputace

- Informace z tisíců sond,load balancerů, FW, Msg & Web gateways
- Vysoká kvalita dat
- Přes 100 miliard zpráv/měsíc
- Milióny URL a IP

www.trustedsource.org
Jak si stojí vaše organizace?



Nejvíce spolehlivé reputation skóre

- 25 výzkumných vědců
- Sofistikovaná analýza chování
- 450,000+ zombies detekováno ka
- Nejlepší sr detectic

COMGUARD

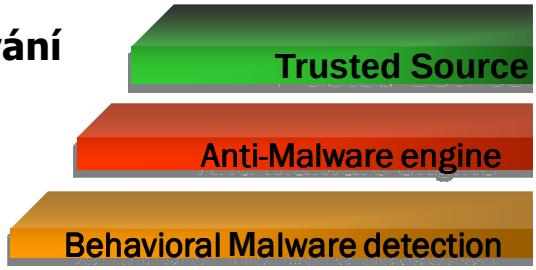
Anti-Malware

Proč Anti-Malware?

- aktualizace Anti-Virových signatur nechávají organizaci vystavenu ohrožení nejen po dobu okna zranitelnosti
- Funkce volané v aktivním kódu nebo skriptu jsou analyzovány na potencionální nežádoucí aktivity
- Odhaluje ve skriptech kódy zneužívající zranitelnosti k zavlečení dalších nežádoucích programů

Vícevrstvý pro-aktivní přístup!

- **Reputace** přidělená **TrustedSource**
- **Signatury Antiviru**
- **Proaktivní vyhodnocení kódu dle chování**
- **Velikost nákazy je irelevantní**
  k možnosti a přesnosti detekce

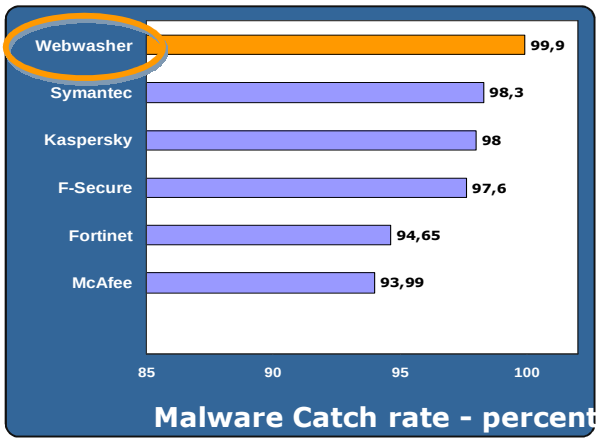


COMGUARD

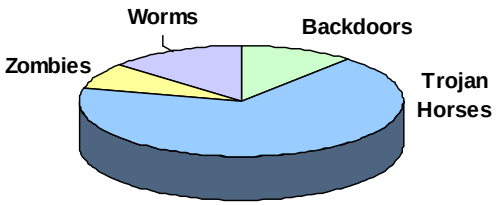
Webwasher® Prověřená kvalita!
Web Gatway Security

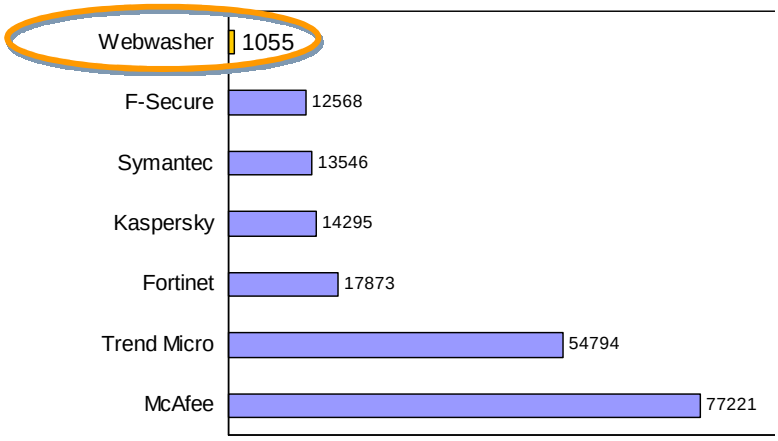
- 01/2008 test AV-Test.org
- **1.024.381** vzorků malware
- **Webwasher - No.1**

2008 AV-Test GmbH, Last Update: 2008-01-22



- 05/2007 test AV-Test.org
- **606.901** vzorků malware
- **Webwasher - No.1**





COMGUARD

URL filtrace

CO PŘINÁŠÍ?

