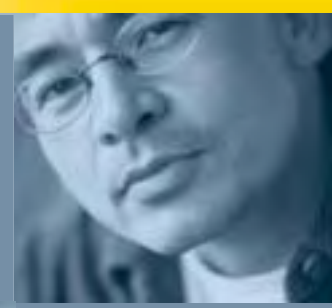
Pošta, která nikdy nespadne!

Konvergence bezpečnosti a dostupnosti



Radek Smolík
Country Manager
Symantec ČR a SR

AGENDA

1. Elektronická pošta jako kritická aplikace
2. Proaktivní bezpečnost poštovních systémů
3. Archivace a vyhledávání v poště
4. Trvalá dostupnost poštovních systémů

Elektronická pošta jako kritická aplikace

Jak to všechno začalo?

- 1851 – v Rochesteru (stát New York) byla založena společnost „The New York and Mississippi Valley Printing Telegraph Company“
- 1861 – dokončení první transkontinetální telegrafické linky
- 1865 – telegrafické spojení mezi Amerikou a Evropou (do Moskvy přes Aljašku)
- 1871 – zavedení převodů peněz přes telegrafickou síť
- 1943 – první mikrovlnné komunikace mezi městy
- 1964 – první transkontinentální mikrovlnné komunikace nahrazující linky
- 1974 – první geosynchronní komunikační satelity

Poslední zpráva – po 145 letech...

Era Ends: Western Union Stops Sending Telegrams

By Robert Roy Britt
LiveScience Managing Editor
posted: 31 January 2006
10:17 pm ET

After 145 years, Western Union has quietly stopped sending telegrams.

On the company's web site, if you click on "Telegrams" in the left-side navigation bar you're taken to a page that ends a technological era with about as little fanfare as possible:

"Effective January 27, 2006, Western Union will discontinue all Telegram and Commercial Messaging services. We regret any inconvenience this may cause you, and we thank you for your loyal patronage. If you have any questions or concerns, please contact a customer service representative."

The decline of telegram use goes back at least to the 1980s, when long-distance telephone service became cheap enough to offer a viable alternative in many if not most cases. Faxes didn't help. Email could be counted as the final nail in the coffin.

A tak vypadá „Nový život“

Western Union Web hack attributed to 'human error'

From... IDG.net

September 13, 2000
Web posted at: 11:20 a.m. EDT (1520 GMT)

by James Evans

(IDG) -- Western Union Holdings Inc. said that its Web site was hacked Friday and the perpetrators gained access to 15,700 customers' credit and debit card information.

"Friday during the day, we learned there was a security breach on our Web site," said Peter Ziverts, spokesman for Western Union. "During an audit of the system, we learned about the breach."

The company is attributing the security breach to human error as a file was left unprotected and gave access to information that provided hackers with a list of names, addresses and credit and debit card information, Ziverts said.

Western Union Web site hacked

update **"Human error" allowed a hacker to copy the credit card and debit card information of about 15,700 customers from Western Union's Web site, the company said today.**

The money-transferring company first learned of the hacking Friday. A Western Union spokesman said the vulnerability was caused when "performance management files" were left open on the site during routine maintenance, allowing the hacker access. He did not know when the maintenance began or how long the site had been left unprotected.

"We are still in the due diligence period," said Peter Ziverts, a spokesman for the Englewood, Colo.-based company. "But this wasn't an architectural problem; this was due to human error."

Ziverts said that he did not know how long the site would be out of service, indicating that it would be "at least a few days."

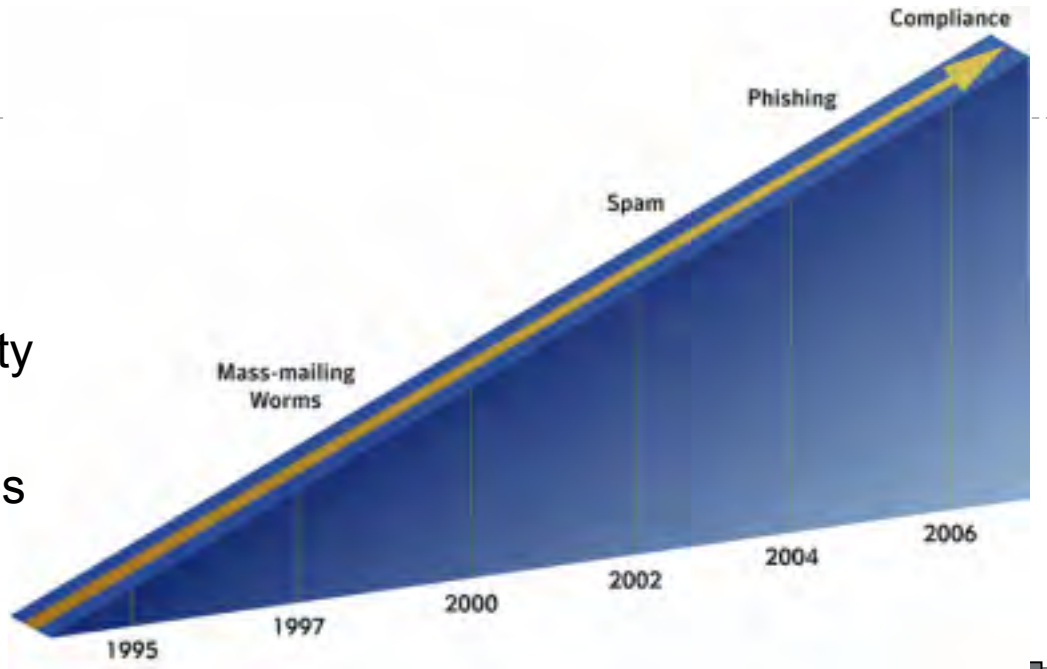
Company representatives began contacting customers during the weekend via email and telephone.

One customer reported learning of the hacking from an answering machine message left by someone identifying himself as a Western Union president.

"Sounds like a big (mistake) on someone's part at a site you'd expect to be locked down tight," the customer said.

Evoluce pošty

- Obchodní pošta vzroste **25% – 30%** do roku 2009 *
- Přes **60%** dnes přijímané pošty je spam**
- **80%** virů a červů vstupuje přes poštovní bránu ***
- **75%** duševního vlastnictví korporací je v poště ****
- Pošta je dnes záznamem obchodních činností

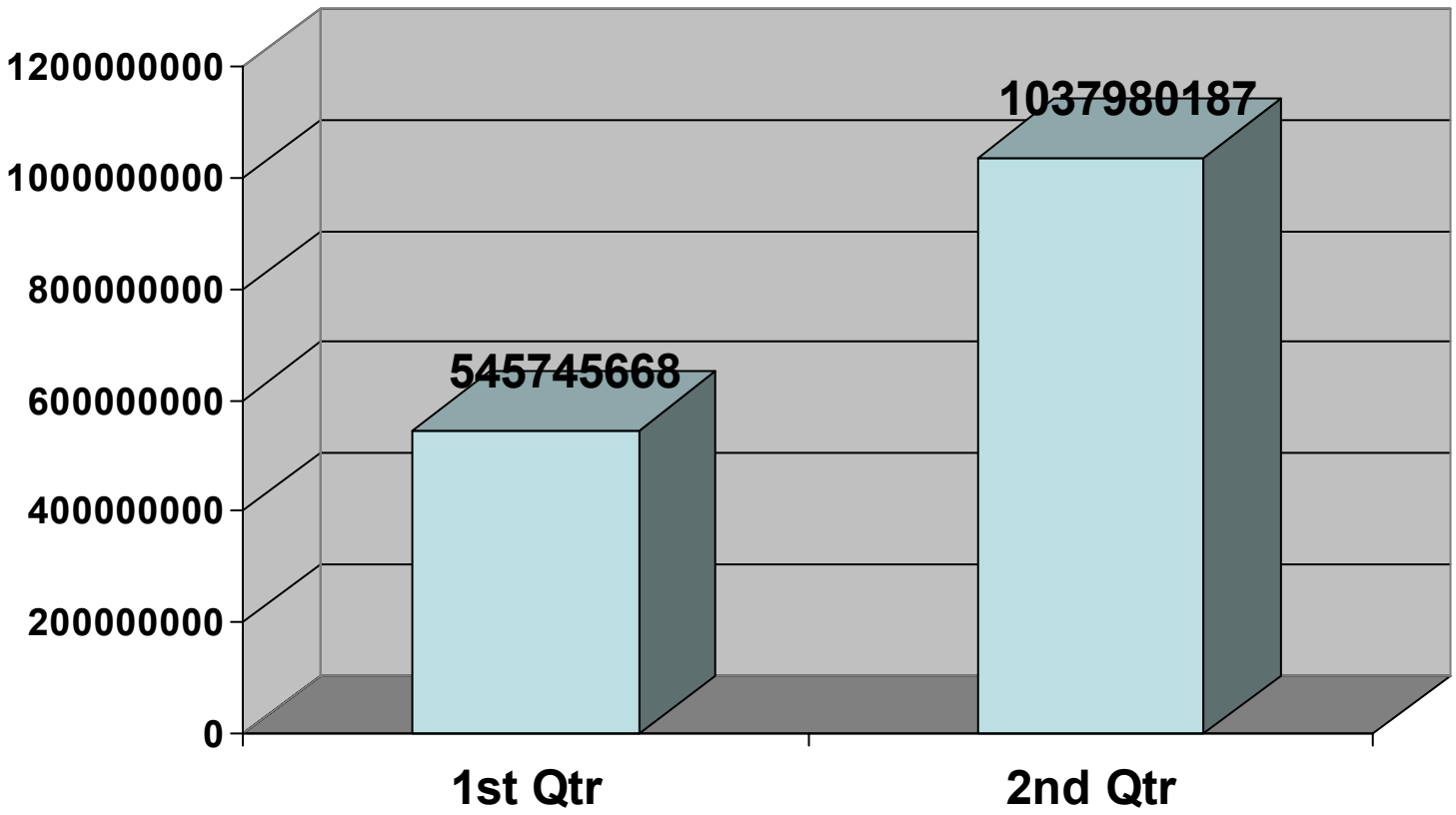


Elektronická pošta se stala primárním médiem naší komunikace. Důsledkem toho je skutečnost, že pošta je de fakto úložištěm obchodních záznamů.

CIO Magazine, Jan 2005

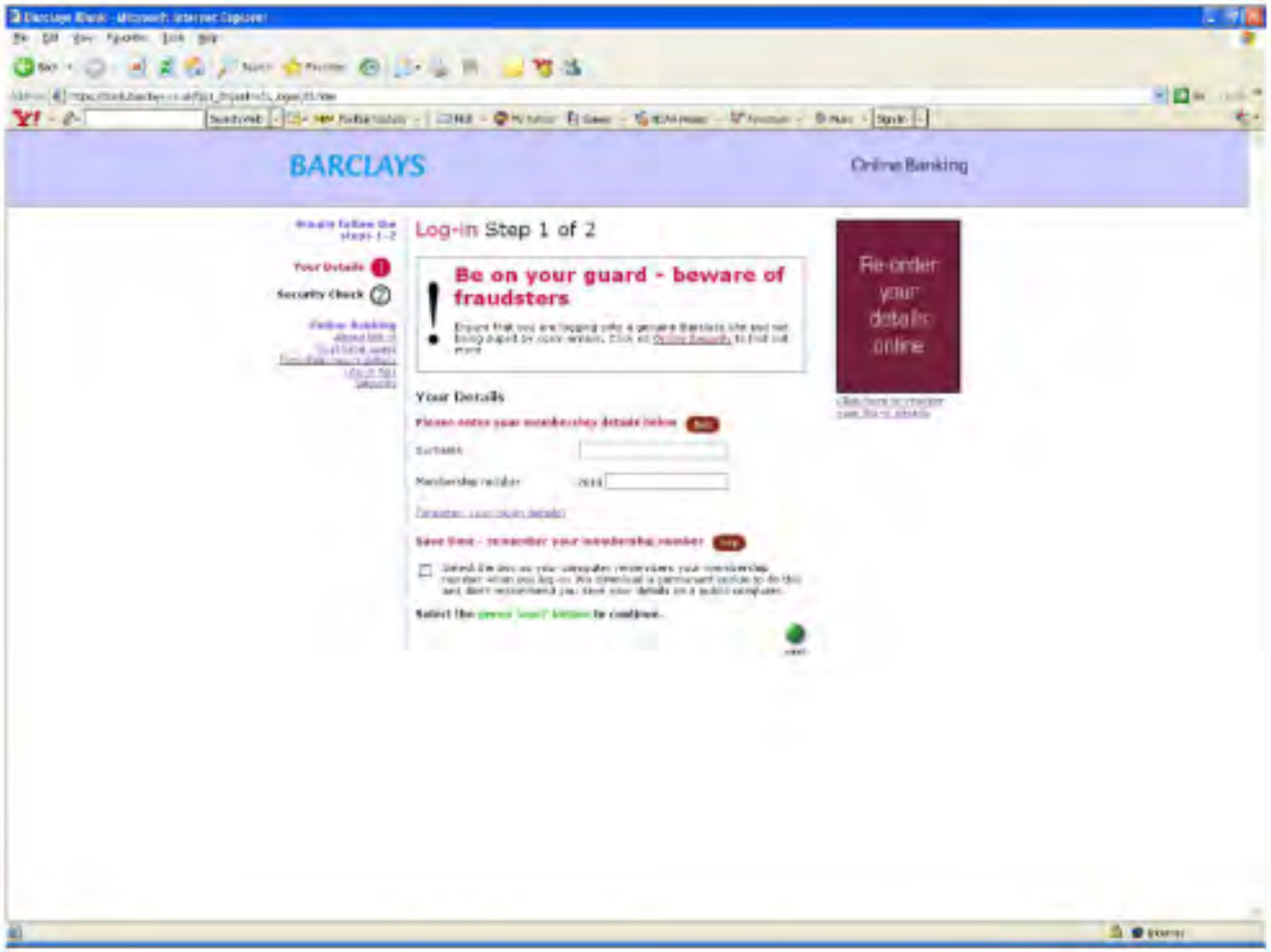
* Gartner (bez spamu)
** Symantec ISTR, Mar 2005
*** IDC
**** Enterprise Strategy Group

Šestiměsíční nárůst phishingu

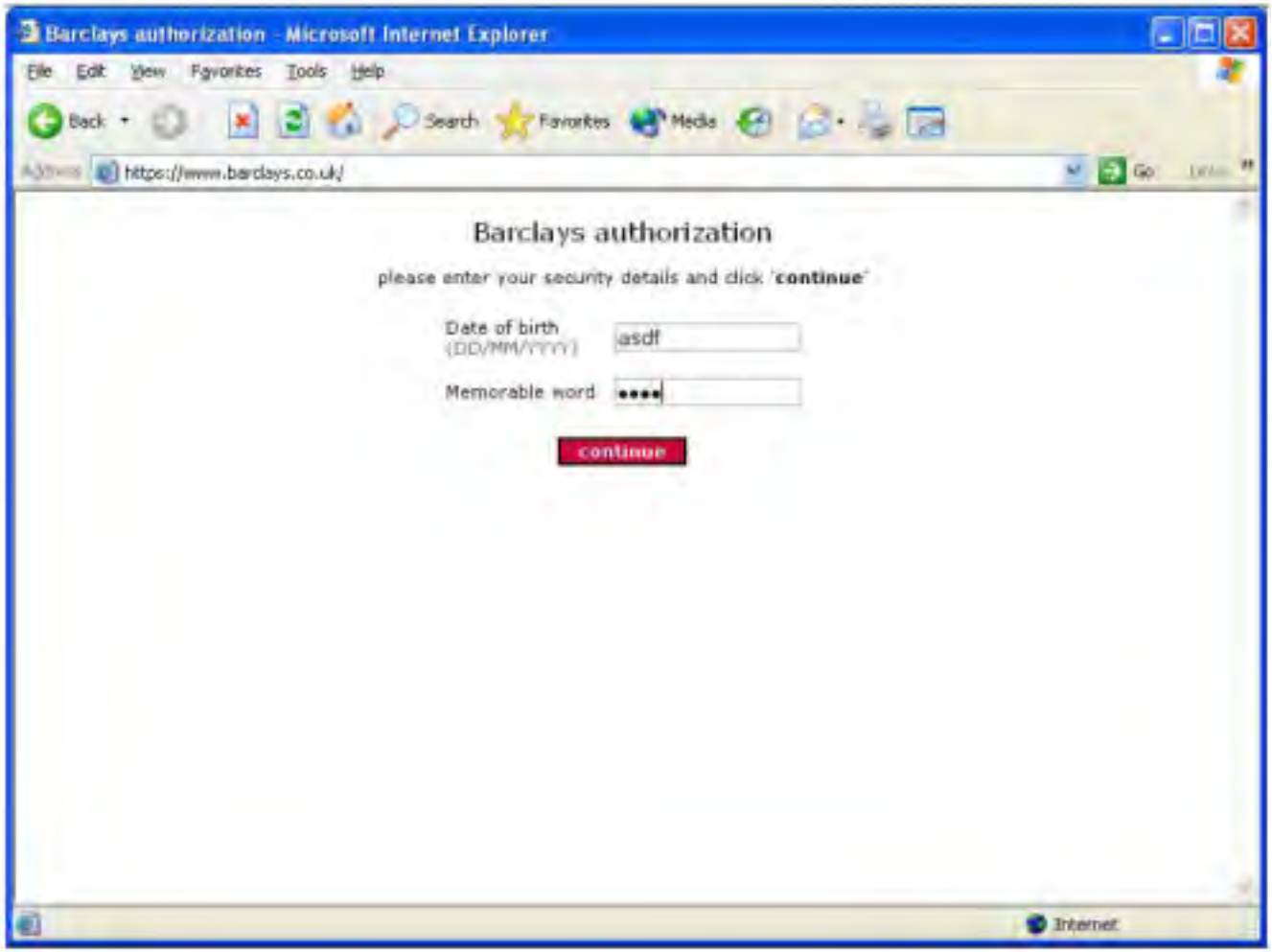


Každý 125 mail v období od 30.6.05 do 30.1.06 byl klamavý!

