YourIT!
Your Logo Goes Here

Network Assessment

Risk Report

Prepared by:
YourIT! Company, Inc.
Prepared for:
Your Prospective Customer
5/2/2013

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 Organizational 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. 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.
✓	Web Server Discovery and Identification	List of web servers and type.
✓	System by System Event Log Analysis	Last 5 System and App Event Log errors for servers.
✓	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.
✓	Network Discovery for non-AD Devices	List of non-AD devices responding to network requests.
✓	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.
✓	Internet Access and Speed Test	Test of Internet access and performance.
✓	External Security Vulnerabilities	List of Detected Issues from External Vulnerability Scan.
✓	Endpoint Security Check	Checks for the status of anti-virus, anti-spyware, local firewalls, and system backups.

Risk Score

The Risk Score is a value from 1 to 10, where 10 represents significant risk and potential issues.

Several critical issues were identified (summarized on the next page). Identified issues should be investigated and addressed immediately.

If additional information is needed, please consult the Full Detail Report.

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.

Inactive Users
We discovered 16 active user accounts that have not logged in within the past 30 days. These accounts should be reviewed and disabled or removed if they are no longer needed. Active accounts that are not in use may pose a security risk and should be addressed with a User Audit.

Inactive Computers
62 computers were found as having not checked in during the past 30 days. This poses no threat, but organization is essential to proper network management and providing accurate domain statistics.

Organizational Units
We discovered 12 populated Organizational Units. You should review the details of the Organization Units to ensure they align with your business and operational needs. Proper alignment is crucial to ensuring security and access policies are adhered to properly.

Password Strength Risks
Local Account Passwords on 1 computer were found to have a Potential Risk. 17 computers were found to have a Severe Risk. These are systems where passwords are extremely weak or are not required and should be rectified to prevent unauthorized access or the potential spread of viruses and worms.

Password Policies
33 enabled domain users have passwords that are set to never expire.

Insecure Listening Ports
23 computers were found to be using potentially insecure protocols. There may be a legitimate business need, but these risks should be assessed individually.

Operating System Support
40 computers were found to be using an Operating System that is in Extended Support which means patching and other updates will be unavailable in the near future.6 computers were found to be using an Operating System that is no longer supported by the manufacturer and should be upgraded.

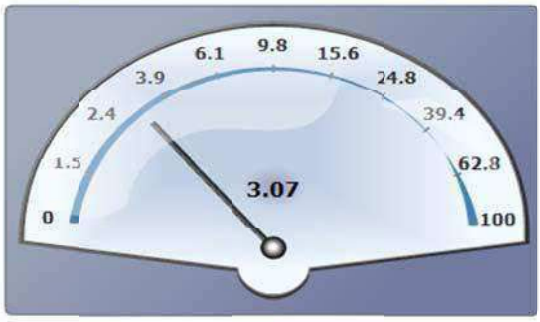
Critical Patches Missing
17 computers were detected as having 1 or more missing critical patches. Maintaining properly patched systems reduces the risk of infection via malware or viruses and improves performance and stability.

Endpoint Security
Anti-virus and anti-spyware was scanned for but not detected on 28 computers.

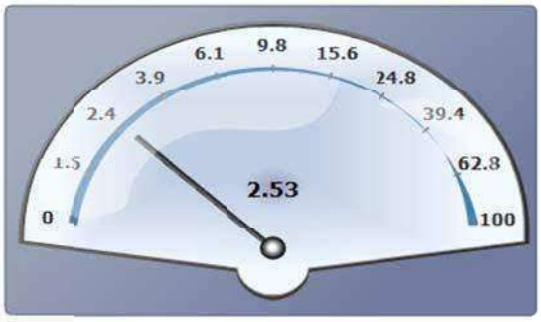
External Security Vulnerabilities
A scan of external vulnerabilities found 2 security holes and 0 security warnings. Security holes pose a major threat to business continuity and should be addressed immediately. Security warnings should be evaluated by a security professional to determine the actual risk and if remediation is necessary.