řízení využívání zdrojů Internetu

- posílí kontrolu
- ochrana před spyware, malware z webových stránek,
- zamezí phishingu,
- **produktivita práce**
- šetří šířku pásma
- posílí firemní ku
- TrustedSource

SECURE COMPUTING
TrustedSource™
Global Intelligence

COMGUARD

Webwasher® Web Gatway Security

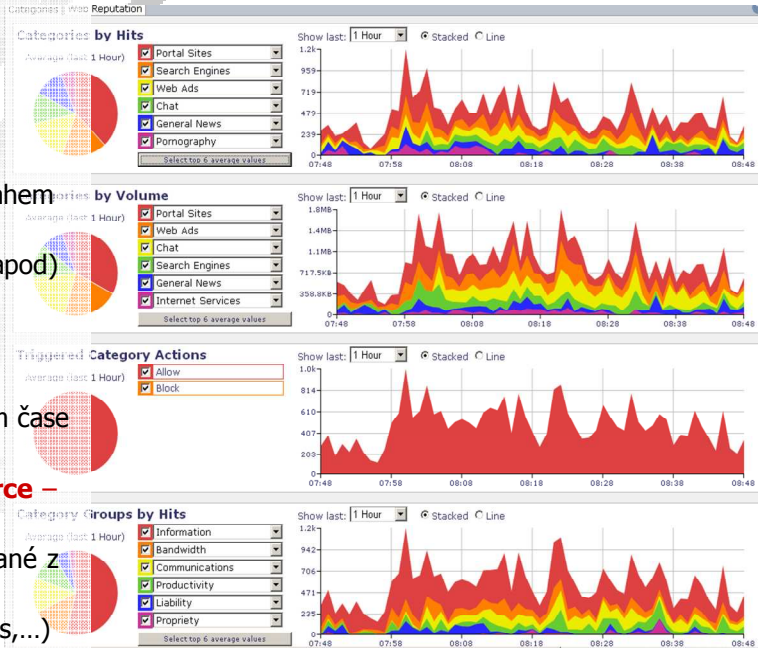
URL-Filtr

- Databáze kategorizovaných URL stránek SmartFilter (> 21 Millionů)
- Více než 90 kategorií

SECURE COMPUTING SmartFilter Web Gateway Security

SECURE COMPUTING TrustedSource Global Intelligence

- Reportovací nástroj v ceně
- Jazyková podpora pro zprávy a hlášení



- Produktivita zaměstnanců
- Chrání zaměstnance před nebezpečným obsahem
- Chrání zaměstnance před nevhodným obsahem
- Šetří internetovou konektivitu (Internetová rádia/TV, stahování souborů dle kategorií apod)

- **Časové a objemové kvóty**,
- Varování před vstupem
- **Real-time Classifier** klasifikuje v reálném čase klíčová slova v HTML kódu
- Napojení na systém reputací **TrustedSource** – lék na nekategorizované stránky hackerů
- Spam a Phishing sites kategorie aktualizované z Trusted Source
- Filtry Reklamy & Soukromí (pop up, cookies,...)

COMGUARD

SSL provoz

Využívají vaši uživatelé https bezpečně?

50% infikovaných stránek šifruje provoz!

- Https není jen o elektronickém bankovnictví
  - Před 5-6 lety bylo znakem přístupů na důvěryhodné zdroje
  - Dnes nabízí většina freemailů ale i warez serverů
  - Stále častěji má šifrování skrýt ***nežádoucí a závadný*** provoz
  - 30% provozu je kompletně šifrováno a ohrožení roste!

