Treasure Valley:IT

Information Technology. Delivered FAST.

Network Assessment

Risk Report

self
bob

4/5/2016

2/11/2016

Discovery Tasks

The following discovery tasks were performed:

✓	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

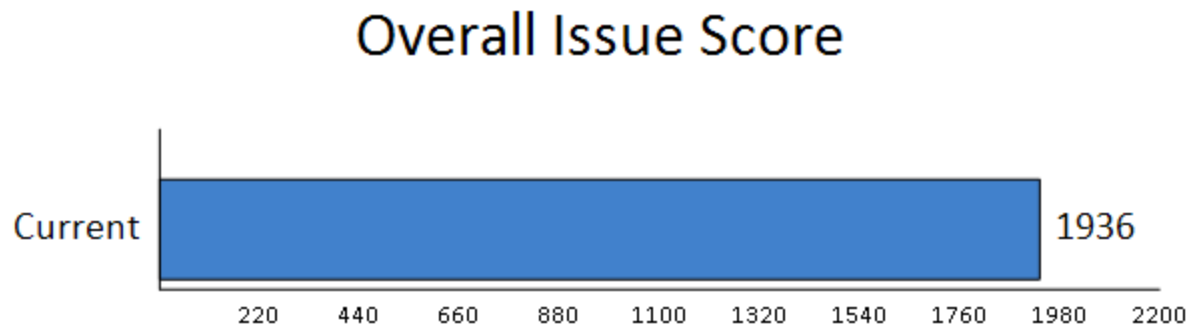
Risk Score

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.



Unsupported Operating Systems (97 pts)

Issue: 3 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.

Anti-virus not installed (94 pts)

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.

Lack of Redundant Domain Controller (85 pts)

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)

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)

Issue: 6 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.

Inactive Computers (15 pts)

Issue: 52 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)

Issue: 29 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.

Un-populated Organization Units (10 pts)

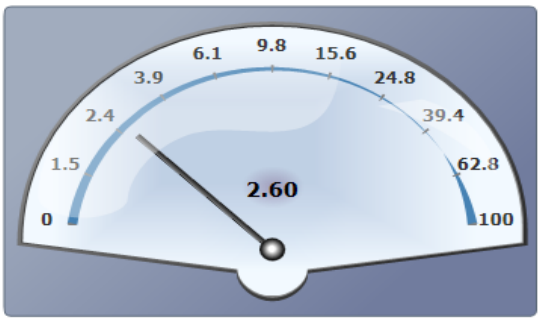
Issue: Empty Organizational Units (OU) were found in Active Directory. They may not be needed and should be removed to prevent misconfiguration.
Recommendation: Remove or populate empty Organizational Units.

Insecure Listening Ports (10 pts)

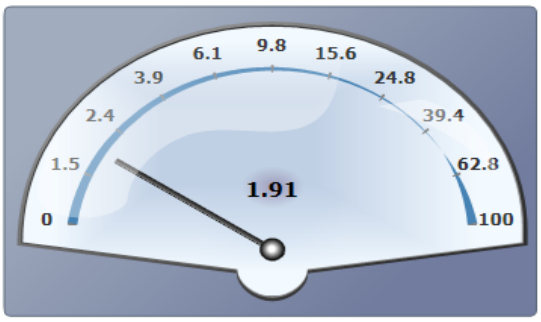
Issue: 1 computerwas found to be using potentially insecure protocols.
Recommendation: There may be a legitimate business need, but these risks should be assessed individually. Certain protocols are inherently insecure since they typically lack encryption. Inside the network, their use should be minimized 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.