Internet Speed Test Results

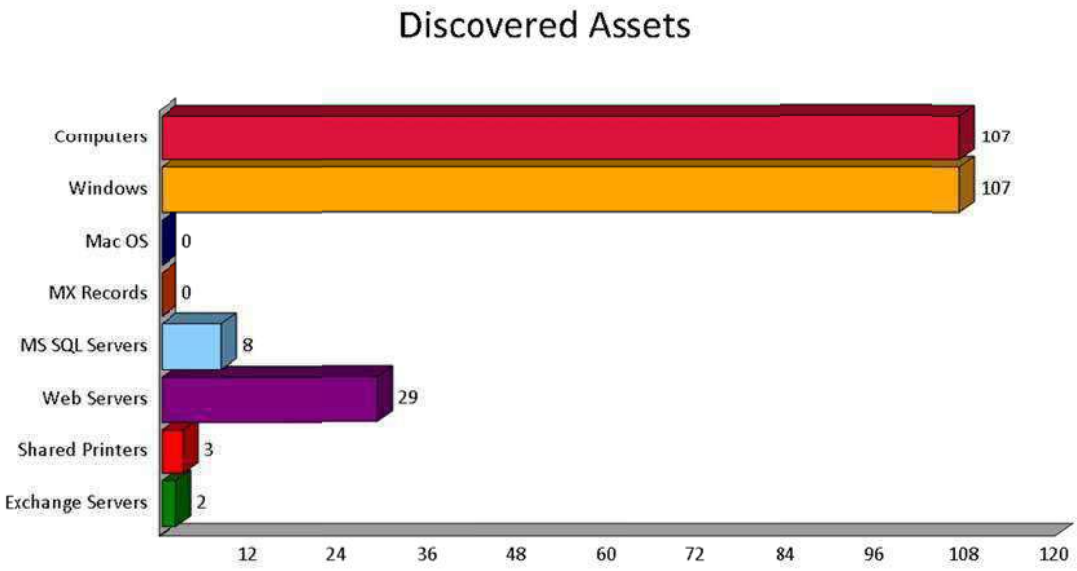
Download Speed: **3.07 Mb/s**



Upload Speed: **2.53 Mb/s**

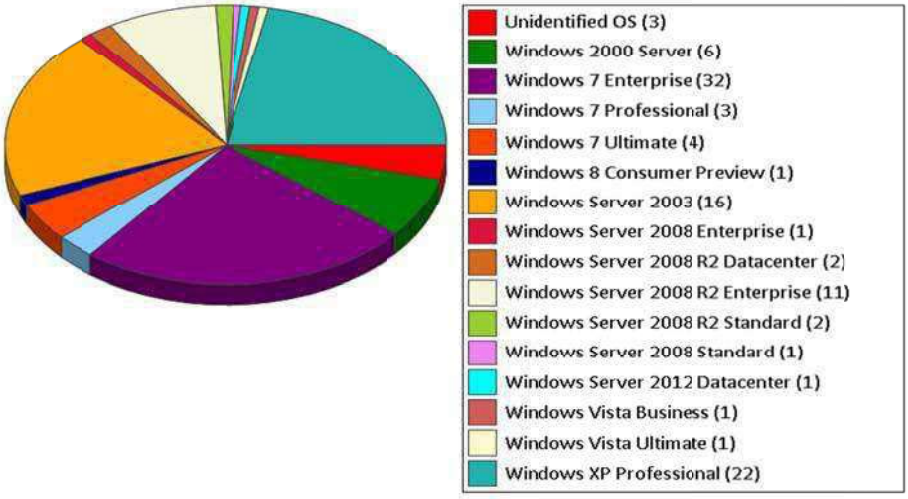


Asset Summary: Discovered Assets

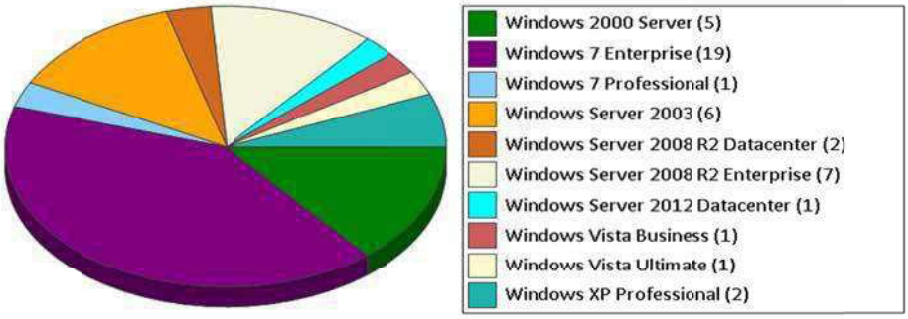