- Jak se brání vaše síť?
  - Nepovolujete https provoz mimo důvěryhodné servery (skutečně stále odoláváte „legitimním" požadavkům uživatelů?)
  - Pouštíte https provoz do vnitřní sítě a bojujete uvnitř... (váš antivirus ale nestačí!, jen málo firem má IPS / antimalware systémy na cílových serverech a stanicích kde je provoz dešifrován)
  - **Bojujete s následky nechráněné sítě...**

ELIMINUJE SLEPÉ MÍSTO VAŠICH OCHRAN

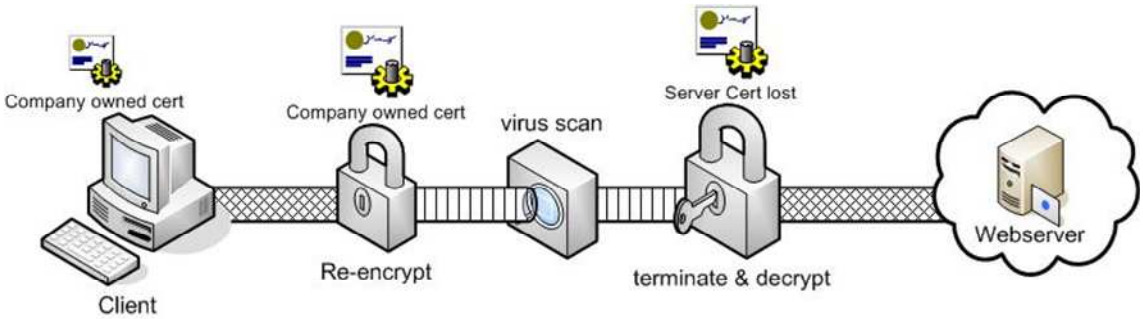
KONTROLUJE ŠIFROVANÝ HTTPS PROVOZ

- **zabraňuje:**
  - průniku hackerů a hackerských kódů v https
  - průniku virů, spyware v souborech přenášených přes https
  - Průniku ostatního škodlivého obsahu skrytého v SSL
  - Úniku citlivých informací (web mail portály apod)

SSL Scanner je HTTPS proxy, která rozdělí spojení mezi prohlížečem a serverem na dvě části. Díky tomu má přístup k rozšifrovanému obsahu spojení.

COMGUARD SSL Skener

- **Plně integrovaný do SCM Webwasher – dešifrovaný obsah není dostupný mimo webwasher engine**
- Umožňuje **centralizovat politiky pro akceptování certifikátů na bráně a kontrolovat platnost a vydavatele!**
- Možno definovat **White list** (tunneling) pro důvěryhodné stránky (ebankovnictví apod) nebo AUTOMATICKY dle URL-Filter kategorií
- „Odkladná lhůta milosti" pro expirované certifikáty
- Podpora pro wildcard-certificates



DLP Gateway protection

Únik citlivých informací z organizace je kritickým faktorem pro reputaci i vznik přímé škody

Webwasher také obsahuje

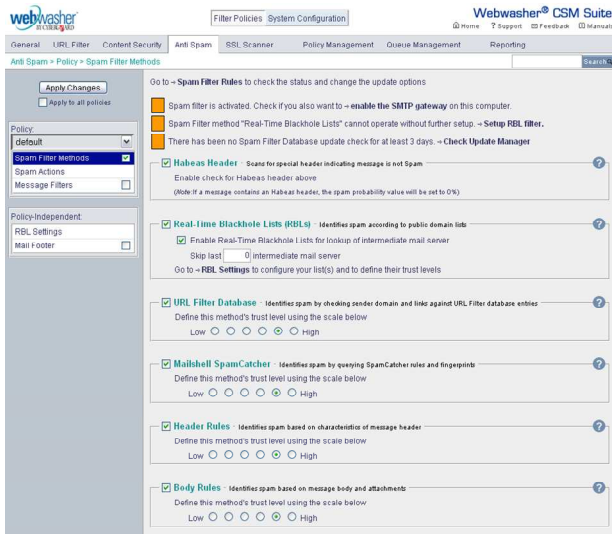
- **Document Inspector** (word, excel, ppt, pdf)
- **Text classification**
- Zahrnuje **obsahové kontroly i pro WebMAIL**
- **Archive handler** (.zip, .gzip, .arj, .tar…)

Omezuje:

- „Vynesení" citlivých informací zaměstnanci
- Omezuje faktor „lidské chyby"

Antispam

- Propojení s TrustedSource.org – odhalení spammerských útoků bez nutnosti zkoumání obsahu
- 7-mi úrovňová detekce spamu
  - ✓ Mailshell®
  - ✓ SpamCatcher™
  - ✓ Pravidla pro Header a body
  - ✓ Bayesovské pravidla
  - ✓ Habeas
  - ✓ RBL seznam
  - ✓ Vyhledávání URL podle URL filtr databáze
- White/Black Listy
- E-mail Filtr (adresát, velikost,…)
- Queue Management (speciální fronta pro spamy ke kontrole)
- Phishing Filter
- **Příchozí i Odchozí!**