Internet Speed Test Results

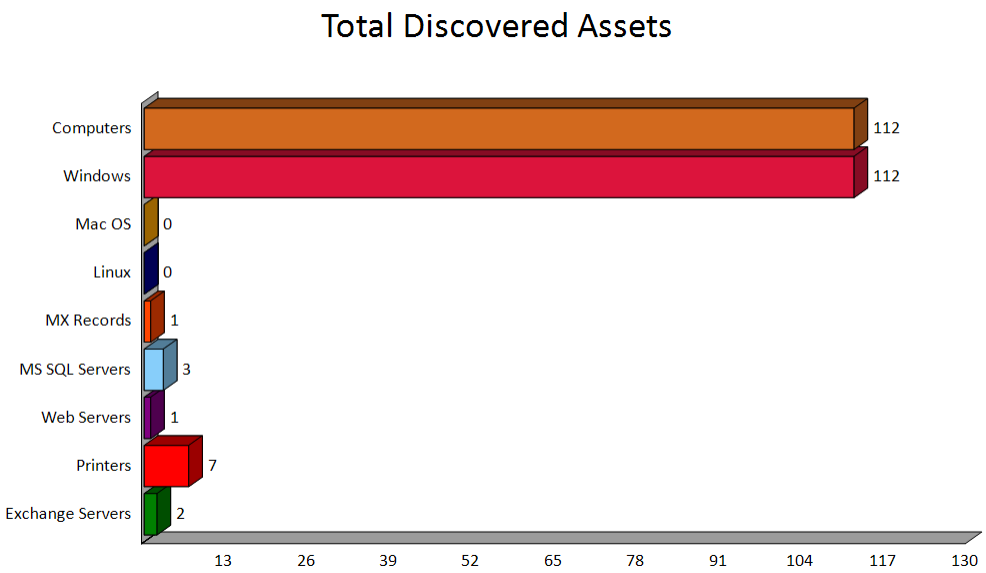
Download Speed: **2.60 Mb/s**



Upload Speed: **1.91 Mb/s**

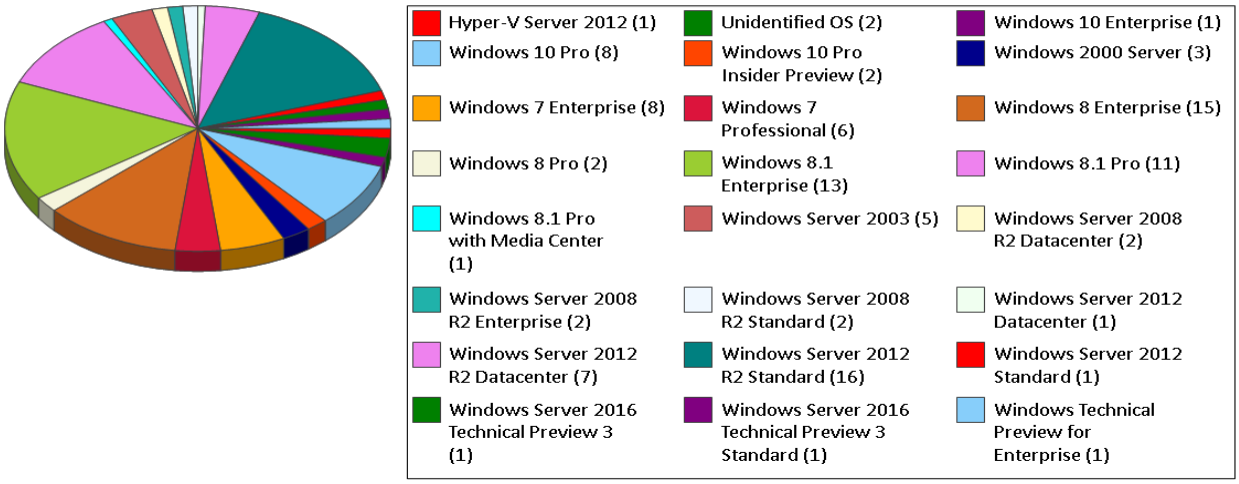


Asset Summary: Total Discovered Assets

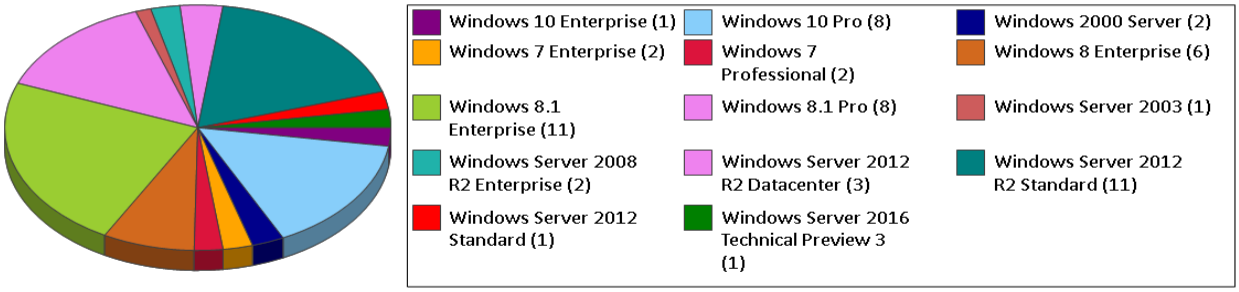


