Network Assessment

Risk Report

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 4/1/2014

Prepared for:
Prospect Or Customer
Prepared by:
365 Managed IT

2/26/2016

Table of Contents

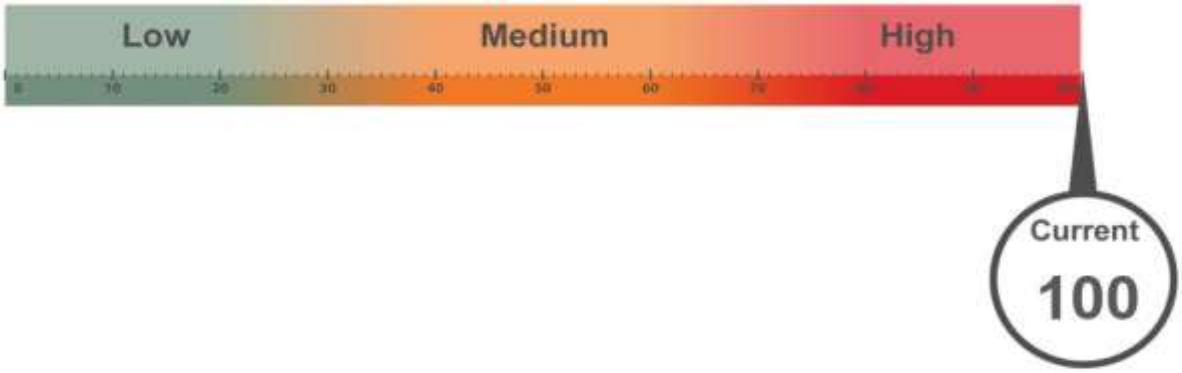
Discovery Tasks

The following discovery tasks were performed:

DISCOVERED	TASK	DESCRIPTION
✓	Detect Domain Controllers	Identifies Domain Controllers and Online status
✓	FSMO Role Analysis	Enumerates FSMO roles at the site
✓	Enumerate Organization Units and Security Groups	Lists the Organizational units and Security Groups with members
✓	User Analysis	List of users in AD, status, and last login/use, which helps identify potential security risks
✓	Detect Local Mail Servers	Mail server(s) found on the network
✓	Detect Time Servers	Time server(s) found on the network
✓	Discover Network Shares	Comprehensive list of Network Shares by Server
✓	Detect Major Applications	Major apps / versions and count of installations
✓	Detailed Domain Controller Event Log Analysis	List of event log entries from the past 24 hours for the Directory Service, DNS Server and File Replication Service event logs
✓	Web Server Discovery and Identification	List of web servers and type
✓	Network Discovery for Non-A/D Devices	List of Non-Active Directory devices responding to network requests
✓	Internet Access and Speed Test	Test of internet access and performance
✓	SQL Server Analysis	List of SQL Servers and associated database(s)
✓	Internet Domain Analysis	“WHOIS” check for company domain(s)
✓	Password Strength Analysis	Uses MBSA to identify computers with weak passwords that may pose a security risk
✓	Missing Security Updates	Uses MBSA to identify computers missing security updates
✓	System by System Event Log Analysis	Last 5 System and App Event Log errors for servers
✗	External Security Vulnerabilities	List of Security Holes and Warnings from External Vulnerability Scan

Risk Score

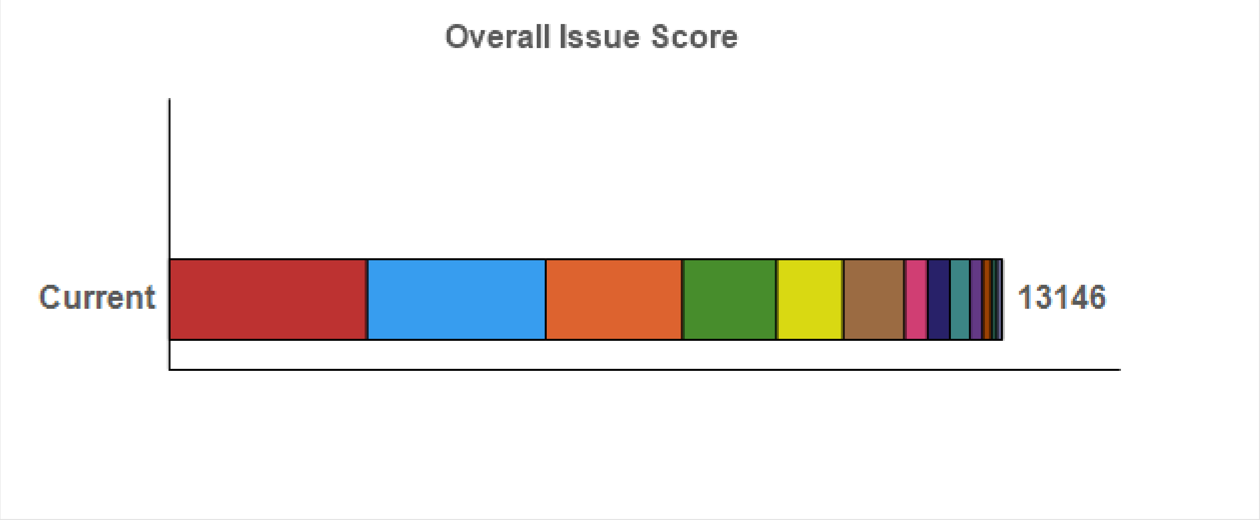
The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues.



Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

Issues Summary

This section contains a summary of issues detected during the Network Assessment process, and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.



Weighted Score: Risk Score x Number of Incidents = Total points: Total percent (%)

User password set to never expire (80 pts each)

3120	***Current Score:*** 80 pts x 39 = 3120 : 23.73%
	Issue: User accounts with passwords set to never expire present a risk of use by unauthorized users. They are more easily compromised than passwords that are routinely changed.
	Recommendation: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

Anti-virus not installed (94 pts each)

2820	***Current Score:*** 94 pts x 30 = 2820 : 21.45%
	Issue: Anti-virus software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.
	Recommendation: To prevent both security and productivity issues, we strongly recommend assuring anti-virus is deployed to all possible endpoints.

