CATALYST
TECHNOLOGY GROUP
Innovating how IT is delivered.sm

26-Sep-2019

Cyber Risk Assessment

Cyber Risk Analysis Update

My Client's Company

Prepared by: YourIT Company

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

Scan Date: 26-Sep-2019

Table of Contents

Cyber Risk Analysis Update Overview

The Cyber Risk Analysis Update aggregates risk analysis from multiple assessments performed on the network, providing you with both a Cyber Risk Score and a high-level overview of the health and security of the network.

The update details the scan tasks undertaken to discover security issues. In addition to the overall Cyber Risk Score, the update also presents separate risk scores for Network and Security. This includes a summary of individual issues, as well as their severity and weighting within the risk analysis.

At the end of the report, you can find a summary of the assets discovered on the network, in addition to other useful information organized by assessment type.

Risk analysis and risk management are not one-time activities. Risk analysis and risk management are dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management process to reduce newly identified or updated risk levels to reasonable and appropriate levels.

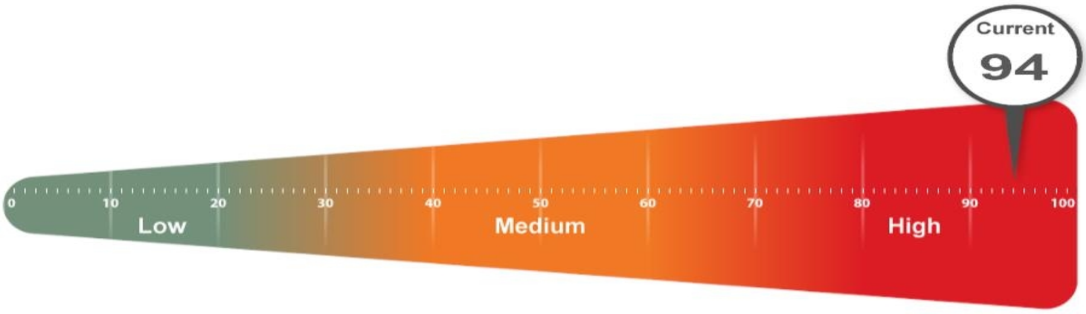
Cyber Risk Discovery Tasks

The following discovery tasks were performed.

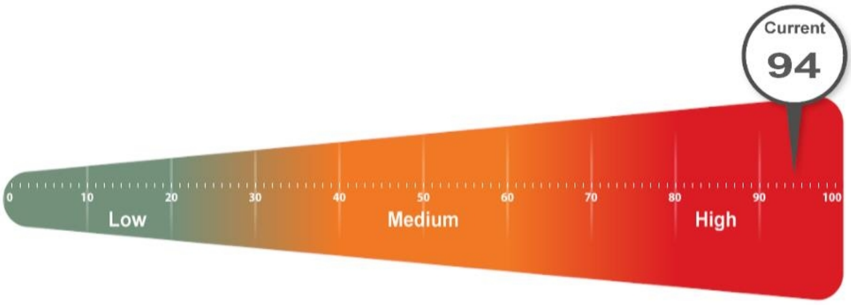
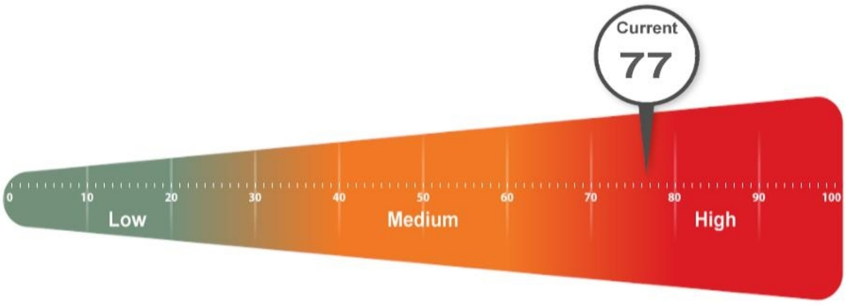
	Task	Description
Network		
□	Detect Domain Controllers	Identifies domain controllers and online status.
□	FSMO Role Analysis	Enumerates FSMO roles at the site.
□	Enumerate Organization Units and Security Groups	Lists the organizational units and security groups (with members).
□	User Analysis	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
□	Detect Local Accounts	Detects local accounts on computer endpoints.
□	Detect Added or Removed Computers	Lists computers added or removed from the Network since the last assessment.
□	Detect Local Mail Servers	Detects mail server(s) on the network.
□	Detect Time Servers	Detects server(s) on the network.
□	Discover Network Shares	Discovers the network shares by server.
□	Detect Major Applications	Detects all major apps / versions and counts the number of installations.
□	Detailed Domain Controller Event Log Analysis	Lists the 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	Lists the web servers and type.
□	Network Discovery for Non-A/D Devices	Lists the non-Active Directory devices responding to network requests.
□	Internet Access and Speed Test	Tests Internet access and performance.
□	SQL Server Analysis	Lists the SQL Servers and associated database(s).
□	Missing Security Updates.	Identifies computers missing security updates.
□	System by System Event Log Analysis	Discovers the five system and app event log errors for servers.
□	External Security Vulnerabilities	Lists the security holes and warnings from External Vulnerability Scan.
Security		
□	Detect System Protocol Leakage	Detects outbound protocols that should not be allowed.
□	Detect Unrestricted Protocols	Detects system controls for protocols that should be allowed but restricted.
□	Detect User Controls	Determines if controls are in place for user web browsing.
□	External Security Vulnerabilities	Performs a detailed External Vulnerability Scan. Lists and categorizes external security threats.
□	Network Share Permissions	Documents access to file system shares.
□	Domain Security Policy	Documents domain computer and domain controller security policies.
□	Local Security Policy	Documents and assesses consistency of local security policies.

Cyber Risk Score

The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.

