HELIXSTORM

NETWORK ASSESSMENT

RISK REPORT

Prepared by: Helixstorm
Prepared for: Prospect Or Customer 12/3/2014

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

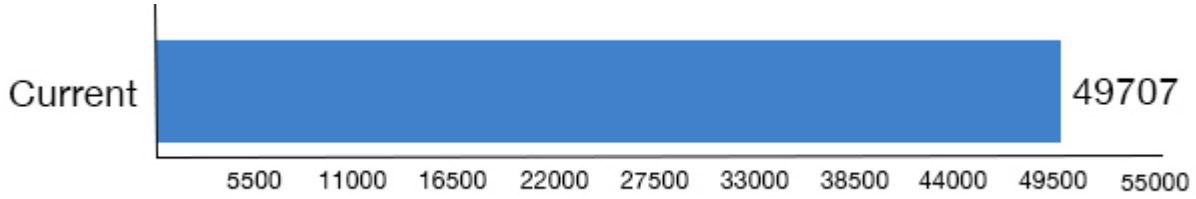
The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues.

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.

Overall Issue Score



Potential Password Strength Risks (100 pts)

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.

Unsupported Operating Systems (97 pts)

Issue: 30 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-spyware 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-spyware is deployed to all possible endpoints.

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.

LOTS of Security patches missing on computers (90 pts)

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 password set to never expire (80 pts)

Issue: User accounts with passwords set to never expire present a risk of use by authorized 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.

Potential Disk Space Issue (68 pts)

Issue: Computers were found with significantly low free disk space.

Recommendation: Free or add additional disk space for the specified drives.

Significantly high number of Domain Administrators (35 pts)

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.

Operating System in Extended Support (20 pts)

Issue: 16 computers were found using an operating system that is in extended supported. Extended support is a warning period before an operating 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: 102 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: 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.

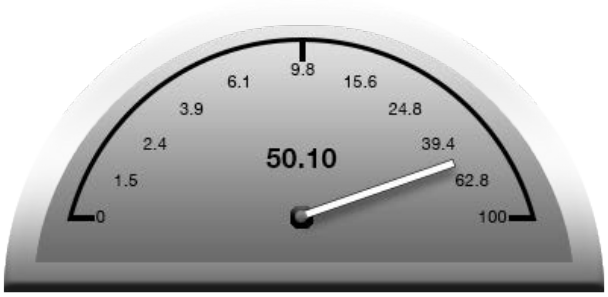
Un-populated Organization Units (10 pts)

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.

