intec
SOLUTIONS, INC
Transforming Business through Innovative Technologies

Network Assessment

Risk Report

Scan Date: 7/30/2016

Prepared for:
ABC Client

Prepared by:
Phil Stinson

8/1/2016

Table of Contents

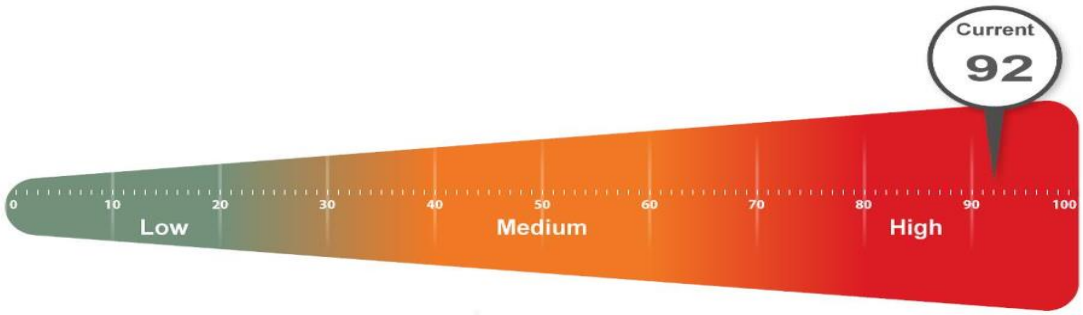
Discovery Tasks

The following discovery tasks were performed:

	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

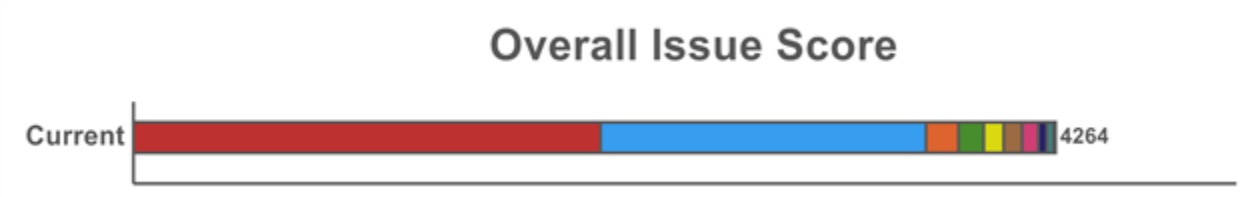
The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues.



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)
2160	***Current Score:*** 80 pts x 27 = 2160: 50.66%
	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.

	Significantly high number of Domain Administrators (35 pts each)
1505	***Current Score:*** 35 pts x 43 = 1505: 35.3%
	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.

	Inactive Computers (15 pts each)
150	***Current Score:*** 15 pts x 10 = 150: 3.52%
	Issue: 10 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.

	User has not logged in in 30 days (13 pts each)
117	***Current Score:*** 13 pts x 9 = 117: 2.74%
	Issue: 9 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.

	Anti-virus not turned on (92 pts each)
92	***Current Score:*** 92 pts x 1 = 92: 2.16%
	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.

	Lack of Redundant Domain Controller (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 1.99%
	Issue: Only one Domain Controller was found on the network. There is a heightened risk of business downtime, loss of data, or service outage due to a lack of redundancy.
	Recommendation: Evaluate the risk, cost, and benefits of implementing a redundant Domain Controller.

	FEW Security patches missing on computers. (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 1.76%
	Issue: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Few is defined as missing 3 or less patches.
	Recommendation: Address patching on computers with missing security patches.

	Operating System in Extended Support (20 pts each)
40	***Current Score:*** 20 pts x 2 = 40: 0.94%
	Issue: 2 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.

	Insecure Listening Ports (10 pts each)
30	***Current Score:*** 10 pts x 3 = 30: 0.7%
	Issue: 3 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.