Asset Summary: Computers

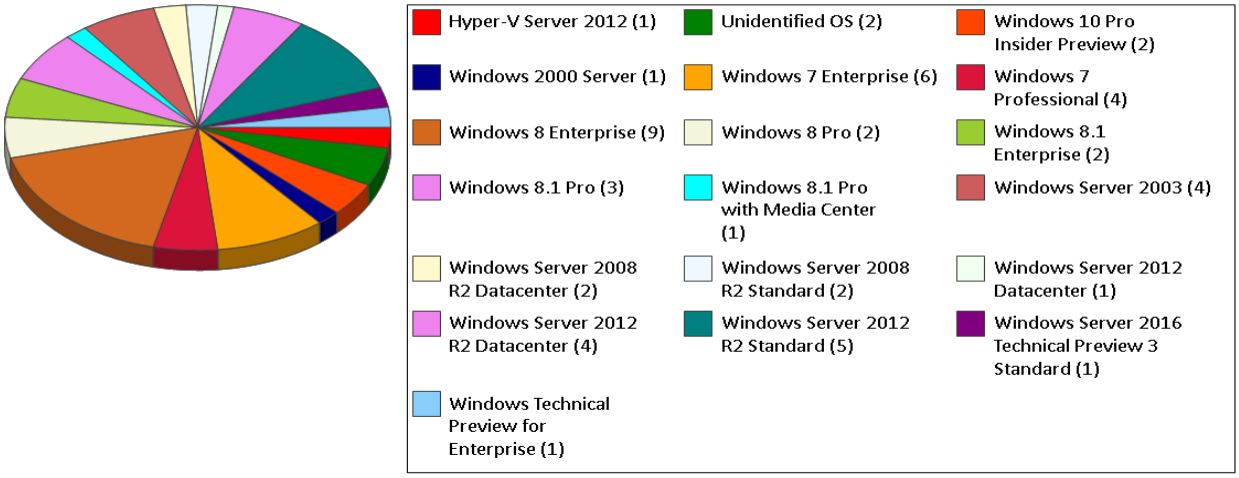
Total Computers by Operating System (112)



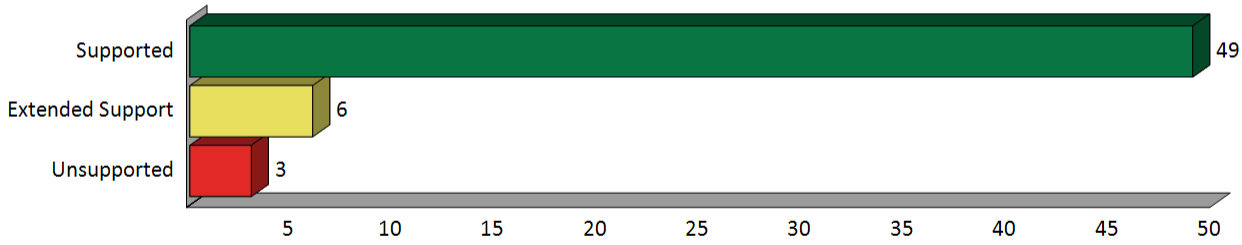
Active Computers by Operating System (59)



Inactive Computers by Operating System (53)