Legitimní login



Druhý krok – spoofovaný přes PWSteal.Botuk



3. krok – zachycená autentikace

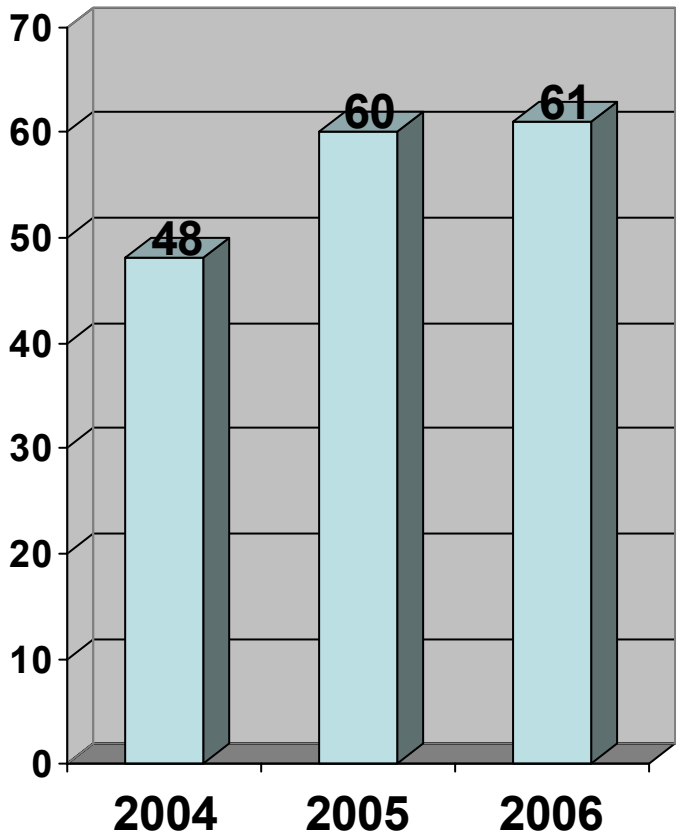
<h1>From URL: https://www.barclays.co.uk/</h1>

<FORM action=login method=post></HEAD>

<BODY><INPUT type=edit value="aaaaaaa">password <INPUT value=aaaaaa>username <INPUT type=submit value="Submit Query"> </FORM>

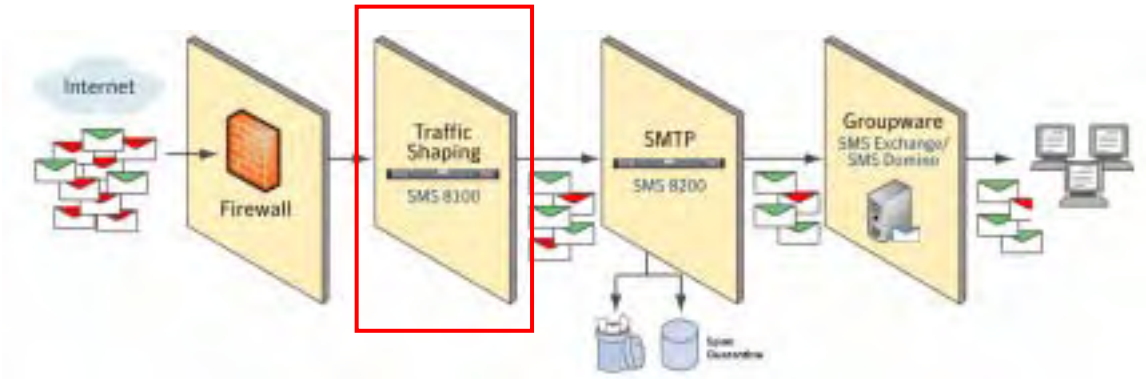
Průměrná míra spamu

- Doporučení:
  - Nasadit technologie IP filtrování a poštovní traffic-shaping
  - ISP společnosti by měly implementovat filtrování odchozích transakcí, aby eliminovaly kompromitované ISP účty a proxy servery
  - Administrátoři by měli zvážit blokování portu 25 v odchozím směru (s výjimkou autorizovaných uživatelů, kteří potřebují odesílat vlastní SMTP poštu



Bezpečnost obsahu pošty

Symantec™ Mail Security 8160 "Traffic-Shaping"



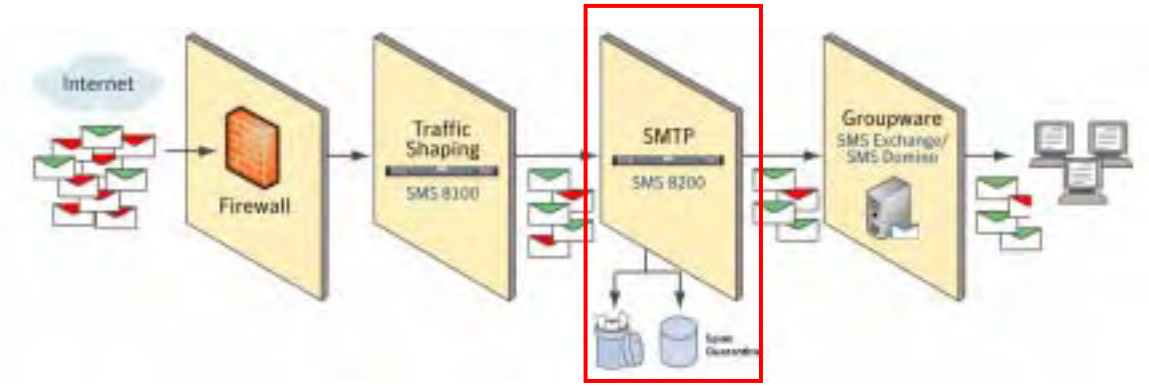
Co to dělá?

- Pracuje jako "antispam router"
- Používá unikátní "traffic-shaping" technologii
- Vzorkuje spam a analyzuje cesty spamování
- Aplikuje QoS vůči SMTP provozu
- Zastavuje odesíláni spammerům

Přínos k bezpečnosti a dostupnosti

- Až 80% redukce objemu spamu, před úrovní MTA
- Žádný negativní vedlejší účinek
- Vyznamné snížení karanténovaného spamu
- Zvýšení výkonnosti interních skannerů a poštovních systémů

Symantec™ Mail Security 8200-Series „Antispam“



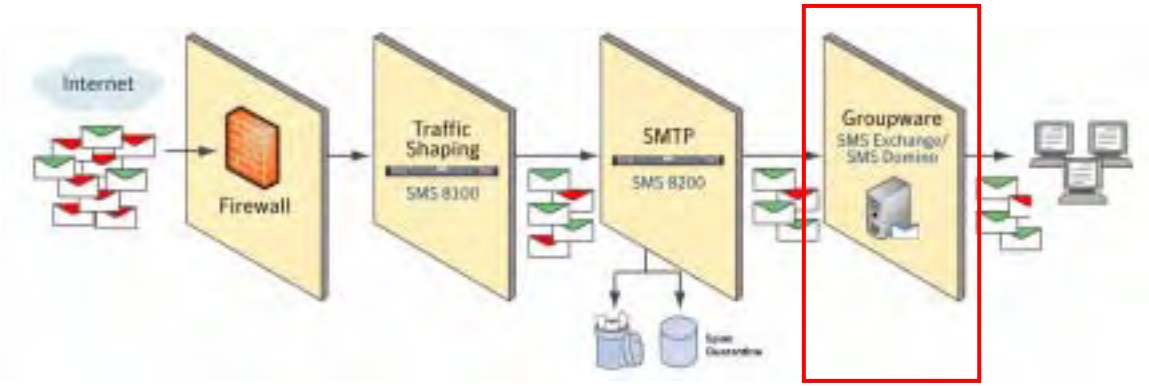
Co to dělá?

- Vyhledávání virů v příchozí a odchozí poště
- Detekce a volitelné karanténování spamu
- Filtrování obsahu nevhodné pošty v obou směrech

Přínos k bezpečnosti a dostupnosti

- Další 95% redukce zbývajícího spamu s přesností 99.999%
- Odstranění poštovních červů a virů na prvním vstupním bodu
- Odstranění nevhodného obsahu a nebezpečných kódů před dosažením úložiště pošty

Symantec™ Mail Security for Microsoft® Exchange
Symantec™ Mail Security for Domino®



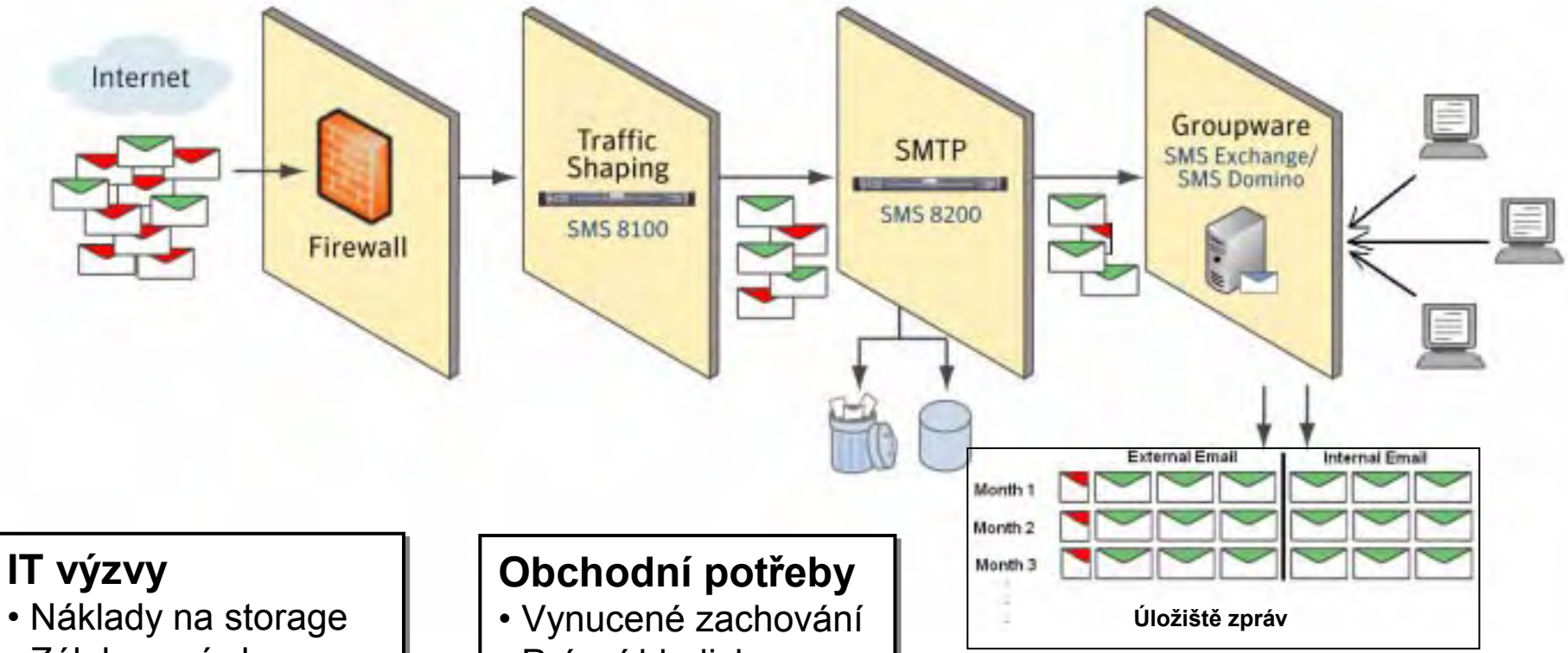
Co to dělá?

- Rezidentní, plánované a vyžádané skanování zpráv v poštovním úložišti
- Vyhledávání virů v příchozím, odchozím a interním poštovním provozu
- Filtrování nevhodného obsahu pošty

Přínos k bezpečnosti a dostupnosti

- Preventivně předchází šíření červů ke koncovým uživatelům
- Schopnost zpětného čištění zpráv v úložišti

Potřeba archivace obsahu a bezpečnosti systému



IT výzvy
- Náklady na storage
- Zálohovací okno
- Stabilní provoz
- Správa PST souborů
- Řízení kvót

Obchodní potřeby
- Vynucené zachování
- Právní hlediska
- Supervize / dohled
- Vynucené odstranění
- Zpráva záznamů

symantec.

Bezpečnost poštovního systému

Pošta je výzvou i pro bezpečnostní tým

- Centralizovaný audit a sledování stavů
- Udržování bezpečnostní shody v čase
- Vynucování bezpečnostní politiky v celé organizaci
- Ochrana v nulových dnech (neznámé hrozby, vnitřní útoky)

Symantec Critical System Protection 5.0 odpovídá kritickému provozu pošty

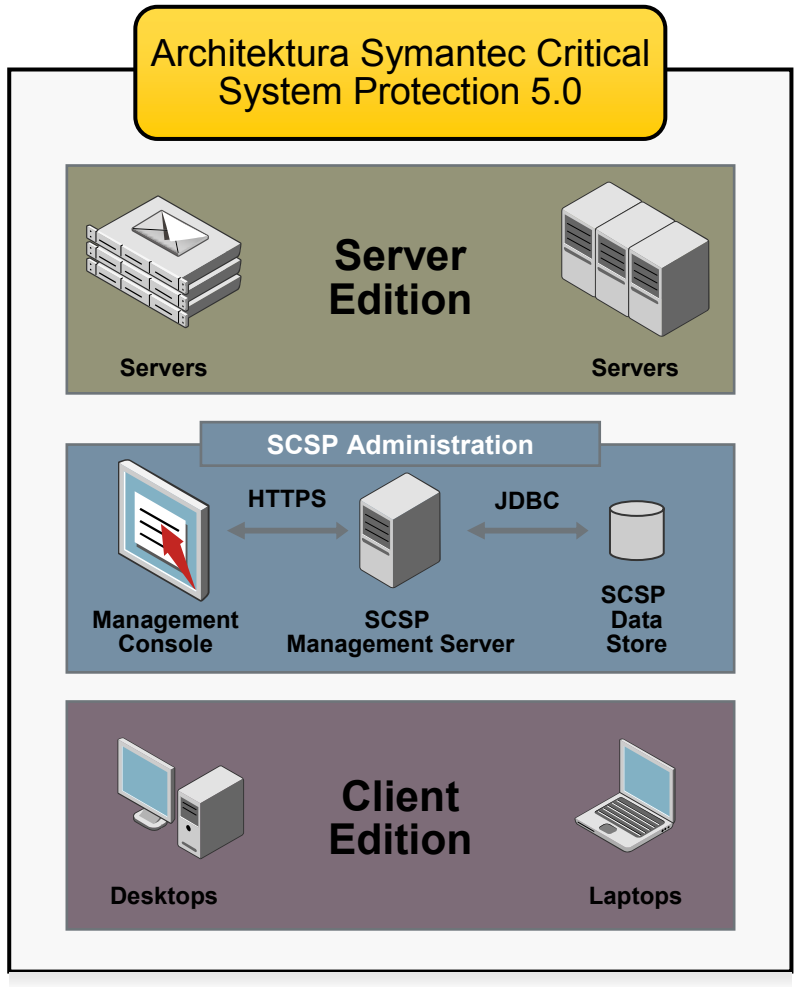
Základní architektura

Edice pro Klienta a Server

- Agent pro kontrolu chování
  - Kernel-mode driver
  - User-mode agent service
- IDS Agent

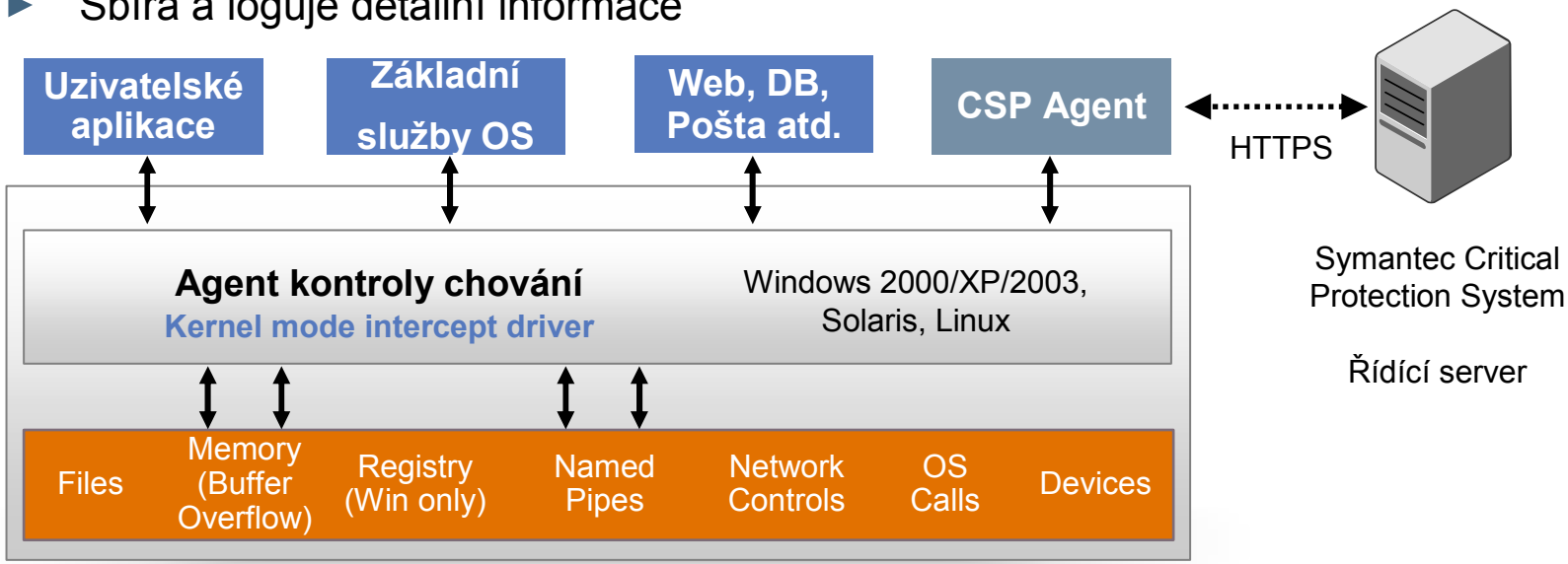
Administrace

- Řídící server
- Řídící konzola
- Databáze
  - MSDE
  - SQL Server



Funkce agenta pro kontrolu chování

- Poskytuje „kernel-mode“ přerušení systémových volání
- Zavádí politiky bez restartů
- Verifikuje vzájemné propojení a návaznost procesů
- Vynucuje politiky
- Chrání před přetečením zásobníků
- Sbírá a loguje detailní informace