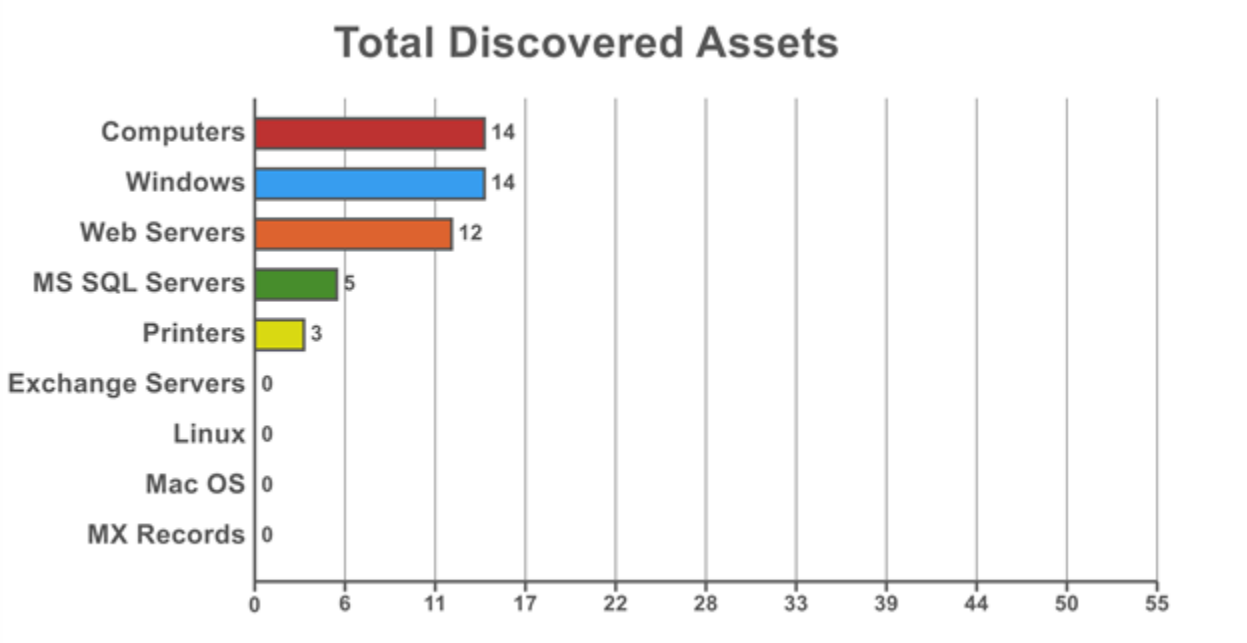
	Un-populated Organization Units (10 pts each)
10	***Current Score:*** 10 pts x 1 = 10: 0.23%
	Issue: Empty Organizational Units (OU) were found in Active Directory. They may not be needed and should be removed to prevent misconfiguration.
	Recommendation: Remove or populate empty Organizational Units.