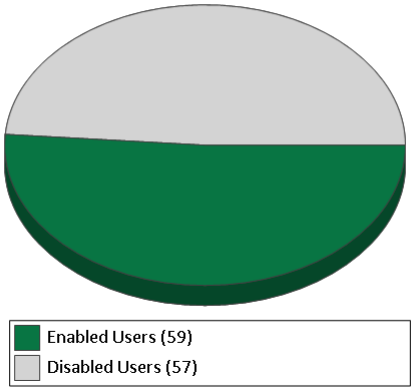


Operating System Support

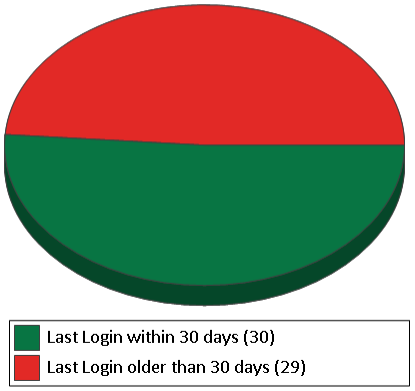


Asset Summary: Users

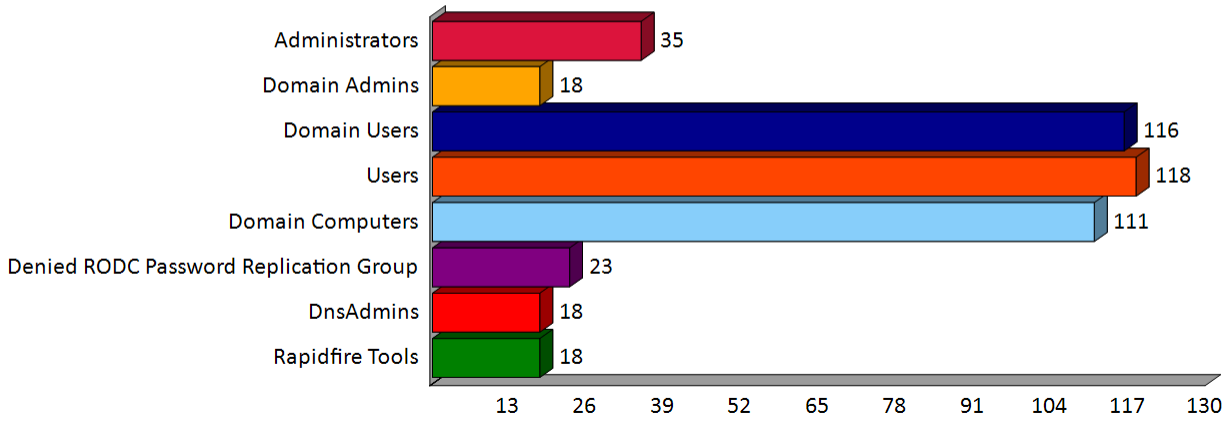
Total Users (116)



Enabled Users (59)



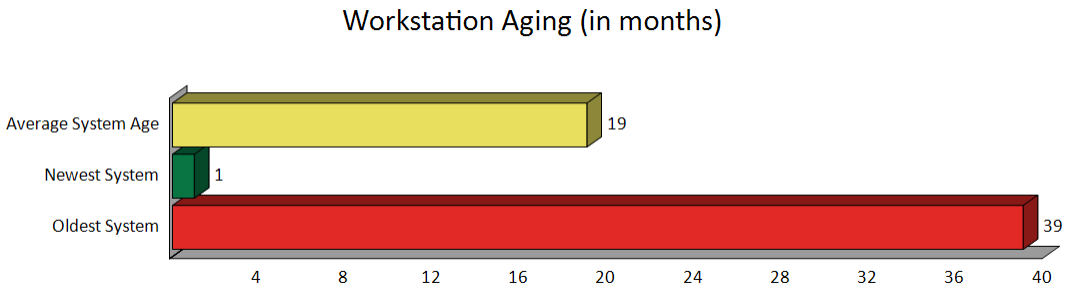
Security Group Distribution
(Admin Groups + Top 5 Non-Admin Groups)



