How Much Does That Computer Really Cost

The OpenVMS Advantage

Agenda

- Introduction
  - What are we calculating & why
- Hard to Calculate Lifecycle Costs (Hidden)
  - Security Threat and Associated Costs
  - Manpower/Staffing Costs
- Total System Operational Costs
- TCO Comparisons
- Other Cost Factors

According to Ziff Davis Enterprise

"While many purchasers of IT solutions evaluate the total lifecycle costs of the solutions they are considering, the initial cost to purchase the solution is normally the single, most dominant consideration. However, a lower cost for a solution across its lifecycle -- from purchase to decommission -- normally necessitates a higher initial price point. An additional consideration is that while the initial purchase cost is specific and must be spent, the calculation of the lifecycle savings that justify it is inherently less accurate. "

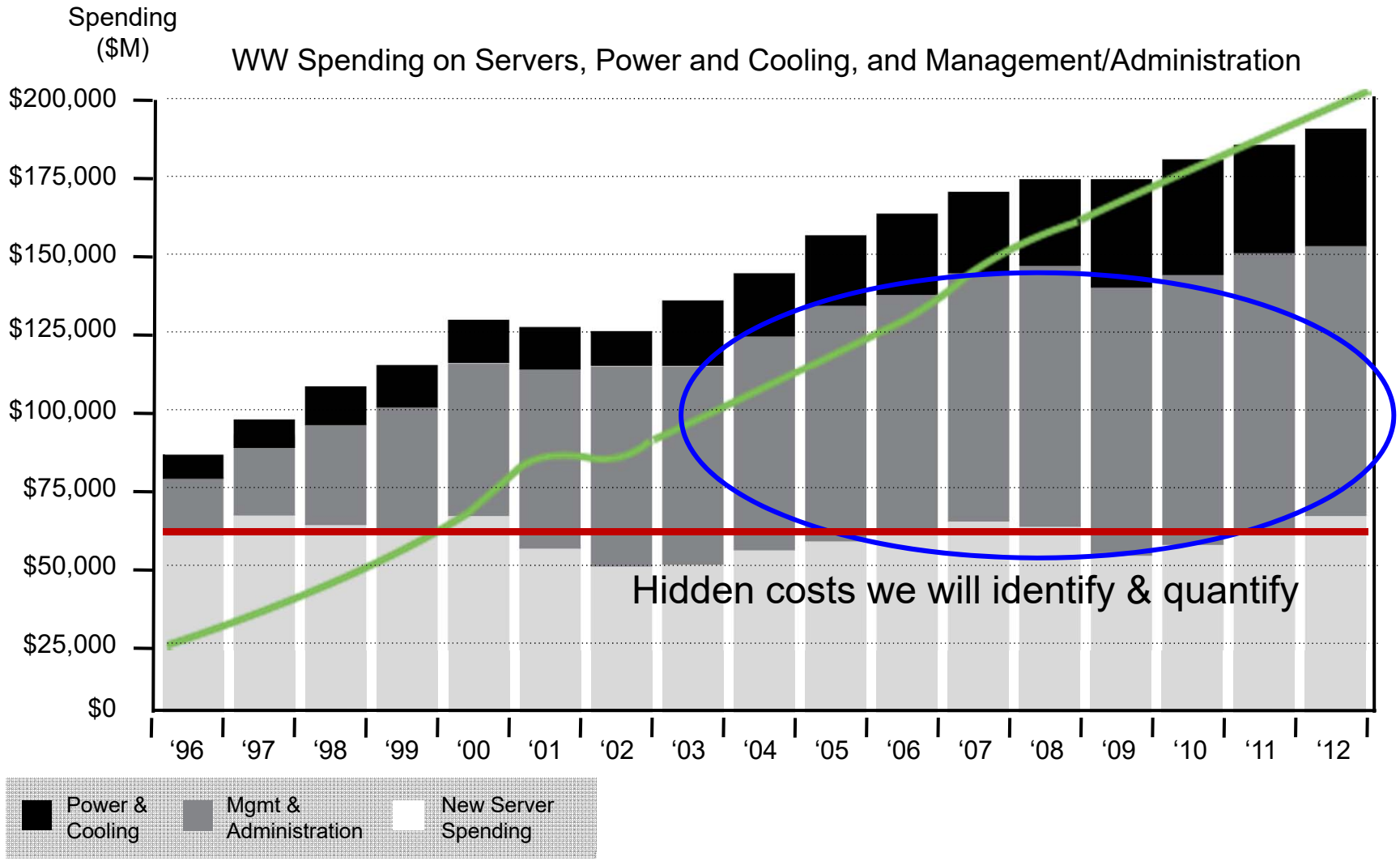
According to Ziff Davis Enterprise

"While many purchasers of IT solutions evaluate the total lifecycle costs of the solutions they are considering, the initial cost to purchase the solution is normally the single, most dominant consideration. However, a lower cost for a solution across its lifecycle -- from purchase to decommission -- normally necessitates a higher initial price point. An additional consideration is that while the initial purchase cost is specific and must be spent, the calculation of the lifecycle savings that justify it is inherently less accurate. "

Until Now!

WORLDWIDE SERVER MARKET (1996-2012)

Operational Costs Rise Dramatically



Source: IDC "Mission-Critical Computing and Unix Systems", Oct 2009

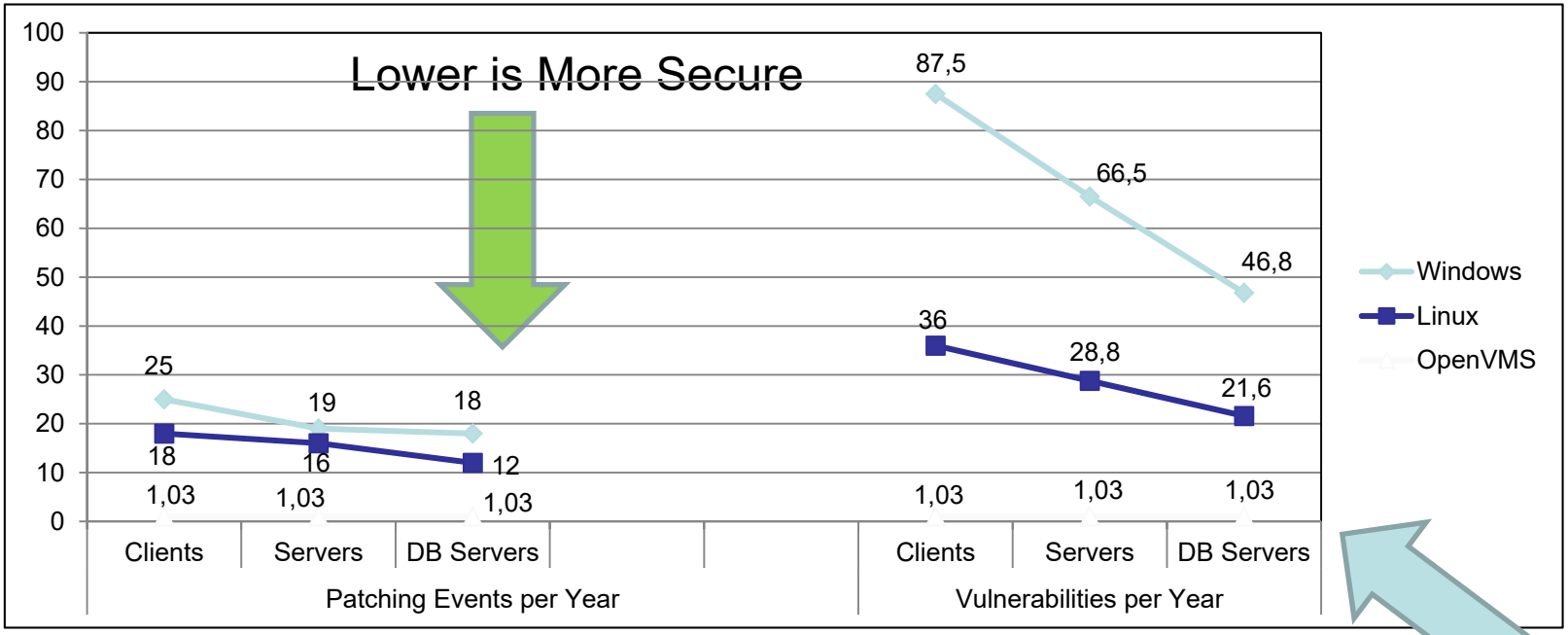
vms Software

Security Threats

and

Associated Costs

Security Patches Per Year



Average Number of Vulnerabilities per Patching Event			
	Windows	Linux	OpenVMS
Clients	3.5	2.0	1.0
Servers	3.5	1.8	1.0
DB Servers	2.6	1.8	1.0

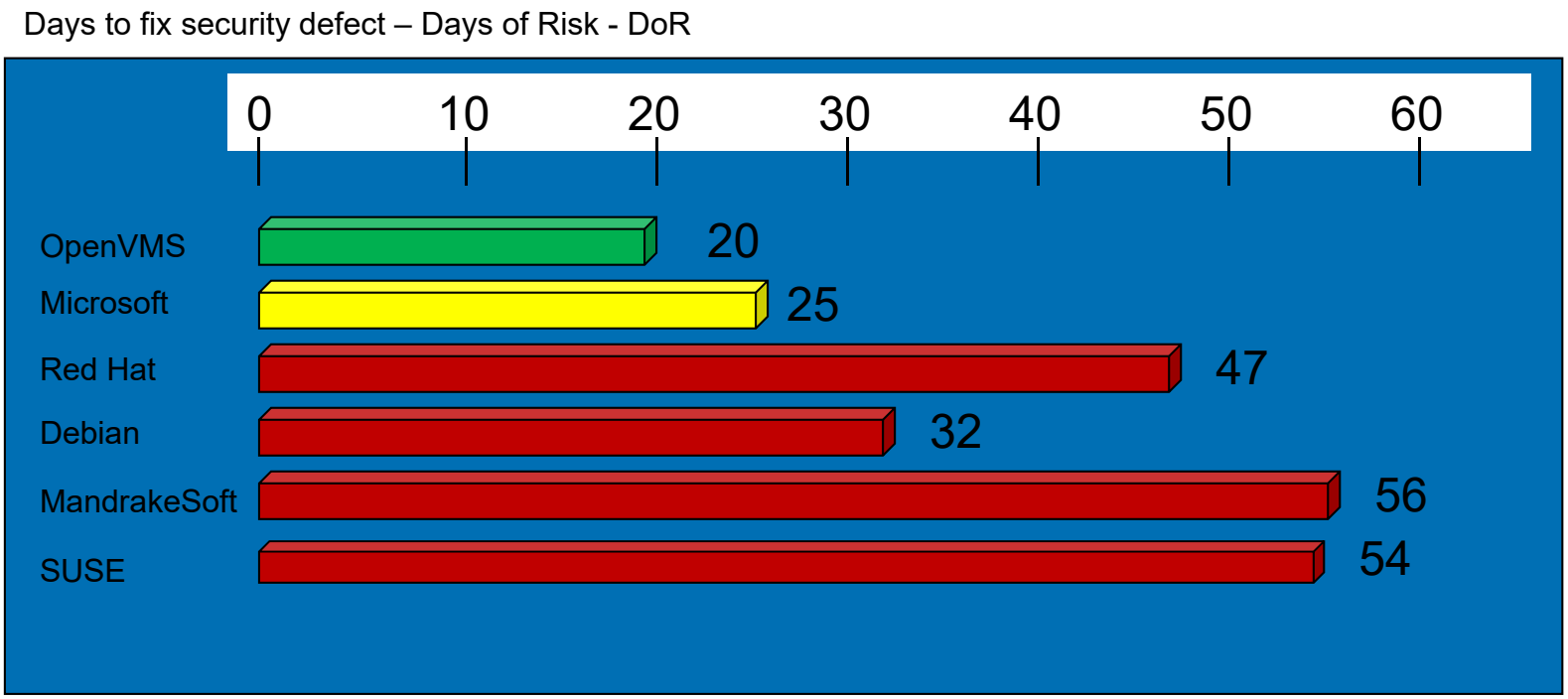
OpenVMS is more than an order of magnitude (>10X) more secure than competitor OSes

VMS – Average per year over 37 years

Source: http://download.microsoft.com/download/1/7/b/17b54d06-1550-4011-9253-9484f769fe9f/TCO_SPM_Wipro.pdf

vms Software

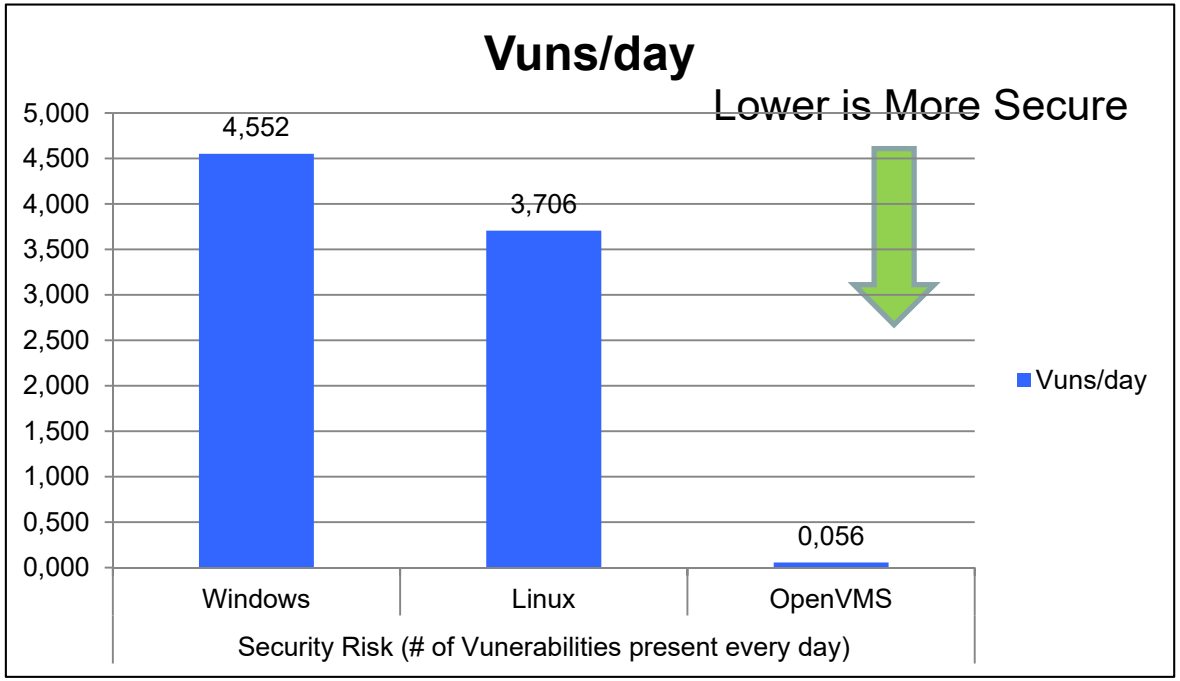
Security Distribution Risk



This is the average time in days to fix a defect (once discovered) and provide a patch kit to the customer