Ochrana v nulových dnech

- Výkonná IPS technologie navržená tak, aby zastavila i zcela nové, nebezpečné útoky na systémy a aplikace ihned, jakmile se objeví
- Předchází zavádění a šíření nebezpečných kódů, aniž by bylo zapotřebí je znát a mít jejich signatury, případně mít nasazen patch
- **Prevence před zneužitím**
  - ✓ Buffer overflow
  - ✓ Zaštítění aplikací
  - ✓ Zaštítění funkcí individuálních operačních systémů
  - ✓ Ochrana registrů a souborů
  - ✓ Vynucování „principu nejmenšího privilegia“
  - ✓ Integrovaný firewall pro zaštítění síťové komunikace v příchozím i odchozím směru

Zodolnění systémů

- „Out of the box“ politiky zamykají operační systém, aplikace a databáze
- Předchází zavádění a spouštění neautorizovaných kódů
- Integrace s adresářovými službami pro snazší správu oprávnění uživatelů

- **Ochrana O/S**
  - ✓ Microsoft Windows®
  - ✓ SUSE Linux®
  - ✓ Sun Solaris™
- **Ochrana aplikací**
  - ✓ Microsoft® Exchange Server
  - ✓ Microsoft Internet Information Server
  - ✓ Microsoft SQL Server
  - ✓ Apache Web Server
  - ✓ Sendmail™
  - ✓ Postfix

Ochrana před Buffer Overflow

- Jak to pracuje:
  - Kontroluje a přerušuje systémové volání
  - Prochází zásobníky a odhaluje podezřelá volání
  - Verifikuje návratové adresy zásobníků v kernelu O/S

- Jestliže je detekováno přetečení zásobníku:
  - Blokuje spuštění zasílaného kódu
  - Varuje administrátora
  - Neukončuje proces !!!

Ochrana před přetečením zásobníků v MS Windows

- Ochrana proti známým i neznámým útokům, které se manifestují jako klasické přepisování paměti
- MS v současnosti uvádí, že 70% jeho kritických zranitelností vede k přetečení zásobníků nebo k podobným přepisování paměti
- Monitoruje využití paměti podle systémových volání a trvale sleduje zásobníky a identifikuje podmínky přetečení
- Okamžitě blokuje spouštění instrukcí mimo platné procesy a jejich svazky

Zaštítění operačních systémů/aplikací

- Jak to pracuje:
  - Identifikuje program, propojení procesů, argumenty příkazů
  - Seskupuje procesy:
    - Základní služby OS: lsass.exe, spoolsv.exe
    - Aplikační služby: mssql.exe, iis.exe
    - Interaktivní programy: winword.exe, excel.exe, iexplore.exe
  - Aplikuje kontroly chování založené na znalosti správného chování procesů
    - Tato chování jsou založena na profilech vytvářených a verifikovaných společností Symantec
  - Pro aplikace neprofilované společností Symantec (zákaznické aplikace apod.)
    - Aplikuje generické “známé špatné chování” kontroly(jako jsou změny spouštěcích klíčů v registrech, přepisování systémových souborů, nelegální přístupy k logům apod.)

Integrovaný firewall

- Jak to pracuje:
  - víceúrovňový filtr
  - nestavový, paketově-inspekční firewall
- Co to dělá:
  - Blokuje příchozí a odchozí TCP a UDP provoz
  - Administrátor může blokovat provoz:
    - dle čísla portu
    - dle protokolu
    - dle IP adresy nebo rozsahu adres

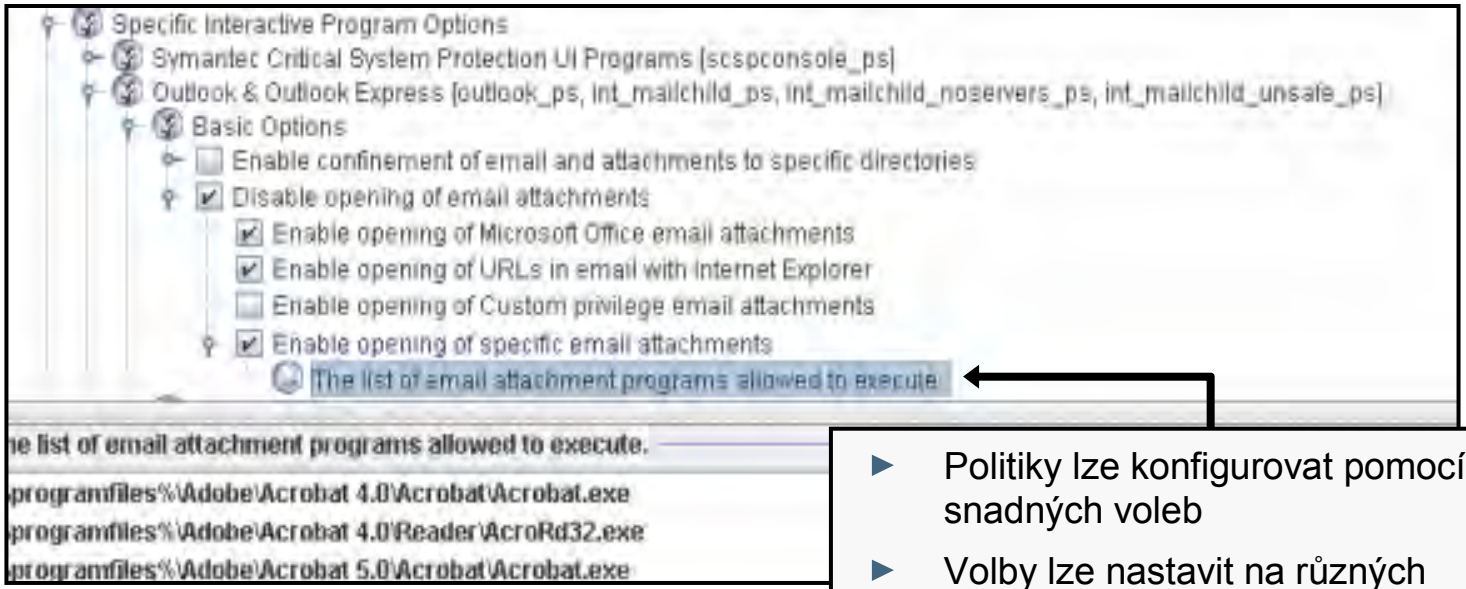
Politiky „Out of the Box“

- Jak to pracuje:
  - Zamyká kritické zdroje systému, včetně:
    - zavádění systému, konfigurace, ovladačů, systémových souborů a registrů
  - Zamyká síťový provoz:
    - Systémové služby a klíčové aplikace (jako je například IIS) mají grantován přístup k síti pouze tehdy, když aktuálně běží
  - Zamyká vytváření nebo modifikaci spustitelných souborů
  - Aktivuje/umožňuje ochranu před přetečením zásobníků

Politiky „Out of the Box“ ve verzi 5.0

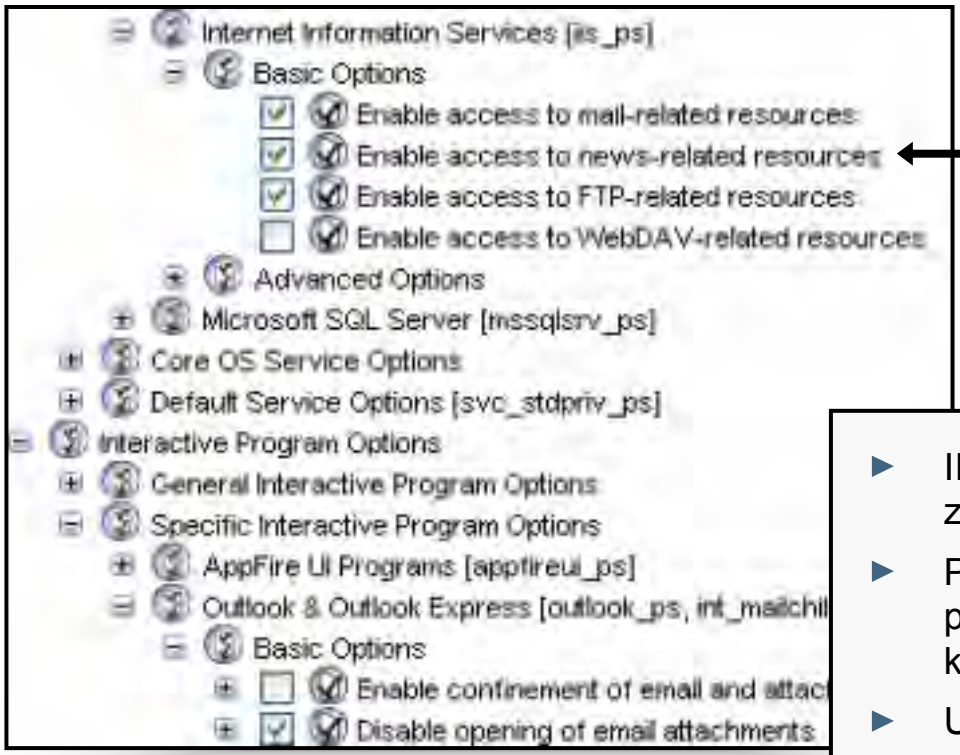
- **Microsoft Windows OS**
- **Microsoft Internet Information Server**
- **Microsoft Exchange**
- **Microsoft SQL Server**
- **Microsoft Outlook & Outlook Express**
- Microsoft Office
- RedHat & SuSE Linux OS
- Solaris OS
- Apache web server
- **Postfix email server**
- **Sendmail email server**

Udržování shody – uvedení „papíru do akce“



- Politiky lze konfigurovat pomocí snadných voleb
- Volby lze nastavit na různých úrovních
- Kontroly mohou být aplikovány na jednotlivé aplikace
- Omezení, které programy mohou spouštět poštovní přílohy apod.

Snadná konfigurace politik pomocí voleb



- IIS má normální přístup k určitým zdrojům
- Pomocí těchto boxů lze omezit přístup ke zdrojům spojených s každou z funkcí
- Udělat to v IIS by vyžadovalo pracnou a složitou manuální konfiguraci pro každou z aplikací

„Chytrá“ odezva na události

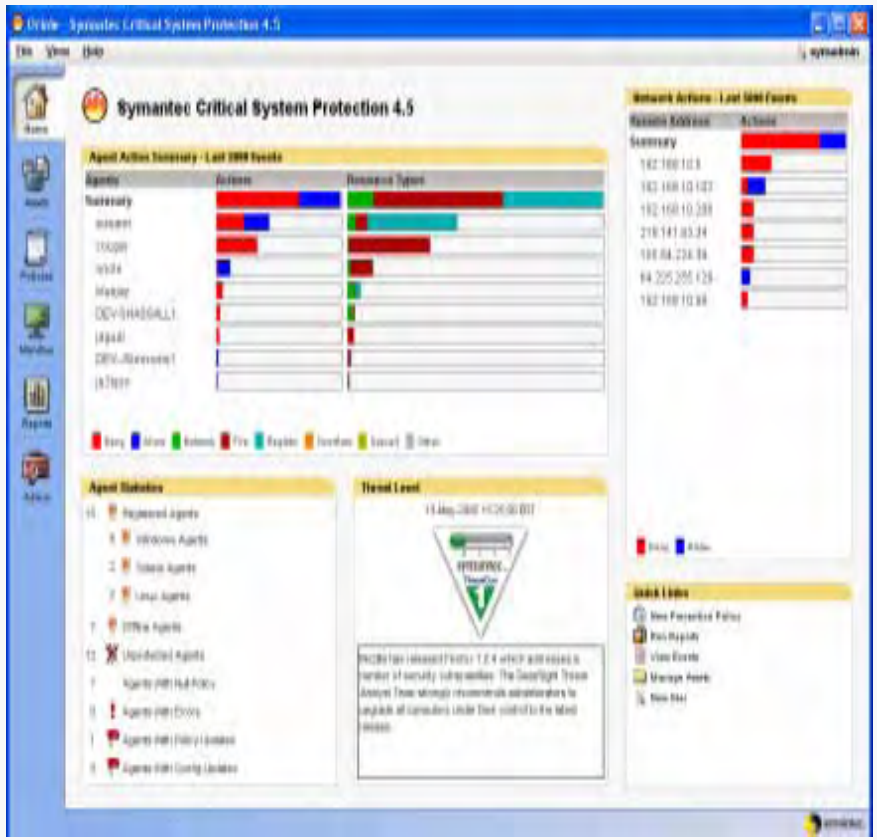
- Umožňuje automatickou odezvu na události s vícerými akcemi a protiopatřeními, která lze přímo podniknout:
  - varování do řídící konzoly
  - upozornění elektronickou poštou
  - SNMP trap
  - zneplatnění útočícího uživatelského účtu
  - spuštění lokálního příkazu (skriptu) jako je rozšířené logování
  - zaznamenání chování pro budoucí analýzu
- Aktivační události, akce a protiopatření jako plně zákaznicky přizpůsobitelné (dle definic v platné bezpečnostní politice)

Ukázky funkcí

Kompletní přehled z jediného místa

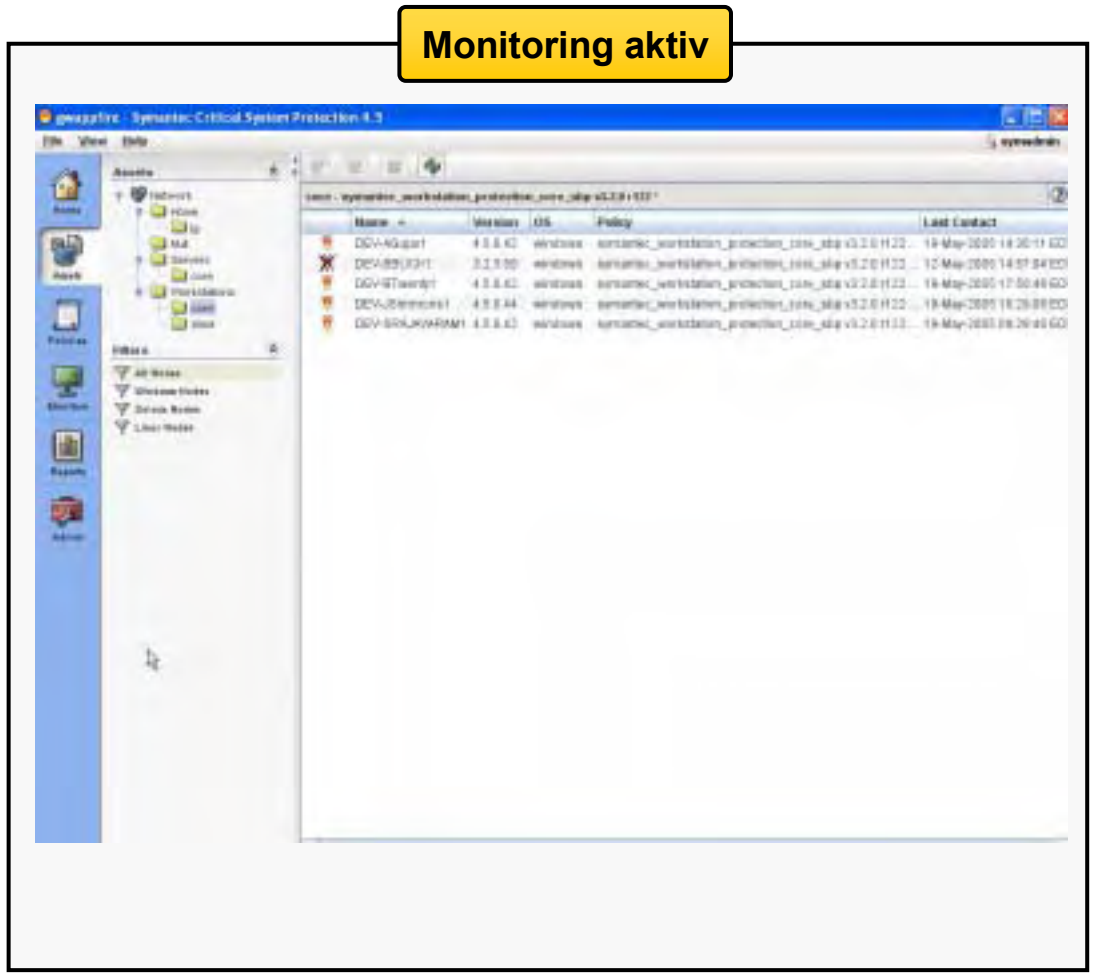
- Souhrnný Dashboard
  - Administrátor ihned vidí detaily pro každý specifický stroj, má přehled o zdrojích a akcích
  - Propojení se Symantec DeepSight™
- Stavové informace „per-machine“
  - Poskytuje statistiky o agentech a umožňuje zavádění na řízené agenty
- Obsahuje rychlé navigace k často používaným funkcím