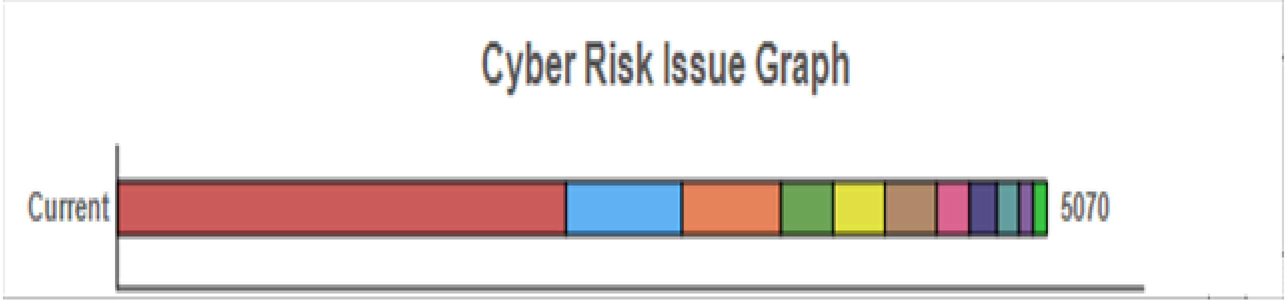


Several critical issues were identified. Identified issues should be investigated and addressed according to the Cyber Risk Analysis Update.

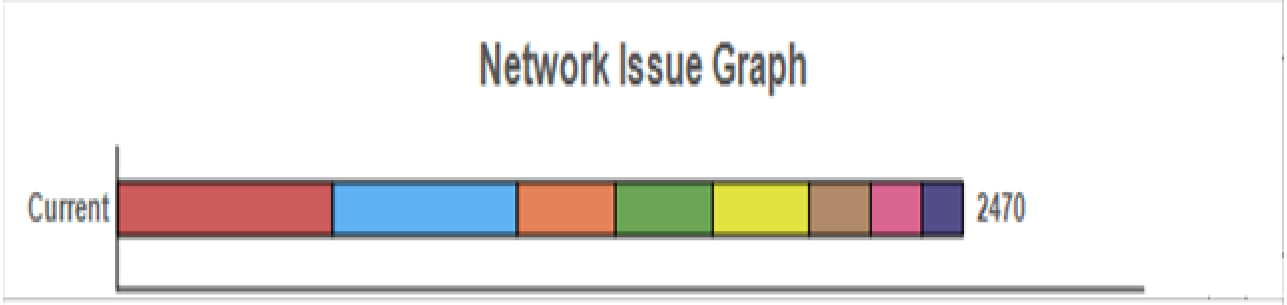
Module	Risk Score
Network	
Security	

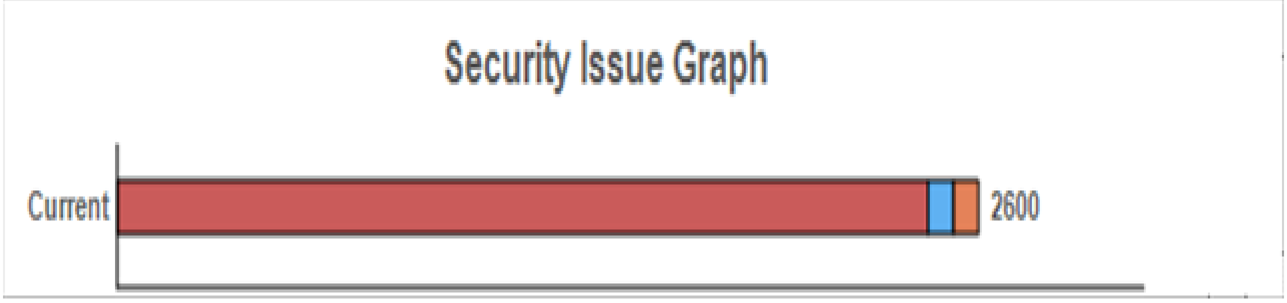
Cyber Risk Issue Graph

This section contains a summary of issues detected during the Cyber Risk 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 (%)





Cyber Risk Issue Summary

Network Issue Summary

	Significantly high number of Domain Administrators (35pts each)
630	***Current Score:*** 35pts x18 = 630: 25.51%
	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.

	User password set to never expire (30pts each)
540	***Current Score:*** 30pts x18 = 540: 21.86%
	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.

	User has not logged on to domain in 30 days (13pts each)
286	***Current Score:*** 13pts x22 = 286: 11.58%
	Issue: Users have not logged on to domain in 30 days. A user that has not logged in for an extended period of time could be a former employee or vendor.
	Recommendation: Disable or remove user accounts for users that have not logged on to active directory in 30 days.

	Anti-virus not installed (94pts each)
282	***Current Score:*** 94pts x3 = 282: 11.42%
	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 ensuring that anti-virus is deployed to all possible endpoints.

	Anti-spyware not installed (94pts each)
282	***Current Score:*** 94pts x3 = 282: 11.42%
	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: Assure that anti-spyware is deployed to all possible endpoints in order to prevent both security and productivity issues.

	Anti-virus not up to date (90pts each)
180	***Current Score:*** 90pts x2 = 180: 7.29%

	Issue: Up to date anti-virus definitions are required to properly prevent the spread of malicious software. Some anti-virus definitions were found to not be up to date.
	Recommendation: Ensure anti-virus definitions are up to date on specified computers.

	Few Security patches missing on computers. (75pts each)
150	***Current Score:*** 75pts x2 = 150: 6.07%
	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 missing 1-3 security patches.

	Operating system in Extended Support (20pts each)
120	***Current Score:*** 20pts x6 = 120: 4.86%
	Issue: Computers are 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.