Source: http://download.microsoft.com/download/1/7/b/17b54d06-1550-4011-9253-9484f769fe9f/TCO_SPM_Wipro.pdf

Security Risk



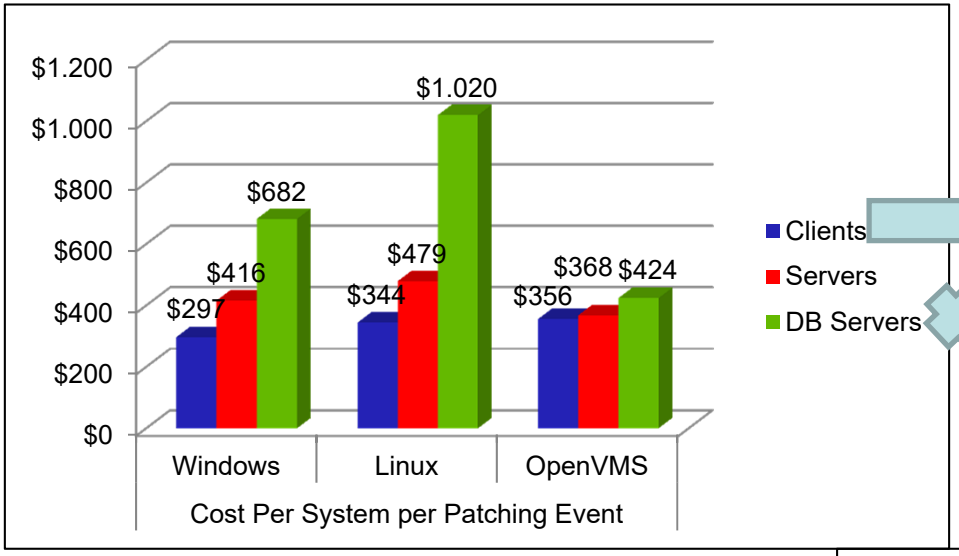
What do the previous slides tell us?

OpenVMS has 66X – 81X less outstanding defects on any given day than competitor OSes

- On Windows servers there are an average of 4.5 vulnerabilities present on any given day
- On Linux servers there are an average of 3.7 vulnerabilities present on any given day
- On OpenVMS servers there are an average of .056 vulnerabilities present on any given day

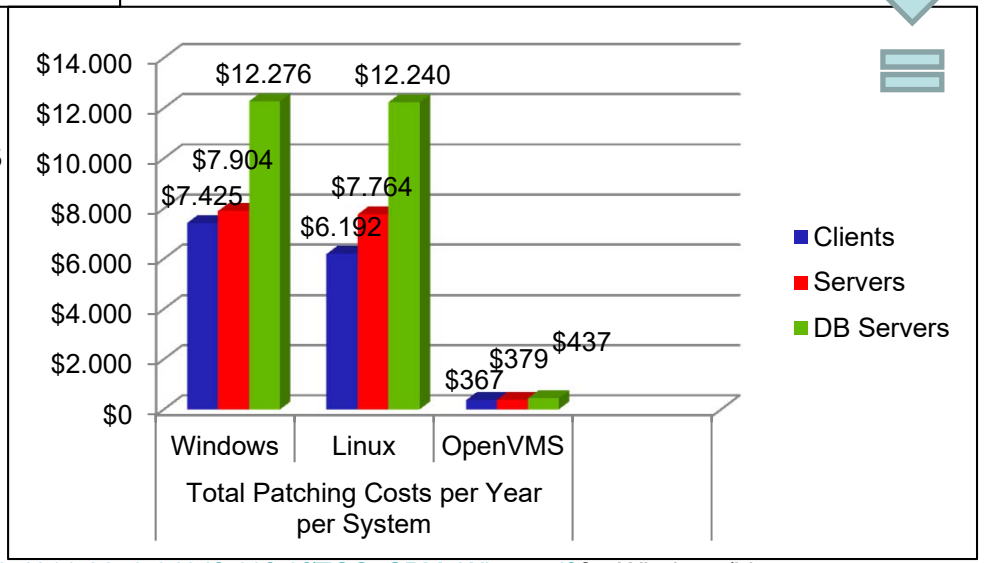
Annual Cost of Security Patching

(Per System – per event & per year)



System	Average Number of Patching Events		
	Windows	Linux	OpenVMS
Clients	25	18	1.03
Servers	19	16	1.03
DB Servers	18	12	1.03

As a more secure OS (significantly fewer patches to apply), OpenVMS is less expensive to patch than Windows and Linux
($7,396 - $11,852 less)



Source: http://download.microsoft.com/download/1/7/b/17b54d06-1550-4011-9253-9484f769fe9f/TCO_SPM_Wipro.pdf for Windows/Linux
OpenVMS Cost Per system = R(C + P)
http://www.absolute.com/Shared/Whitepapers/ABT-AM-PPM-WP-E.sflb.ashx

vms Software

Staffing Cost

Staffing

Clients – End Users supported per System Manager

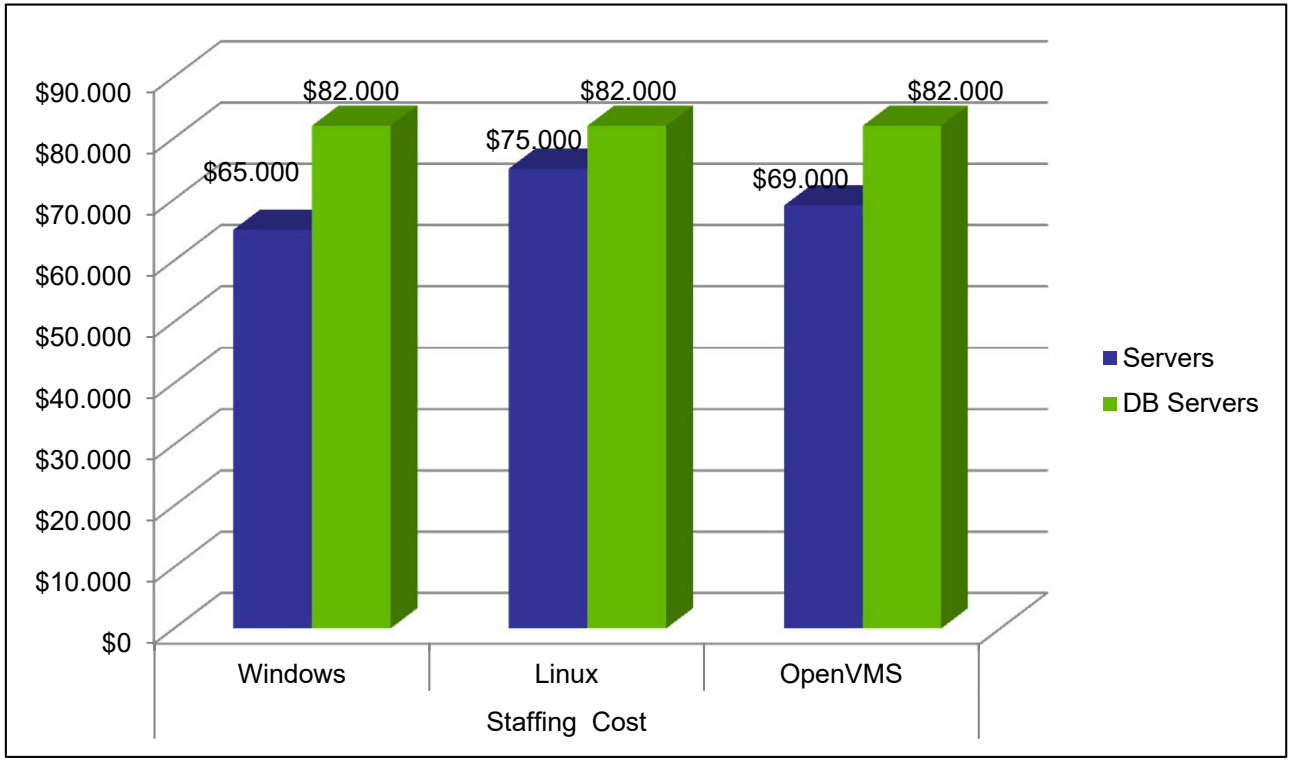
Servers – Servers managed per System Manager

System	Windows	Linux	OpenVMS
Clients	75:1 – 100:1	30:1 - 40:1	50:1 – 60:1
Servers	10:1 – 20:1	30:1 – 40:1	50:1 – 60:1
DB Servers	10:1 – 20:1	30:1 – 40:1	50:1 – 60:1

http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2846915-2,00.html
Yankee group Report - 2005 North American Linux and Windows TCO Comparison, Part 1 – Windows/Linux
Computer World - http://itbenchmark.wordpress.com/2011/03/18/virtualization-and-adminserver-ratio/ 7-2010
OpenVMS - Source: NASA, MSFC – Huntsville Operations Support Center
http://www.lesscher.nl/Portals/0/ITems08/TCO%20ROI%20Overview.pdf

Staffing Costs

(System Manager)



US national average per year

Salary in some US cities may be higher

http://www.simplyhired.com/a/salaries-k-windows+system+manager-jobs.html

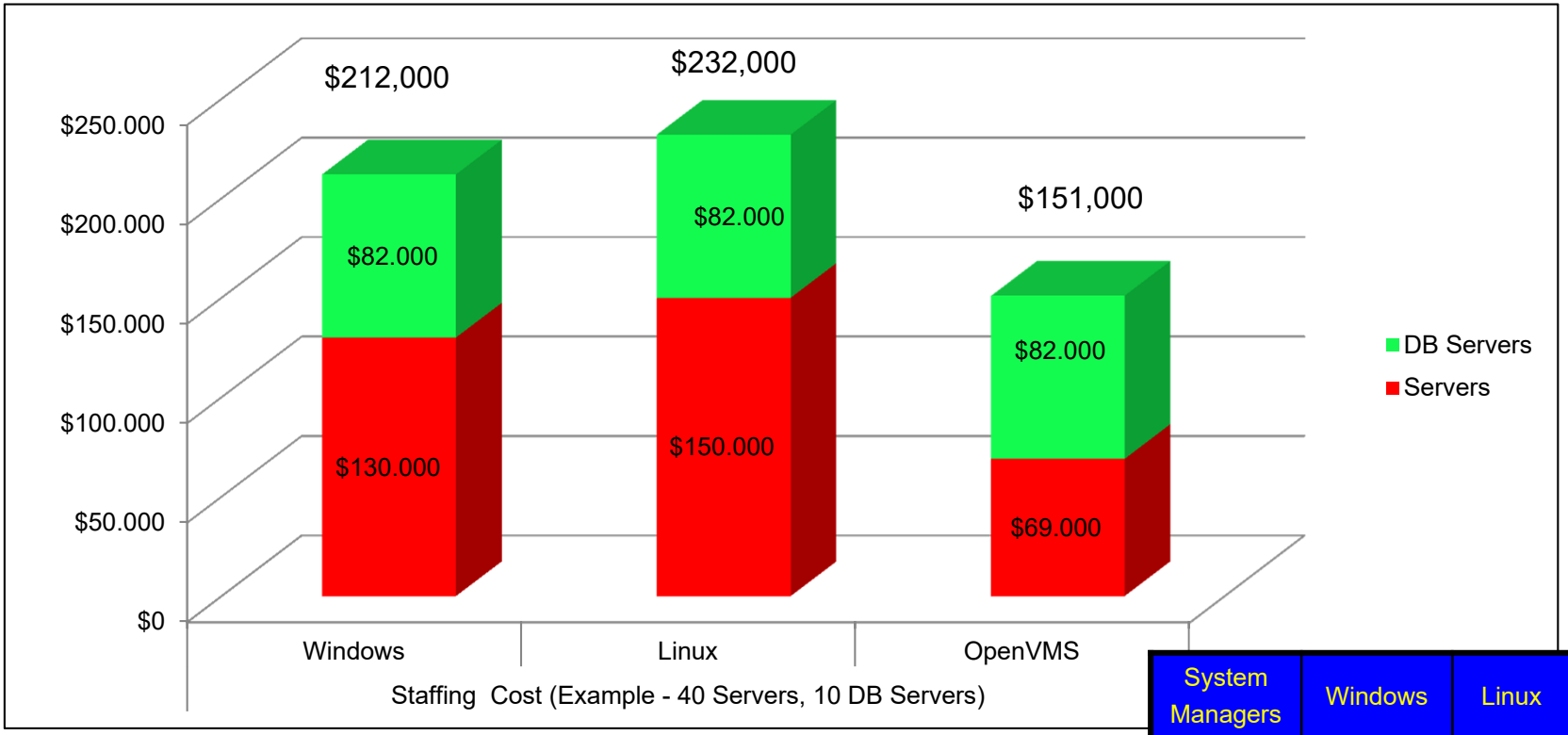
http://www.simplyhired.com/a/salaryies-k-Oracle+db-jobs.html

http://www.simplyhired.com/a/salaries-k-linux+db+system+manager-jobs.html

http://www.simplyhired.com/a/salaries-k-OpenVMS+system+manager-jobs.html

Staffing Costs

Example



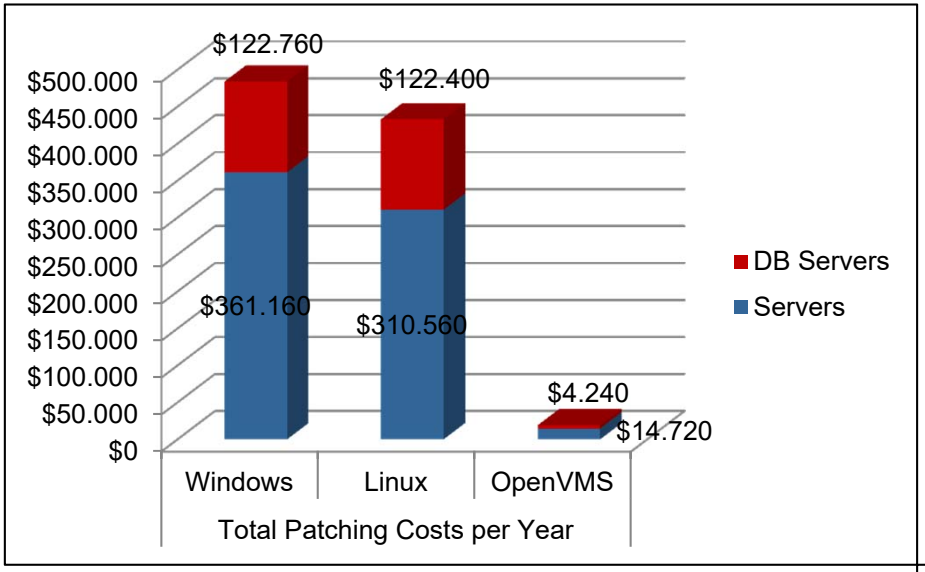
System Managers	Windows	Linux	OpenVMS
Servers (40)	2	2	1
DB Servers (10)	1	1	1