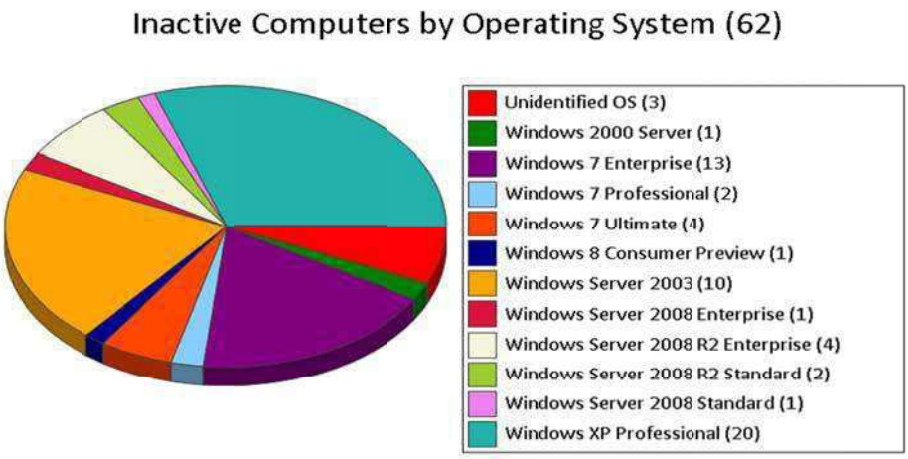
Asset Summary: Computers

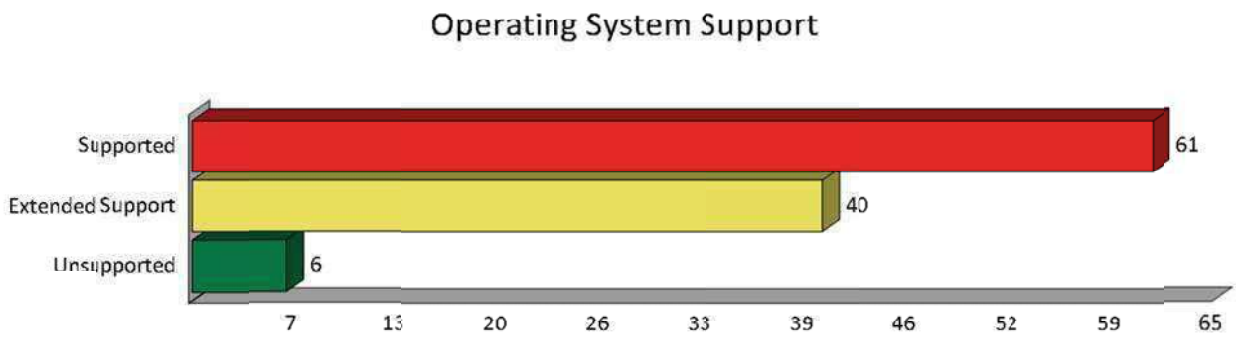
Total Computers by Operating System (107)



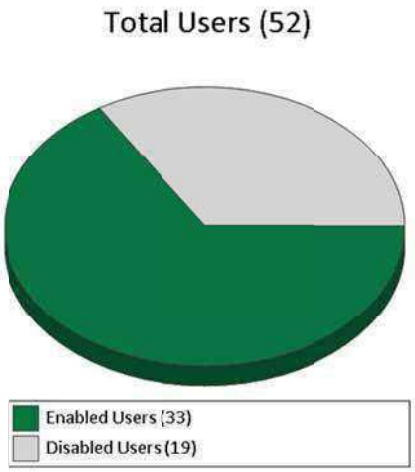
Active Computers by Operating System (45)