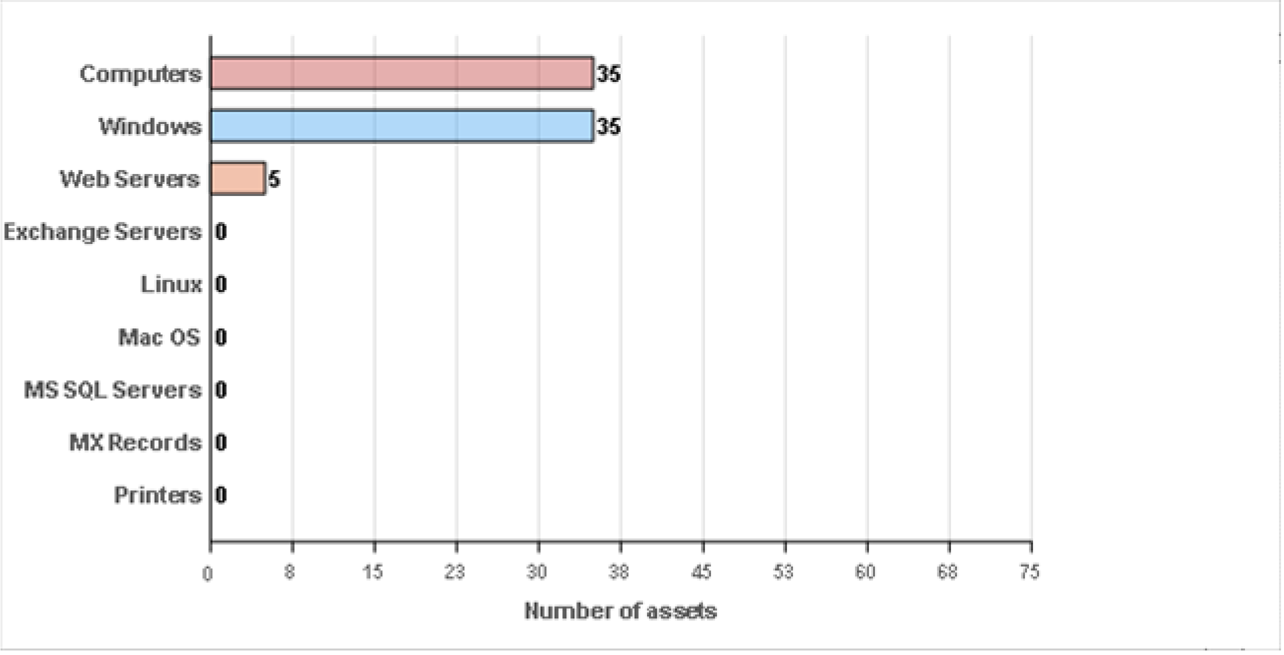
Security Issue Summary

	Automatic screen lock not turned on. (72pts each)
2448	***Current Score:*** 72pts x34 = 2448: 94.15%
	Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.
	Recommendation: Enable automatic screen lock on the specified computers.

	Account lockout disabled (77pts each)
77	***Current Score:*** 77pts x1 = 77: 2.96%
	Issue: Account lockout (disabling an account after a number of failed attempts) significantly reduces the risk of an attacker acquiring a password through a brute force attack.
	Recommendation: Enable account lockout for all users.

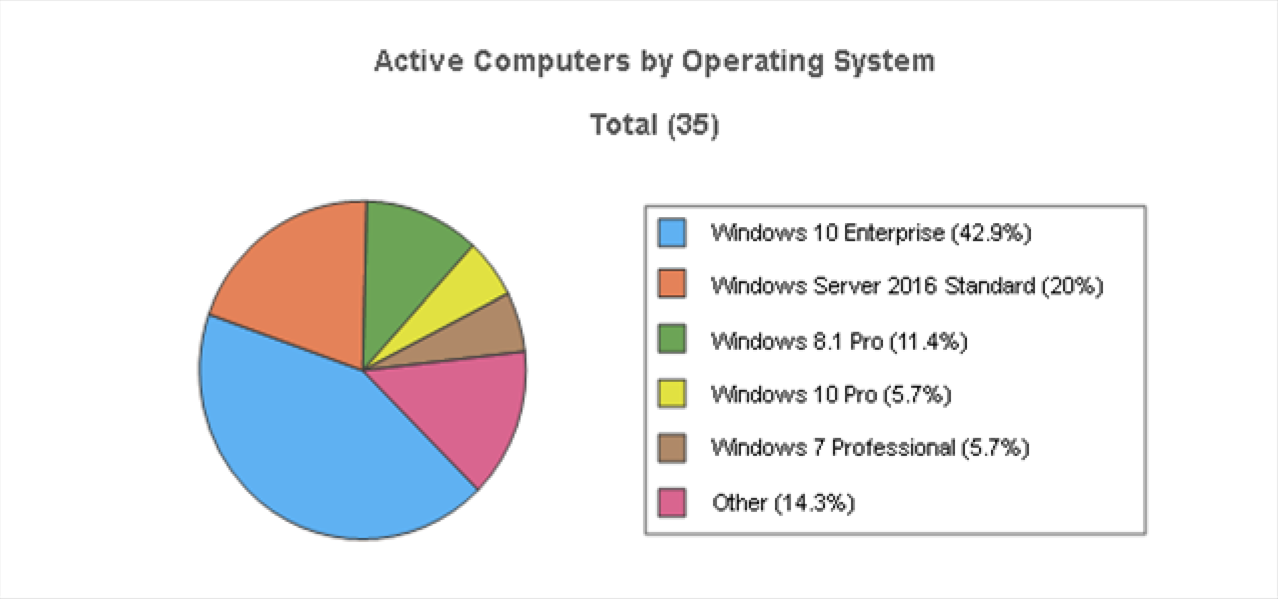
	Medium severity external vulnerabilities detected (75pts each)
75	***Current Score:*** 75pts x1 = 75: 2.88%
	Issue: Medium severity external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.
	Recommendation: Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed.

Asset Summary: Total Discovered Assets

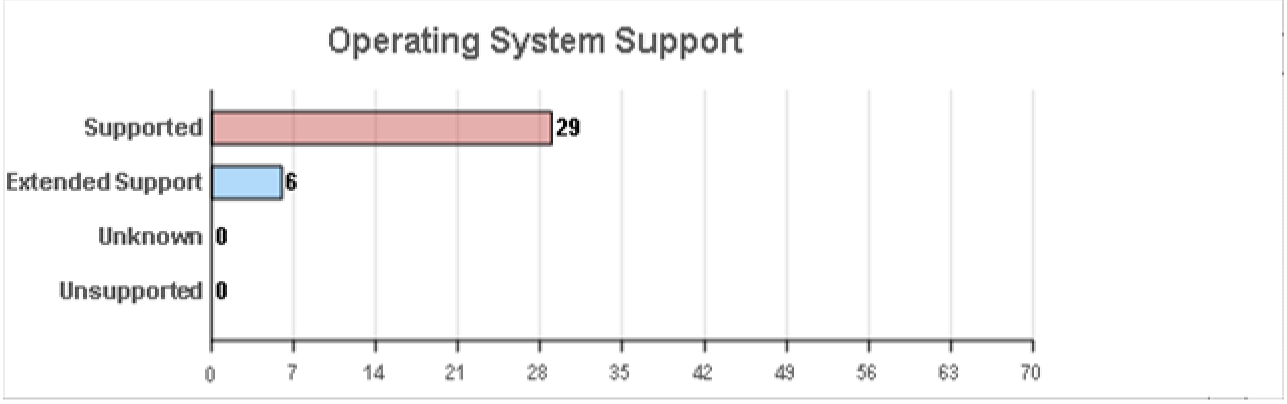


Asset Summary: Active Computers

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.