Number of System Managers and their costs to manage 40 Application servers and 10 DB servers

OpenVMS ($151,000) is less expensive to manage than Windows ($212,000) and Linux ($232,000)

System Operational Costs

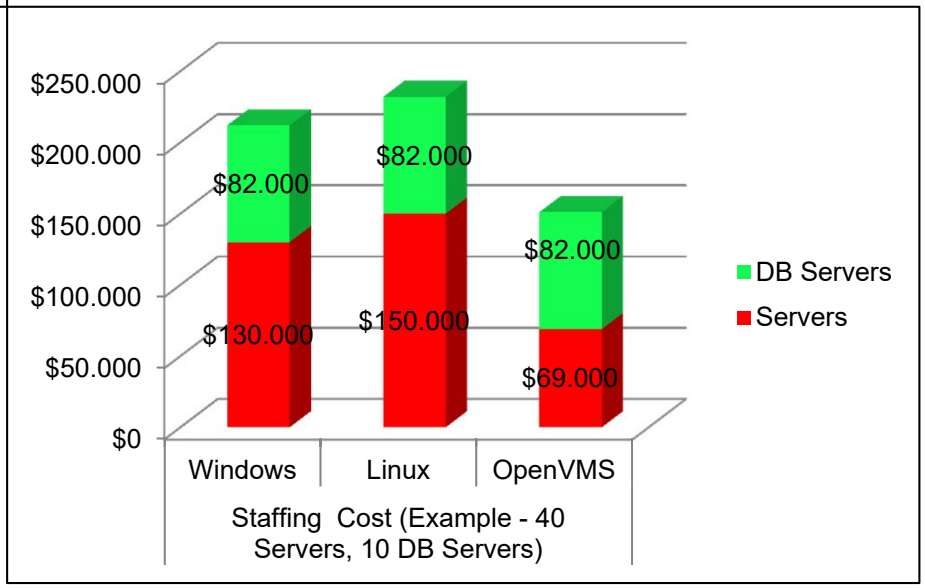
Yearly Operational Costs
(From Previous Example)



For 40 application servers and 10 DB servers

As a more secure OS, VMS is significantly less expensive to patch than Windows and Linux - ($414,000 - $464,960 less)

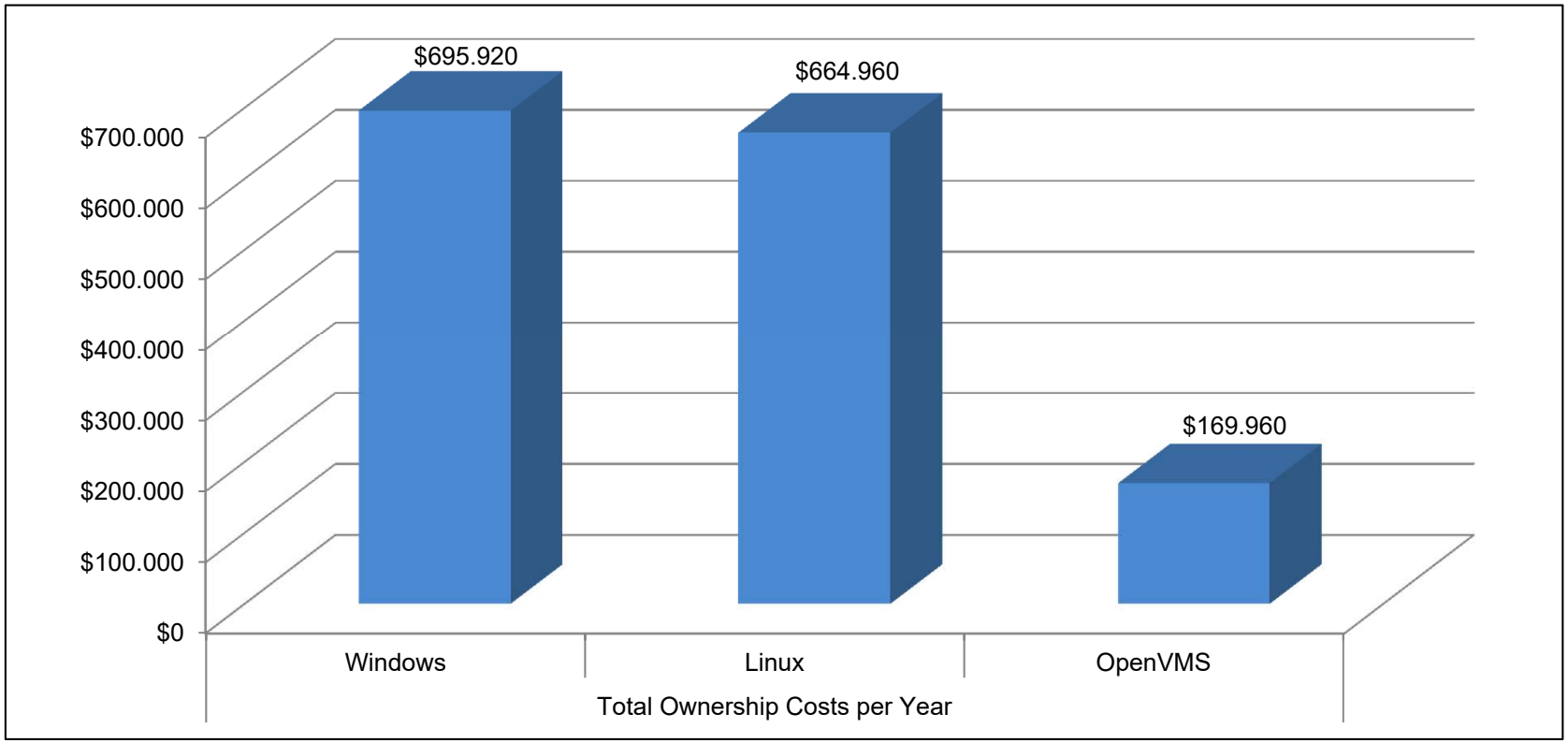
With the highest server to system Manager ratio, VMS requires fewer System Managers which reduces personnel costs - ($61,000 - $81,000 less)



vms Software

Total Yearly Operational Costs
(From Previous Example)

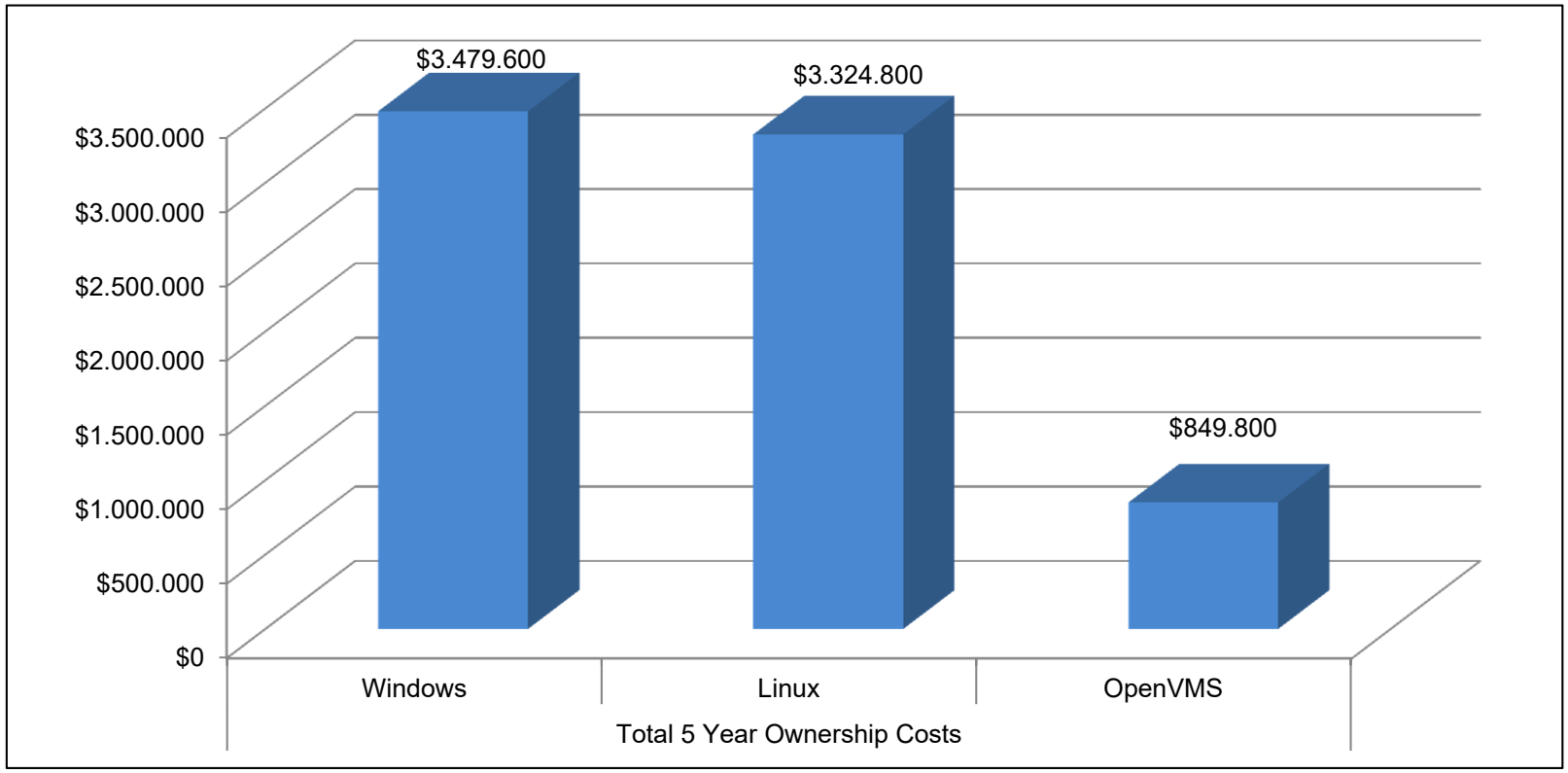
For 40 application servers and 10 DB servers



OpenVMS is 3.9X more cost effective to operate than Linux and 4.1X more cost effective to operate than Windows

5 Year Lifecycle Operational Costs
(From Previous Example)

For 40 application servers and 10 DB servers

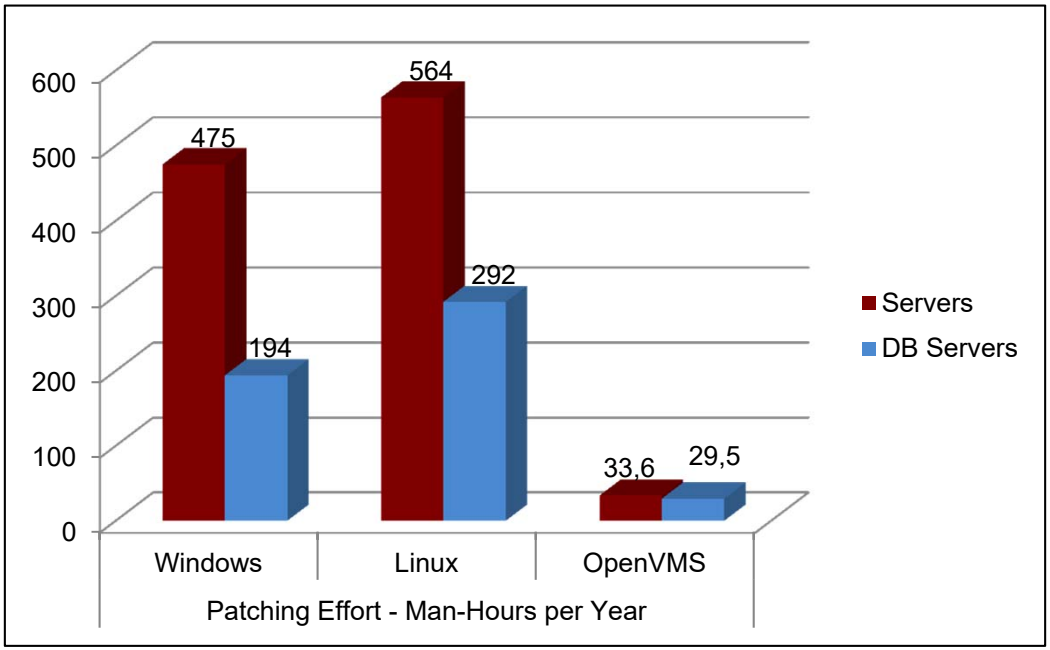


With OpenVMS you can cut $2.47M – $2.62M from the IT budget or provide this amount of business innovation back to your organization over the lifecycle of your system

Patching Effort – Man-Hours per Year

(From Previous Example)

For 40 application servers, 10 DB servers



This is the amount of time System Managers spend annually doing remedial/patching work instead of providing innovation for the organization

OpenVMS System Managers can spend 12X – 15X more time on innovation (less time on patching)

- Windows – Server + DB Server time is 669 hours or 3.8 months
- Linux – Server + DB Server time is 856 hours or 4.9 months
- OpenVMS – Server + DB Server time is 63 hours or 0.3 months