Internet Speed Test Results

Download Speed: **38.85 Mb/s**

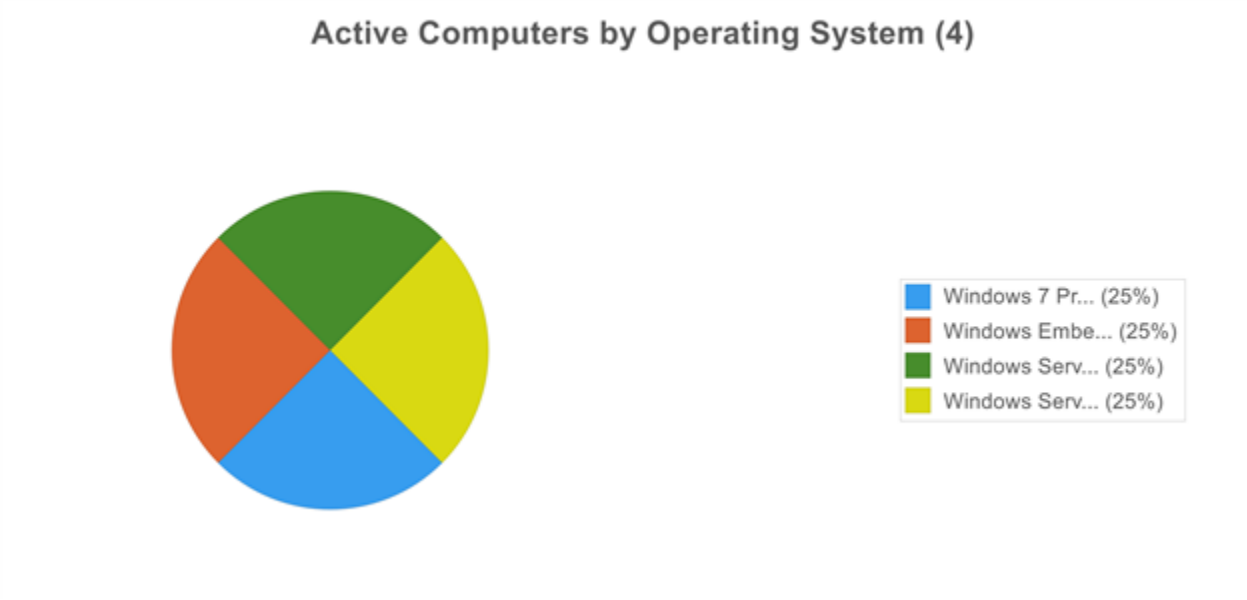
Upload Speed: **6.07 Mb/s**

Asset Summary: Total Discovered Assets

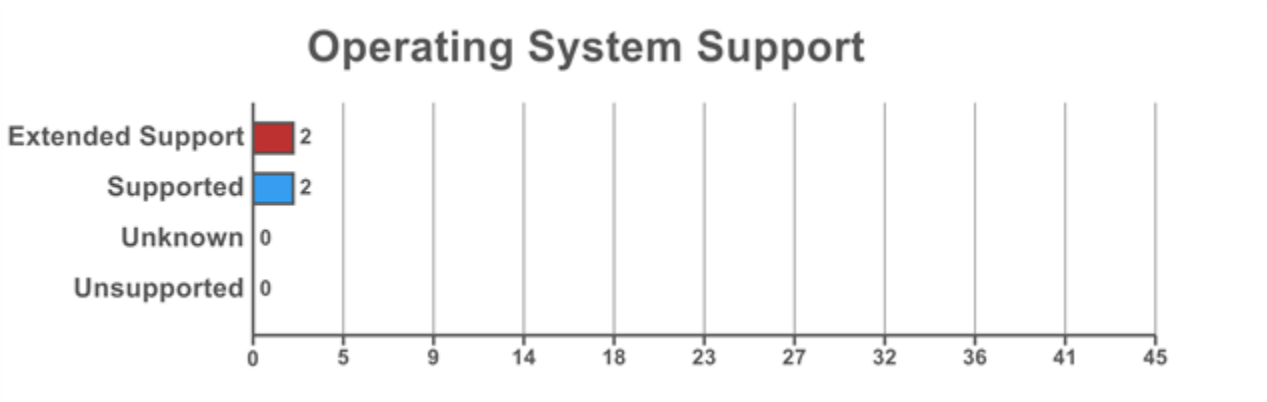


Asset Summary: Active Computers

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.