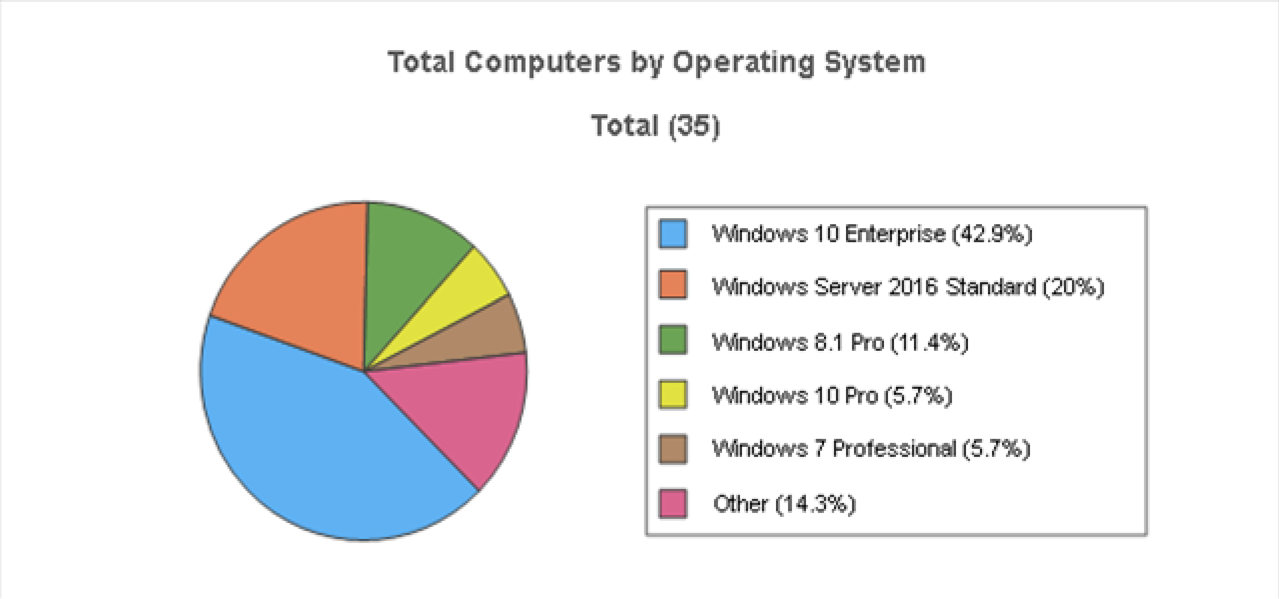


	Operating System	Total	Percent
	Top Five		
🟦	Windows 10 Enterprise	15	42.9%
🟧	Windows Server 2016 Standard	7	20%
🟩	Windows 8.1 Pro	4	11.4%
🟨	Windows 10 Pro	2	5.7%
🟫	Windows 7 Professional	2	5.7%
	Total - Top Five	**30**	**85.7%**
	Other		
🟥	Windows Server 2012 R2 Standard	2	5.7%
🟥	Windows 10 Enterprise 2015 LTSB	1	2.9%
🟥	Windows 10 Enterprise N	1	2.9%
🟥	Windows Server 2012 Standard Evaluation	1	2.9%
	Total - Other	**5**	**14.3%**
	Overall Total	**35**	**100%**


Operating System Support
Supported
29
Extended Support
6
Unknown
0
Unsupported
0
0
7
14
21
28
35
42
49
56
63
70

Asset Summary: All Computers

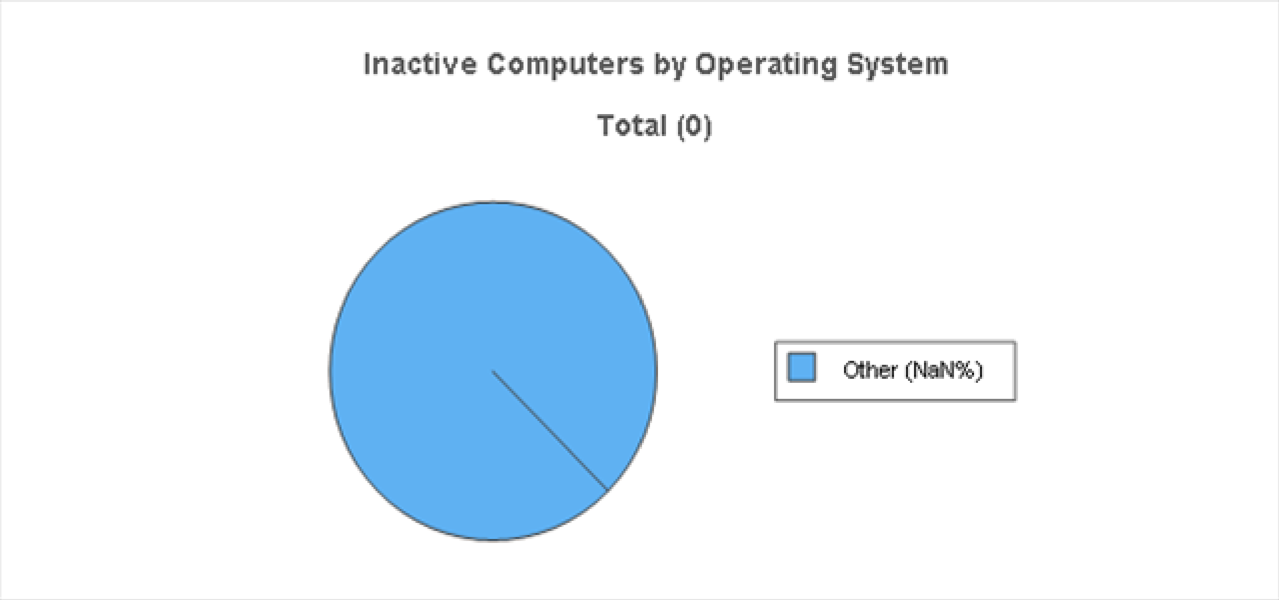
The list of all computers includes computers that may no longer be active but have entries in Active Directory (in a domain environment).