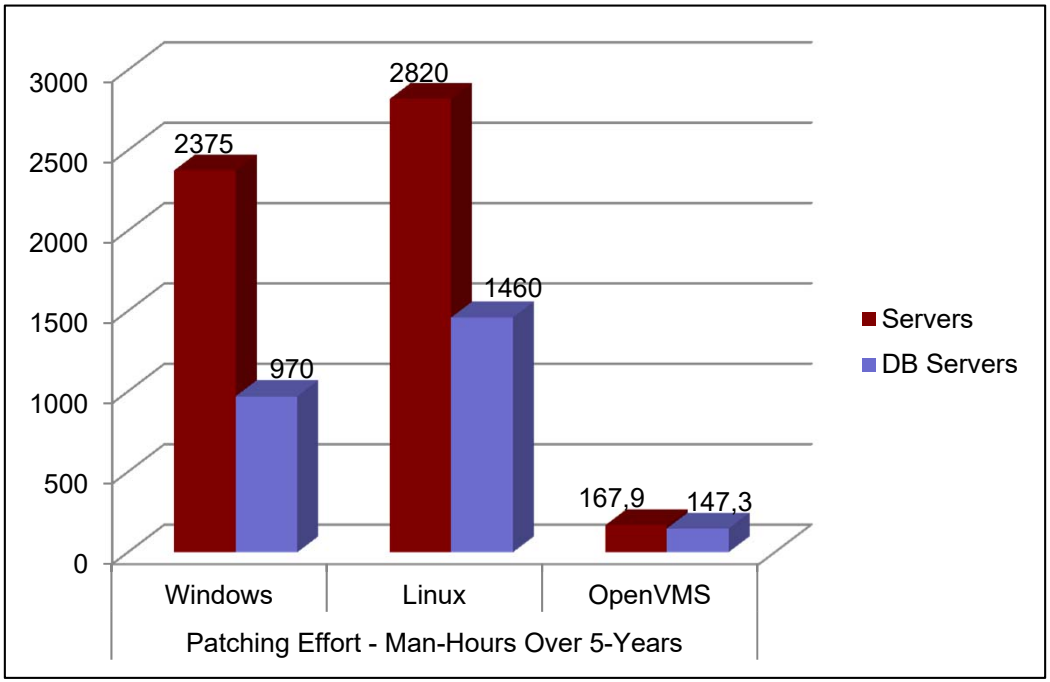
Source: http://download.microsoft.com/download/1/7/b/17b54d06-1550-4011-9253-9484f769fe9f/TCO_SPM_Wipro.pdf for Windows/Linux

OpenVMS – Patch Set up time + (Number of Systems x patch time) * patches per year

5-Year Life Cycle Patching Effort

(Man-Hours Total From Previous Example)

For 40 application servers, 10 DB servers



This is the amount of time System Managers spend over the 5-year lifecycle of the server doing remedial/patching work instead of providing innovation for the organization

Windows - 31% Wasted Time
Linux - 41% Wasted Time
OpenVMS – 2.6% Wasted Time

- Windows – Server + DB Server time is 3345 hours or 19.2 months
- Linux – Server + DB Server time is 4280 hours or 24.6 months
- OpenVMS – Server + DB Server time is 315 hours or 1.81 months

Source: http://download.microsoft.com/download/1/7/b/17b54d06-1550-4011-9253-9484f769fe9f/TCO_SPM_Wipro.pdf for Windows/Linux

OpenVMS – Patch Set up time + (Number of Systems x patch time) * patches per year

vms Software

TCO Comparison

5-Year TCO Server Configuration

Prices are US list	Windows	Linux*	OpenVMS
10 DB Servers	BL620 with 8-cores 32 GB Memory 2 – 146GB Internal Disks RAID 1 Dual Port FC HBA Windows 2008 R2 $398,965	BL620 with 8-cores 32 GB Memory 2 – 146GB Internal Disks RAID 1 Dual Port FC HBA RHEL 5 $328,635	BL860i2 with 8-cores 32 GB Memory 2 – 146GB Internal Disks RAID 1 Dual Port FC HBA OpenVMS BOE $448,809
40 Application Servers	BL460 with 4-cores 16 GB Memory 2 – 146GB Internal Disks RAID 1 Dual Port FC HBA Windows 2008 R2 $874,365	BL460 with 4-cores CPU 16 GB Memory 2 – 146GB Internal Disks RAID 1 Dual Port FC HBA RHEL 5 $592,085	BL860i2 with 4-cores 16 GB Memory 2 – 146GB Internal Disks RAID 1 Dual Port FC HBA OpenVMS BOE $1,077,644
List Price	**$1,273,330**	**$920,720**	**$1,526,453**

All configurations used 42U Racks, Rack PDUs, C7000 Blade Enclosures, ProCurve 6120 Ethernet Blade Switches and B-Series 8/12 FC Switches and 5-Year 24x7 Warranty on HW & SW

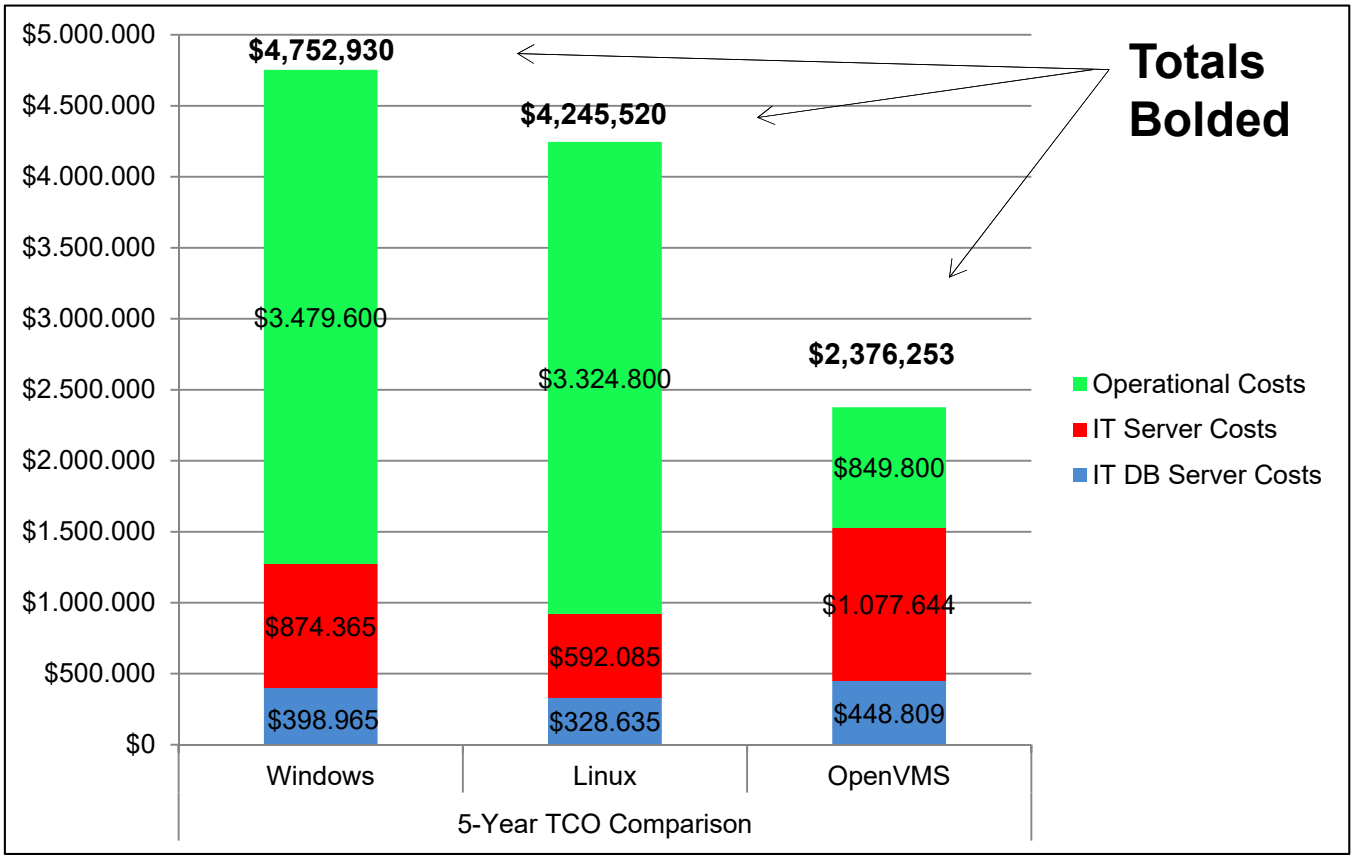
* Linux SW Warranty only 3-year 24x7

vms Software

5-Year TCO Comparison

(From Previous Example)

For 40 application servers, 10 DB servers



OpenVMS is:

44% less than Linux

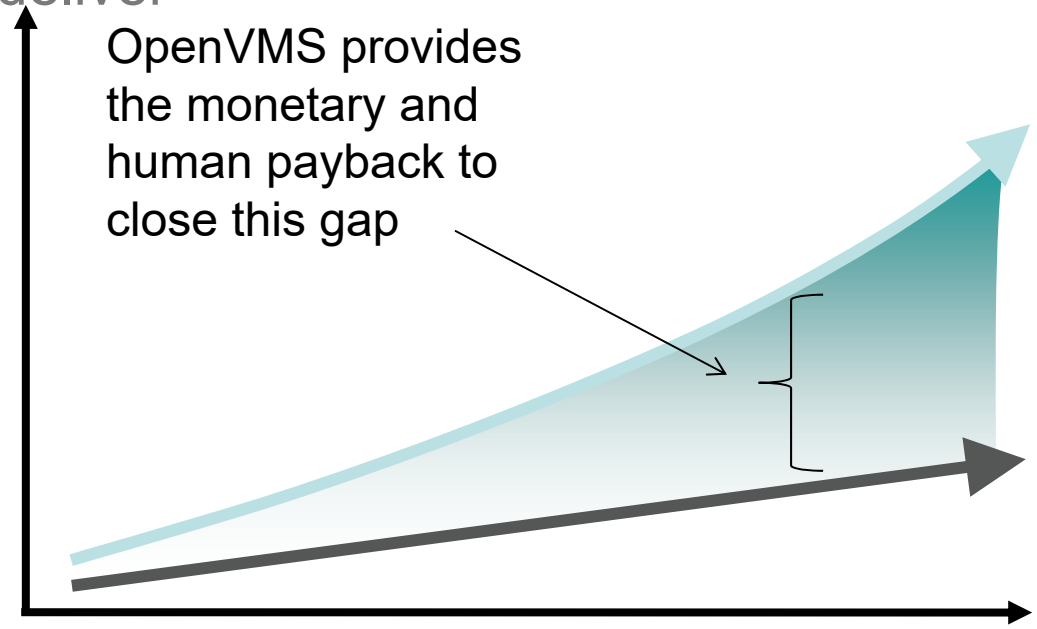
50% less than Windows

OpenVMS is $1.87M less expensive than Linux and $2.38M less than Windows over a 5 year lifecycle period

vms Software

IT's biggest challenge

The growing gap between business demands and IT's ability to deliver



Explosive growth in business applications and supporting infrastructure

versus

IT's investment to enable more effective service delivery

Applications	Infrastructure	IT management
• Enterprise upgrades • New architectures (SOA) • Rich media applications	• 2x servers every 5 years • 2x storage every year • Virtualization	• Limited budget growth • Tribal organizations • Manual processes

Other Costs

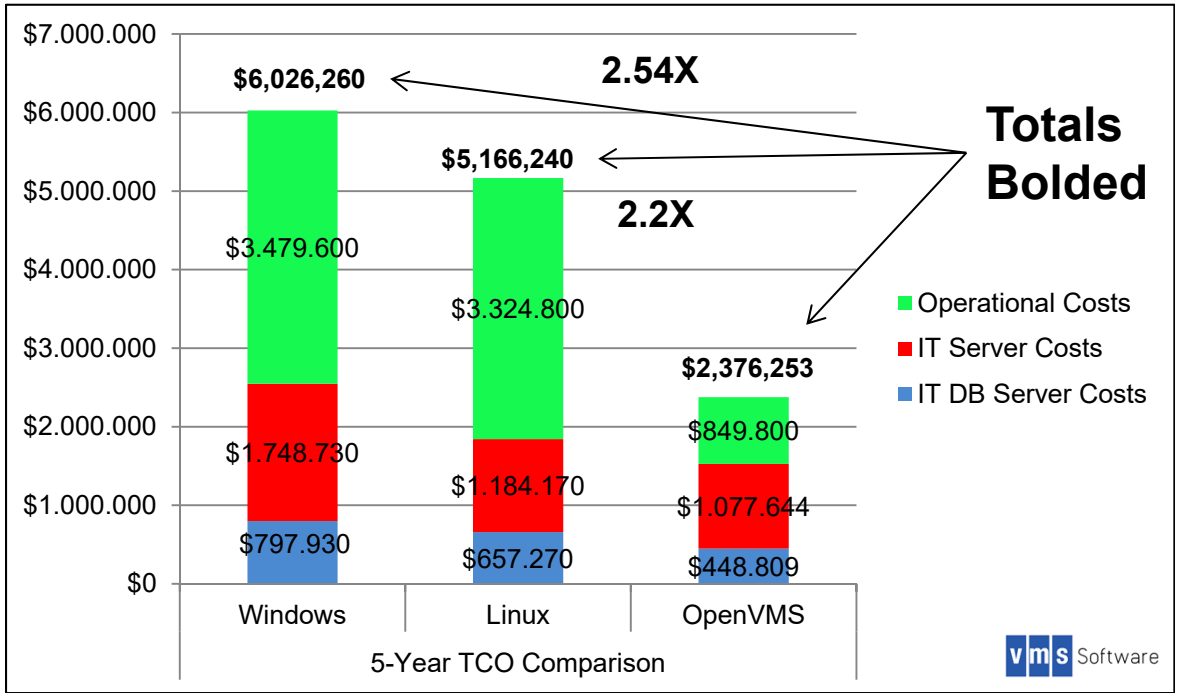
Other Cost Factors

Server Lifecycle	OpenVMS Servers	X86 servers
	5 years	3 years

X86 servers are typically replaced by a customer every 3 years whereas OpenVMS servers are replaced by a customer at a minimum every 5 years

The Result?

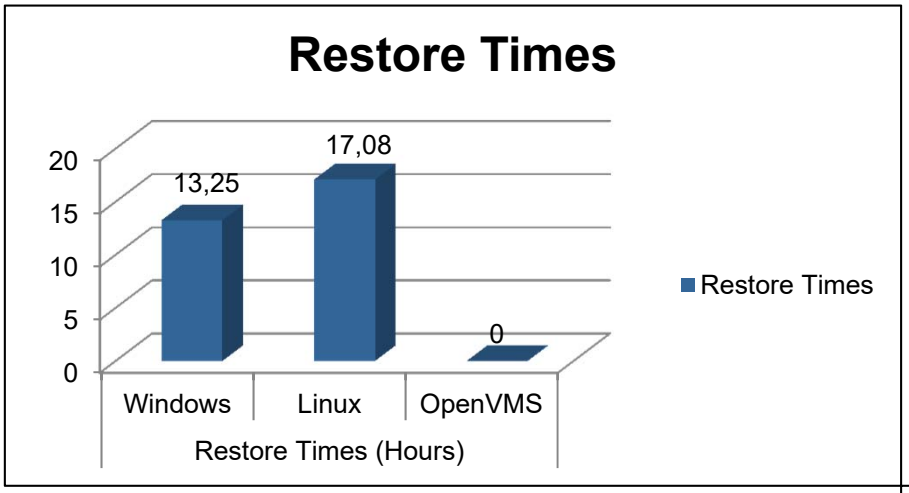
In a 5 year lifecycle you will have to buy an x86 hardware 2 times, further increasing the costs of an x86 solution. You will have to buy OpenVMS hardware only once.