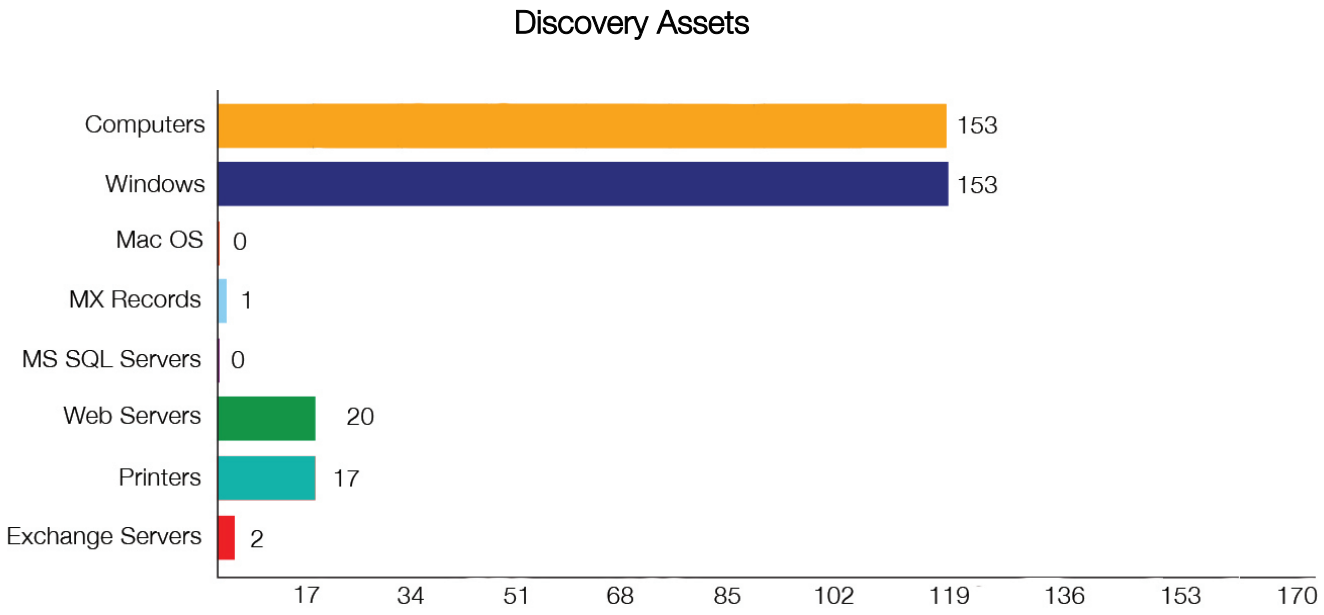
INTERNET SPEED TEST RESULTS

Download Speed: **50.10 Mb/s**



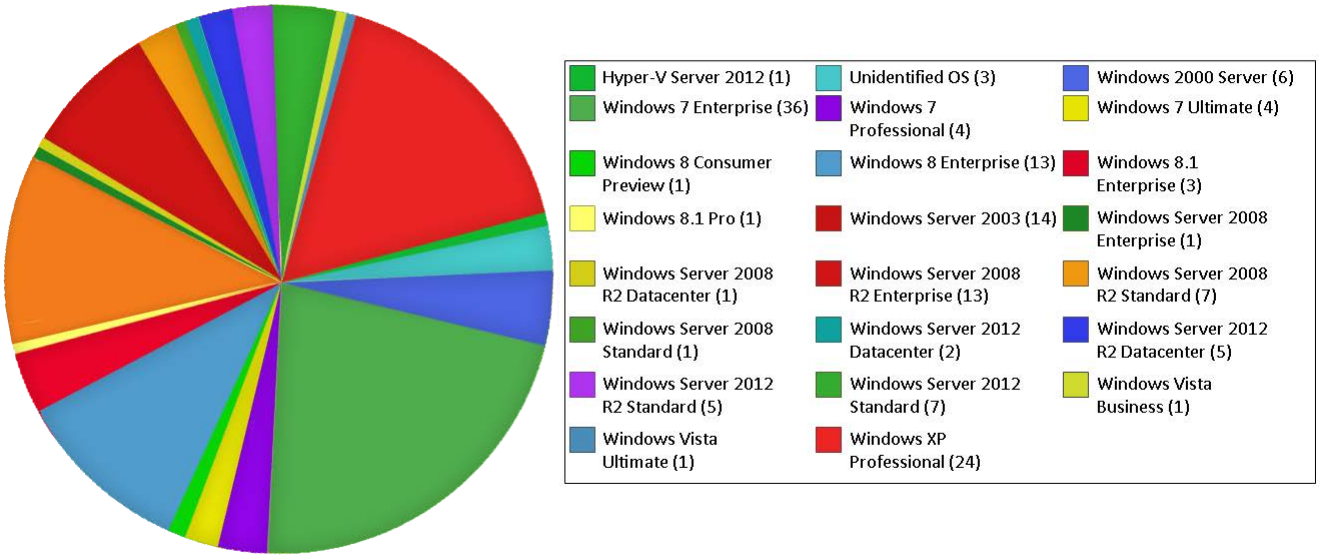
Upload Speed: **22.02 Mb/s**

ASSET SUMMARTY: DISCOVERY ASSETS