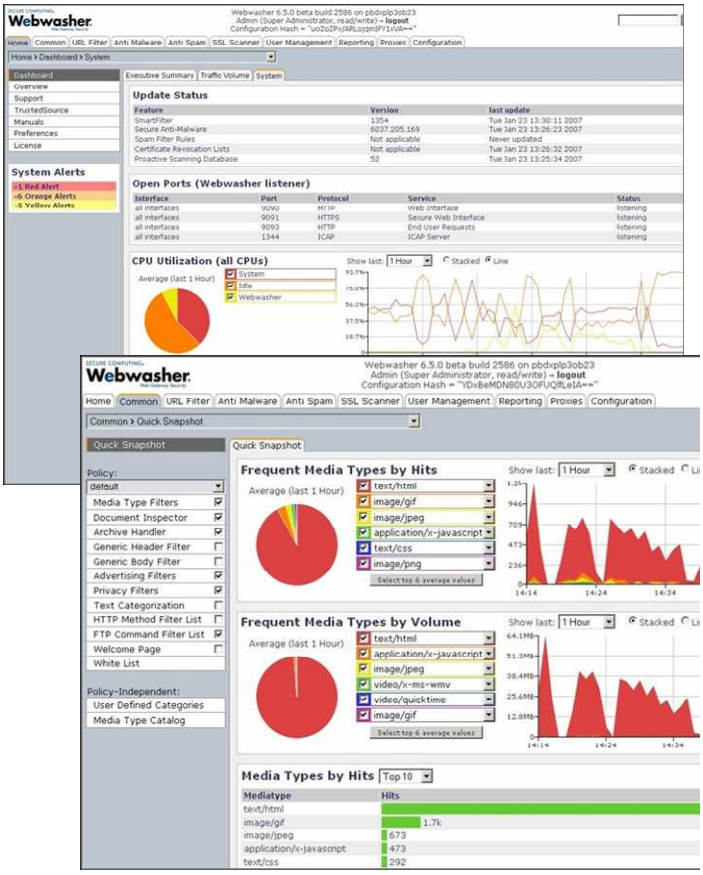


COMGUARD a.s., Vídeňská 119b Brno, Freyova 27 Praha, obchod@comguard.cz, www.comguard.cz

COMGUARD

Reportovací nástroje

- Barevné, přehledné **uživatelsky definovatelné reporty**
- **Drill down** reportů pro data-mining
- Snadná definice dotazů
- Automatické / plánované události
  - **Generování reportů**
  - **Distribuce e-mailů**
  - **Shromažďování a import logů do databáze**
  - **Management růstu databáze**
  - **Zálohování databáze (MaxDB only)**
- Uživatelské rozhraní typu browser
- Proaktivní policy management
- „**Keep an eye** on potential problem areas"
- **Oracle, MS-SQL Server, or MaxDB database support**

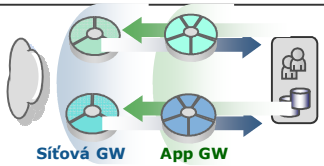


COMGUARD

Secure Computing

secure computing

Přímé Zaměření



- Všestranné & integrované „enterprise gateway security"
- Síťové & Aplikační brány, Příchozí & Odchozí ochrana
- Jedna z největších nezávislých „security" společností

Vedoucí postavení na trhu

- #1 v SCM Appliances
- #1 v Mail sec. appl.
- #2 v URL řešení IDC
- 60% z Fortune 500; 56% z DJ Global 50; 70% z top 25 bank

Technologická dominance

- TrustedSource Internetový systém vyhodnocení důvěry v reálném čase – PROAKTIVNÍ OCHRANA
- Nejvíce všestranné, integrované aplikační „gateway security" řešení
- 80 mezinár. patentů