Anti-spyware not installed (94 pts each)

2162	***Current Score:*** 94 pts x 23 = 2162 : 16.45%

	Issue: Anti-spyware software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.
	Recommendation: To prevent both security and productivity issues, we strongly recommend assuring anti-spyware is deployed to all possible endpoints.

	Inactive Computers (15 pts each)
1485	***Current Score:*** 15 pts x 99 = 1485 : 11.3%
	Issue: 99 computers were found as having not checked in during the past 30 days.
	Recommendation: Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, or powered on.

	Significantly high number of Domain Administrators (35 pts each)
1050	***Current Score:*** 35 pts x 30 = 1050 : 7.99%
	Issue: More than 30% of the users are in the Domain Administrator group and have unfettered access to files and system resources. Compromised Domain Administrator accounts pose a higher threat than typical users and may lead to a breach.
	Recommendation: Evaluate the need to have more than 30% of users in the Domain Administrator group and limit administrative access to the minimum necessary.

	Unsupported Operating Systems (97 pts each)
970	***Current Score:*** 97 pts x 10 = 970 : 7.38%
	Issue: 10 computers were found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk.
	Recommendation: Upgrade or replace computers with operating systems that are no longer supported.

	LOTS of Security patches missing on computers (90 pts each)
360	***Current Score:*** 90 pts x 4 = 360 : 2.74%
	Issue: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Lots is defined as missing 3 or more patches.
	Recommendation: Address patching on computers with missing security patches.

	User has not logged in in 30 days (13 pts each)
351	***Current Score:*** 13 pts x 27 = 351 : 2.67%
	Issue: 27 Users that have not logged in in 30 days could be from a former employee or vendor and should be disabled or removed.
	Recommendation: Disable or remove user accounts for users that have not logged in in 30

	days.

	Operating System in Extended Support (20 pts each)
320	***Current Score:*** 20 pts x 16 = 320 : 2.43%
	Issue: 16 computers were found using an operating system that is in extended supported. Extended support is a warning period before an operating system is no longer supported by the manufacturer and will no longer receive support or patches.
	Recommendation: Upgrade computers that have operating systems in Extended Support before end of life.

	Potential Password Strength Risks (100 pts each)
200	***Current Score:*** 100 pts x 2 = 200 : 1.52%
	Issue: Local account passwords on 2 were found to be potentially weak. Inadequate or weak passwords on local accounts can allow a hacker to compromise the system. It can also lead to the spread of malicious software that can cause business and productivity affecting issues.
	Recommendation: We recommend placing adequate password strength requirements in place and remediate the immediate password issues on the identified systems.

	Potential Disk Space Issue (68 pts each)
136	***Current Score:*** 68 pts x 2 = 136 : 1.03%
	Issue: Computers were found with significantly low free disk space.
	Recommendation: Free or add additional disk space for the specified drives.

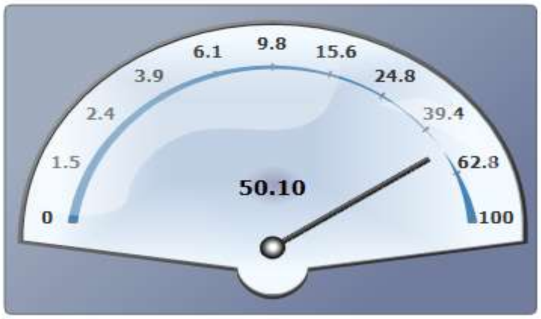
	Anti-virus not turned on (92 pts each)
92	***Current Score:*** 92 pts x 1 = 92 : 0.7%
	Issue: We were unable to determine if an anti-virus software is enabled and running on some computers.
	Recommendation: Determine if anti-virus is enabled properly.

	Insecure Listening Ports (10 pts each)
70	***Current Score:*** 10 pts x 7 = 70 : 0.53%
	Issue: 7 computers were found to be using potentially insecure protocols.
	Recommendation: There may be a legitimate business need, but these risks should be assessed individually. Certain protocols are inherently insecure since they typically lack encryption. Inside the network, their use should be minimized as much as possible to prevent the spread of malicious software. Of course, there can be reasons these services are needed and other means to protect systems which listen on those ports. We recommend reviewing the programs listening on the network to ensure their necessity and security.

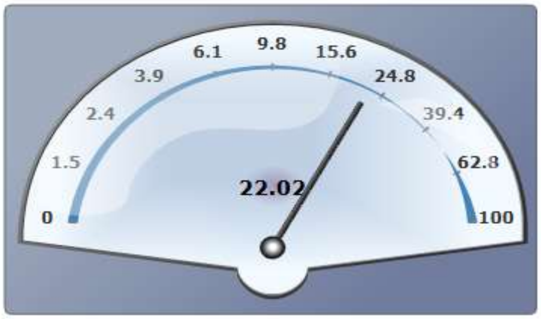
	Un-populated Organization Units (10 pts each)
10	***Current Score:*** 10 pts x 1 = 10 : 0.08%
	Issue: Empty Organizational Units (OU) were found in Active Directory. They may not be needed and should be removed to prevent misconfiguration.
	Recommendation: Remove or populate empty Organizational Units.