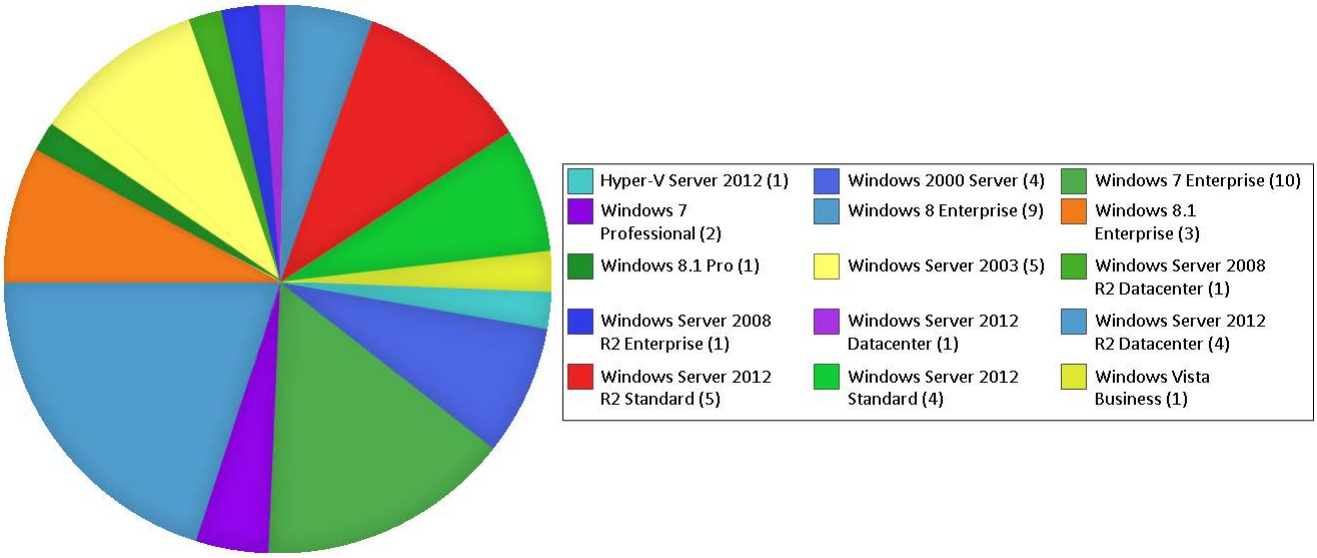


ASSET SUMMARTY: COMPUTERS

Total Computers by Operating System (154)

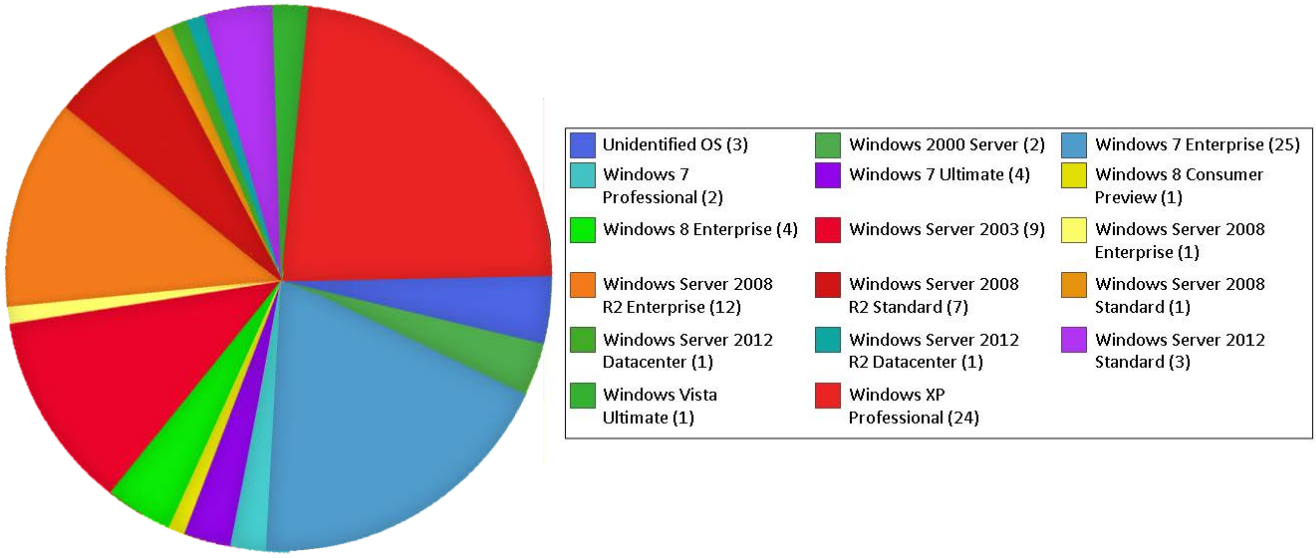


Active Computers by Operating System (52)