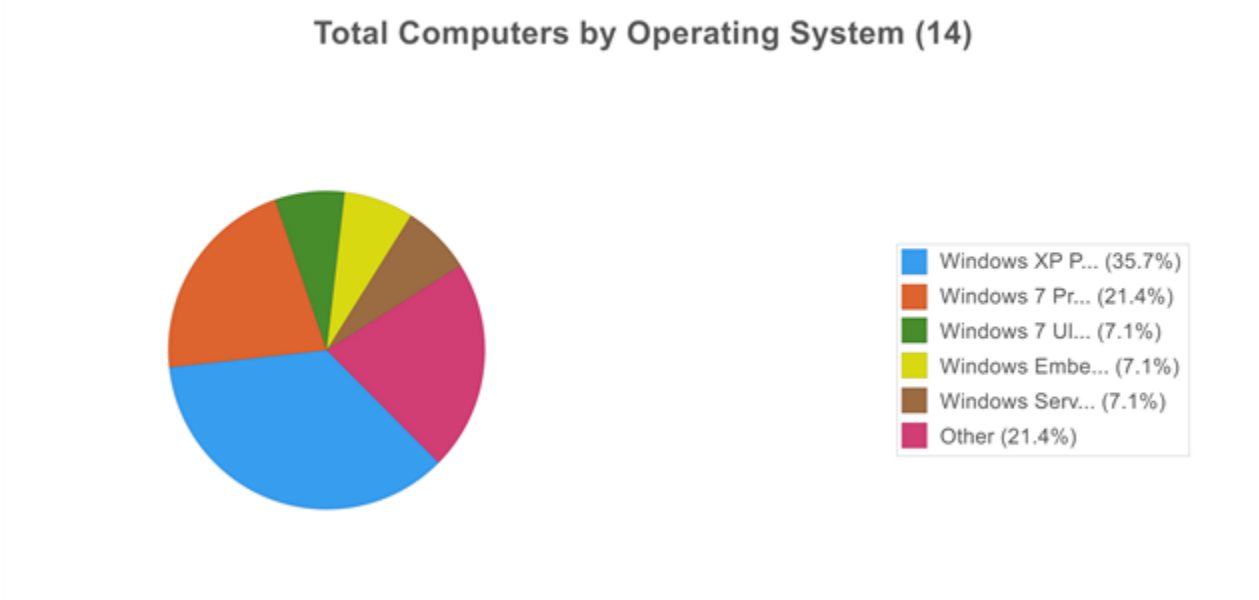


Operating System	Total	Percent
Top Five		
Windows 7 Professional	1	25%
Windows Embedded Standard	1	25%
Windows Server 2008 R2 Standard	1	25%
Windows Server 2012 R2 Standard	1	25%
Total - Top Five	**4**	**100%**
Other		
Total - Other	**0**	**0%**
Overall Total	**4**	**100%**