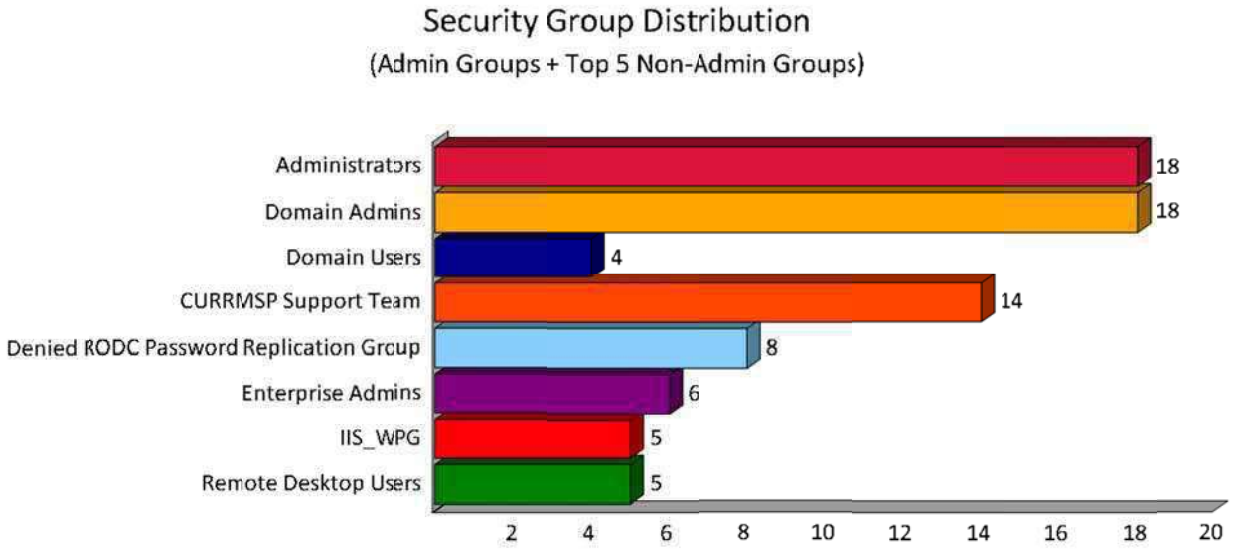



Inactive Computers by Operating System (62)
Unidentified OS (3)
Windows 2000 Server (1)
Windows 7 Enterprise (13)
Windows 7 Professional (2)
Windows 7 Ultimate (4)
Windows 8 Consumer Preview (1)
Windows Server 2003 (10)
Windows Server 2008 Enterprise (1)
Windows Server 2008 R2 Enterprise (4)
Windows Server 2008 R2 Standard (2)
Windows Server 2008 Standard (1)
Windows XP Professional (20)

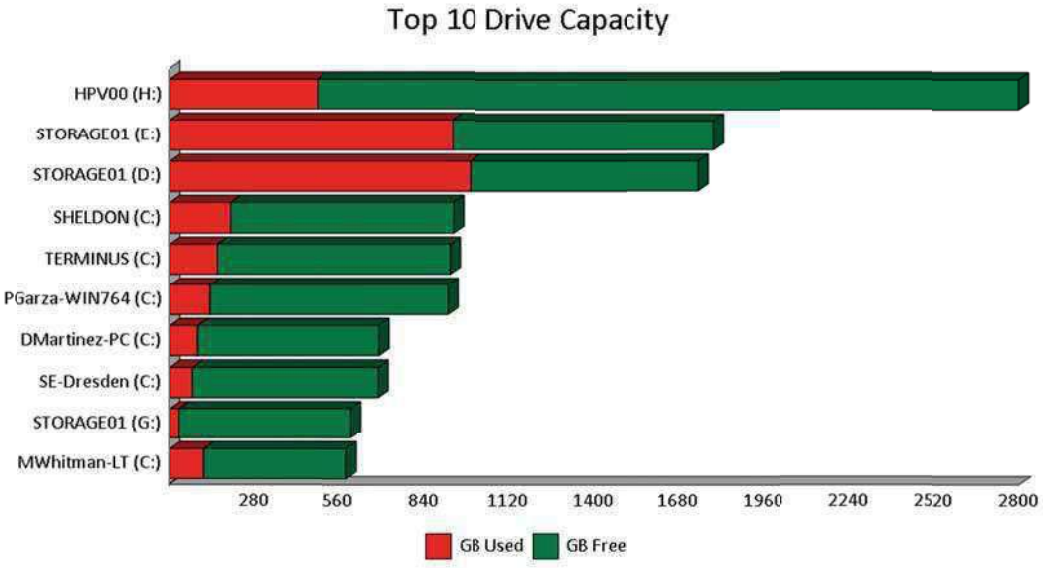

Operating System Support
Supported
Extended Support
Unsupported
61
40
6
7
13
20
26
33
39
46
52
59
65