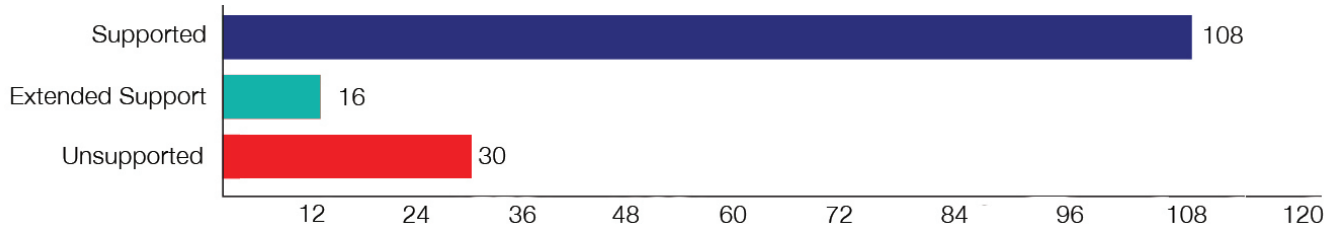


ASSET SUMMARTY: COMPUTERS

Inactive Computers by Operating System (101)

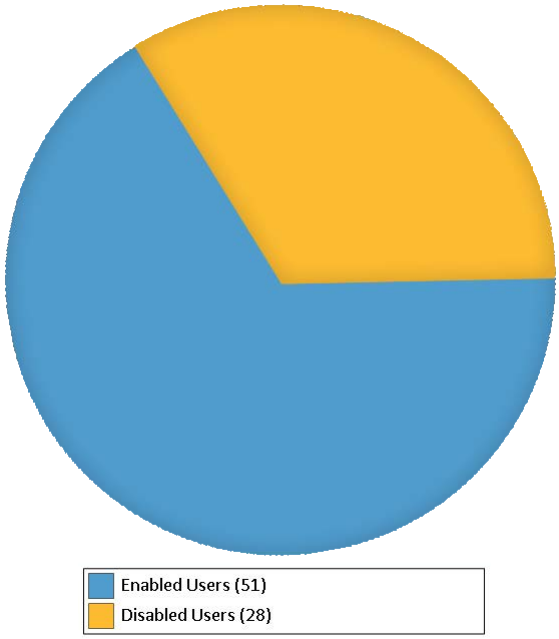


Active Computers by Operating System (52)