Operating System Support
Extended Support
2
Supported
2
Unknown
0
Unsupported
0
0
5
9
14
18
23
27
32
36
41
45

Asset Summary: All Computers

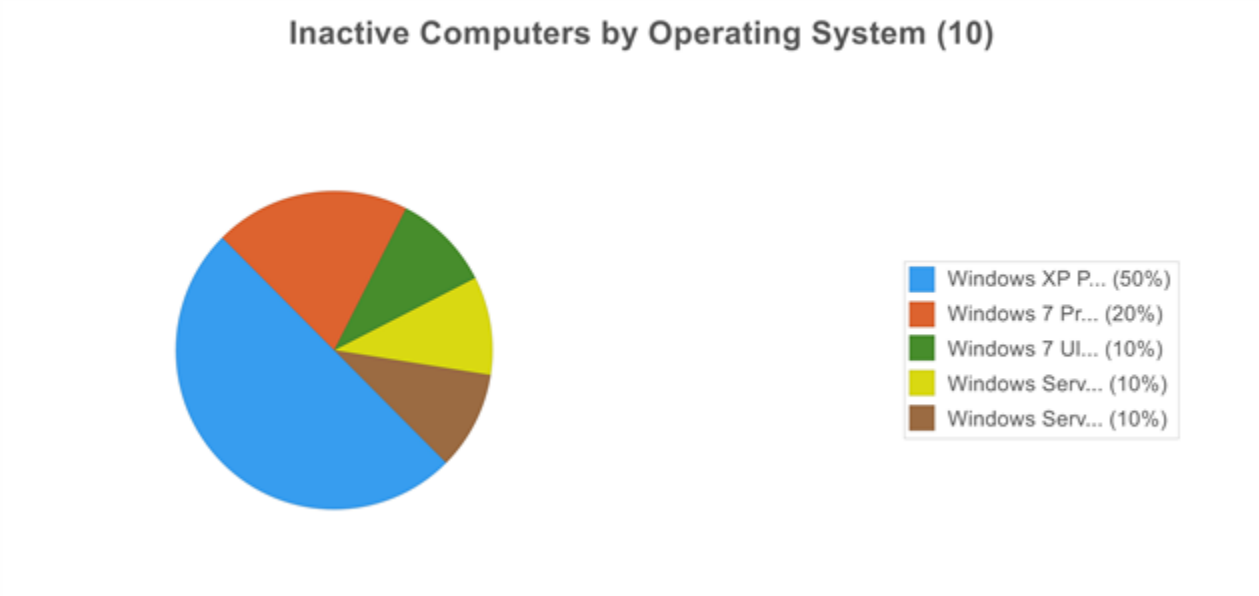
The list of all computers includes computers that may no longer be active but have entries in Active Directory (in a Domain environment).