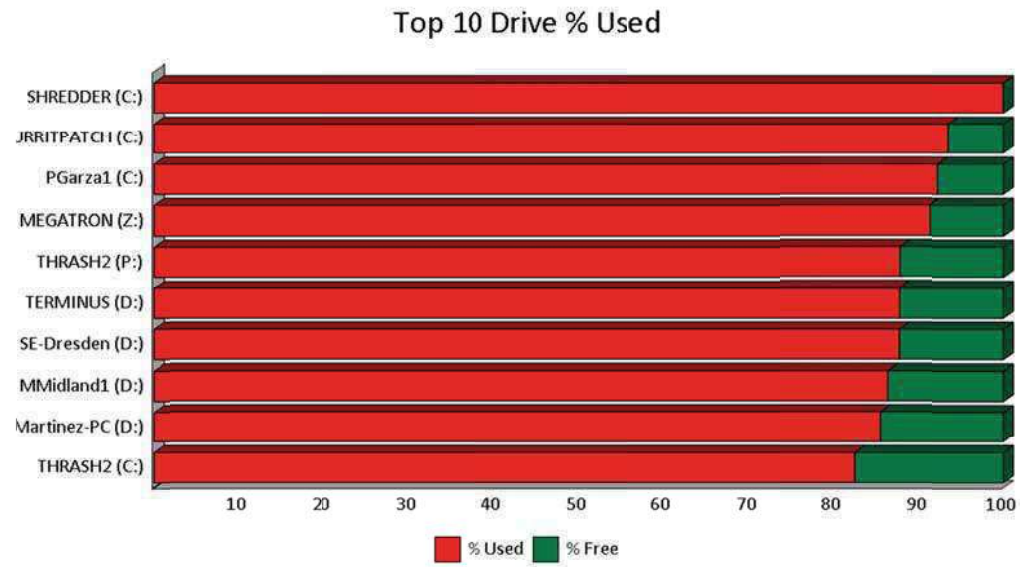
Asset Summary: Users

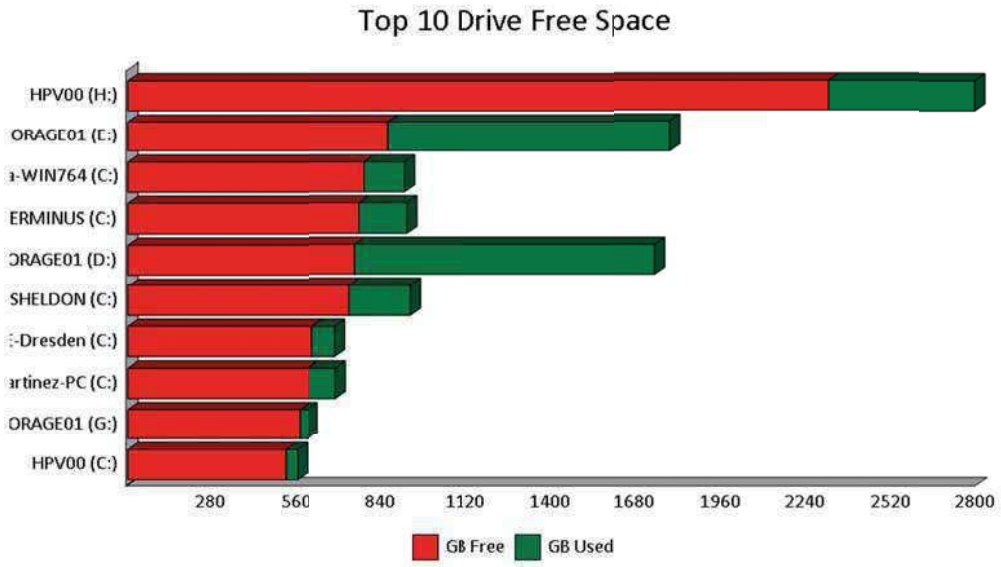




Asset Summary: Storage






Top 10 Drive Free Space
HPV00 (H:)
ORAGE01 (E:)
a-WIN764 (C:)
ERMINUS (C:)
ORAGE01 (D:)
SHELDON (C:)
:-Dresden (C:)
artinez-PC (C:)
ORAGE01 (G:)
HPV00 (C:)
280
560
840
1120
1400
1680
1960
2240
2520
2800
GB Free
GB Used