Internet Speed Test Results

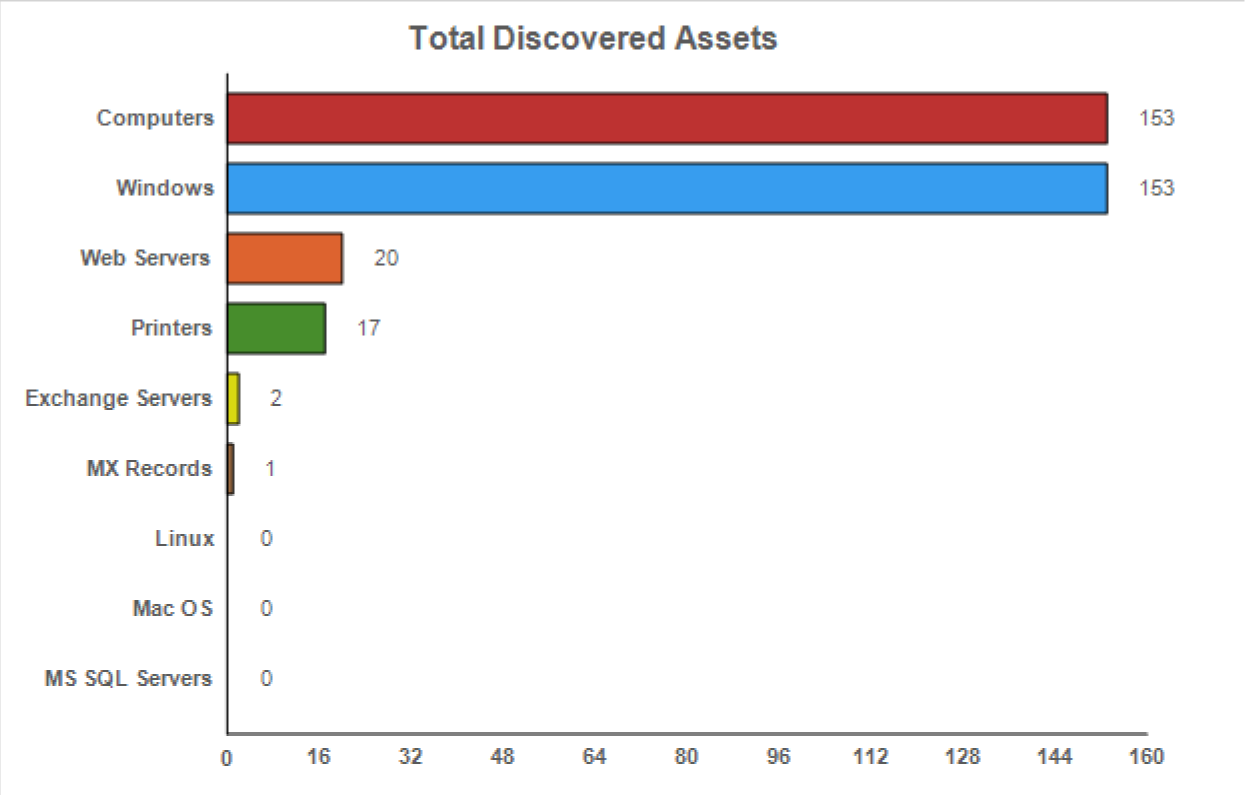
Download Speed: **50.10 Mb/s**



Upload Speed: **22.02 Mb/s**

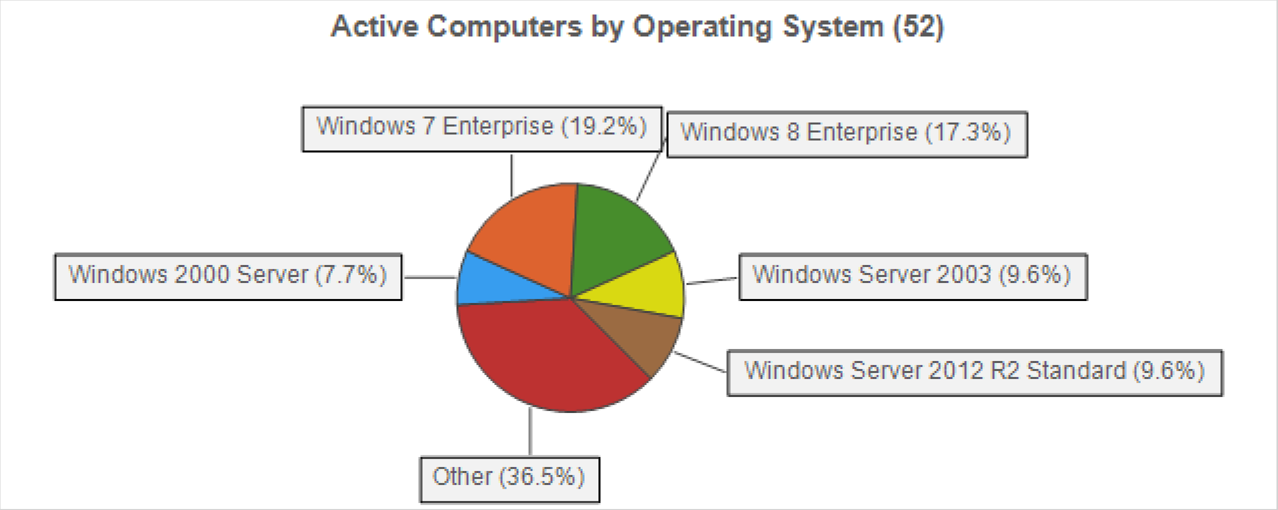


Asset Summary: Total Discovered Assets

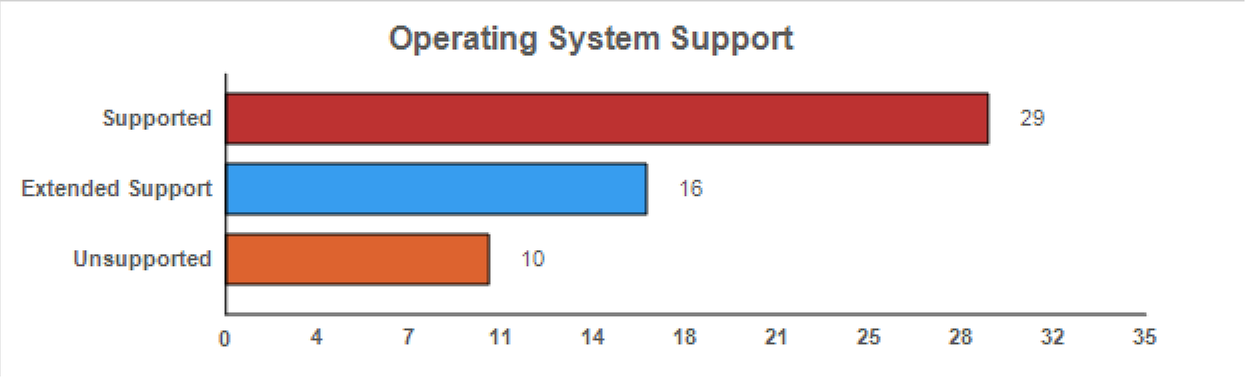


Asset Summary: Active Computers

Active Computers are defined as computers that were either actively responding at the time of the scan or have checked in with Active Directory within the past 30 days.