	Operating System	Total	Percent
	Top Five		
🟦	Windows 10 Enterprise	15	42.9%
🟧	Windows Server 2016 Standard	7	20%
🟩	Windows 8.1 Pro	4	11.4%
🟨	Windows 10 Pro	2	5.7%
🟫	Windows 7 Professional	2	5.7%
	Total - Top Five	**30**	**85.7%**
	Other		
🟥	Windows Server 2012 R2 Standard	2	5.7%
🟥	Windows 10 Enterprise 2015 LTSB	1	2.9%
🟥	Windows 10 Enterprise N	1	2.9%
🟥	Windows Server 2012 Standard Evaluation	1	2.9%
	Total - Other	**5**	**14.3%**
	Overall Total	**35**	**100%**

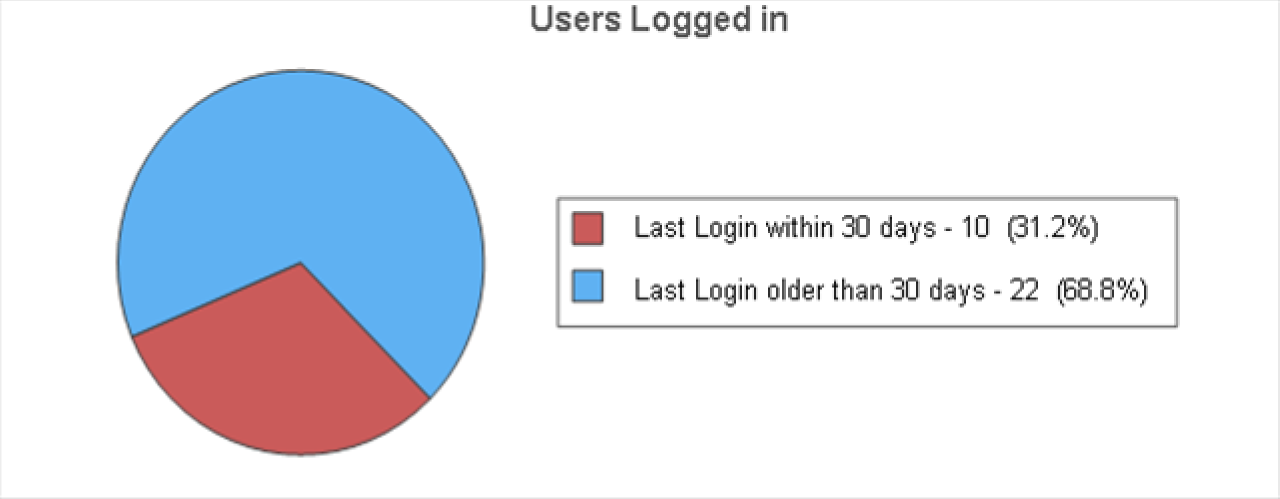
Asset Summary: Inactive Computers

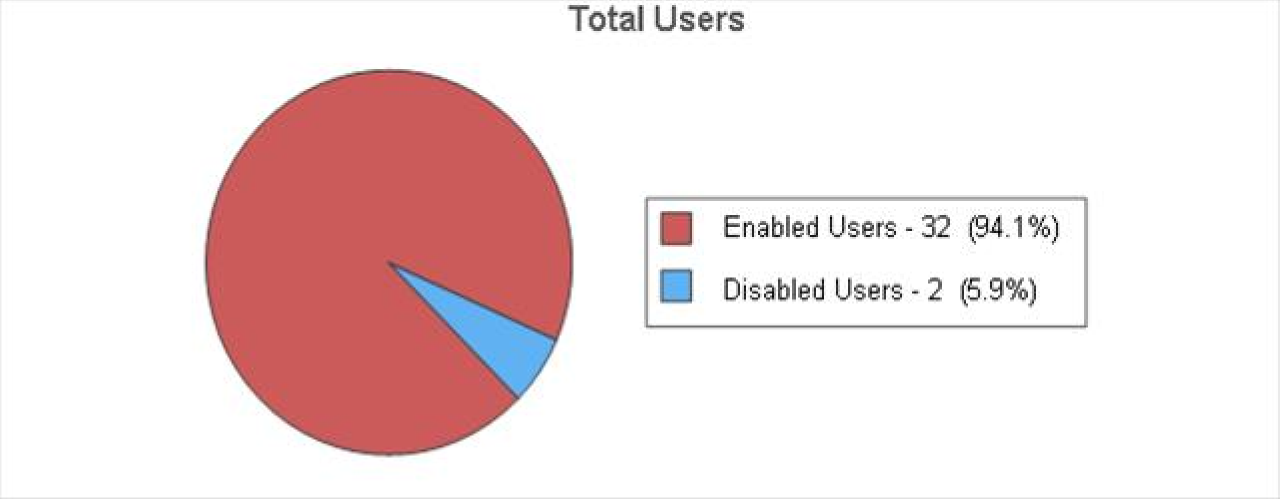
Inactive computers are computers that could not be scanned or have not checked into Active Directory in the past 30 days.