Consequences of not Patching

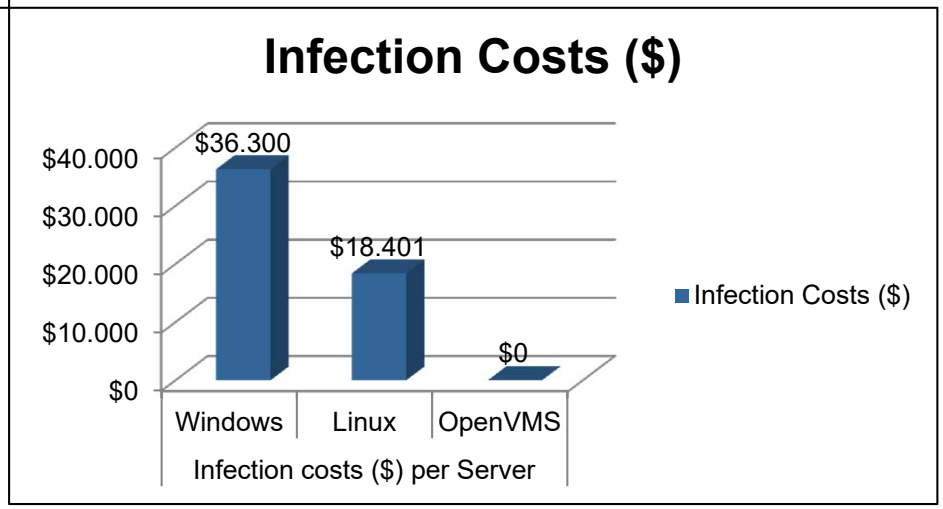
(Downtime & Downtime Costs)

According to Absolute Software ½ of your systems will become infected!



With a per server restore time of:

Equates to the following costs per server per year:



* There are no known viruses for OpenVMS

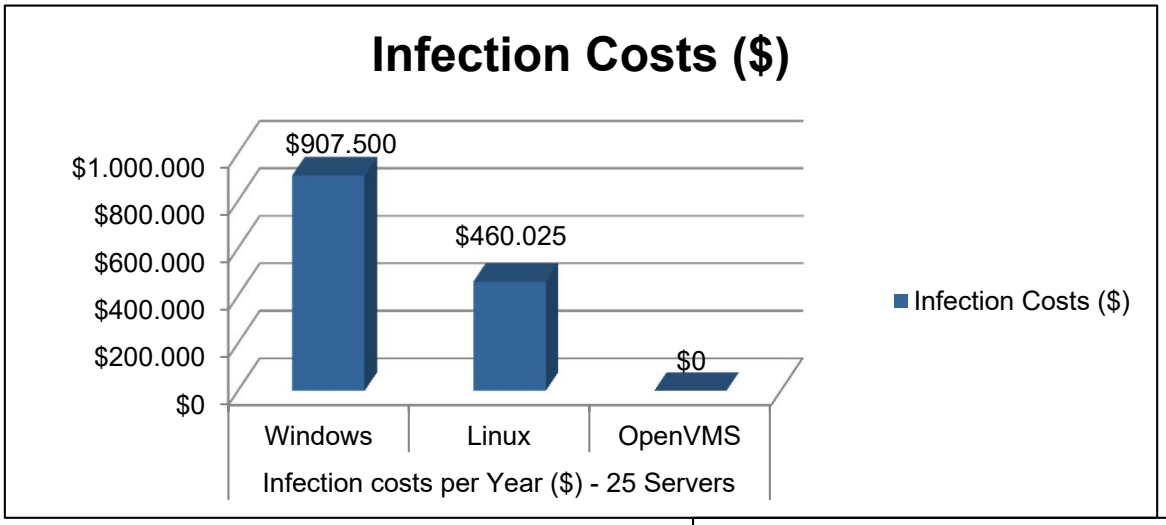
Yankee group Report - 2005 North American Linux and Windows TCO Comparison, Part 1 – Windows/Linux

vms Software

Consequences of not Patching

(Downtime Costs From Previous Example)

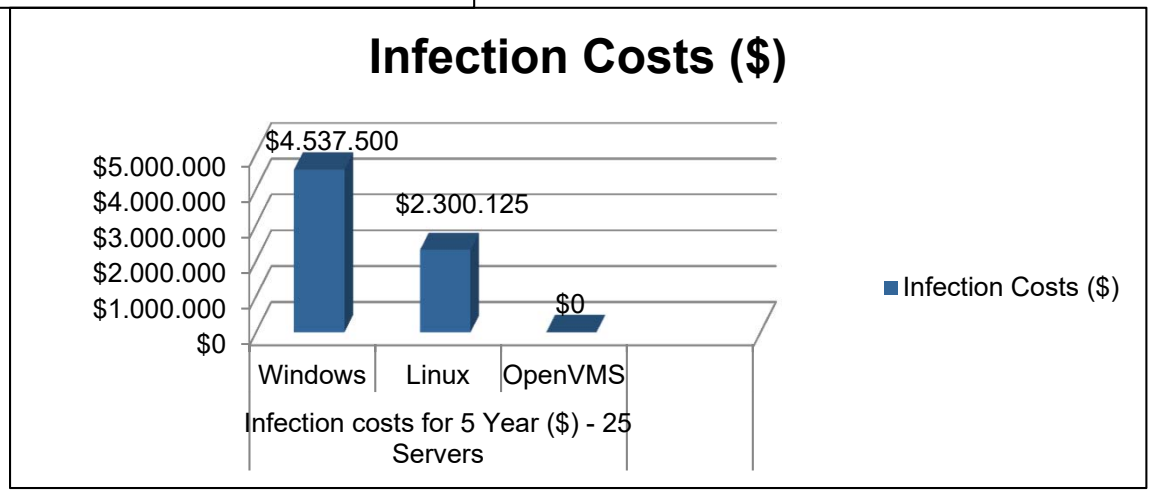
According to Absolute Software ½ of your systems will become infected!



Yearly Restore costs

For 40 application servers, 10 DB servers
With 25 of them infected

5 year lifecycle restore costs



* There are no known viruses for OpenVMS

http://www.absolute.com/Shared/Whitepapers/ABT-AM-PPM-WP-E.sflb.ashx

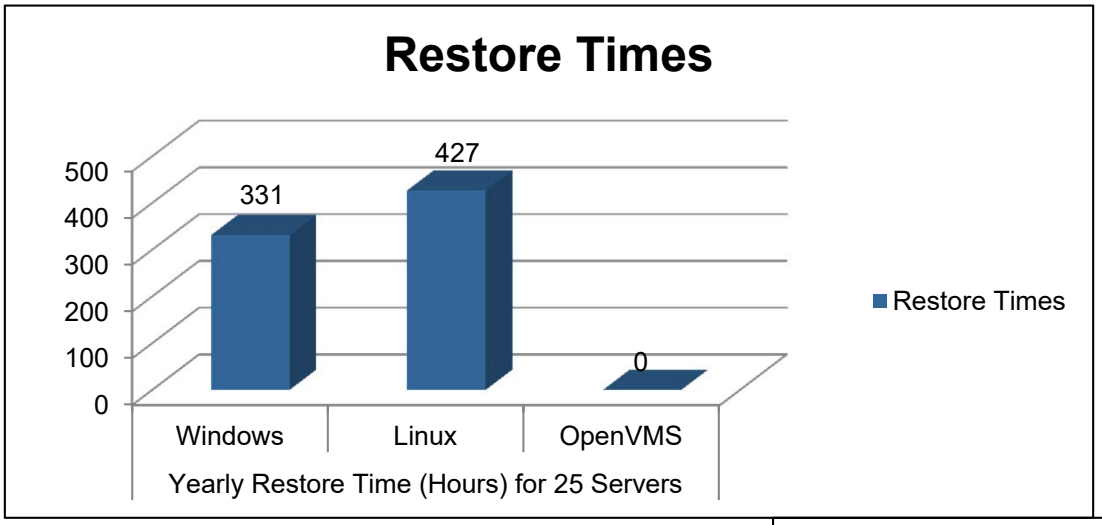
Yankee group Report - 2005 North American Linux and Windows TCO Comparison, Part 1 – Windows/Linux

vms Software

Consequences of not Patching

(Downtime From Previous Example)

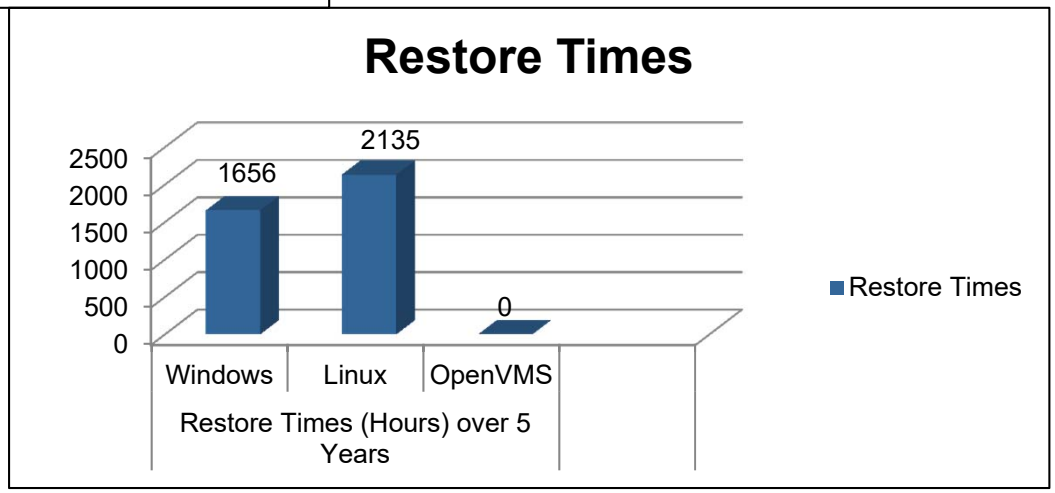
According to Absolute Software ½ of your systems will become infected!



Yearly Restore Time

For 40 application servers, 10 DB servers
With 25 of them infected

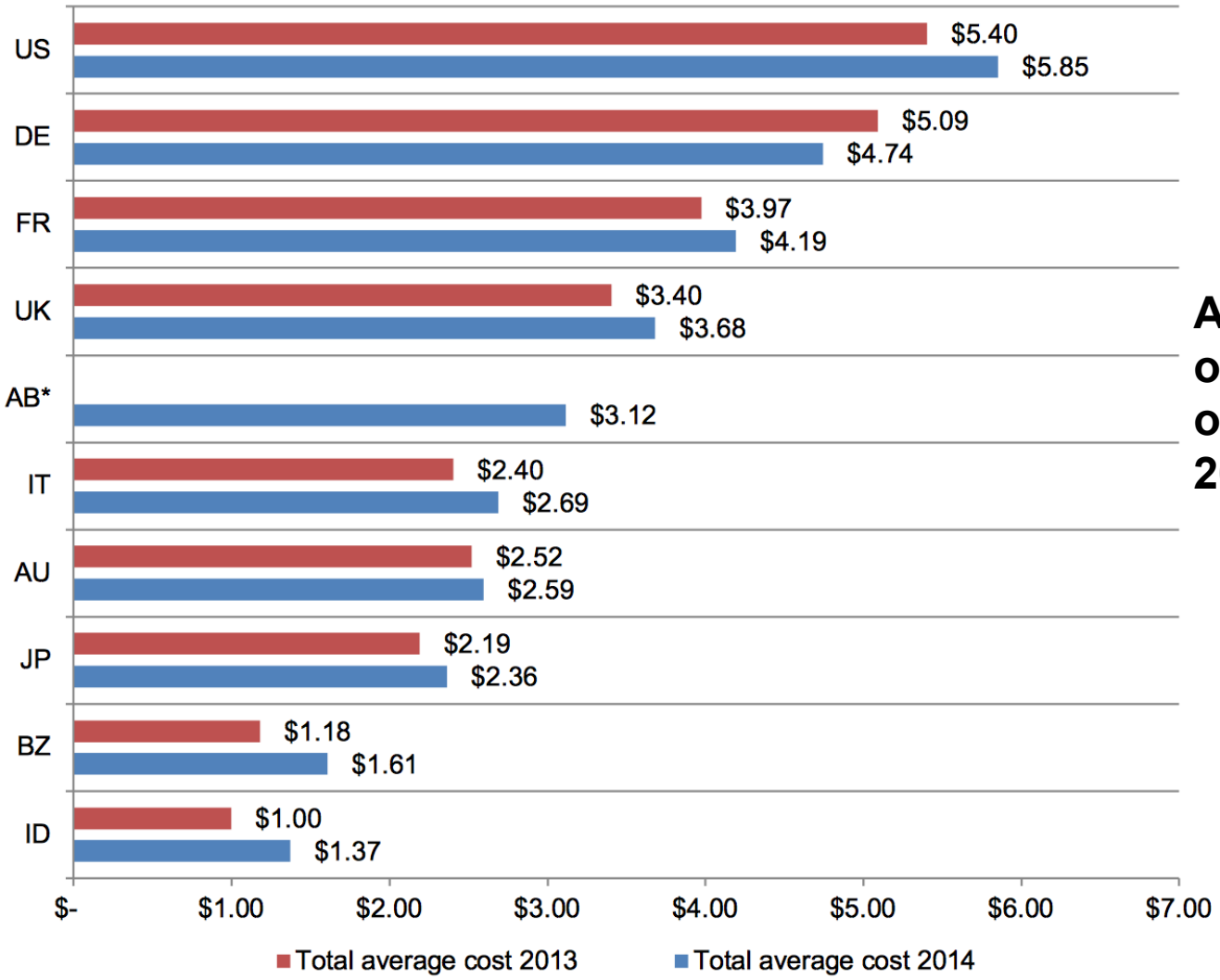
5 year Lifecycle Restore Time



* There are no known viruses for OpenVMS
http://www.absolute.com/Shared/Whitepapers/ABT-AM-PPM-WP-E.sflb.ashx

vms Software

Average Costs per Data Breach



Average organizational cost of a data breach, 2013-14 (in $M)