Dashboard



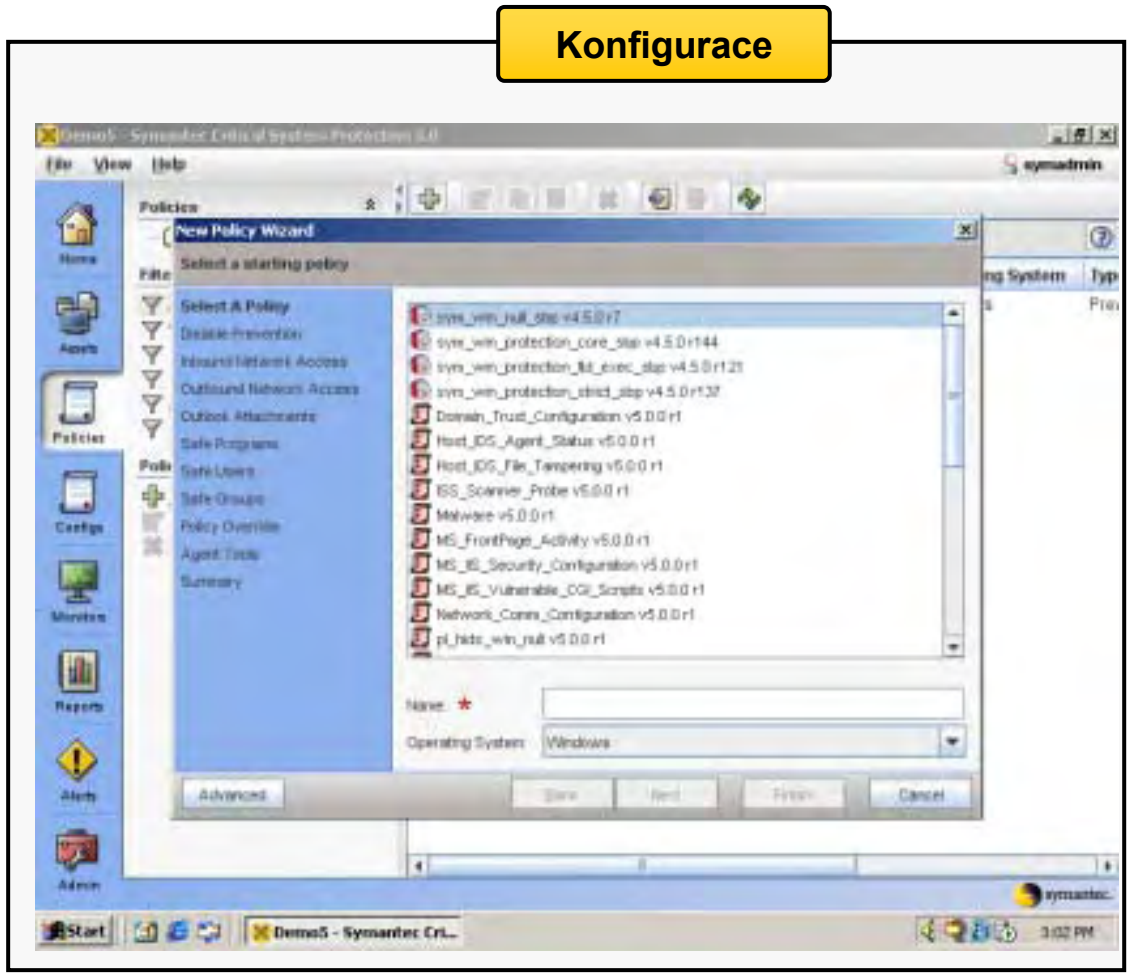
Monitorování aktiv

- Flexibilní seskupování aktiv
  - Umožňuje administrátorům, aby aktiva libovolně seskupovali
  - Agenti mohou být uspořádáni do skupin a skupiny si mohou být logicky podřízeny (podskupiny)
- Politiky lze aplikovat na skupiny, na skupiny skupin, na podskupiny i na individuální agenty
- Stav agenta, verze aktuální politiky, typ OS, informace o četnosti „heartbeat” komunikace a provozním stavu



Konfigurace politiky

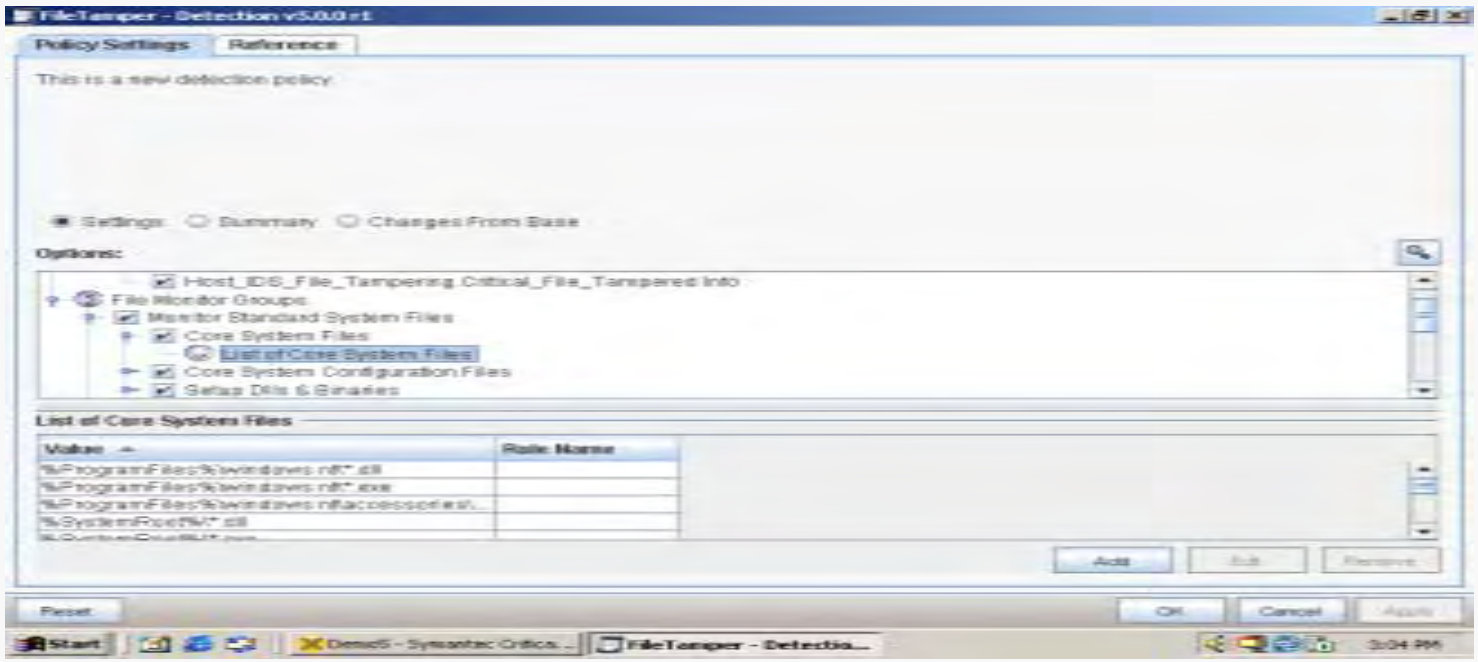
- Umožňuje administrátorům spravovat verze a udržovat konfigurace politik
- Politiky lze aplikovat i na vícenásobné skupiny současně
- Minimalizuje nastavování komponent a podporuje efektivnost práce administrátorů



Možnosti konfigurace politik

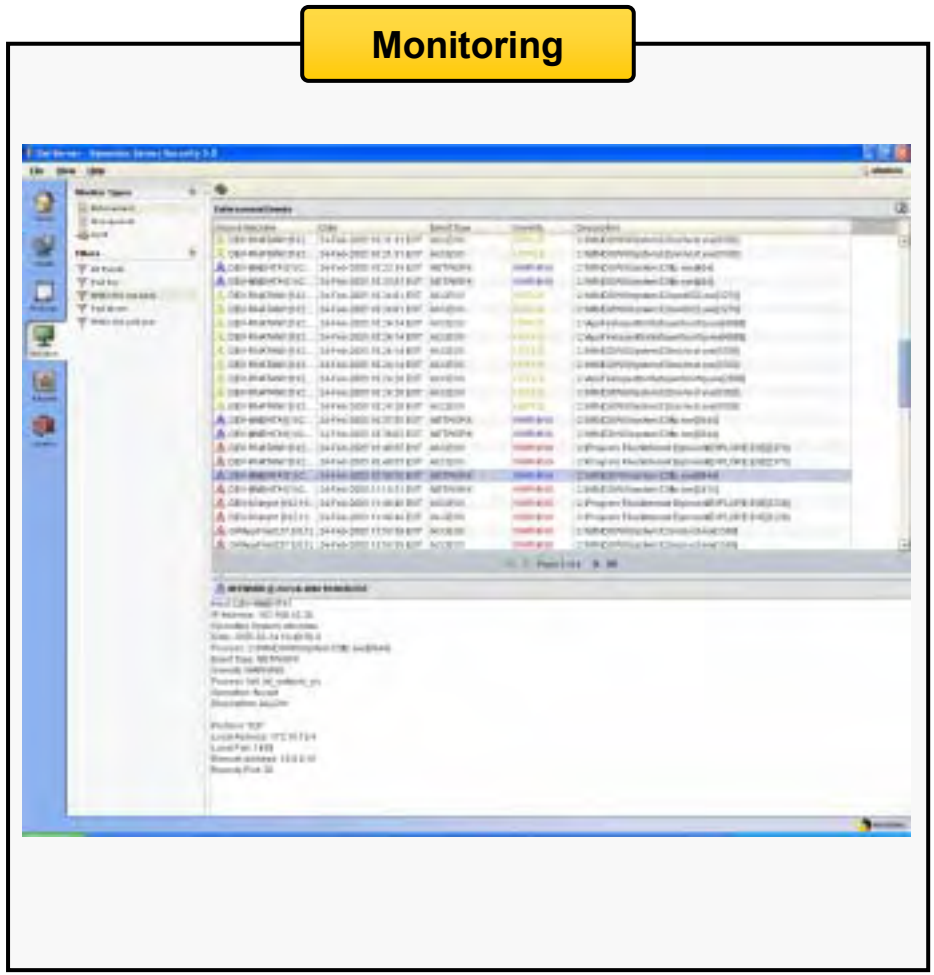
- Politiky jsou konfigurovány jednoduchým stylem voleb jako “Enable/Disable”
- Umožňuje administrátorům nastavit možnosti na různých úrovních
- Kontroly mohou být zaváděny i na jednotlivé aplikace

Granulární konfigurace



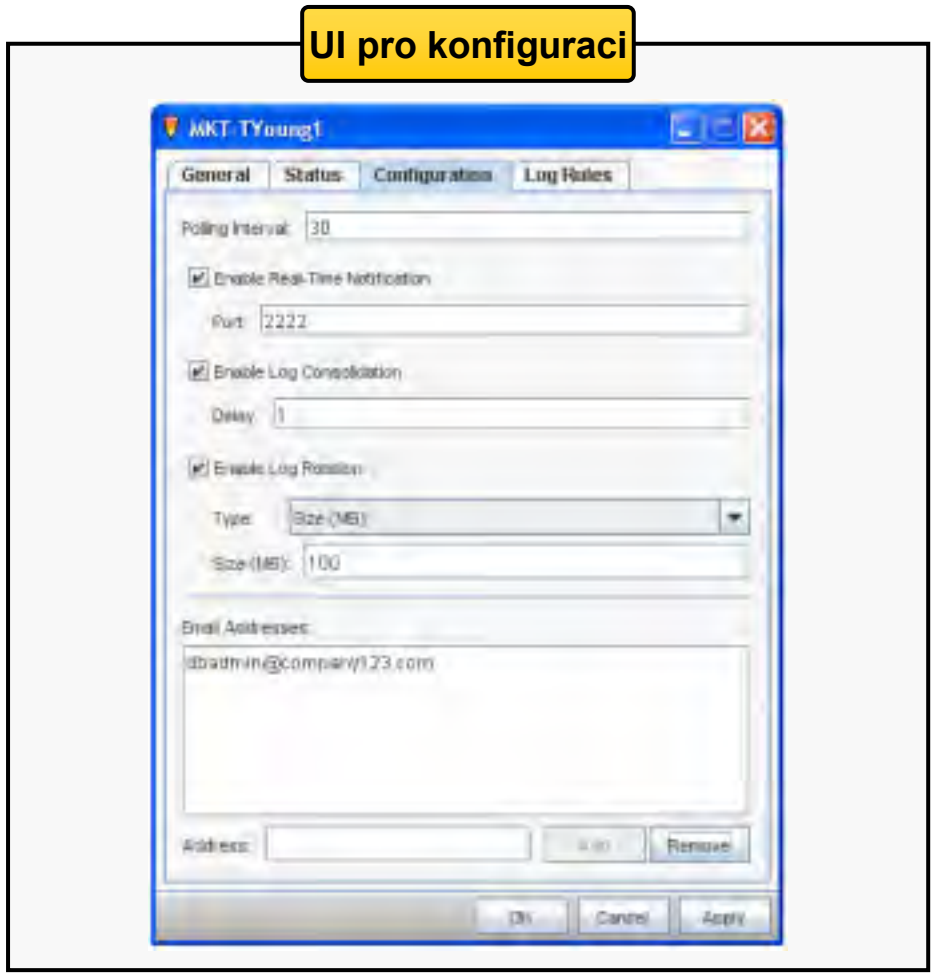
Monitorování sytémových i síťových aktivit

- Monitorování v reálném čase
- Informace o narušeních, které lze detailně prohledávat:
  - Stroj
  - IP adresa
  - Operační systém
  - Proces
  - Zdroj
  - Typ události
  - Závažnost
  - Provoz
  - Dispozice (Povolení/Zákaz)
- Další informace o síťových událostech
  - Protokol
  - Port (lokální i vzdálený)
  - Adresa (lokální i vzdálená)



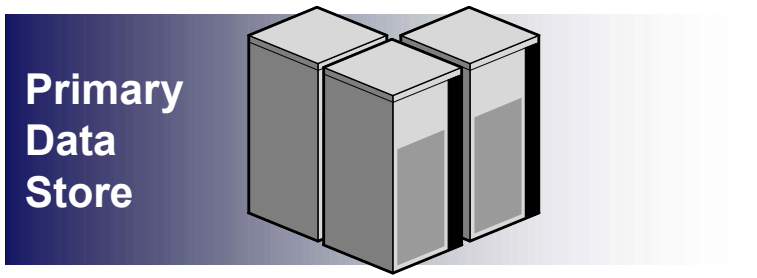
Konfigurace vlastností

- Konfigurace na úrovni skupiny nebo agenta
  - Interval hlášení
  - Konsolidace logů
  - Frekvence rotace logů
  - Adresa pro SMTP varování