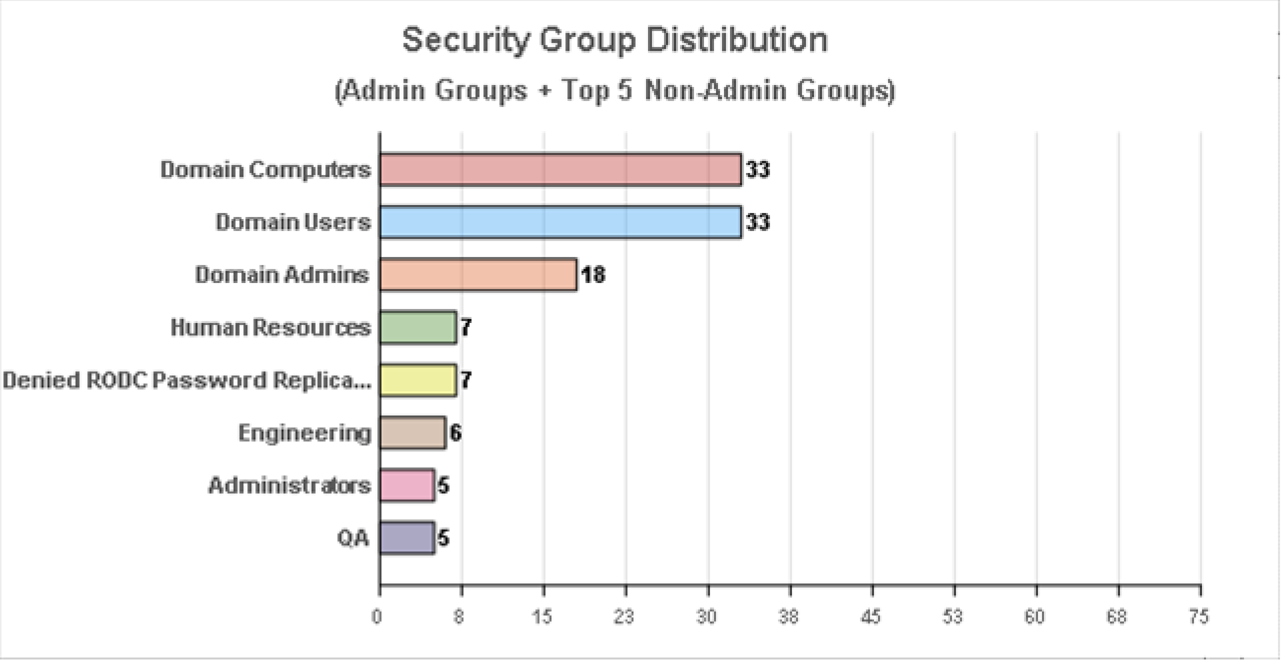


Operating System	Total	Percent
Top Five		
Total - Top Five	**0**	**NaN%**
Other		
Total - Other	**0**	**NaN%**
Overall Total	**0**	**100%**

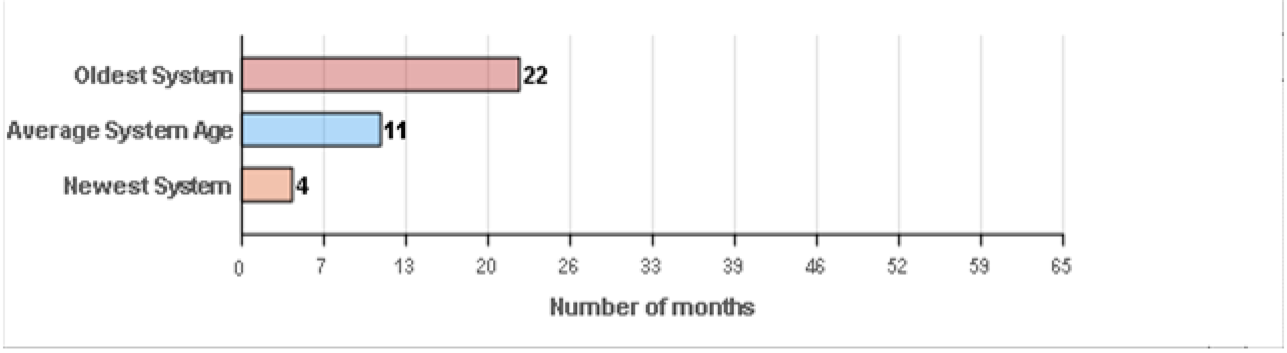
Asset Summary: Users



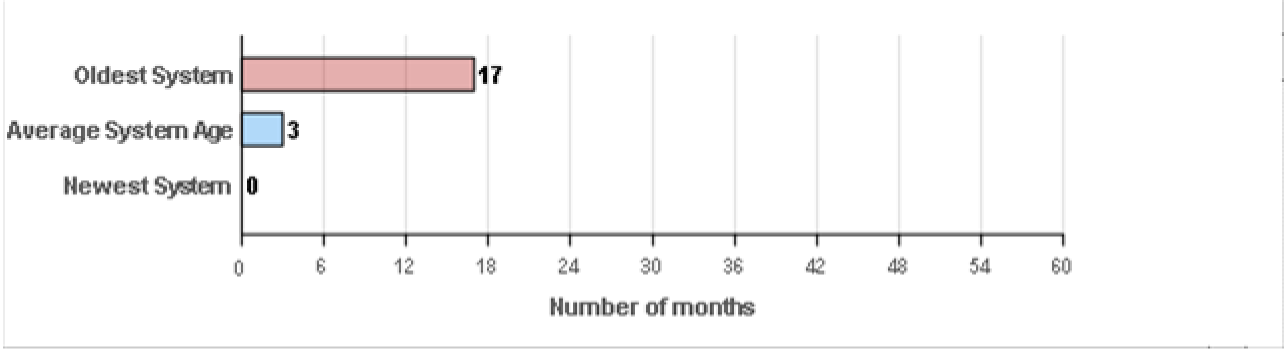



Security Group Distribution
(Admin Groups + Top 5 Non-Admin Groups)
Domain Computers
33
Domain Users
33
Domain Admins
18
Human Resources
7
Denied RODC Password Replica...
7
Engineering
6
Administrators
5
QA
5
0
8
15
23
30
38
45
53
60
68
75