Postavení & Finanční Síla

- obrat více než $250M
- Ziskovost
- ~ 900 zaměstnanců
- Zastoupení - 106 zemí

Osvědčená „enterprise-class security" řešení, na které se můžete spolehnout

Security řešení s přesnou & spolehlivou ochranou

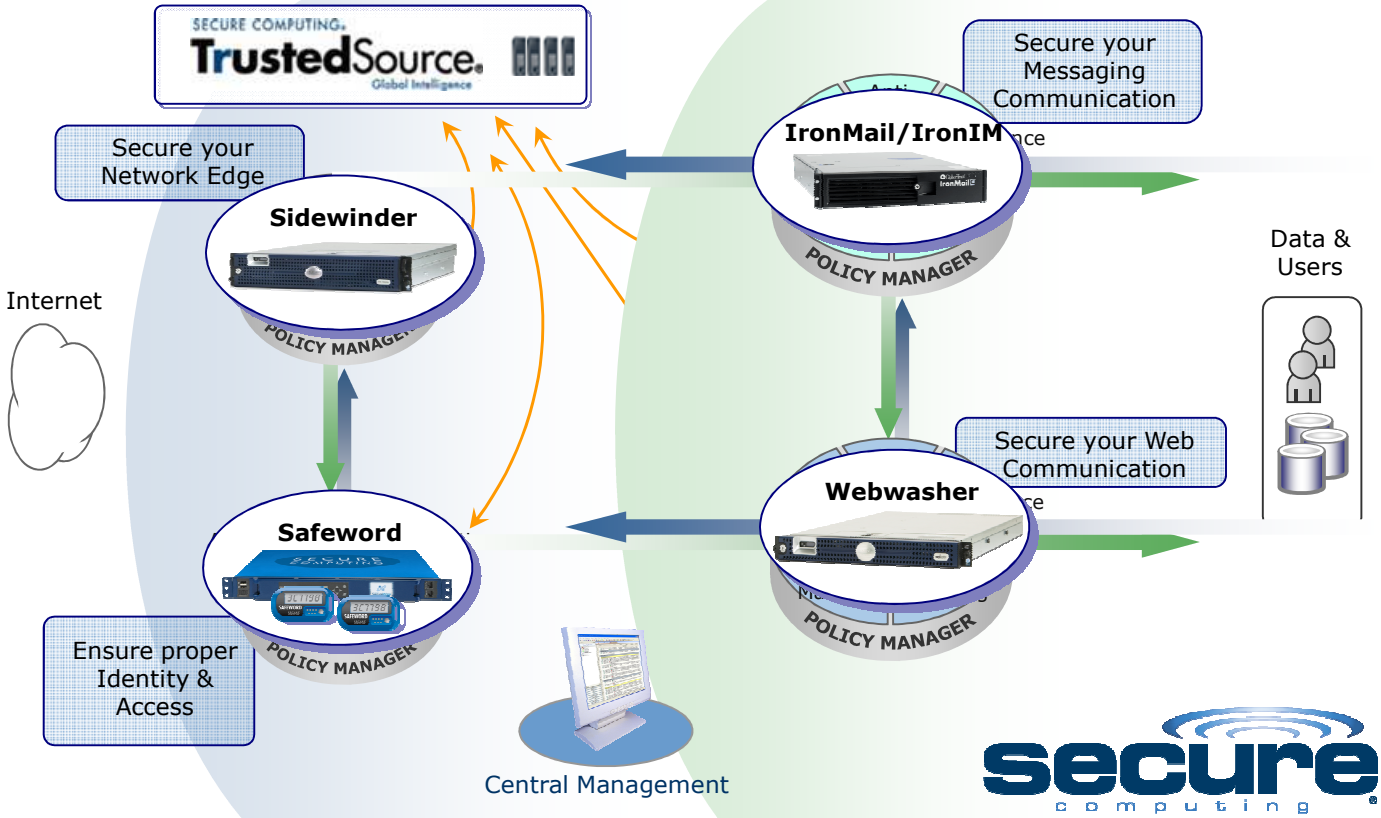
Minimální administrace, nejnižší náklady (TCO)

Trvalý výkon – ochrana Vašich investic; S do nových technologií; Celosvětový servis & podpora

COMGUARD a.s., Vídeňská 119b Brno, Freyova 27 Praha, obchod@comguard.cz, www.comguard.cz

COMGUARD

Enterprise Gateway Security



Network Gateway **Application Gateway**

COMGUARD

Otázky? Náměty?

Děkuji Vám za pozornost

COMGUARD a.s.

Distributor Secure Computing pro Slovensko, Českou republiku a Ukrajinu

jan.dymacek@comguard.cz

Partneři na Slovensku

Platinum Partner: Ness Slovensko

Gold Partneři: LYNX, Tempest, Gratex