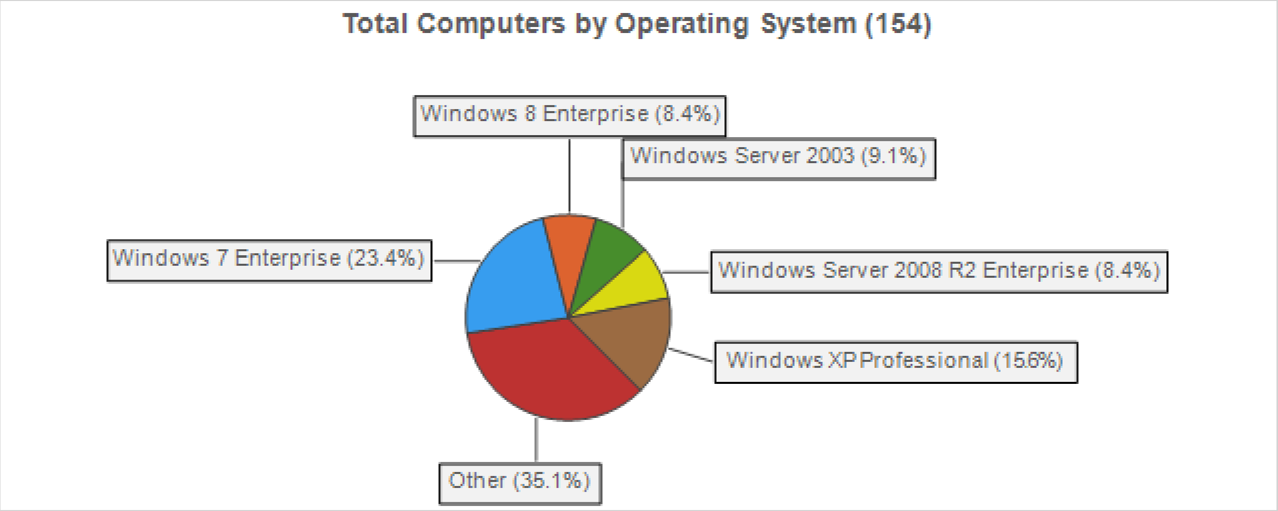


Operating System	Total	Percent
Top Five		
Windows 7 Enterprise	10	19.2%
Windows 8 Enterprise	9	17.3%
Windows Server 2003	5	9.6%
Windows Server 2012 R2 Standard	5	9.6%
Windows 2000 Server	4	7.7%
Total - Top Five	**33**	**63.5%**
Other		
Windows Server 2012 R2 Datacenter	4	7.7%
Windows Server 2012 Standard	4	7.7%
Windows 8.1 Enterprise	3	5.8%
Windows 7 Professional	2	3.8%
Hyper-V Server 2012	1	1.9%
Windows 8.1 Pro	1	1.9%
Windows Server 2008 R2 Datacenter	1	1.9%
Windows Server 2008 R2 Enterprise	1	1.9%
Windows Server 2012 Datacenter	1	1.9%
Windows Vista Business	1	1.9%
Total - Other	**19**	**36.5%**
Overall Total	**52**	**100%**


Operating System Support
Supported
29
Extended Support
16
Unsupported
10
0
4
7
11
14
18
21
25
28
32
35

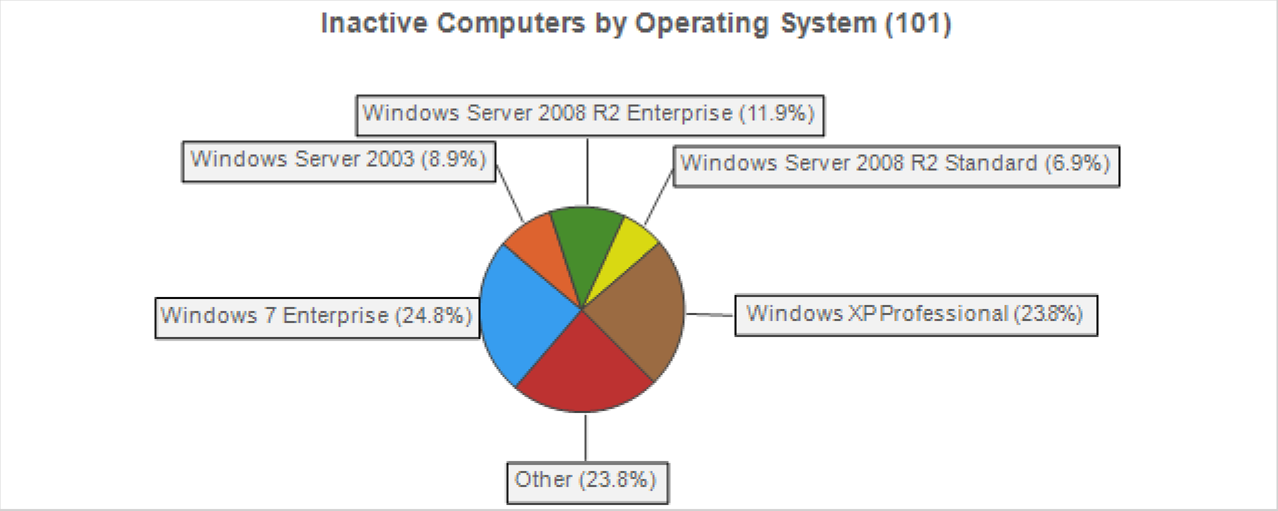
Asset Summary: All and Inactive Computers

The list of all computers includes computers that may no longer be active but have entries in Active Directory (in a Domain environment). Inactive Computers are computers that could not be scanned or have not checked into Active Directory in the past 30 days.