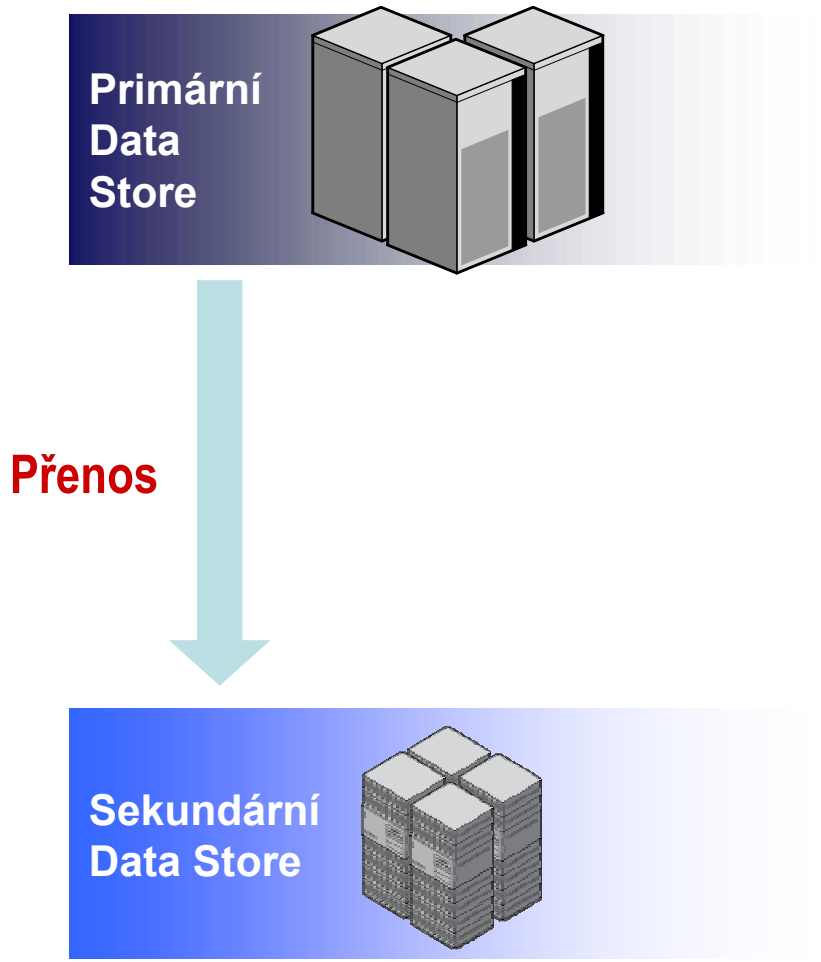


Archivace pošty

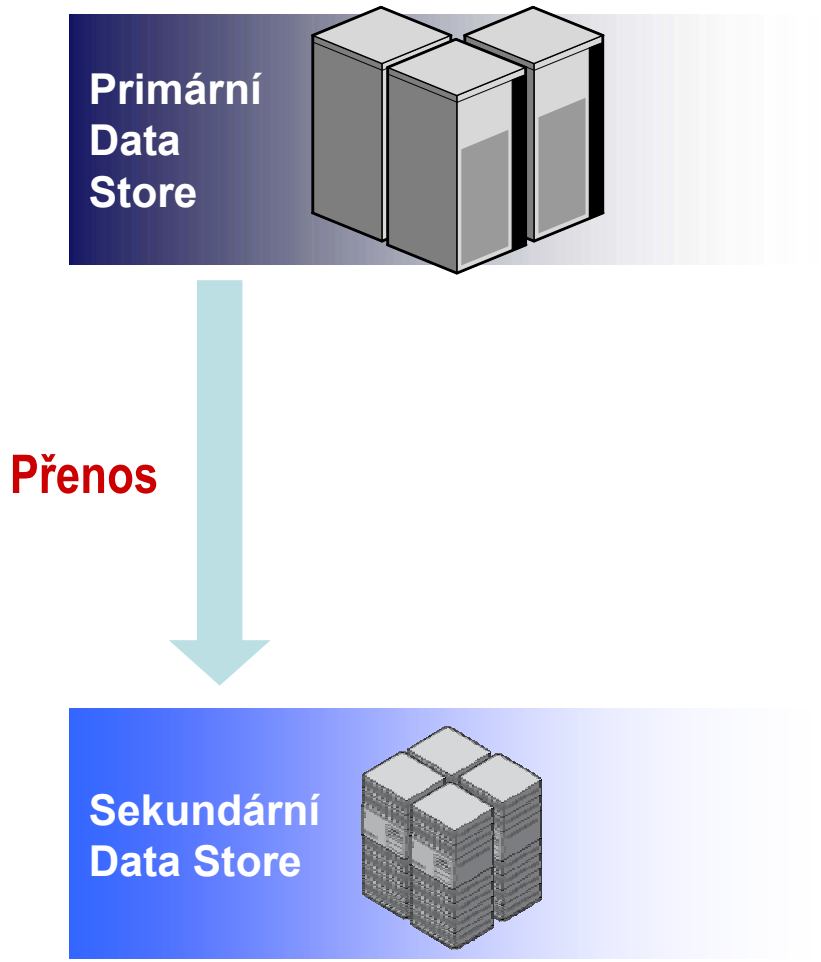
Enterprise Vault



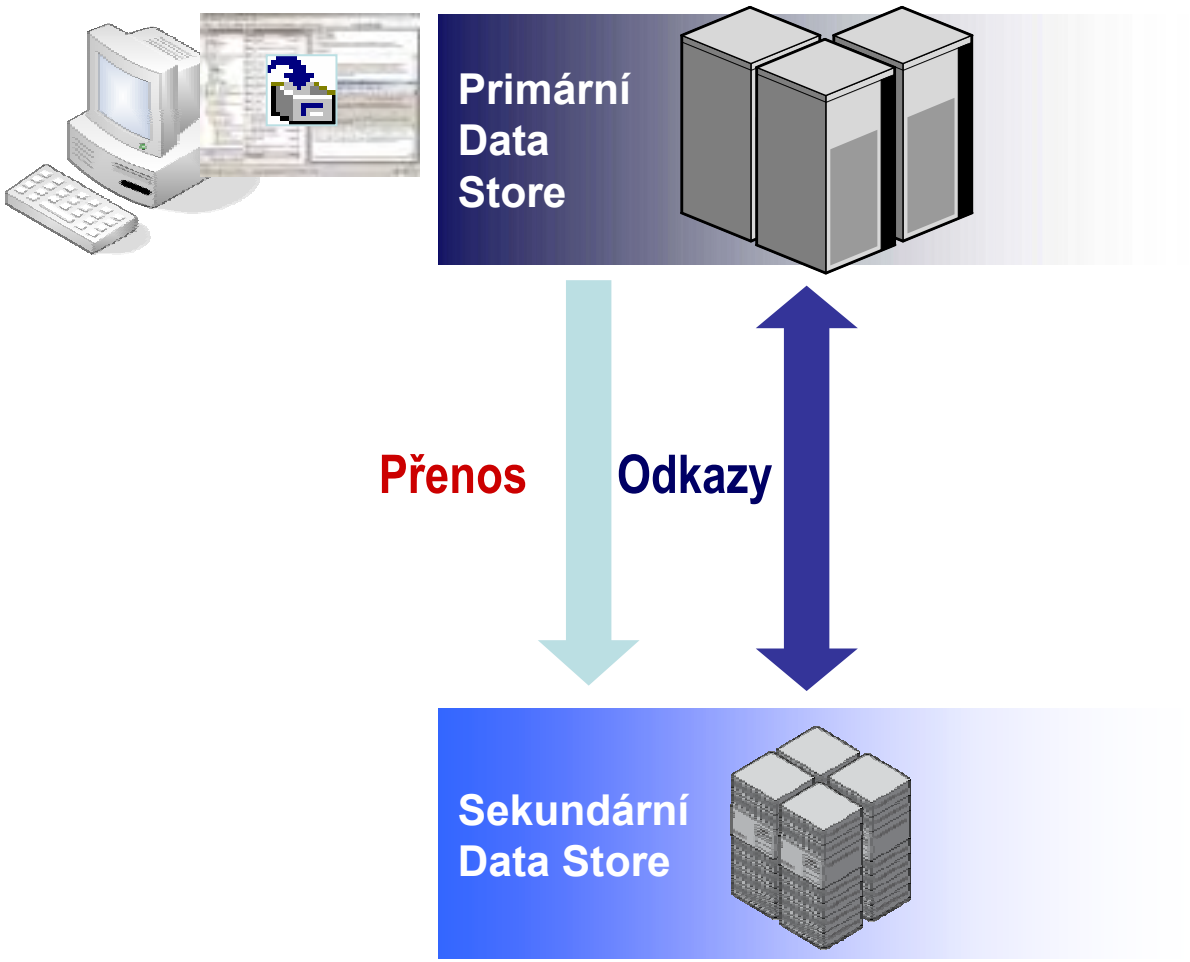
Enterprise Vault



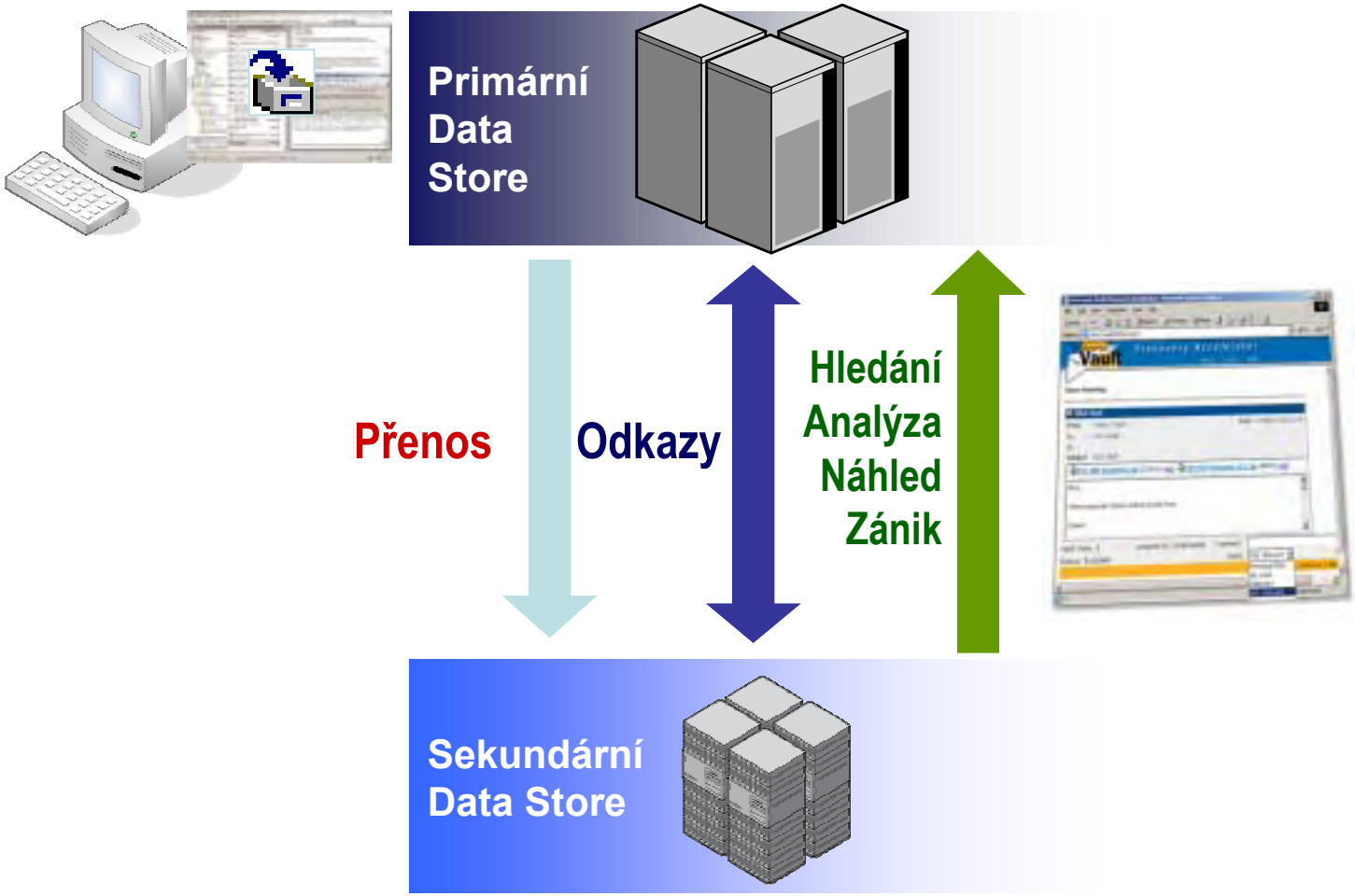
Enterprise Vault



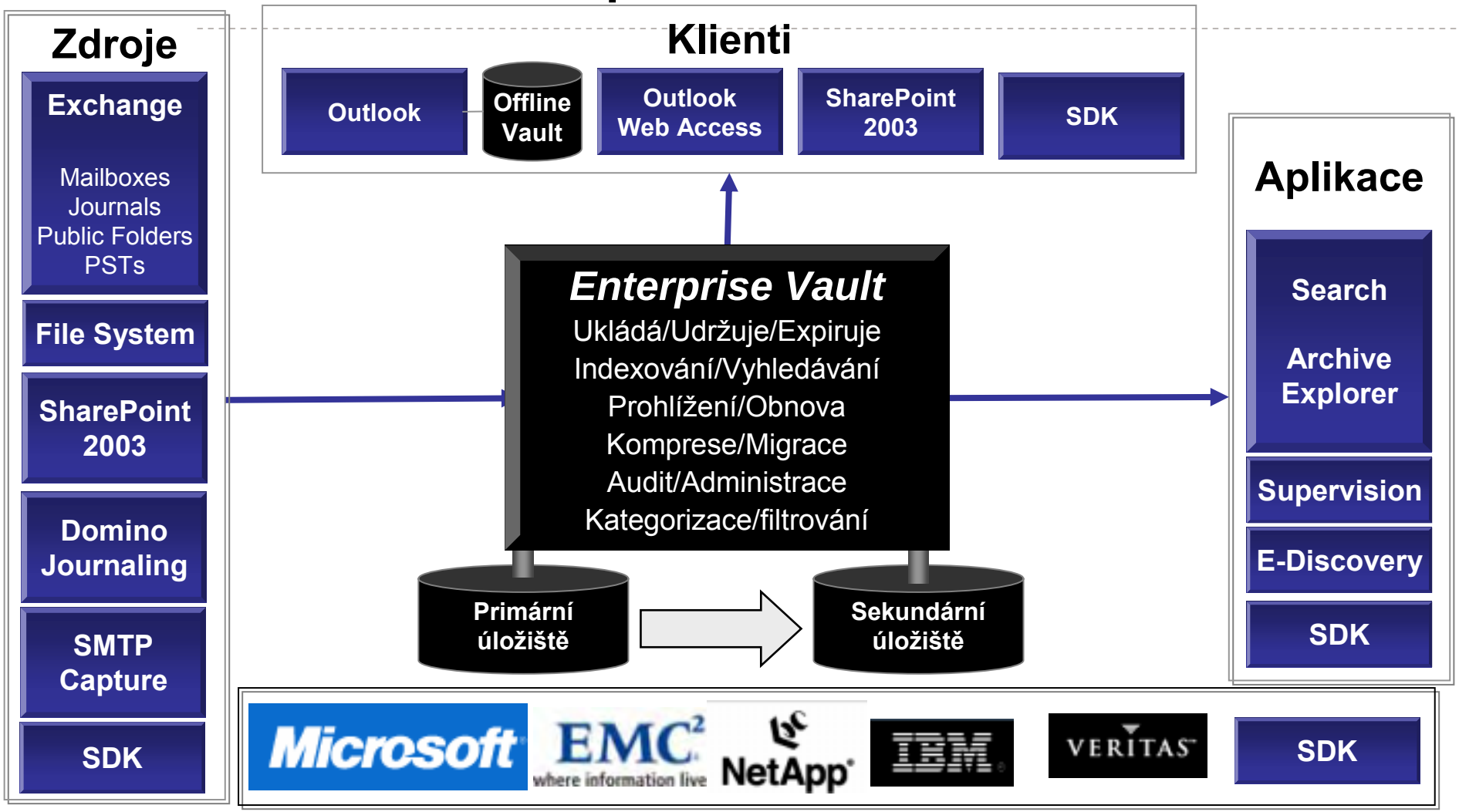
Enterprise Vault



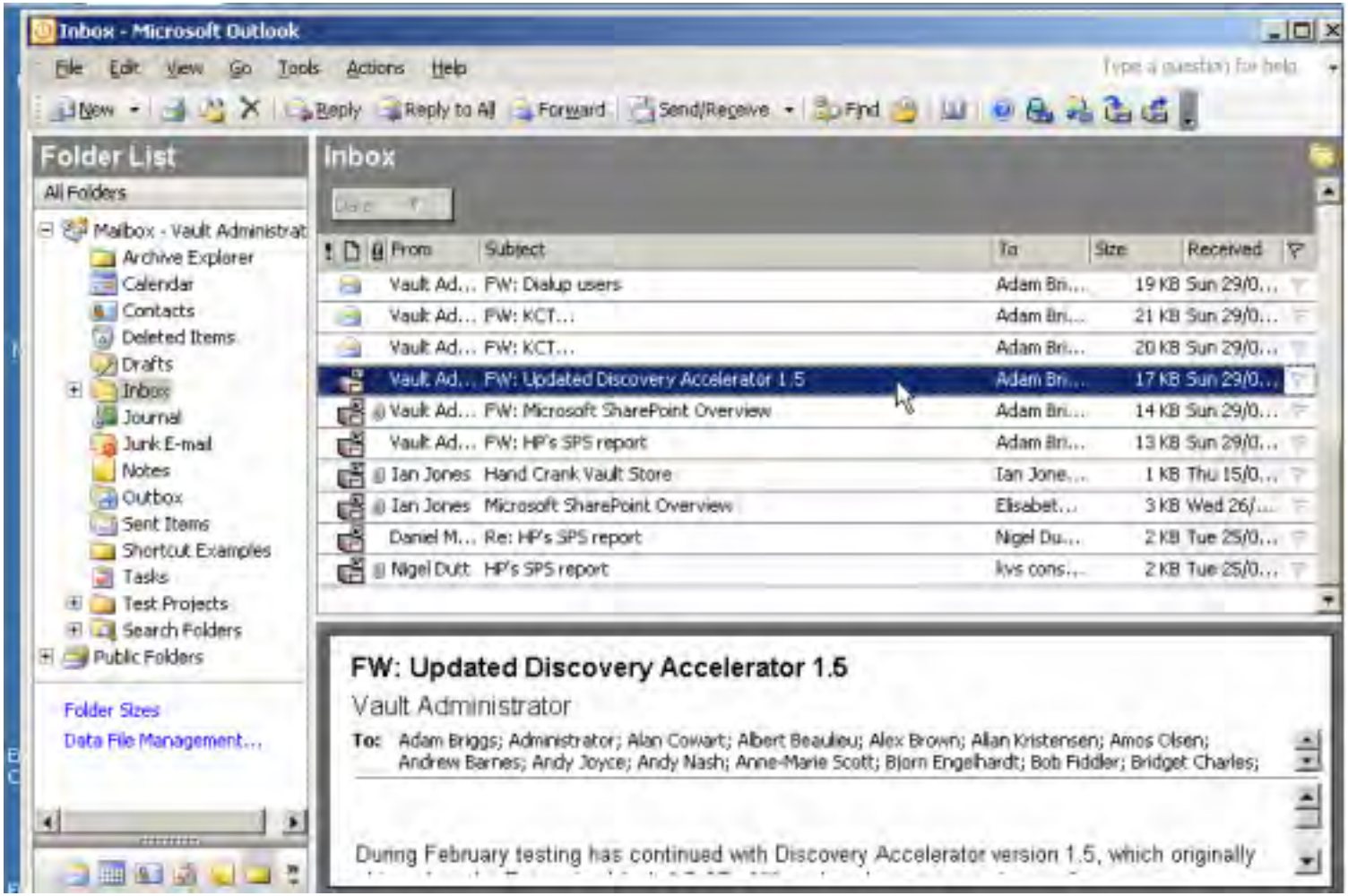
Enterprise Vault



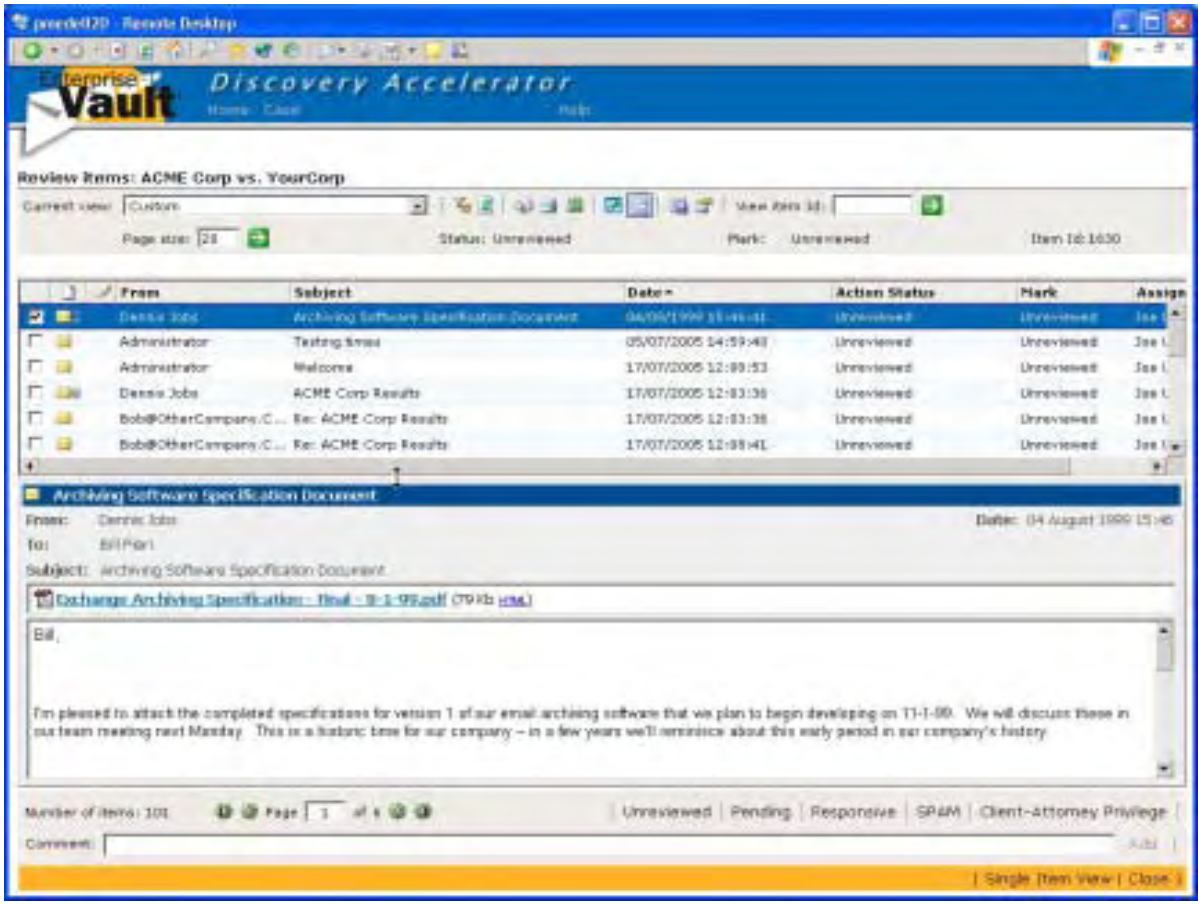