Operating System	Total	Percent
Top Five		
Windows XP Professional	5	35.7%
Windows 7 Professional	3	21.4%
Windows 7 Ultimate	1	7.1%
Windows Embedded Standard	1	7.1%
Windows Server 2003	1	7.1%
Total - Top Five	**11**	**78.6%**
Other		
Windows Server 2008 R2 Standard	1	7.1%
Windows Server 2008 Standard	1	7.1%
Windows Server 2012 R2 Standard	1	7.1%
Total - Other	**3**	**21.4%**
Overall Total	**14**	**100%**

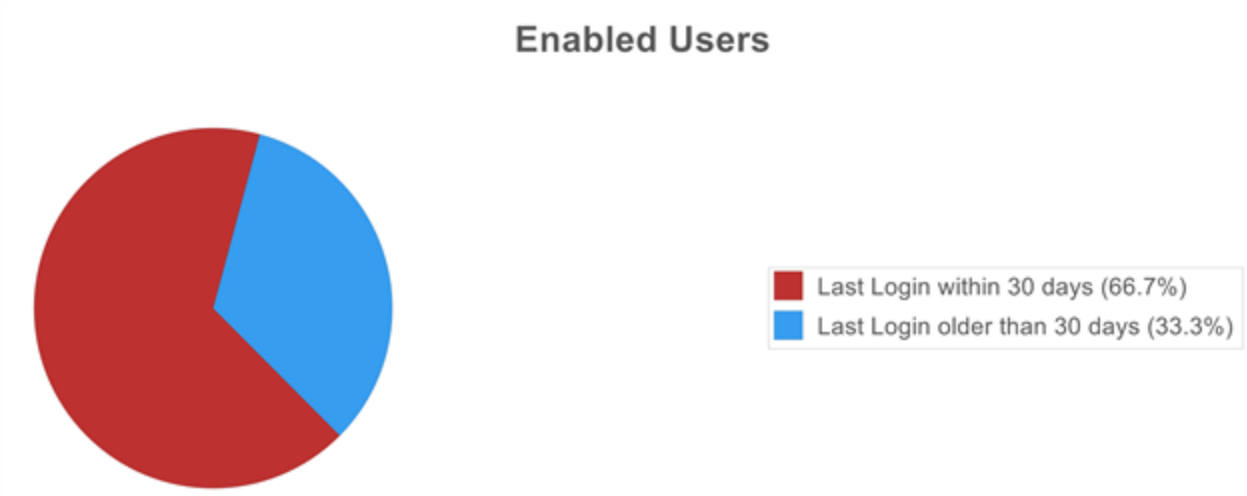
Asset Summary: Inactive Computers

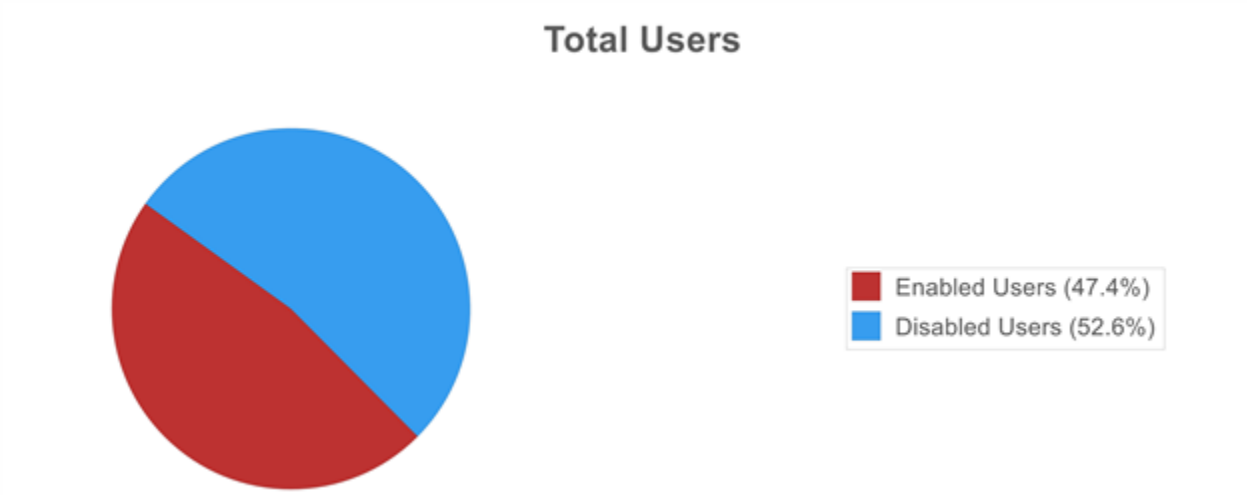
Inactive Computers are computers that could not be scanned or have not checked into Active Directory in the past 30 days.