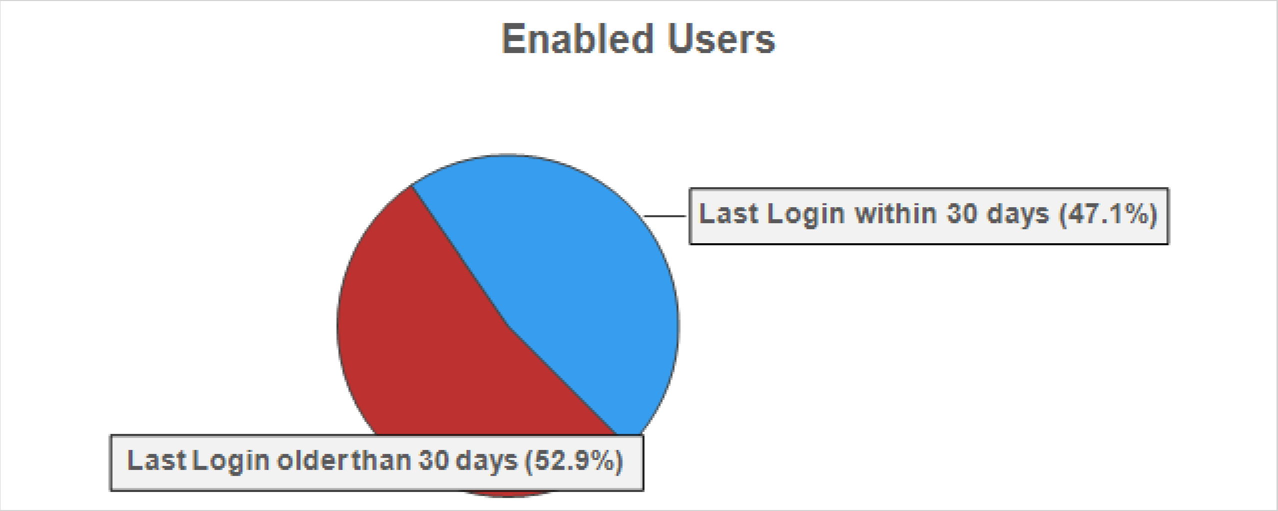
Operating System	Total	Percent
Top Five		
Windows 7 Enterprise	36	23.4%
Windows XP Professional	24	15.6%
Windows Server 2003	14	9.1%
Windows 8 Enterprise	13	8.4%
Windows Server 2008 R2 Enterprise	13	8.4%
Total - Top Five	**100**	**64.9%**
Other		
Windows Server 2008 R2 Standard	7	4.5%
Windows Server 2012 Standard	7	4.5%
Windows 2000 Server	6	3.9%
Windows Server 2012 R2 Datacenter	5	3.2%
Windows Server 2012 R2 Standard	5	3.2%
Windows 7 Professional	4	2.6%
Windows 7 Ultimate	4	2.6%
Unidentified OS	3	1.9%
Windows 8.1 Enterprise	3	1.9%
Windows Server 2012 Datacenter	2	1.3%
Hyper-V Server 2012	1	0.6%

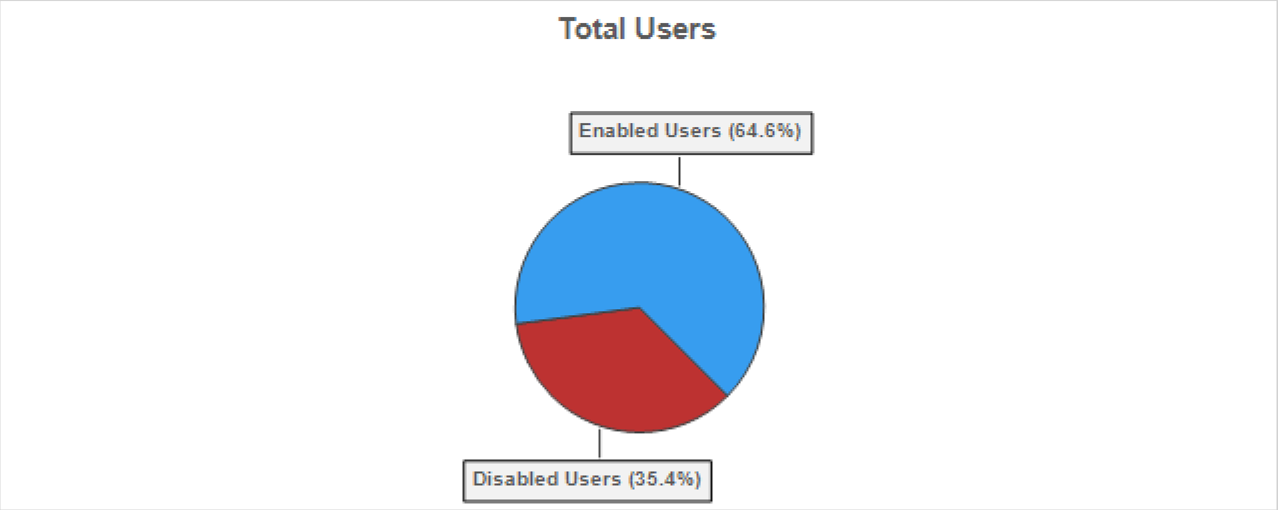
Operating System	Total	Percent
Windows 8 Consumer Preview	1	0.6%
Windows 8.1 Pro	1	0.6%
Windows Server 2008 Enterprise	1	0.6%
Windows Server 2008 R2 Datacenter	1	0.6%
Windows Server 2008 Standard	1	0.6%
Windows Vista Business	1	0.6%
Windows Vista Ultimate	1	0.6%
Total - Other	**54**	**35.1%**
Overall Total	**154**	**100%**