Architektua Enterprise Vault



Bez nárazu na koncového uživatele !!!

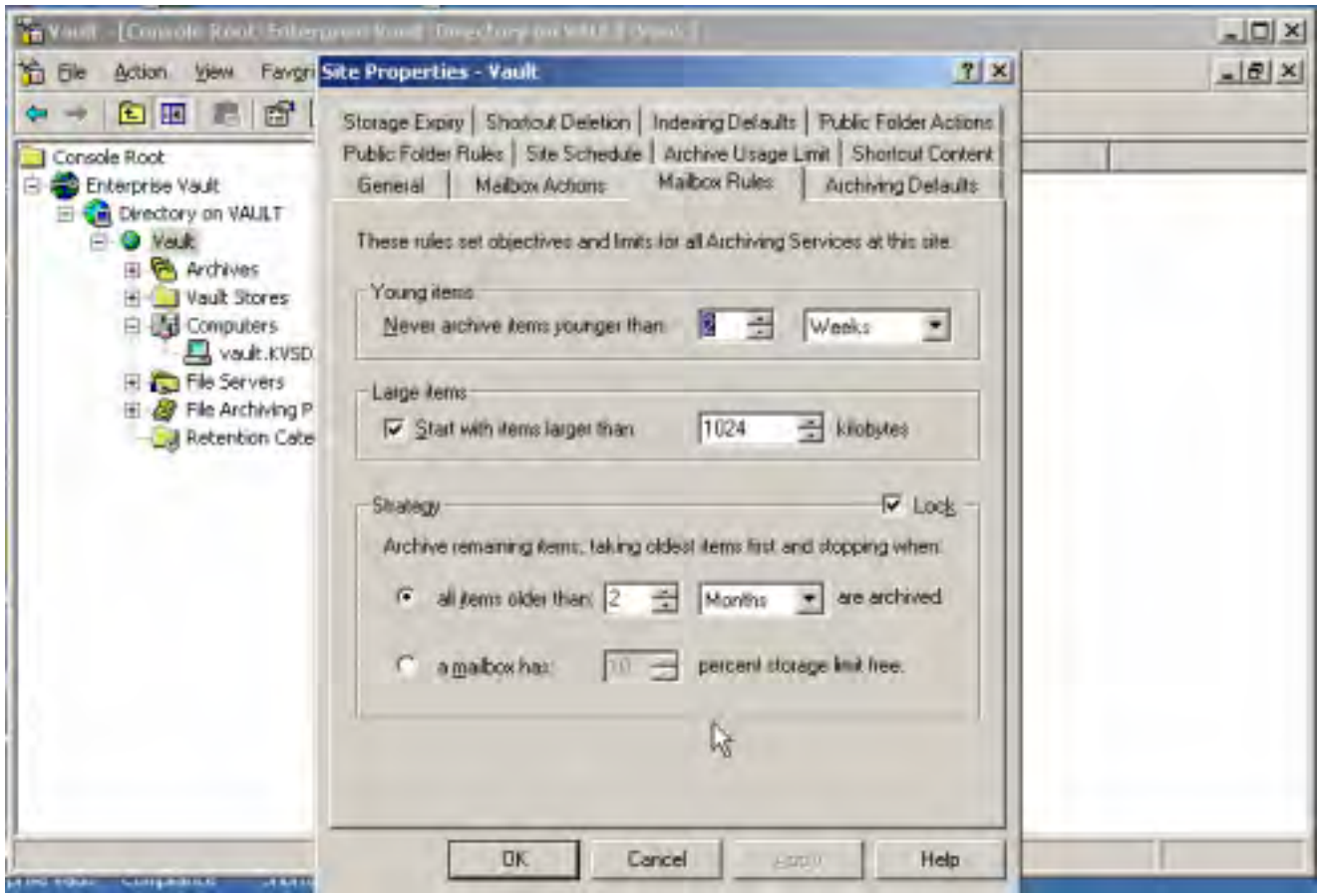


Discovery Accelerator – vytvořen pro právní účely

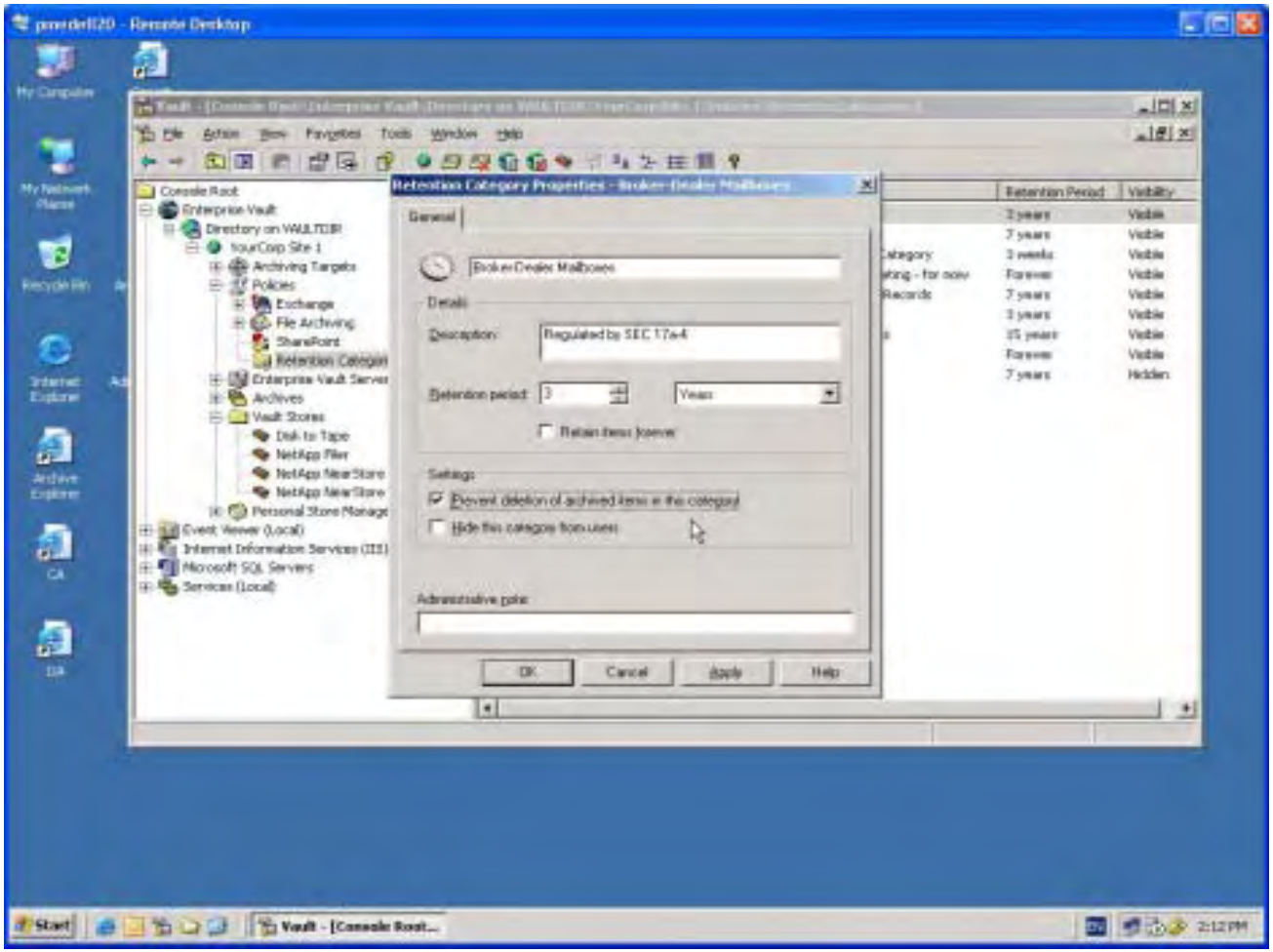


- Postaven na účelech
- Web-based rozhraní
- Roles-based přístup
- Vytváření případů
- Přidělení rolí
- Nastavení hledání
- Prohlížení a označení
- Export a další použití