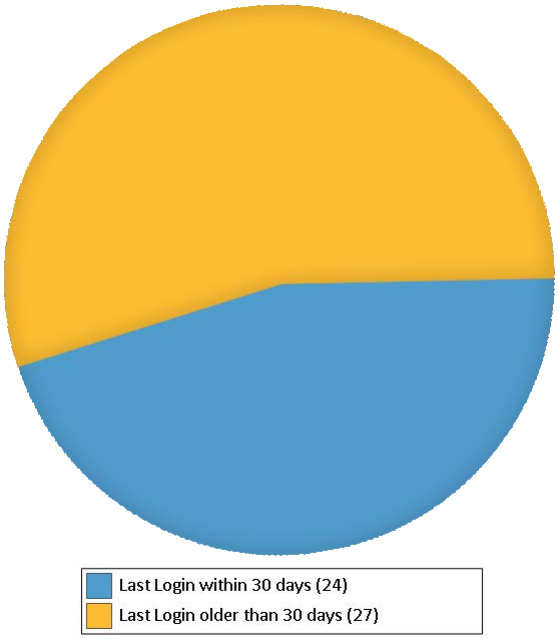


ASSET SUMMARY: USERS

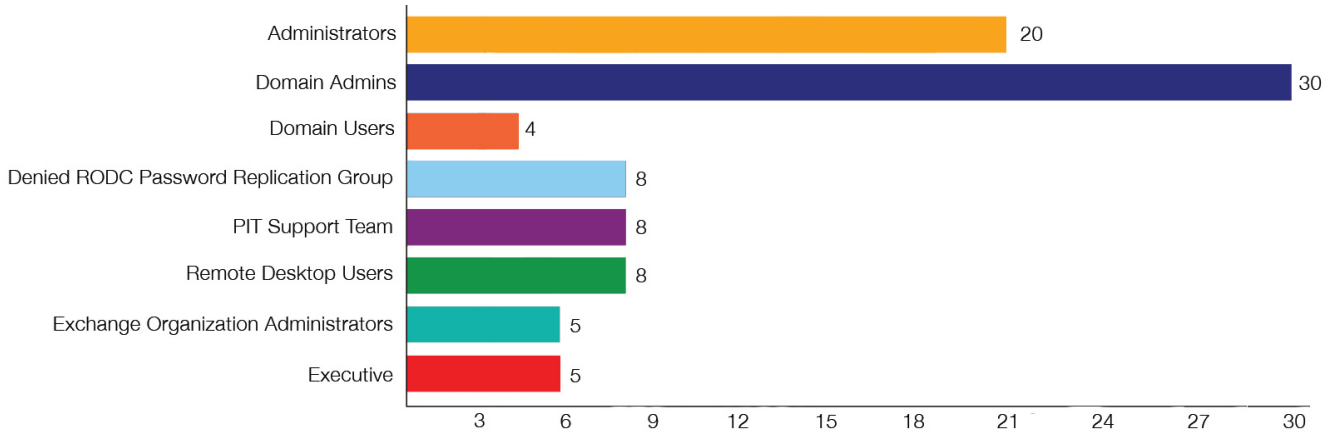
Total Users (79)



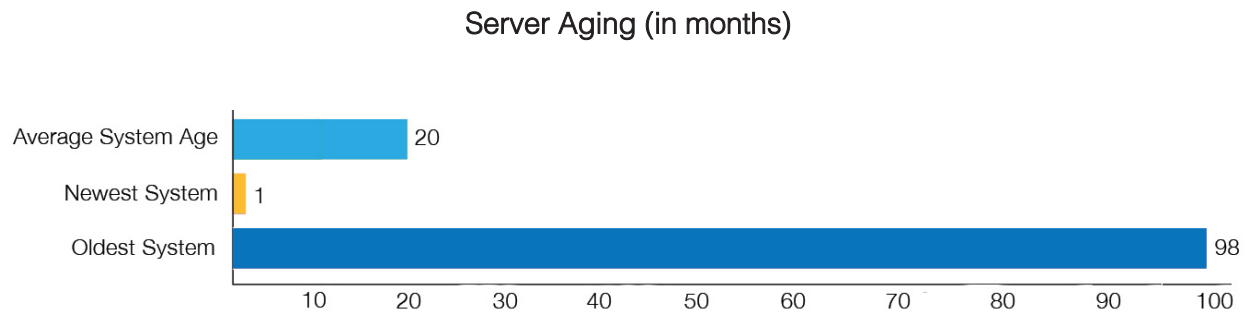
Enabled Users (51)



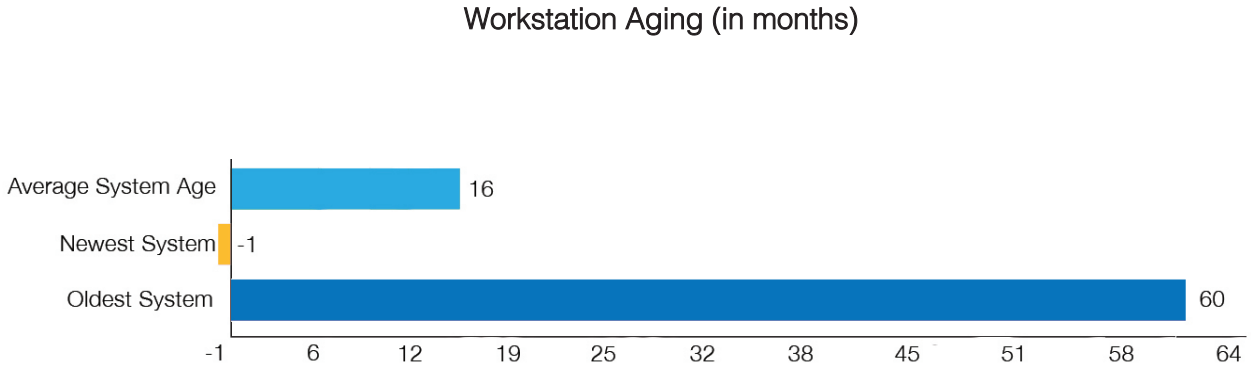
Security Group Distribution
(Admin Groups + Top 5 Non-Admin Groups)