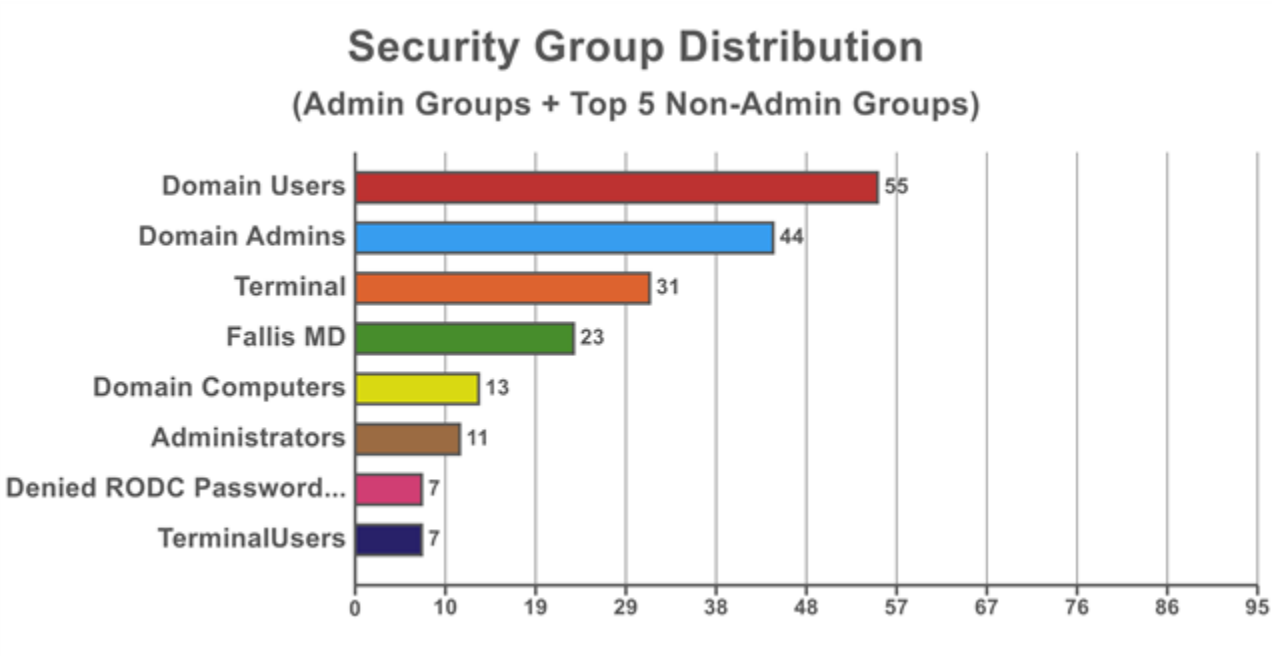


Operating System	Total	Percent
Top Five		
Windows XP Professional	5	50%
Windows 7 Professional	2	20%
Windows 7 Ultimate	1	10%
Windows Server 2003	1	10%
Windows Server 2008 Standard	1	10%
Total - Top Five	**10**	**100%**
Other		
Total - Other	**0**	**0%**
Overall Total	**10**	**100%**

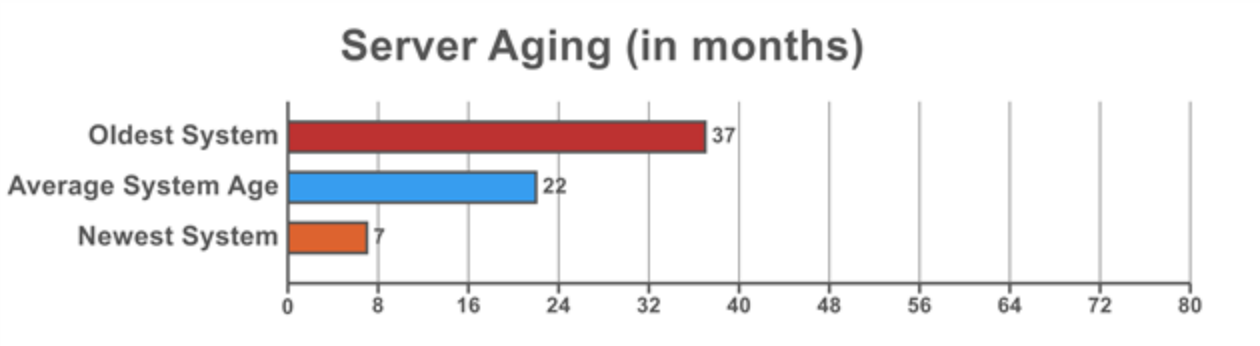
Asset Summary: Users






Security Group Distribution
(Admin Groups + Top 5 Non-Admin Groups)
Domain Users
Domain Admins
Terminal
Fallis MD
Domain Computers
Administrators
Denied RODC Password...
TerminalUsers
55
44
31
23
13
11
7
7
0
10
19
29
38
48
57
67
76
86
95