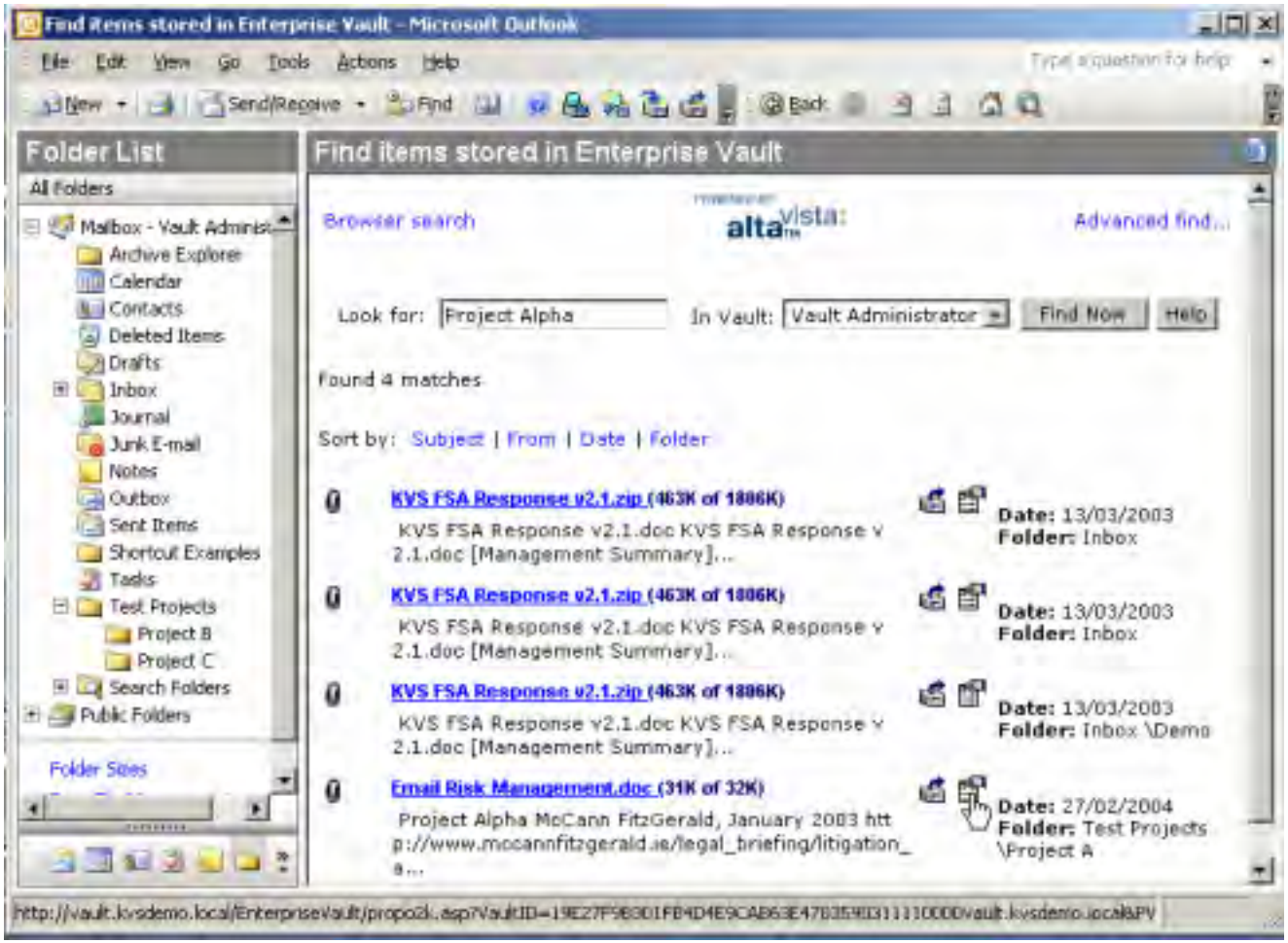
Flexibilní politiky archivace



Flexibilní retenční politiky

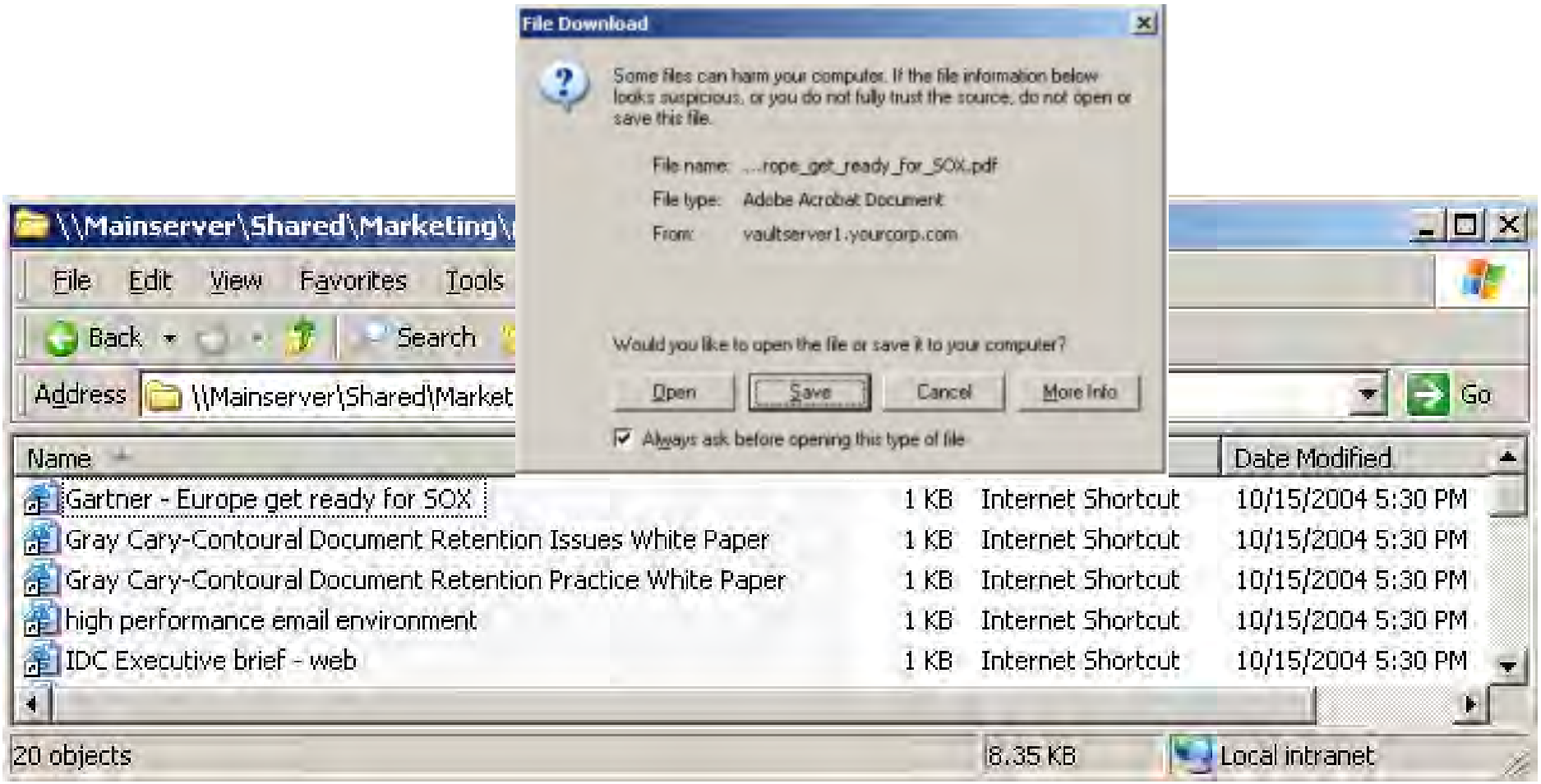


Integrované vyhledávání

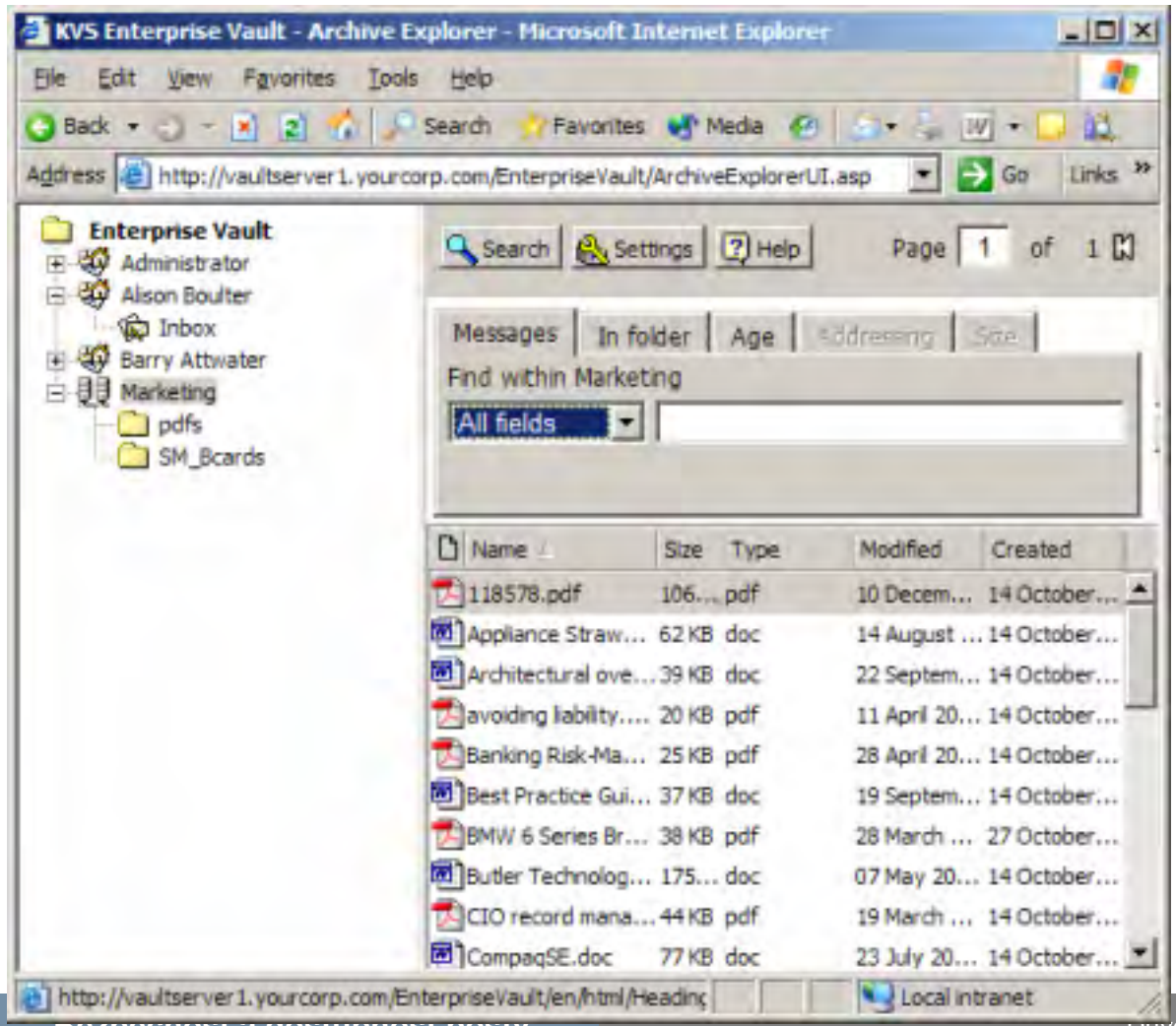


Pohled na soubory v archivu (přes EV službu)

Práce s uloženými internetovými odkazy



Vyhledání a obnova koncovým uživatelem

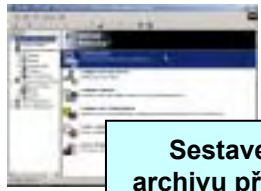


- Volitelné indexování
- Metadata a obsah souboru
- Podpora 250+ typů
- Web-based hledání
- End-user obnova
- Archive Explorer (Web-based dir pohled)

Propojení zálohování a archivace

Integrované obnovení dat/vyvolání zprávy uživatelem

Integrované řízení zálohování a archivace



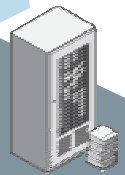
Sestavení archivu přímo z existující pásek se zálohami

Proces archivace

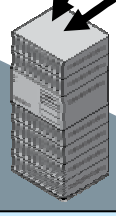
Optimalizace zálohování pomocí archivace statických dat

Proces zálohování

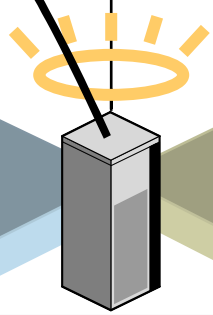
Vault



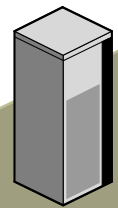
Library Archive



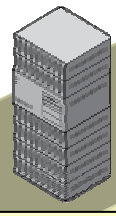
Disk Archive



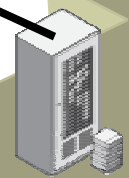
Primary Data



Mirror



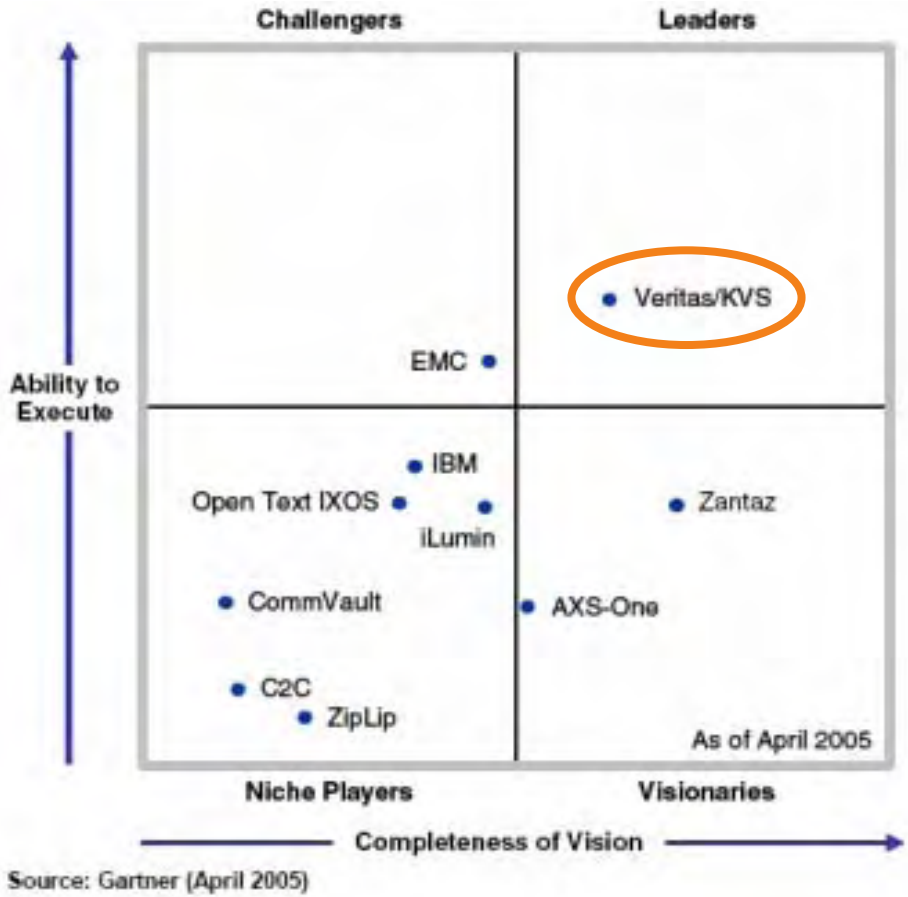
Disk Stage



Tape

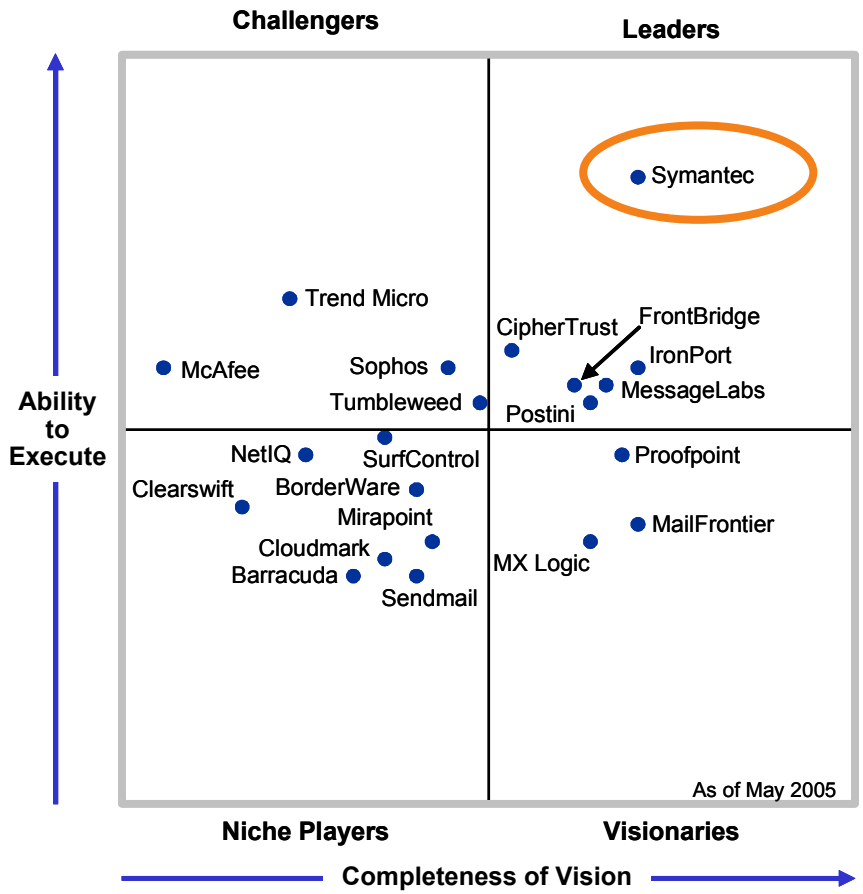
Migrace archivu na pásky pomocí NetBackup

Vedoucí postavení v archivaci pošty



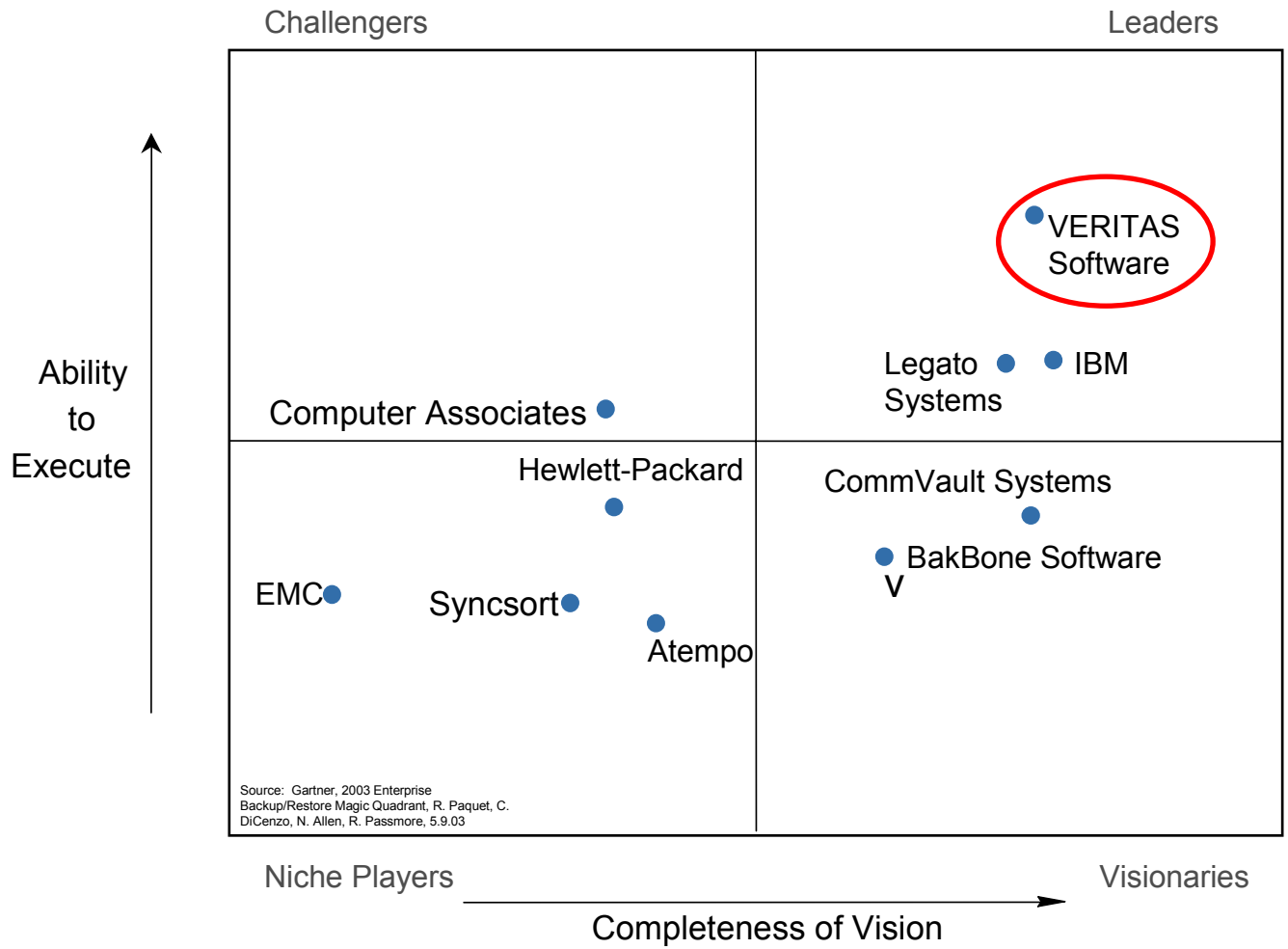
Gartner 2005 Magic Quadrant for E-mail Active-Archiving Market

Vedoucí postavení v bezpečnosti pošty



Gartner 2005 Magic Quadrant for E-mail Security Boundary

Vedoucí postavení v zálohování a obnově



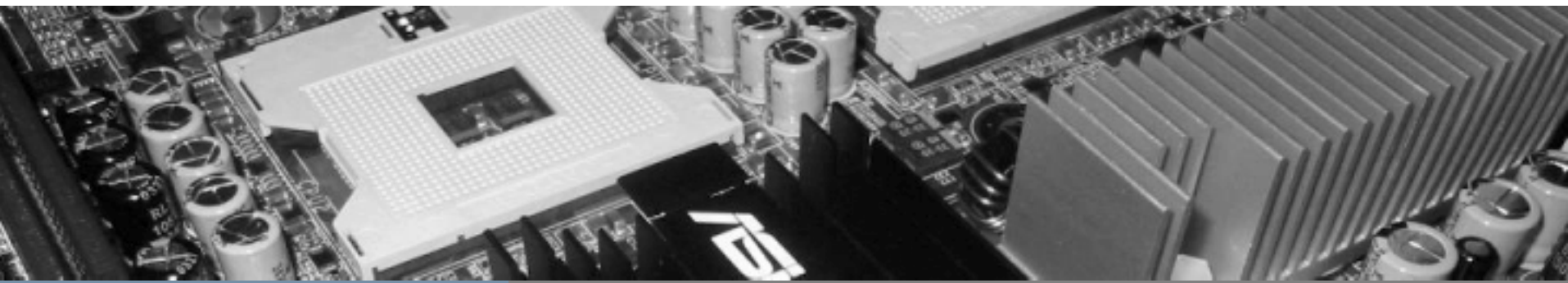
Vysoká dostupnost pošty

Dosažení vhodné úrovně dostupnosti

Časté omyly v chápání vysoké dostupnosti

- Je to extrémně nákladné
- Je to velmi složité
- Je obtížné měřit efekt
- Je to jiný problém než obnova po výpadcích
- Nelze to testovat

- To platí JEN KDYŽ VOLÍTE TRADIČNÍ PŘÍSTUPY !!!