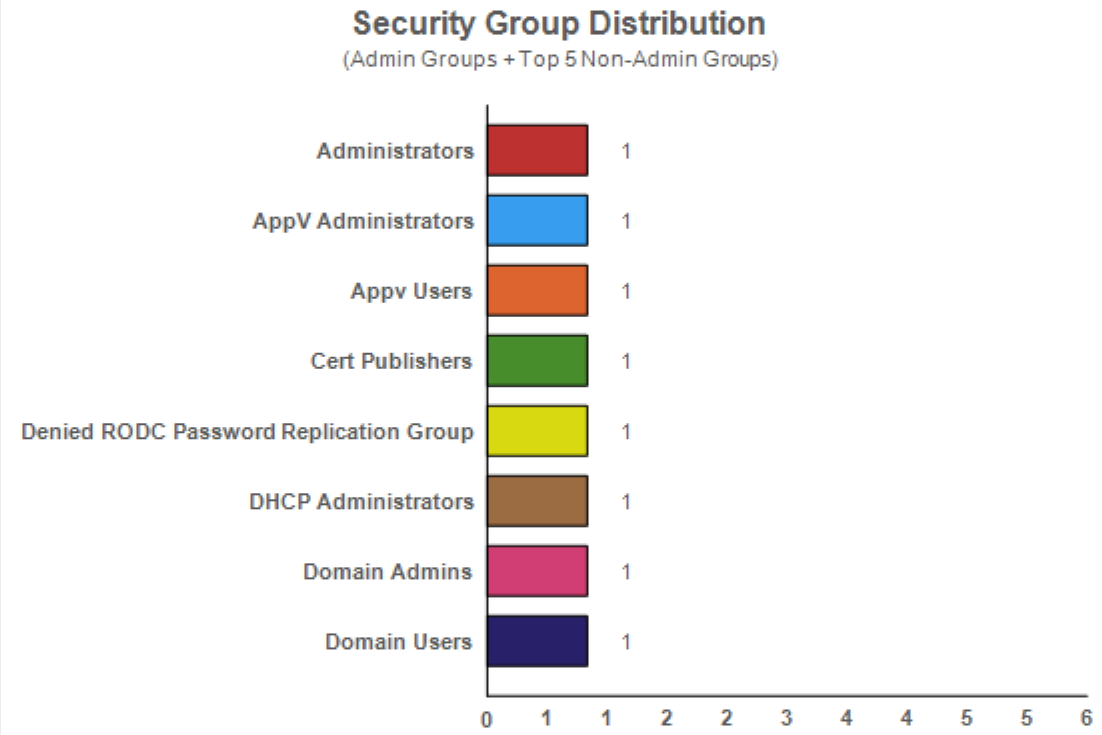


Operating System	Total	Percent
Top Five		
Windows 7 Enterprise	25	24.8%
Windows XP Professional	24	23.8%
Windows Server 2008 R2 Enterprise	12	11.9%
Windows Server 2003	9	8.9%
Windows Server 2008 R2 Standard	7	6.9%
Total - Top Five	**77**	**76.2%**
Other		
Windows 7 Ultimate	4	4%
Windows 8 Enterprise	4	4%
Unidentified OS	3	3%
Windows Server 2012 Standard	3	3%
Windows 2000 Server	2	2%
Windows 7 Professional	2	2%
Windows 8 Consumer Preview	1	1%
Windows Server 2008 Enterprise	1	1%
Windows Server 2008 Standard	1	1%
Windows Server 2012 Datacenter	1	1%
Windows Server 2012 R2 Datacenter	1	1%
Windows Vista Ultimate	1	1%
Total - Other	**24**	**23.8%**
Overall Total	**101**	**100%**

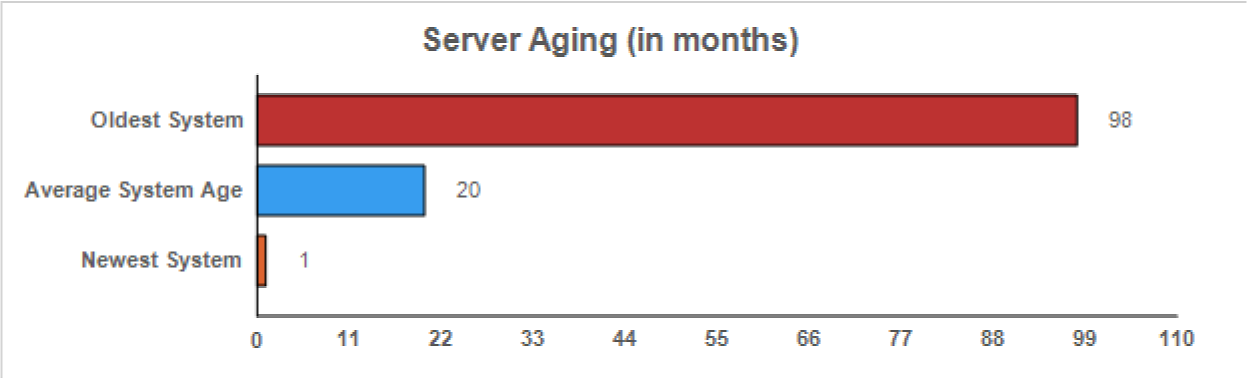
Asset Summary: Users



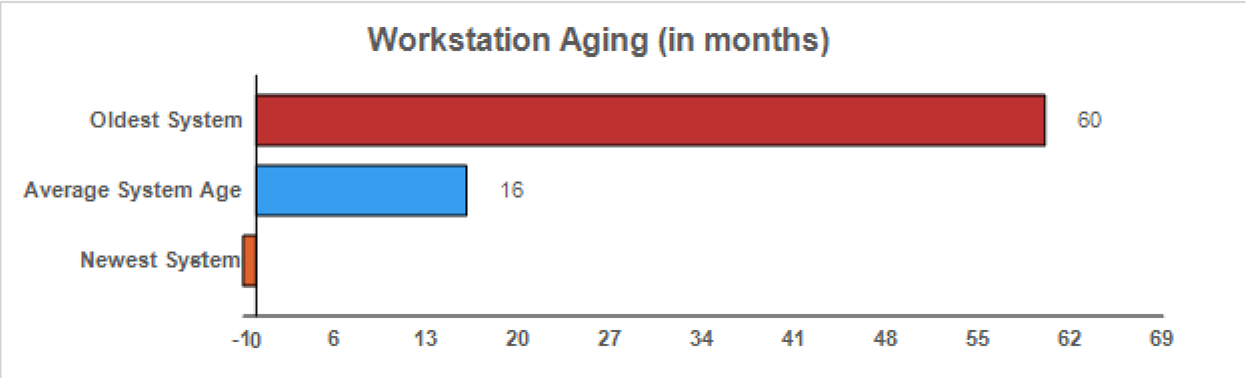



Security Group Distribution
(Admin Groups + Top 5 Non-Admin Groups)
Administrators
1
AppV Administrators
1
Appv Users
1
Cert Publishers
1
Denied RODC Password Replication Group
1
DHCP Administrators
1
Domain Admins
1
Domain Users
1
0
1
1
2
2
3
4
4
5
5
6