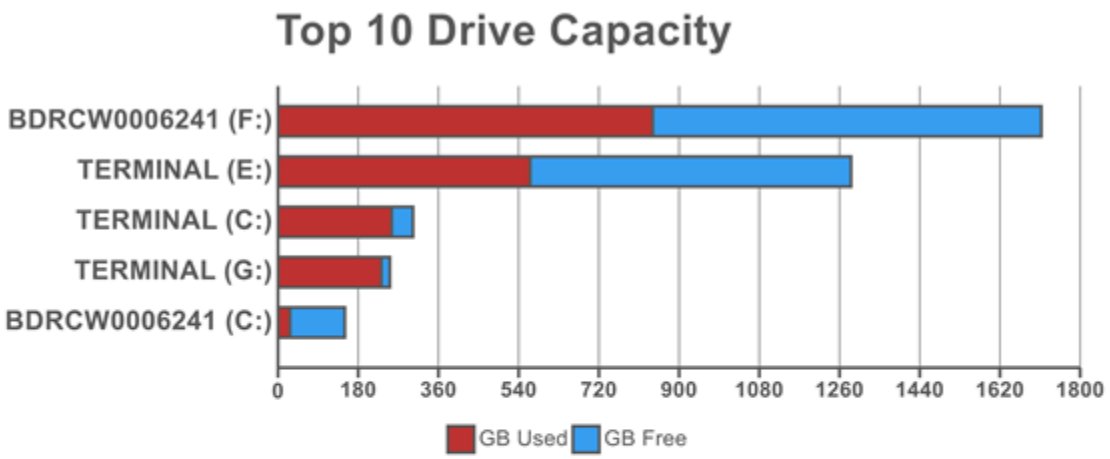
Server Aging

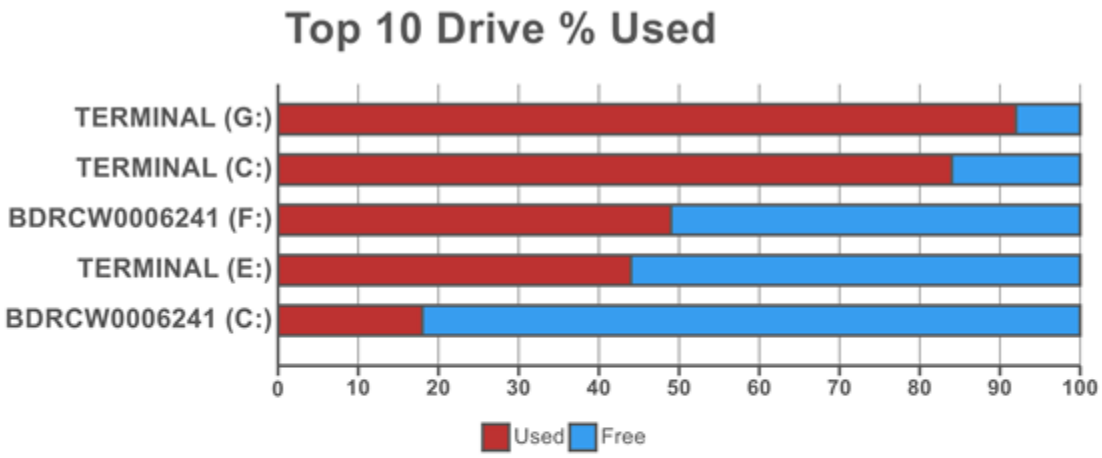


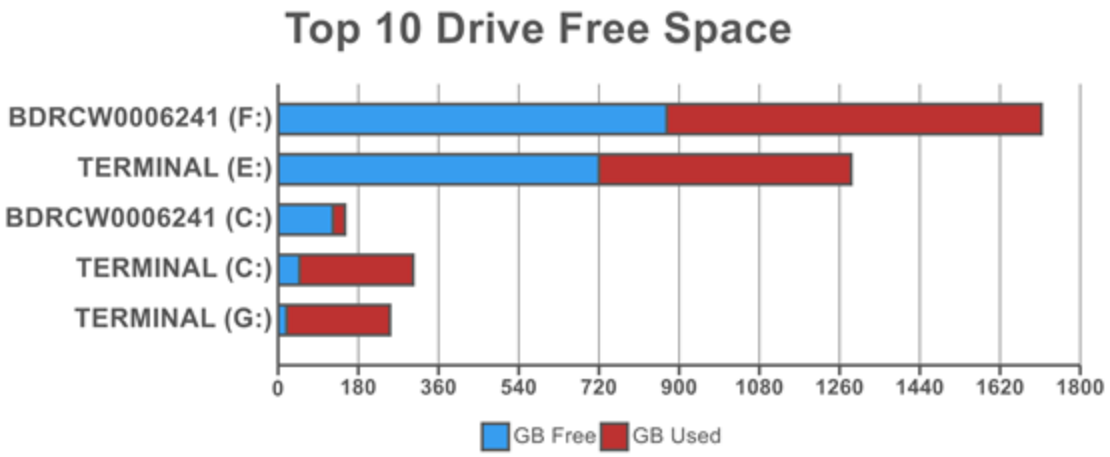
Workstation Aging

No Workstation Aging data could be determined.

Asset Summary: Storage






Top 10 Drive Free Space
BDRCW0006241 (F:)
TERMINAL (E:)
BDRCW0006241 (C:)
TERMINAL (C:)
TERMINAL (G:)
0
180
360
540
720
900
1080
1260
1440
1620
1800
GB Free
GB Used