SERVER AGING

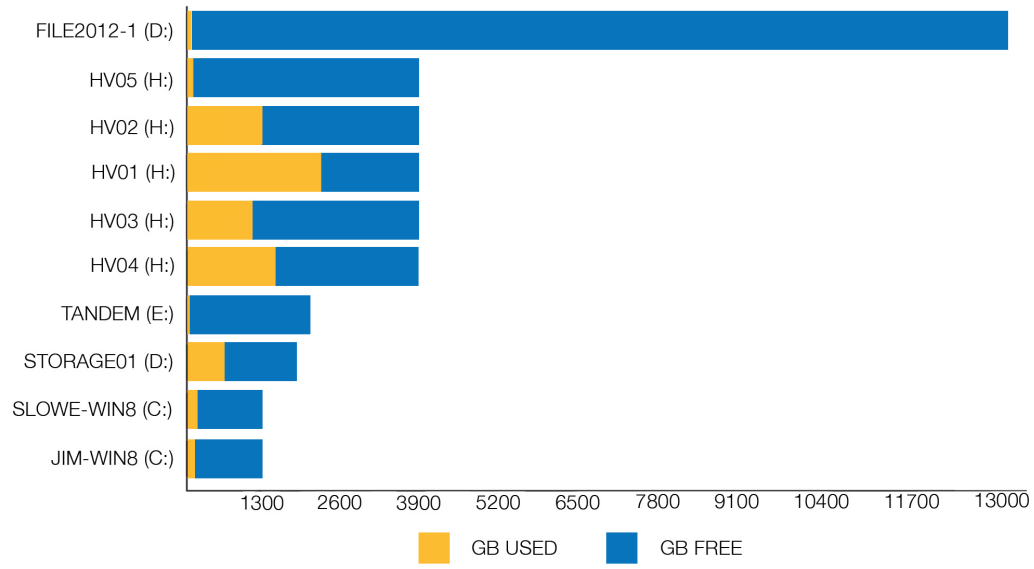


WORKSTATION AGING

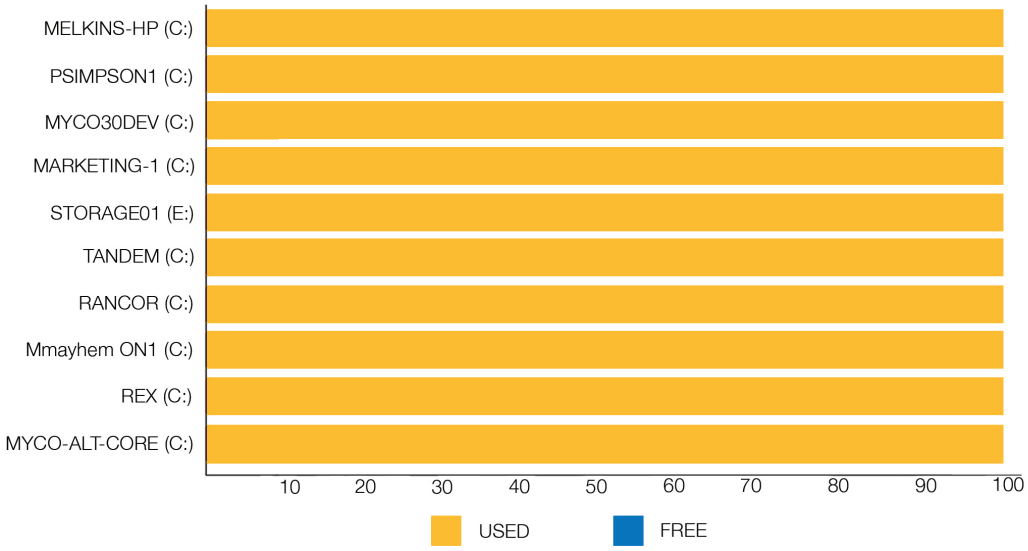


ASSET SUMMARY STORAGE

Top 10 Drive Capacity



Top 10 Drive % Used



Top 10 Drive Free Space