<u>Per Record</u>

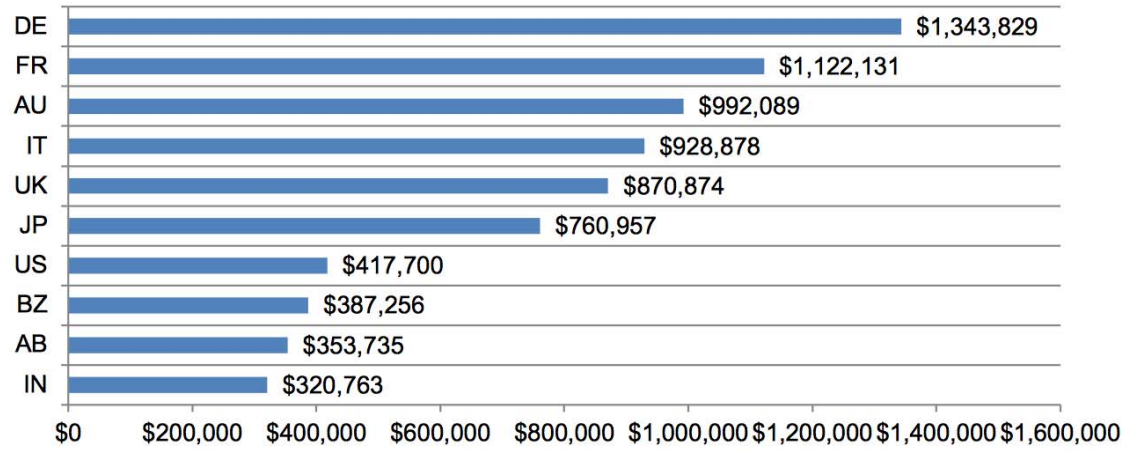
$246 - US
$215 - UK

http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

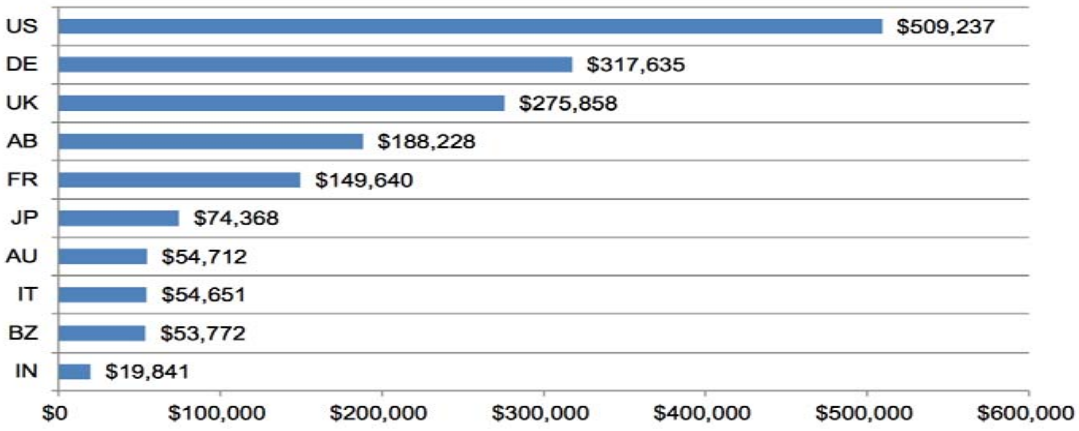
vms Software

Average Data Breach Costs

(by Cost Activity)



Detection/Escalation



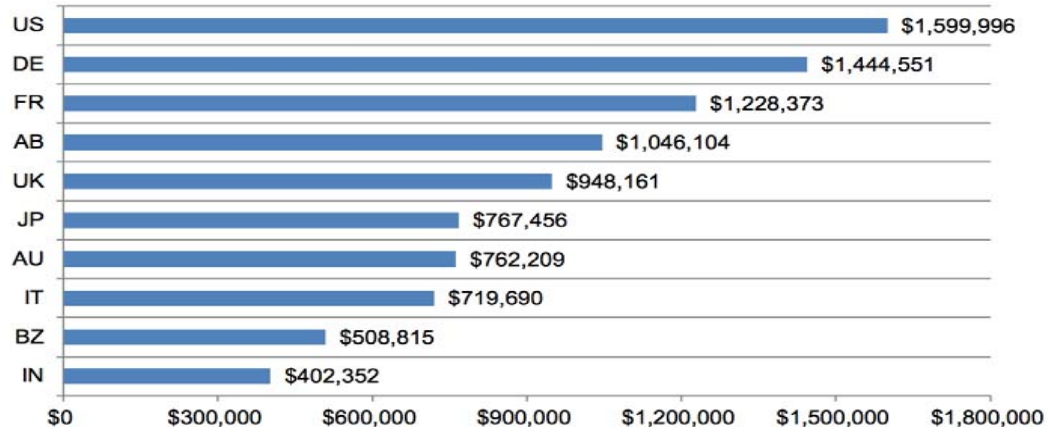
Average data breach cost by cost activity, 2014

Notification

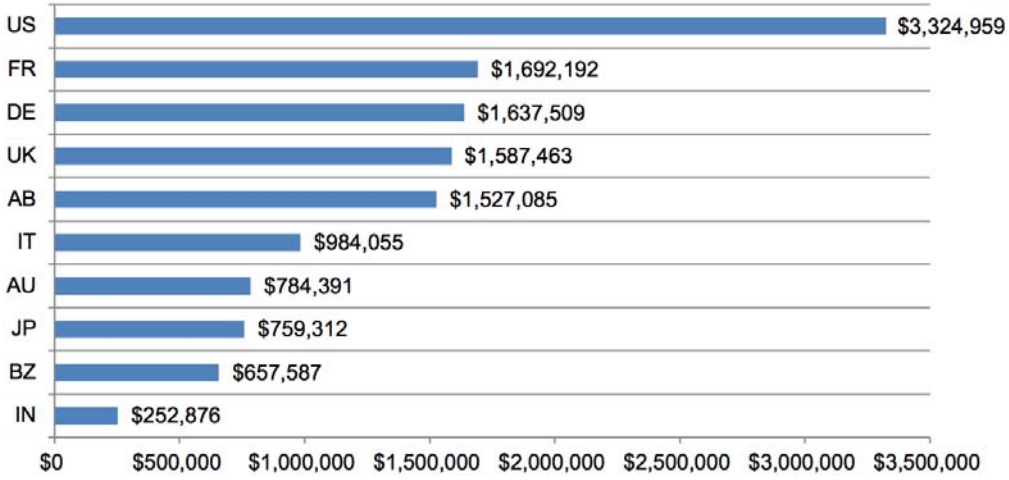
http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03027USEN&attachment=SEL03027USEN.PDF#loaded

Average Data Breach Costs

(by Cost Activity)



Post Data Breach Costs

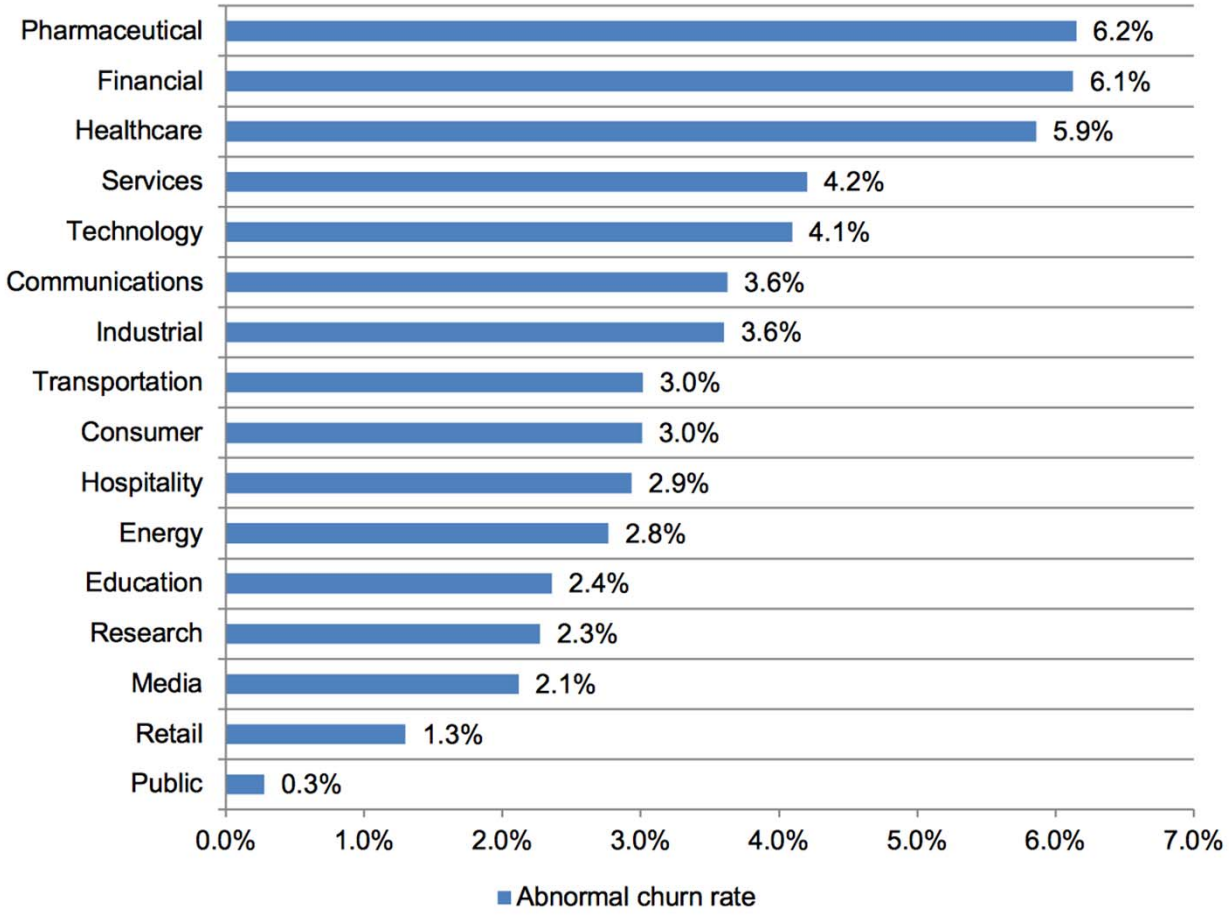


Average data breach cost by cost activity, 2014

Lost Business

http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03027USEN&attachment=SEL03027USEN.PDF#loaded

Customer Churn Rates



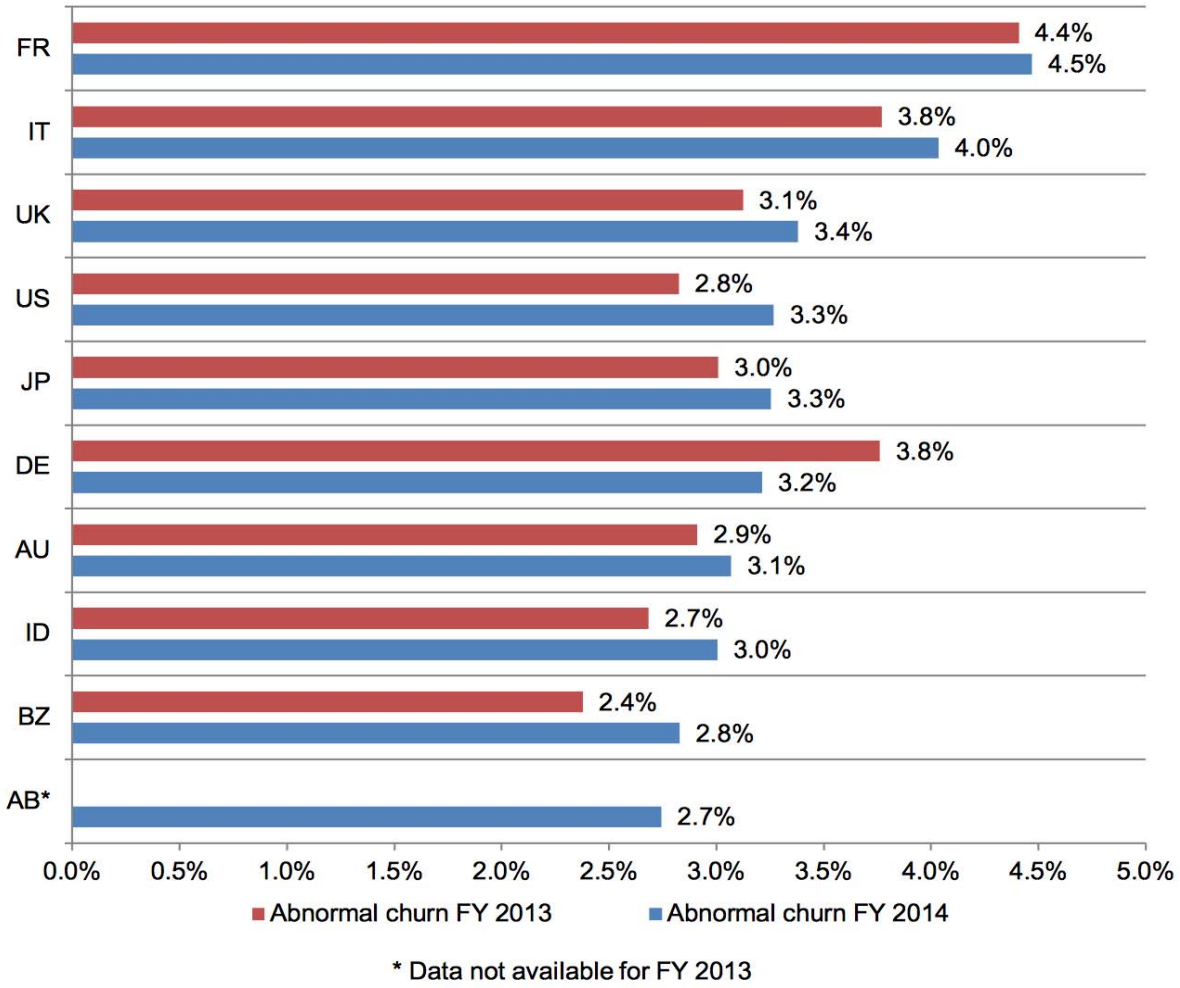
Abnormal churn rates following data breaches by industry classification, 2014

Customer turnover in direct response to breaches remains the main driver of data breach costs

http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03027USEN&attachment=SEL03027USEN.PDF#loaded

Customer Churn Rates

(By Country)