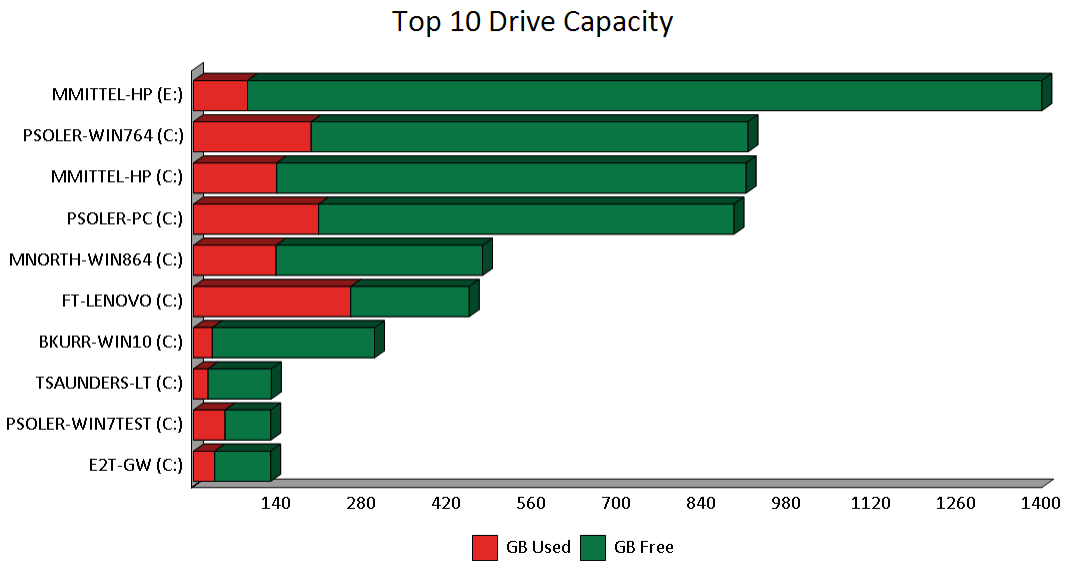
Server Aging

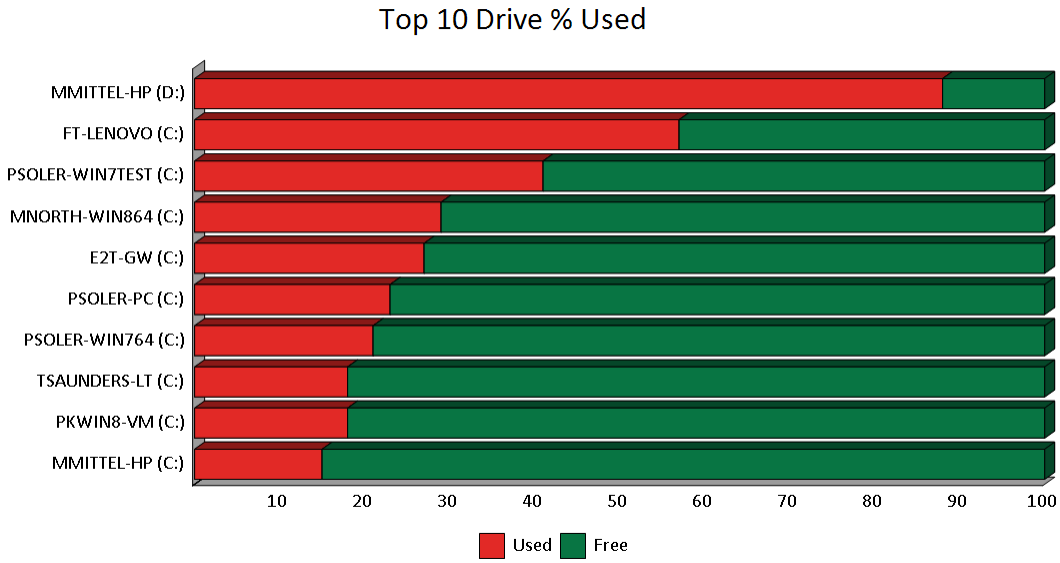
No Server Aging data could be determined.

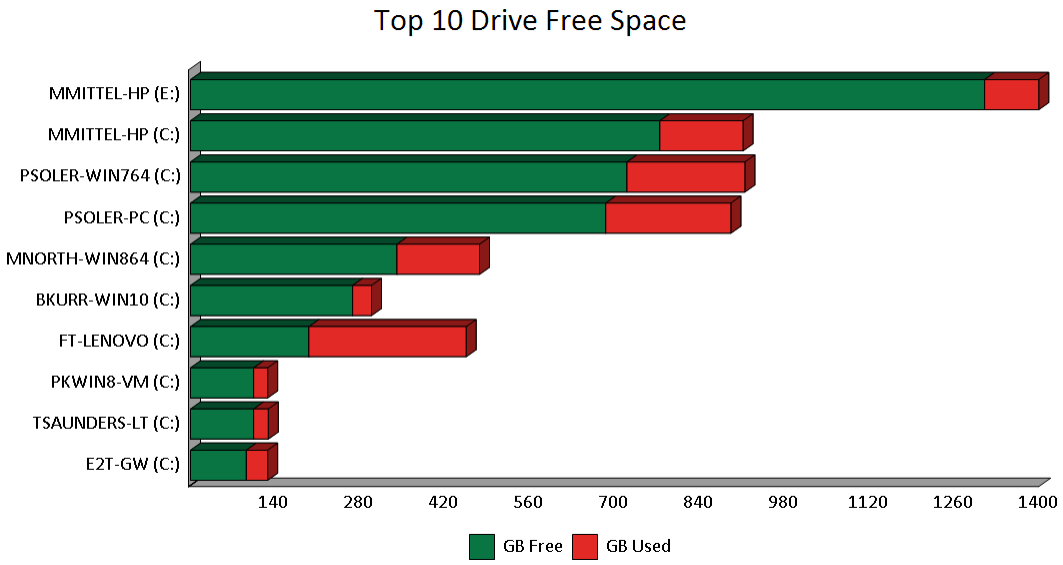
Workstation Aging



Asset Summary: Storage






Top 10 Drive Free Space
MMITTEL-HP (E:)
MMITTEL-HP (C:)
PSOLER-WIN764 (C:)
PSOLER-PC (C:)
MNORTH-WIN864 (C:)
BKURR-WIN10 (C:)
FT-LENOVO (C:)
PKWIN8-VM (C:)
TSAUNDERS-LT (C:)
E2T-GW (C:)
140
280
420
560
700
840
980
1120
1260
1400
GB Free
GB Used