Vysoká dostupnost nemusí být extrémně nákladná

Mýtus:

- Hardwarová redundance
- Omezené O/S
- Ubohá míra využití

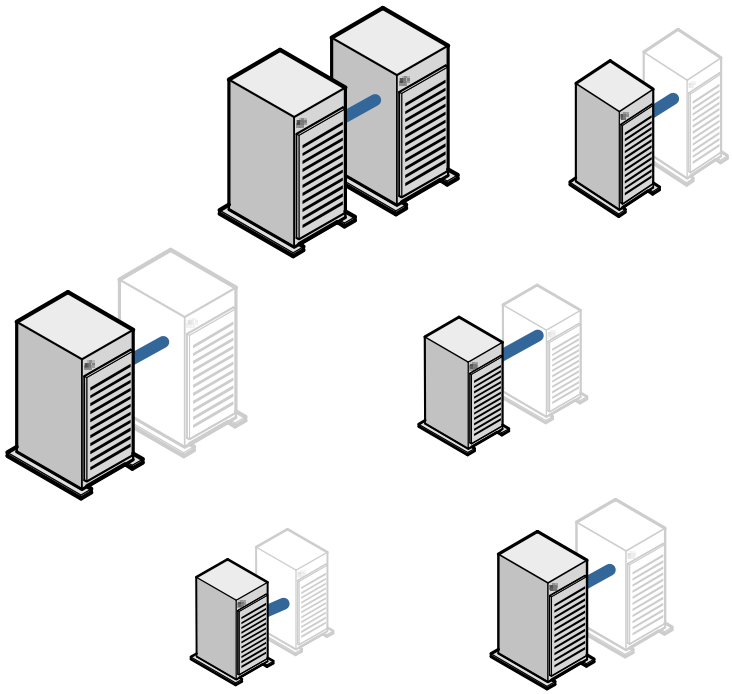
Doporučení:

Přidejte clusterování, ne hardware

- Všechny platformy
- Optimální využití serverů

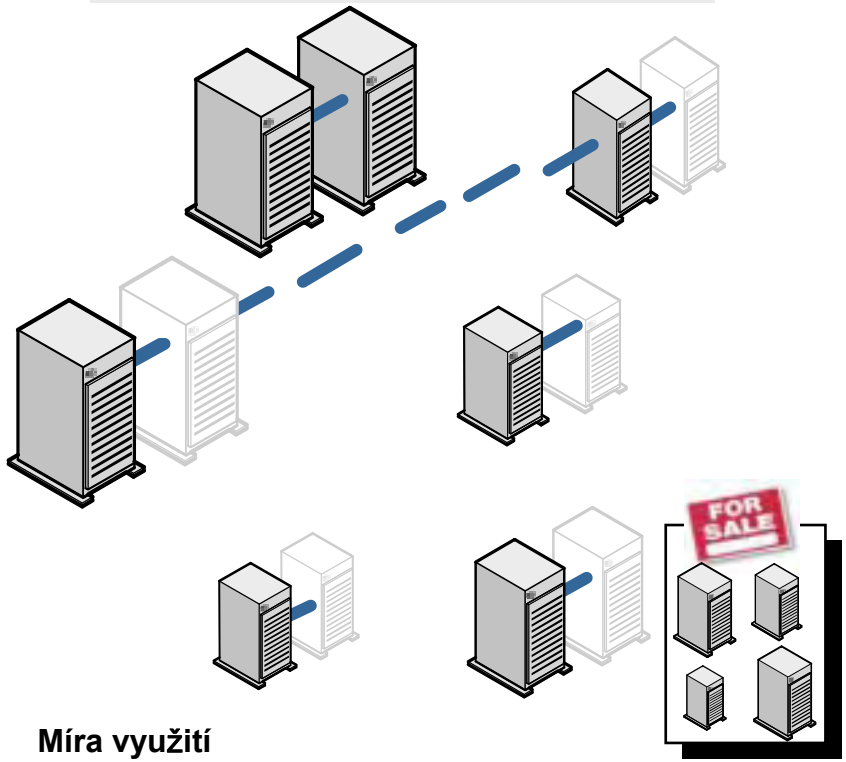
Zvýšení hodnoty HW investic

Tradiční přístup



Míra využití:

Doporučený přístup

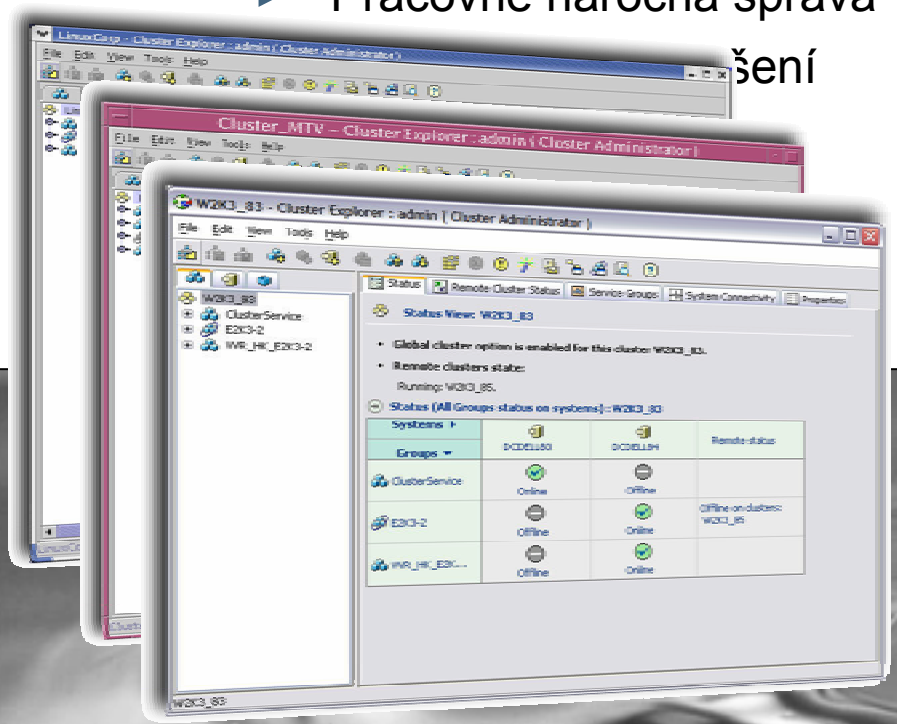


Míra využití

Vysoká dostupnost nemusí být vůbec složitá

Mýtus:

- Nákladná instalace
- Nejistota v konfiguracích
- Pracovně náročná správa
- šení



Doporučení:

VERITAS Cluster Server

- Nákladově efektivní instalace
- Cluster simulator
- Jednoduchá správa
- 5 platforem → 1 řešení

Dostupnost může být přesně měřena

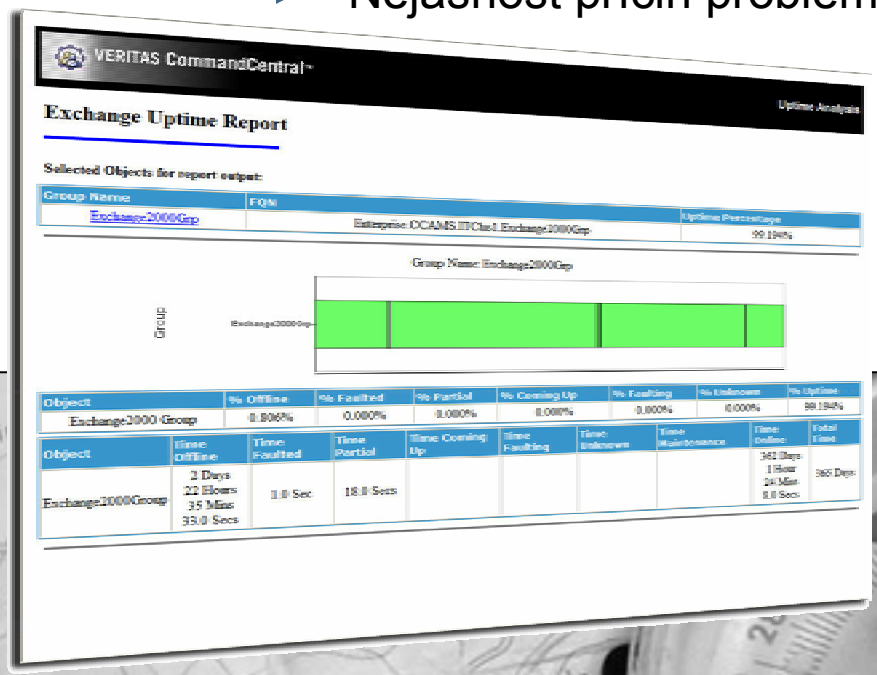
Mýtus:

- Neměřitelná SLA
- Žádné historické zprávy
- Nejasnost příčin problémů

Doporučení:

Použijte integrovaný reporting

- Sleduje dostupnost
- Hlásí výsledky
- Identifikuje problémy a jejich příčiny



Obnova po výpadcích může být vzdálena jedno kliknutí

Mýtus:

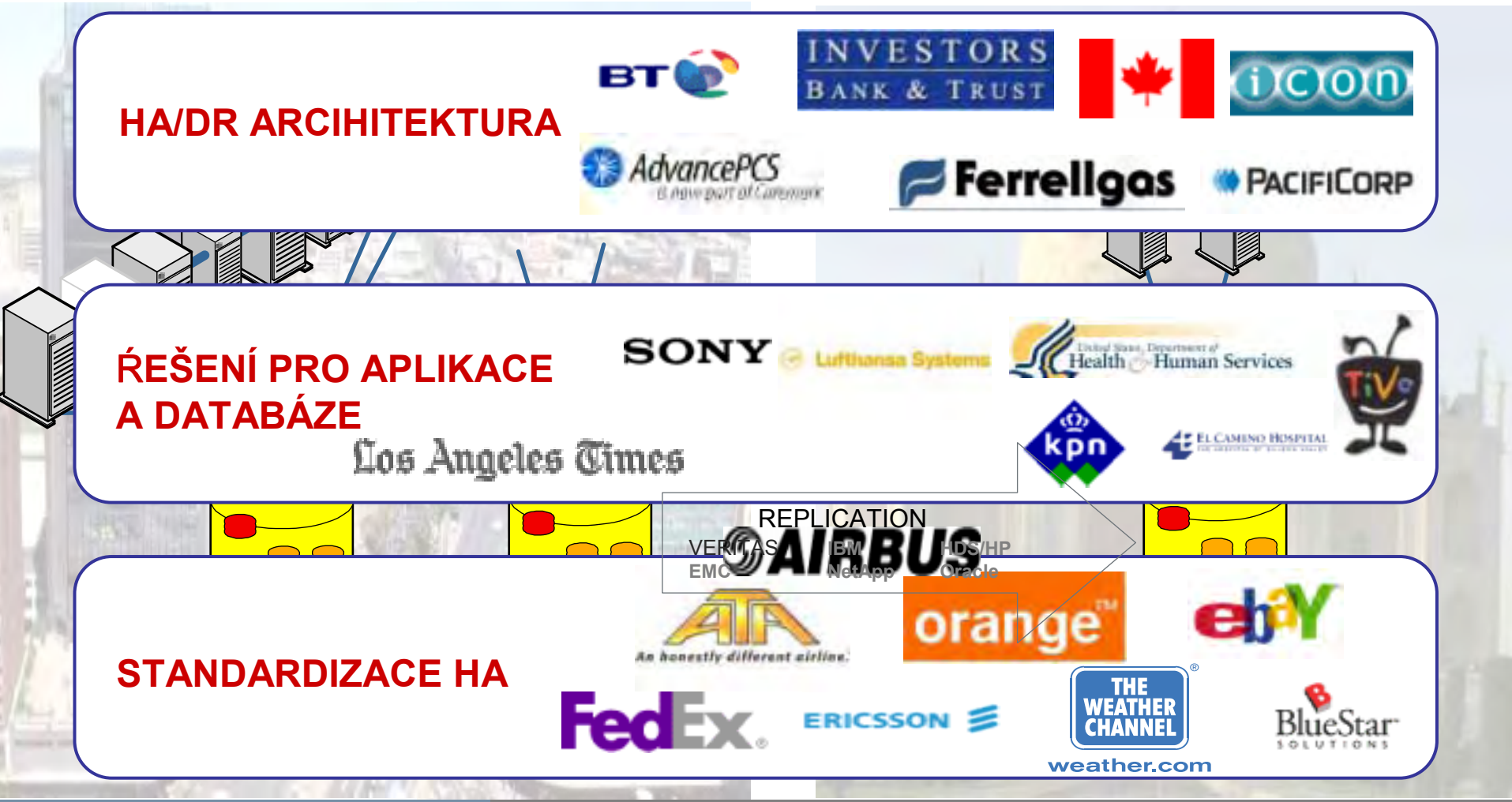
- Extrémně nákladné
- A co aplikace?
- Nedosažitelné

Doporučení:

Chraňte data a aplikace

- Integrovaná technologie
- Automatizované kroky obnovy

Řešení dostupnosti datových center



Replikace může být neprůstřelná a efektivní

Tradiční přístup:

- Příliš nákladná řešení
- Zcela proprietární
- Nepokryje vzdálenost

Doporučení:

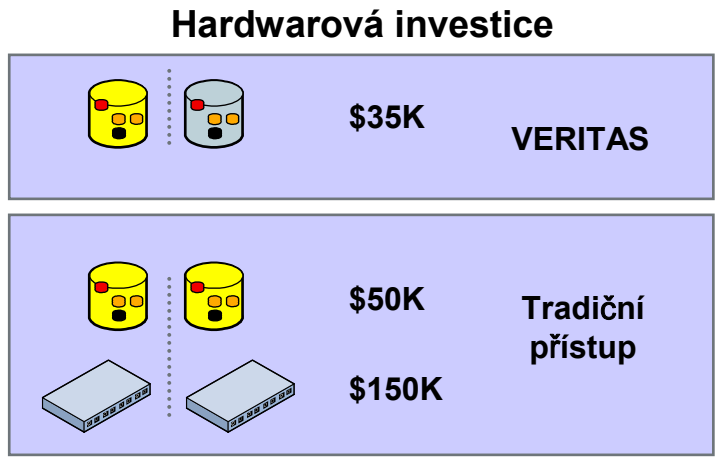
Replikovaný Volume

Neprůstřelná replikace přes…

- jakýkoliv hardware
- jakoukoliv síť
- na jakoukoliv vzdálenost

“Náklady byly důležitým kritériem. Narozdíl od konkurentů, VERITAS Volume Replicator nevyžadoval další hardware a dramaticky snížil celkové náklady pořizovaného řešení.”

IT Director, Banco Santander International



Dostupnost může být snadno testována

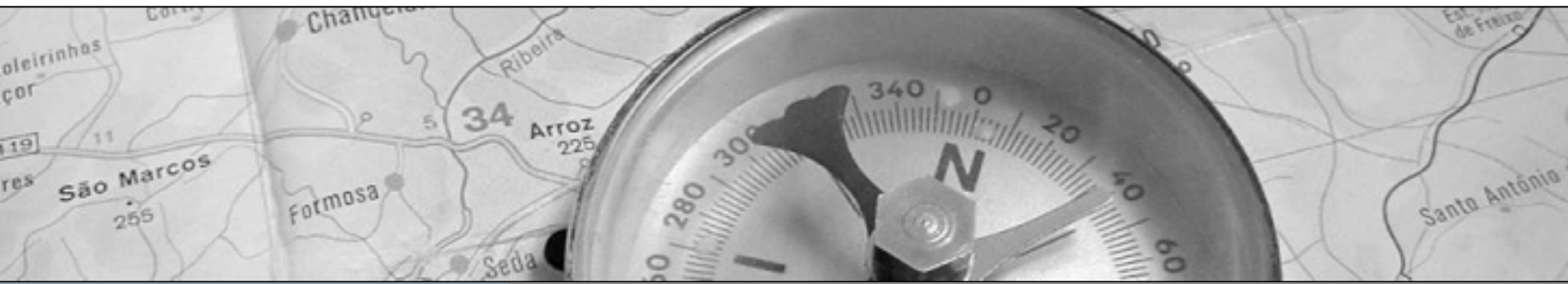
Mýtus:

- Přetrvává riziko výpadku
- Časová náročnost ověření
- Slepá víra v účinnost

Doporučení:

Spusťte „Firedrills“

- Žádné produkční dopady
- Kdykoliv
- Znalosti a jistota



symantec.

Děkuji za pozornost