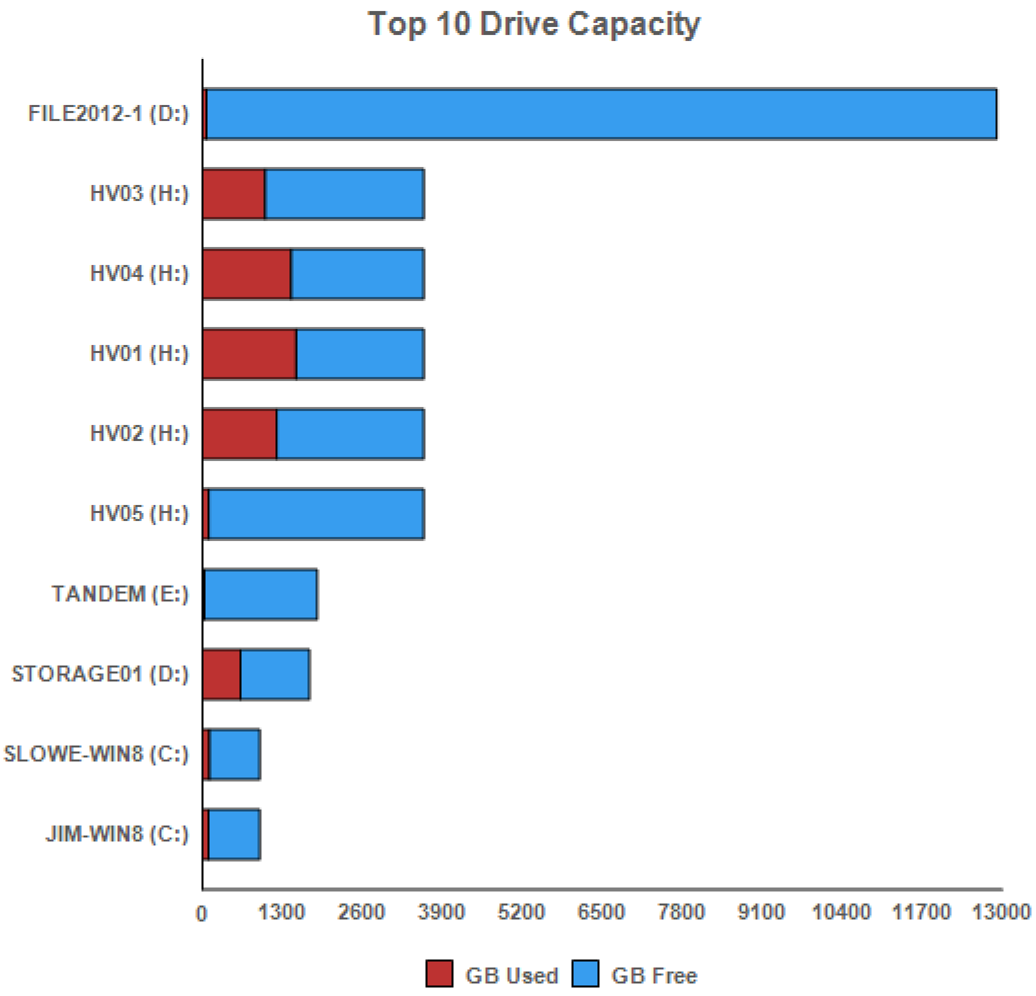
Server Aging

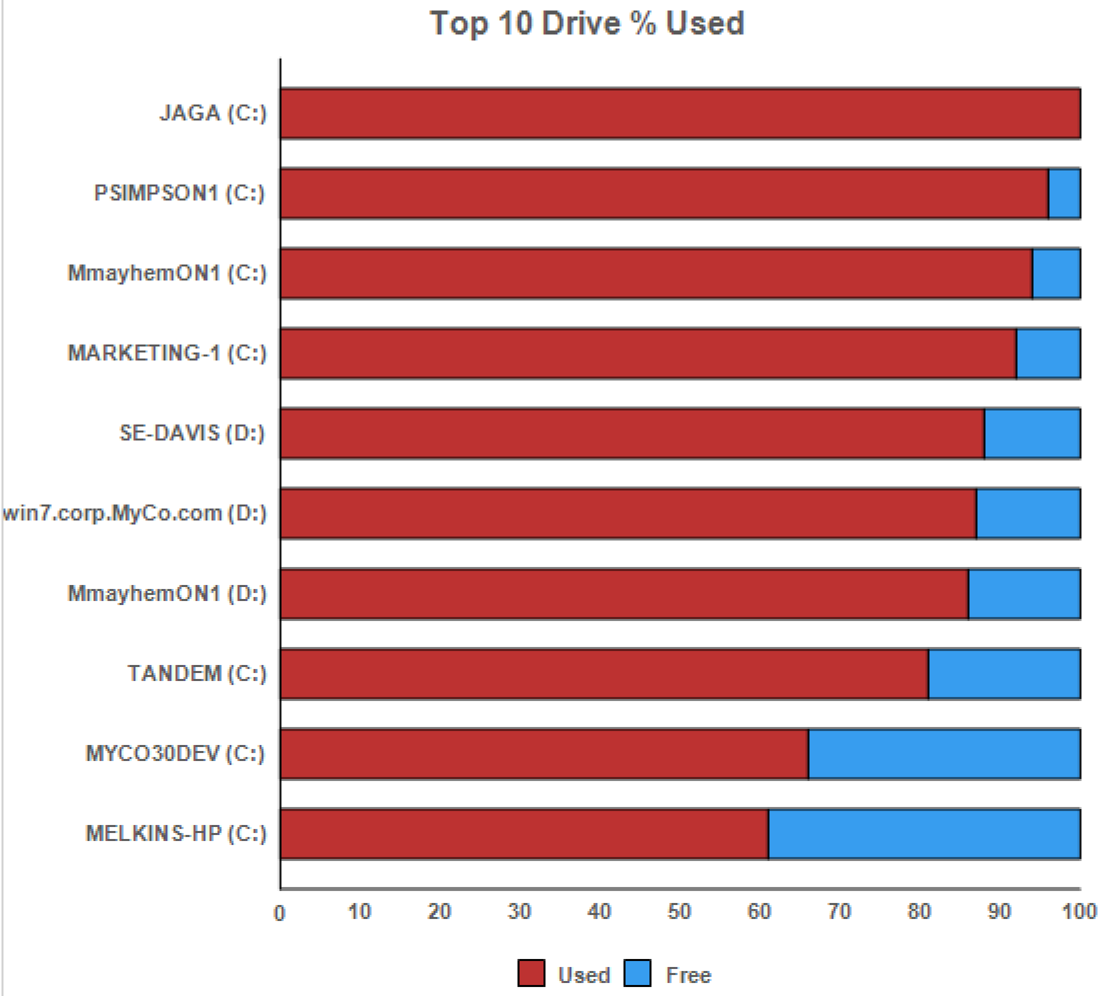


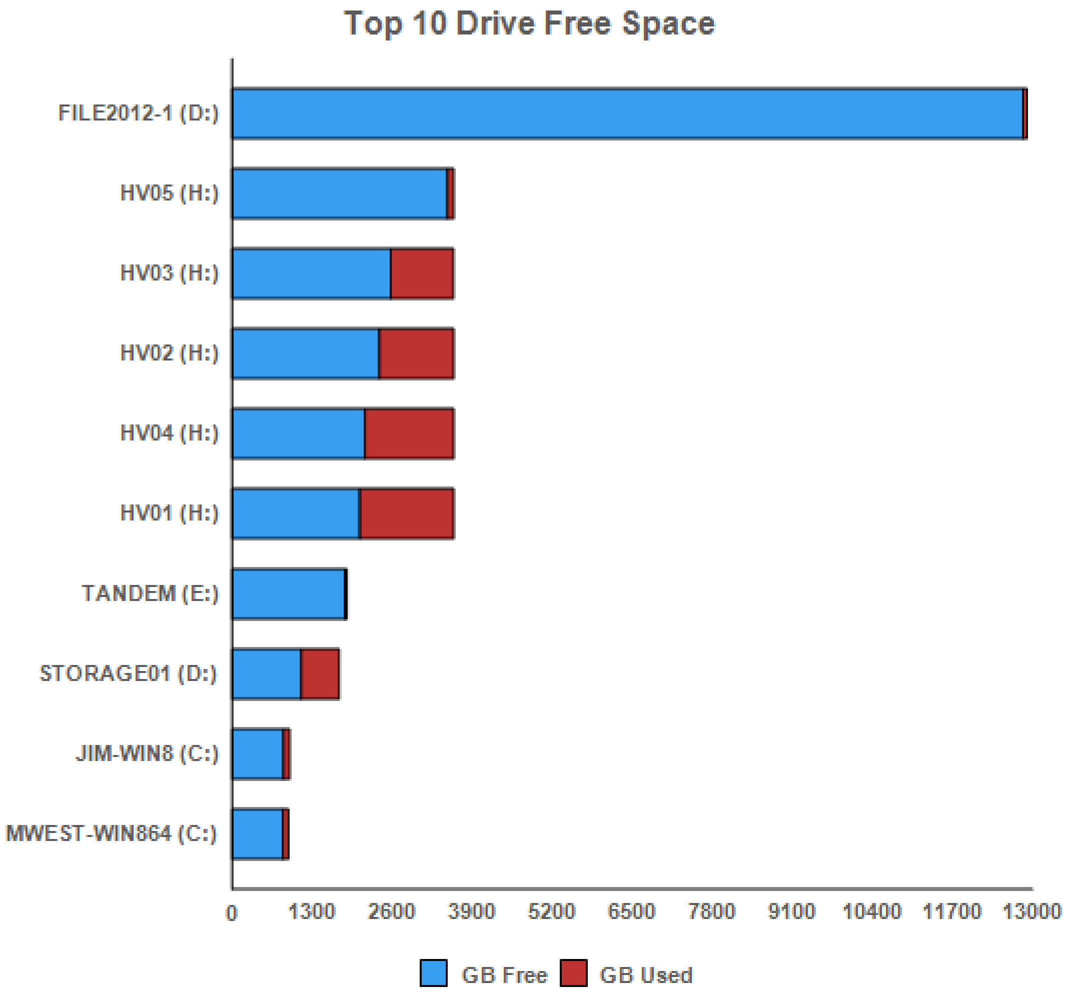
Workstation Aging



Asset Summary: Storage




Top 10 Drive % Used
JAGA (C:)
PSIMPSON1 (C:)
MmayhemON1 (C:)
MARKETING-1 (C:)
SE-DAVIS (D:)
win7.corp.MyCo.com (D:)
MmayhemON1 (D:)
TANDEM (C:)
MYCO30DEV (C:)
MELKINS-HP (C:)
0
10
20
30
40
50
60
70
80
90
100
Used
Free


Top 10 Drive Free Space
FILE2012-1 (D:)
HV05 (H:)
HV03 (H:)
HV02 (H:)
HV04 (H:)
HV01 (H:)
TANDEM (E:)
STORAGE01 (D:)
JIM-WIN8 (C:)
MWEST-WIN864 (C:)
0
1300
2600
3900
5200
6500
7800
9100
10400
11700
13000
GB Free
GB Used