Abnormal churn rates following data breaches by industry classification, 2014

Customer turnover in direct response to breaches remains the main driver of data breach costs

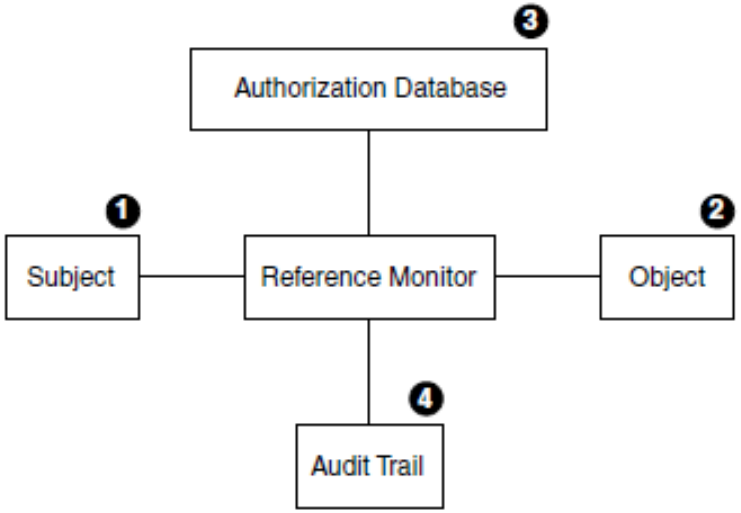
http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03027USEN&attachment=SEL03027USEN.PDF#loaded

The OpenVMS Advantage
Summary

- Reduced OS security patch rate by >10X
- Reduced daily OS security vulnerabilities by 66X – 81X
- Reduced yearly per system OS patch costs by ~30X
- Reduced System management costs by 20% - 60%
- Reduced yearly & 5 year Lifecycle operational costs by 70% - 90%
- Reduced wasted System management time by 12X – 15X
- Reduced TCO by 44% - 50% (2.2X-2.5X OpenVMS systems for 1 Windows/Linux)
- Reduced Data Breaches (at the OS level) and its associated costs

What makes OpenVMS so Secure

VMS Security Model



Reference Monitor Concept

Item	Element	Description
1	Subjects	Active entities, such as user processes, that gain access to information on behalf of people.
2	Objects	Passive repositories of information to be protected, such as files.
3	Authorization database	Repository for the security attributes of subjects and objects. From these attributes, the reference monitor determines what kind of access (if any) is authorized.
4	Audit trail	Record of all security-relevant events, such as access attempts, successful or not.

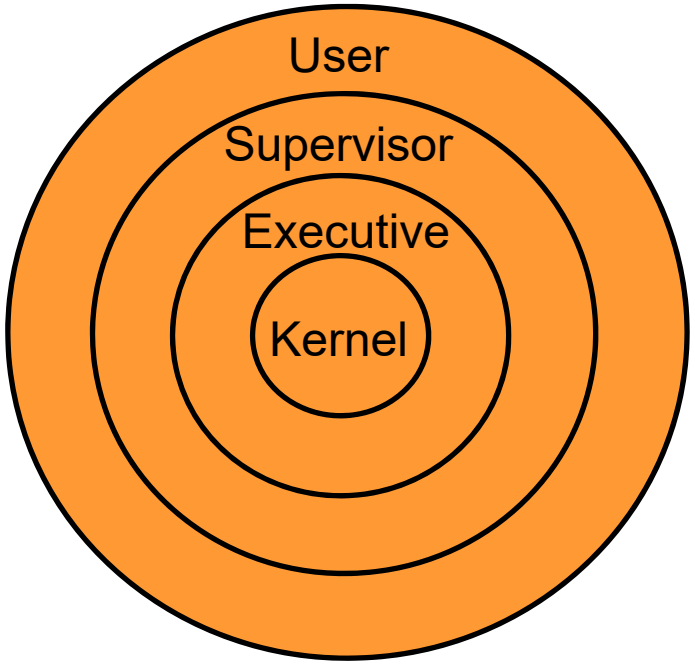
http://h71000.www7.hp.com/doc/84final/ba554_90015/ba554_90015.pdf

VMS Security

- OpenVMS was designed from day one with the aim of making a “crash proof” system
- 4 access modes – user / supervisor / exec/ kernel
- Isolates trusted system code from un-trusted user code
- “Firewall” system components to limit the impact of bugs

VMS Security – Hierarchical Protection Domains

(Protection Rings)



Kernel – executes the VMS kernel including memory management, interrupt handling and I/O

Executive – executes many system service calls including file and record management services

Supervisor – executes other system services and user commands (DCL)

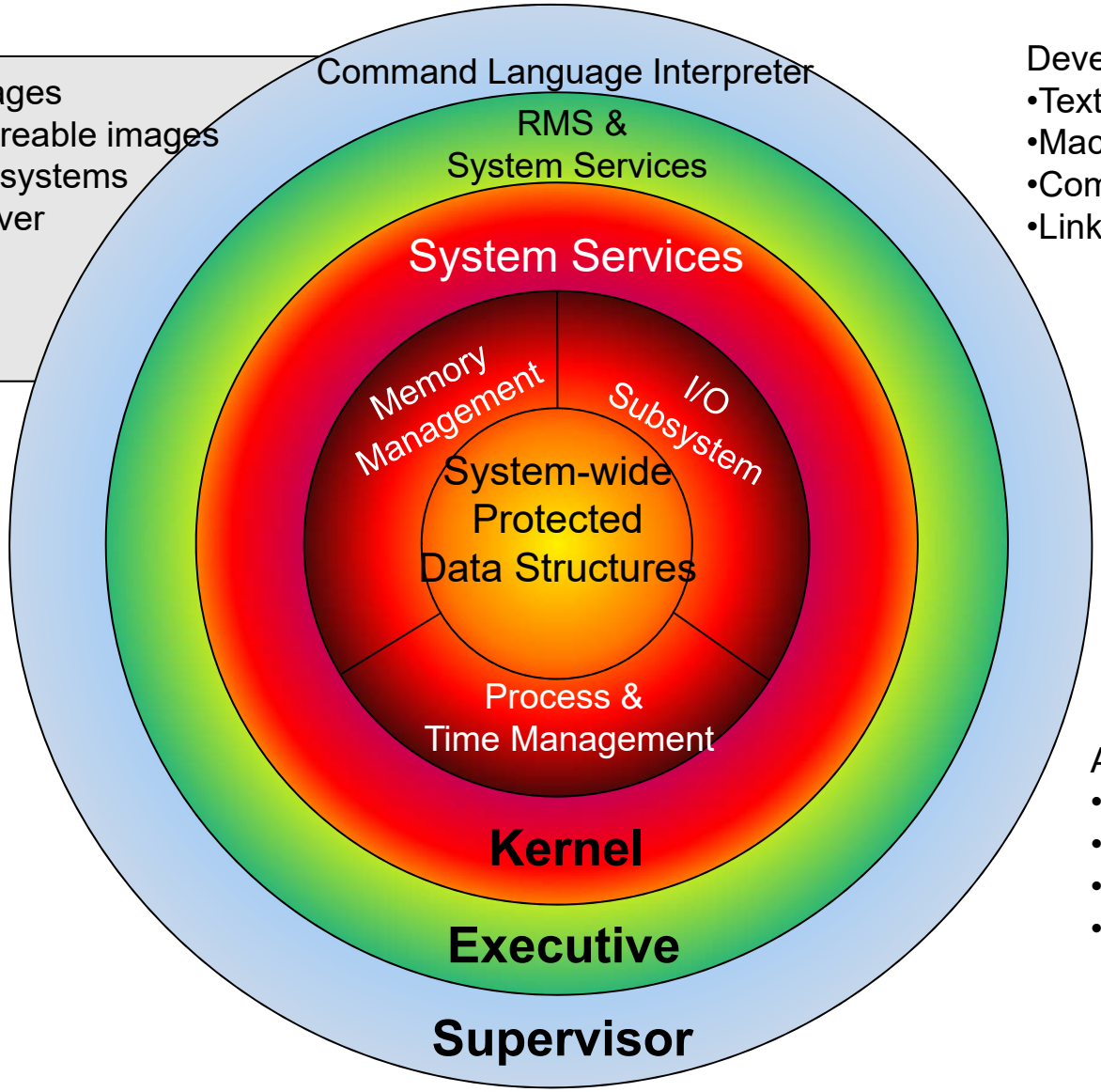
User – executes user programs and utilities such as compilers, editors, linkers and debuggers

Linux and Windows

Uses 2 rings – Supervisor and User

http://en.wikipedia.org/wiki/Ring_(computer_security)
http://h71000.www7.hp.com/doc/84final/ba554_90015/ba554_90015.pdf

VMS System Layering



•Privileged Images
•Protected shareable images
•Protected subsystems
•Privileged server processes

Development Tools
•Text editors
•Macro
•Compilers
•Linker

Run Time Library
(General)
•Math library
•String handling
•Screen management
•Misc LIB functions

User

Run Time Library
(Language-specific)
•CRTL
•FORTRAN
•PASCAL
•BASIC

Assorted Utilities
•COPY
•HELP
•DIRECTORY
•SORT

vms Software

OpenVMS Security

Privileges:

OpenVMS has 39 separate user privileges that are divided in 7 categories. Privileges restrict the use of certain system functions to processes created on behalf of authorized users.

1. None: No privileges
2. Normal: Minimum privileges to use the system effectively
3. Group: Potential to interfere with members of the same group
4. Devour: Potential to consume noncritical systemwide resources
5. System: Potential to interfere with normal system operation
6. Objects: Potential to compromise object security
7. All: Potential to control the system

These restrictions protect the integrity of the operating system's performance and, thus, the integrity of service provided to users.

http://h71000.www7.hp.com/doc/84final/ba554_90015/ba554_90015.pdf

OpenVMS Security

Passing Data to the Executive

OpenVMS uses a data structure called a descriptor, that describes the data type, size, and address of a data structure being passed between OpenVMS modes. The format of a descriptor is:

- Length of Data being passed
- Data Type code
- Descriptor class code
- Address of first byte

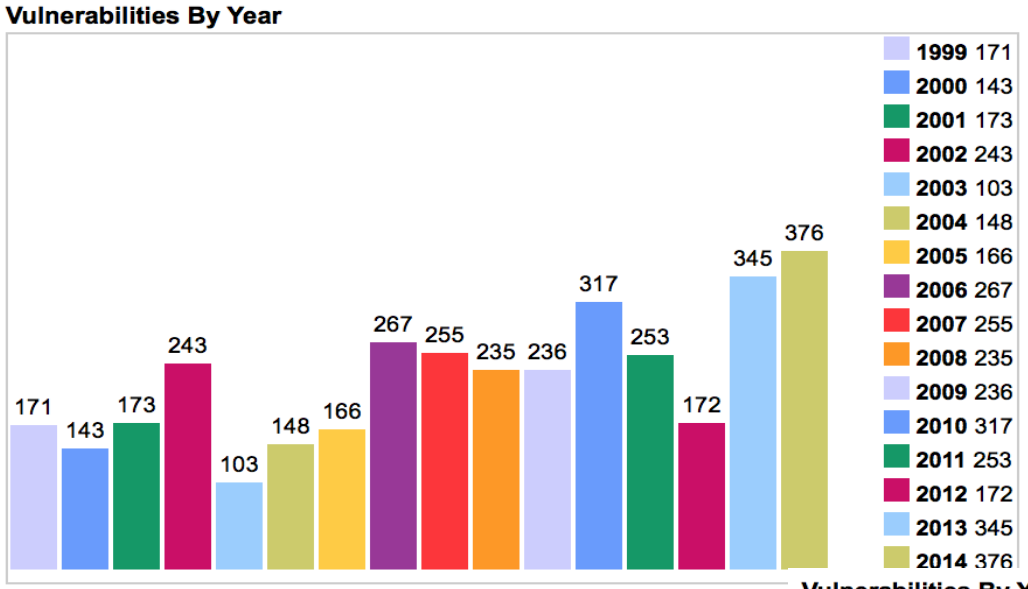
By Comparison:

Linux and Windows passes data by a NULL terminated string

http://h71000.www7.hp.com/doc/84final/ba554_90015/ba554_90015.pdf

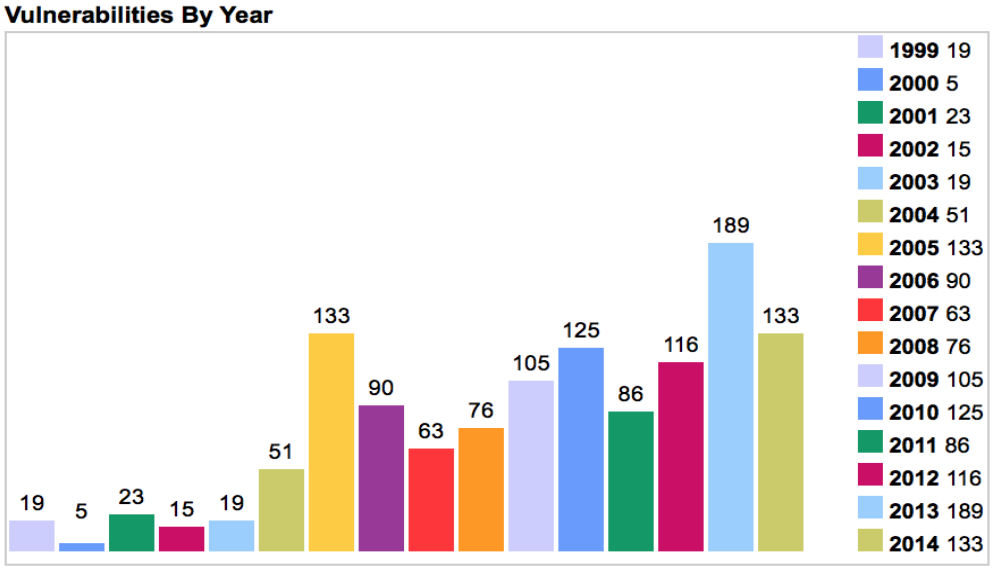
Show me the security numbers

Vulnerability Graph



Microsoft- 3603 - total

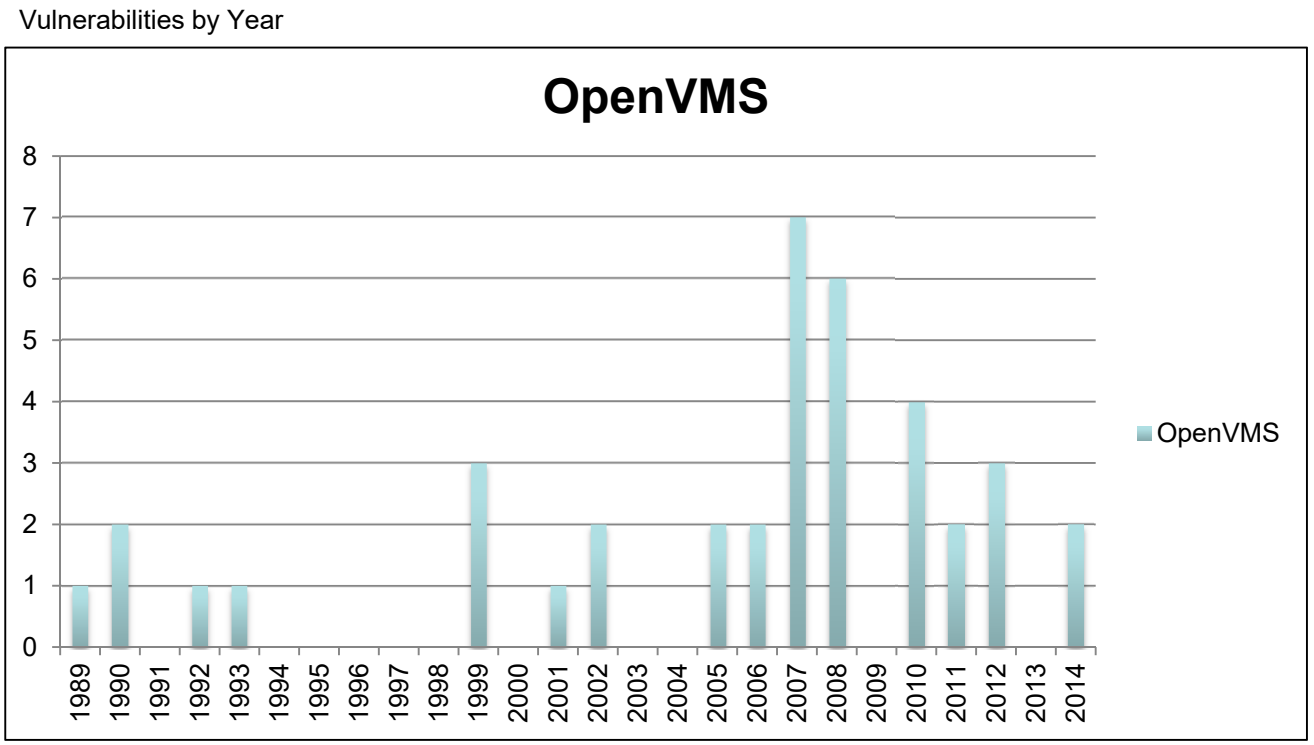
Linux – 1248 total



Source: www.cvedetails.com

vms Software

Vulnerability Graph



Total – 38 over 37 years

Source: http://cve.mitre.org and http://www.cert.org/historical/advisories/

Microsoft Security Concerns

From: New American - December 16, 2014

“New Microsoft Security Fix Is Worse Than the Problem”

“This is not the first time a Microsoft update has disabled systems. Moving forward from here, many security experts are recommending that users disable automatic updates and download and install new updates only after any bugs have been discovered and fixed.”

http://www.thenewamerican.com/tech/computers/item/19735-new-microsoft-security-fix-is-worse-than-the-problem

Microsoft Security Concerns

A bumper harvest patch of updates for October

November 2014 Patch Tuesday: Microsoft released 4 critical fixes, 14 total updates

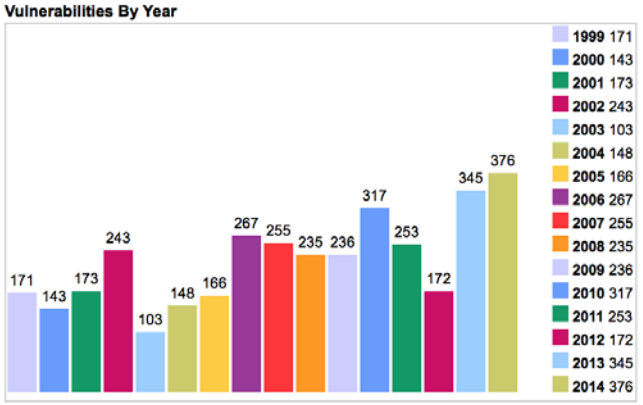
Patch Tuesday Dec 2014: 7 fixes, 3 critical patches for Windows, IE and Office

Microsoft releases emergency patch to stymie Windows Server attacks

Microsoft patches 3 zero-days including Sandworm on Patch Tuesday

November Patch Tuesday: A massive update with a few misses

Microsoft patches 2 critical, 7 important flaws on August 2014 'Update Tuesday'



http://www.networkworld.com/article/2846204/microsoft-subnet/nov-2014-patch-tuesday-microsoft-released-4-critical-fixes-14-total-updates.html

Antivirus Security Concerns

From: Security Affairs – July 30, 2014
The Register– July 29, 2014

14 antivirus apps found to have security problems

"AV engines make your computer more vulnerable with a varying degree of performance penalty [and] is as vulnerable to zero day attacks as the applications it tries to protect from. [It] can even lower the operating system exploiting mitigations." COSEINC researcher Joxean Koret says.

http://www.theregister.co.uk/2014/07/29/antivirus_blood_splattered_as_biz_warned_audit_or_die/
http://securityaffairs.co/wordpress/27165/hacking/serious-flaws-antivirus-engines.html

Open-source Security Concerns

From: FCW – The Business of Federal Technology

October 23, 2014

"Most third-party and open source components do not undergo the same level of security scrutiny as custom-developed software," Veracode warned.

“The common use of reusable, pre-fabricated software components from open source developers for IT systems, the company said, could leave large openings in security that increase the risk of data breaches, malware injections and denial-of-service attacks. “

http://fcw.com/articles/2014/10/23/open-source-security.aspx?m=1

Open-source Security Concerns

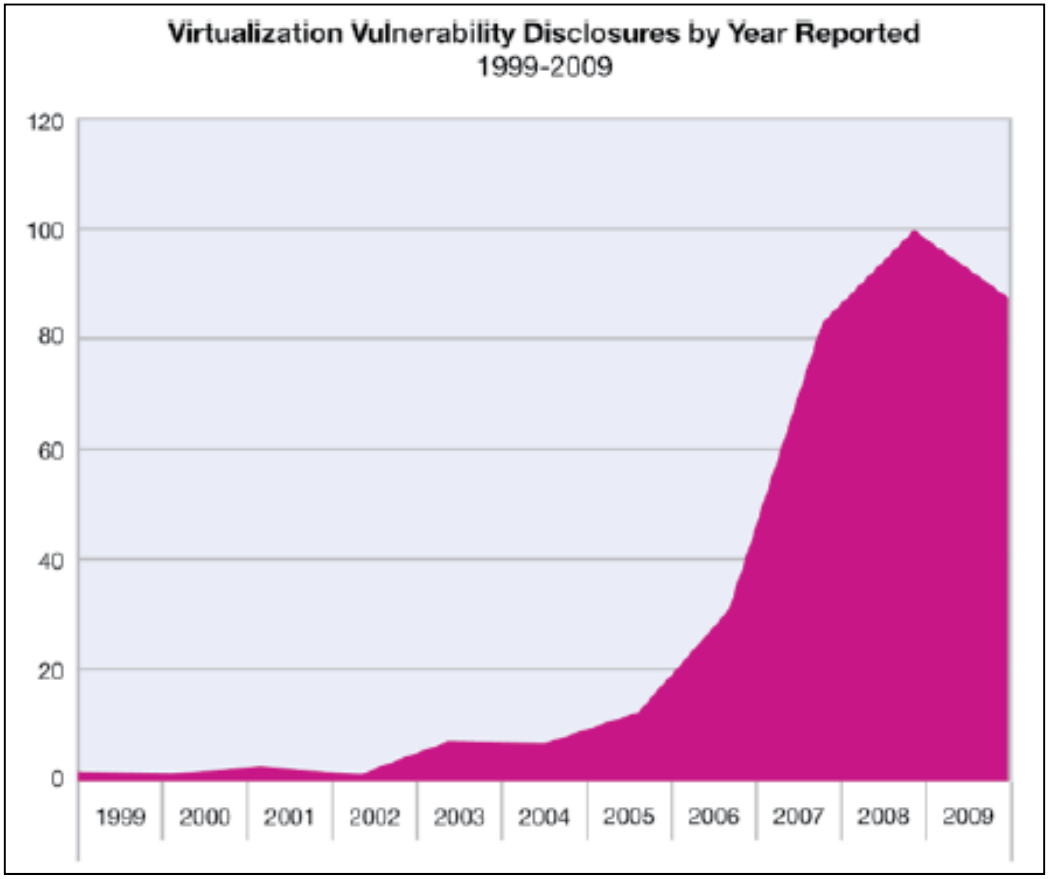
From: Silicon Angle – November 12, 2014

"… open source developers don't always adhere to best practices when it comes to security such as conducting regular security audits and using static analysis, found Coverity Inc.'s Spotlight report. The Coverity Scan Security Spotlight identifies several common defects and exposures (CVEs) in open source code, and identifies that the GoToFail vulnerability could have been detected in the scan."

"The provider of application development testing added its Security Advisor to the Coverity Scan service, which resulted in the discovery of almost 4,000 defects. Almost 2400 of these were high severity defects, followed by 1330 low severity and 260 and so medium severity."

http://siliconangle.com/blog/2014/11/12/coverity-security-report-open-source-projects-badly-need-security-programs/

Virtualization Security Concerns



Vulnerability disclosures over the past decade for virtualization products provided by the following vendors:

- **Citrix**
- **IBM**
- **Linux VServer**
- **LxCenter**
- **Microsoft**
- **Oracle**
- **Parallels**
- **RedHat**
- **VMware**

The use of hypervisor technology by malware and rootkits installing themselves as a hypervisor below the operating system can make them more difficult to detect because the malware could intercept any operations of the operating system …

http://www-304.ibm.com/businesscenter/fileserve?contentid=207480


vms
Software

Q&A

vms Software

Backup Slides

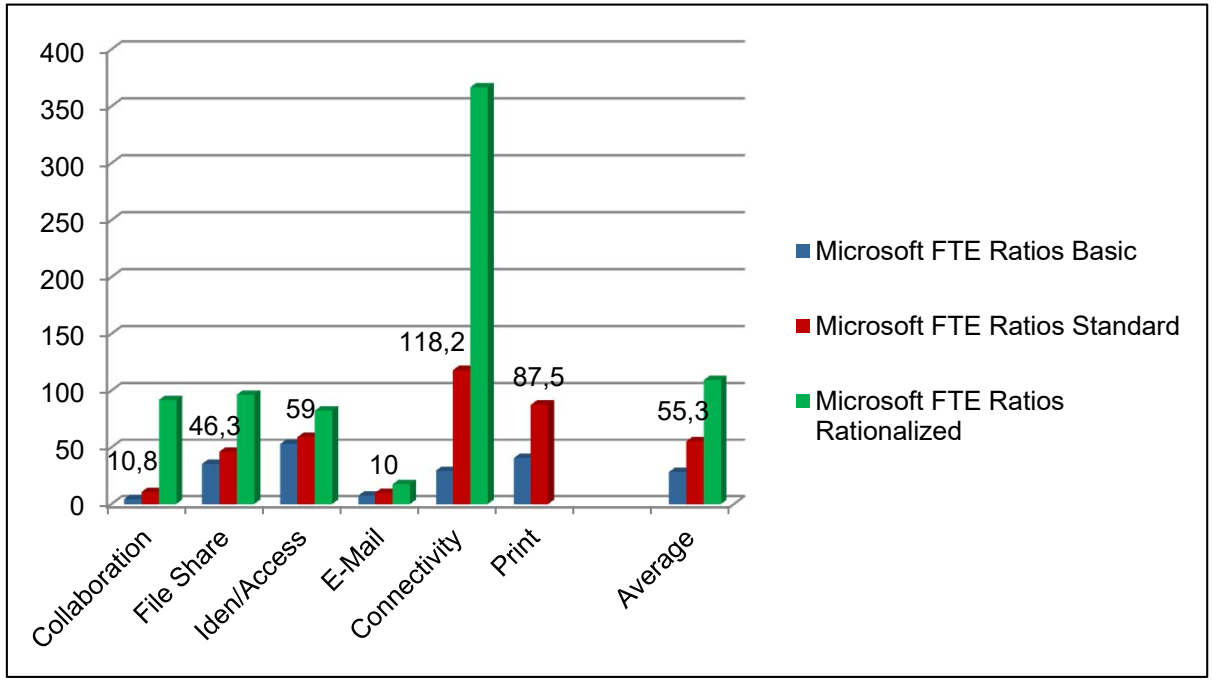
Server to System Manager Ratio

From ComputerWorld:

"One enterprise IT manager told us the ratio for physical servers was roughly 50:1, another working for a government organisation said 15-20:1, and an IT director at a research and development outfit noted that in a mid-size organisation a system administrator could maintain 10-14 servers per week or if their role was merely maintenance (i.e. no projects, no debugging, etc) then they could look after 25-35 servers per week."

http://www.computerworld.com.au/article/352635/there_best_practice_server_system_administrator_ratio_/

Server to System Manager Ratio



Standard Ratios are highlighted (RED bar) in graph

Basic: No Automation
Standard: Some Automation
Rationalized: Considerable Automation

From: Microsoft Best Practices Report - 2009

OpenVMS Systems Require Fewer Human Resources

From Harvard Research Group:

Of those users surveyed, 63% said that fewer people are required to run their OpenVMS servers compared to their non-OpenVMS servers … OpenVMS servers are much easier to manage and therefore reduce the TCO by requiring less staff than the competition to keep them up and running.

Antivirus Security Concerns

From: SiteApproved

Problems With Anti-virus Programs Found

… Vulnerabilities found recently in McAfee, Symantec, and Trend Micro software could let hackers compromise and even control computers running certain versions of their products. While most antivirus software is distributed via a network download, making it difficult for a hacker to get to the code, these flaws further highlight the problems with the antivirus industry's traditionally reactive approach to protection, …

http://siteapproved.com/securityhackpop.htm

Antivirus Security Concerns

From: ZDNet – February 25, 2011

Microsoft fixes hole in its antivirus engine

… "The update addresses a privately reported vulnerability that could allow elevation of privilege if the Microsoft Malware Protection Engine scans a system after an attacker with valid log-on credentials has created a specially crafted registry key," the advisory says. "An attacker who successfully exploited the vulnerability could gain the same user rights as the LocalSystem account. …

http://siteapproved.com/securityhackpop.htm