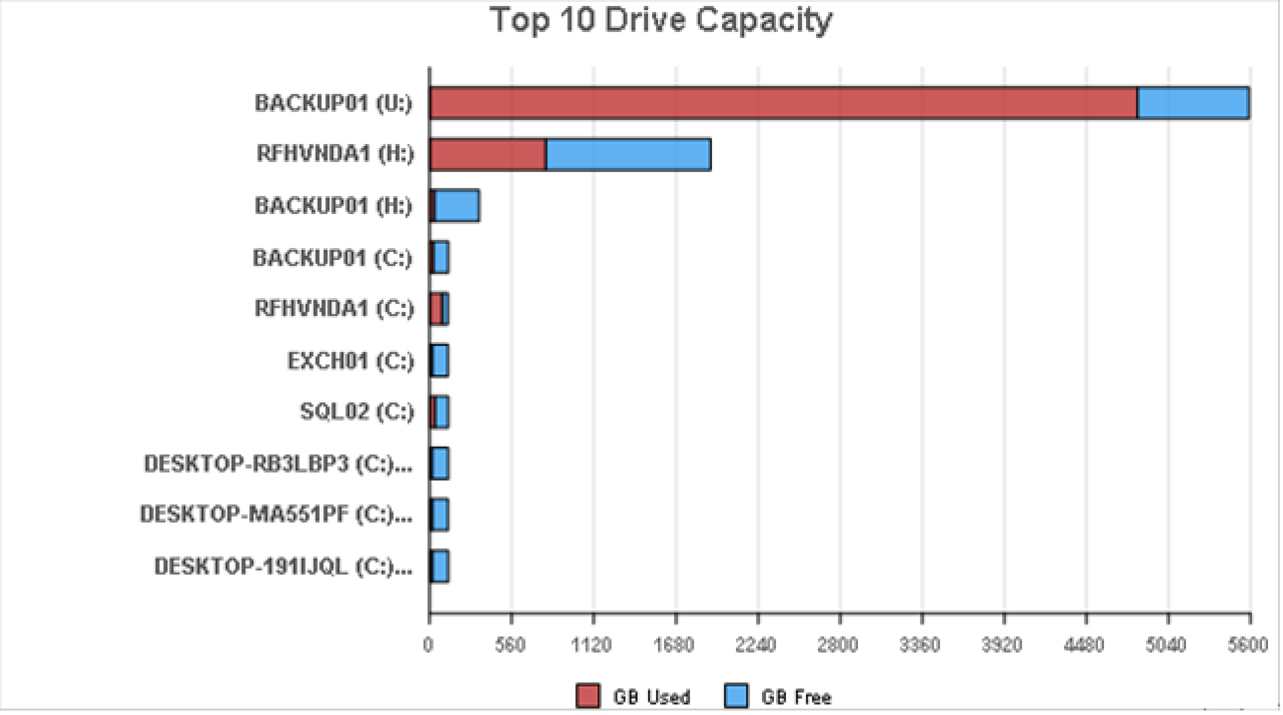
Server Aging

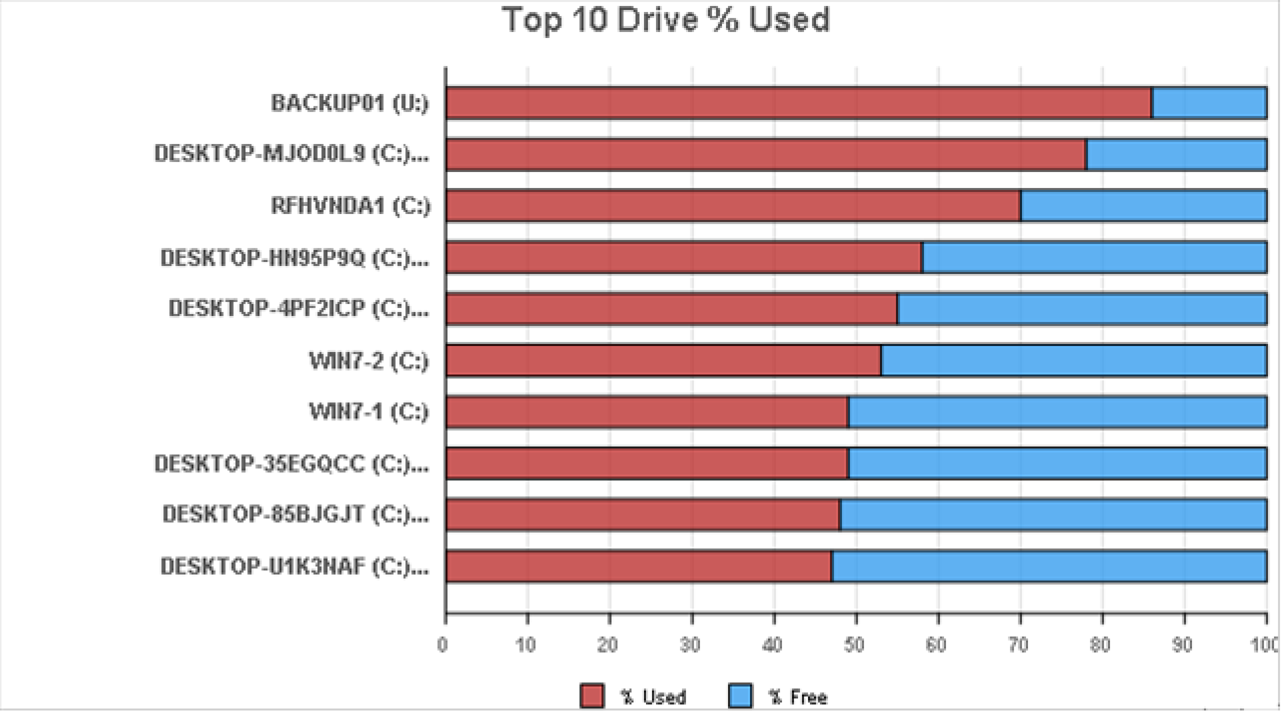


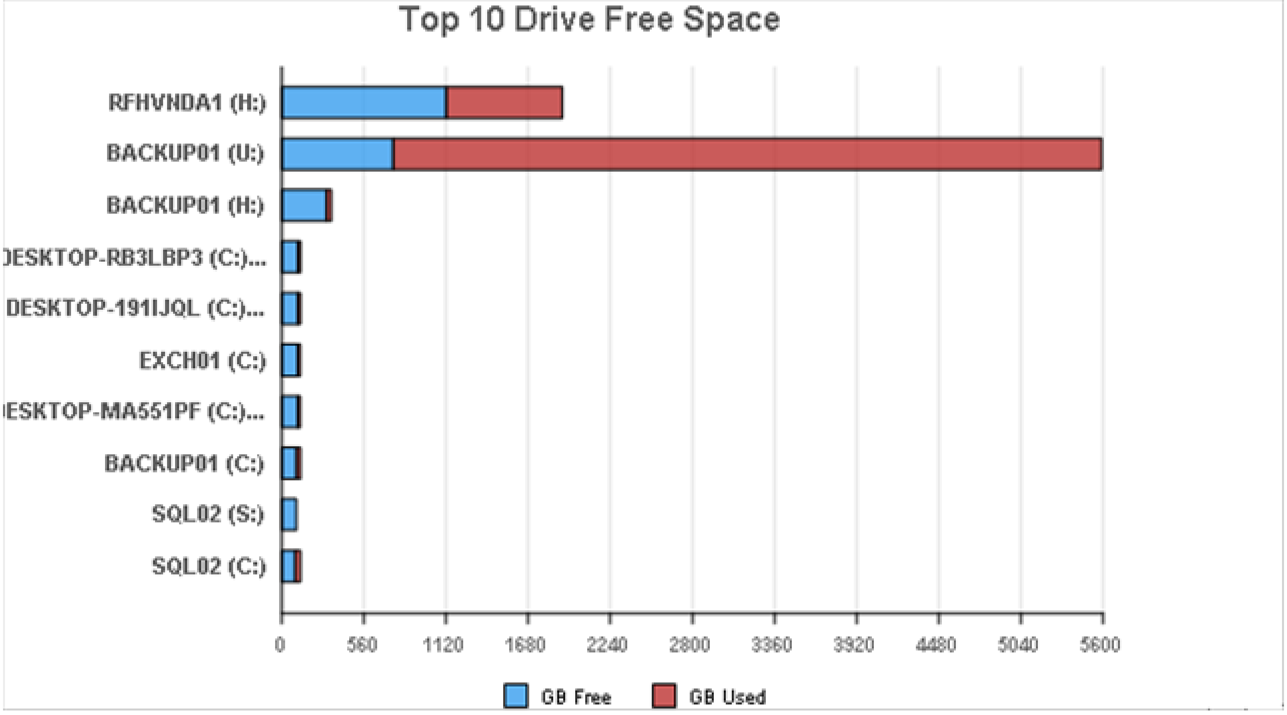
Workstation Aging



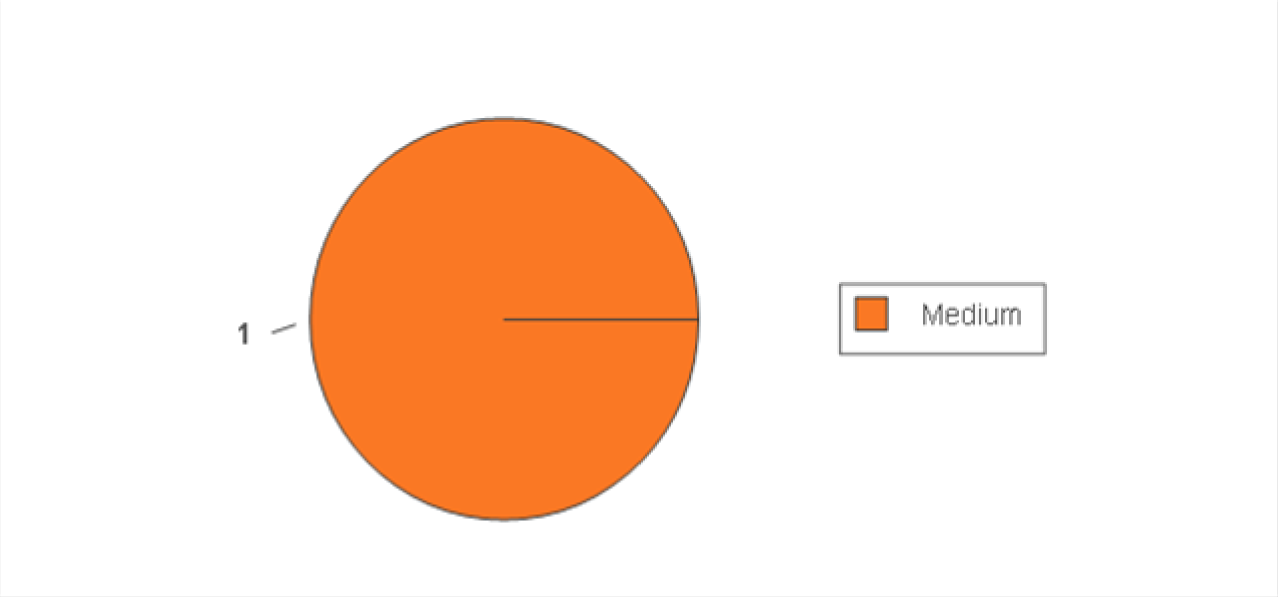
Asset Summary: Storage





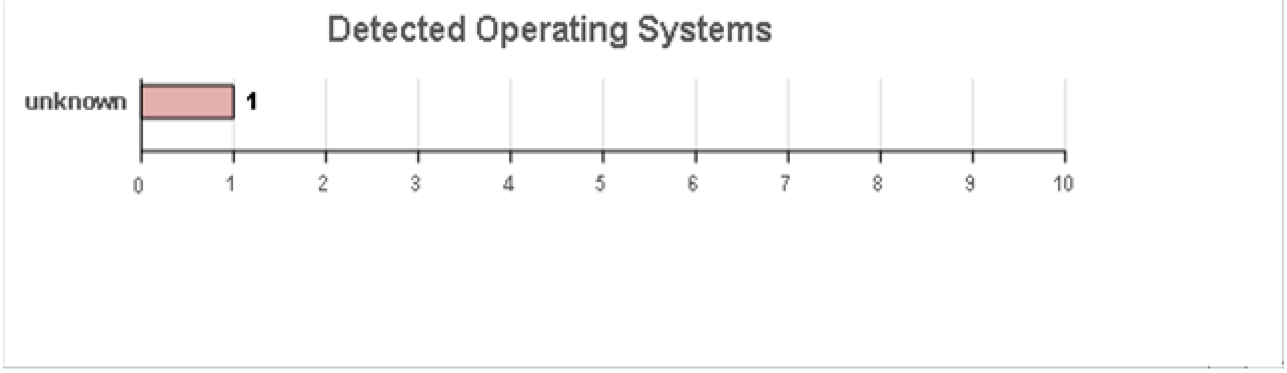

Top 10 Drive Free Space
RFHVNDA1 (H:)
BACKUP01 (U:)
BACKUP01 (H:)
DESKTOP-RB3LBP3 (C:)...
DESKTOP-191IJQL (C:)...
EXCH01 (C:)
DESKTOP-MA551PF (C:)...
BACKUP01 (C:)
SQL02 (S:)
SQL02 (C:)
0
560
1120
1680
2240
2800
3360
3920
4480
5040
5600
GB Free
GB Used

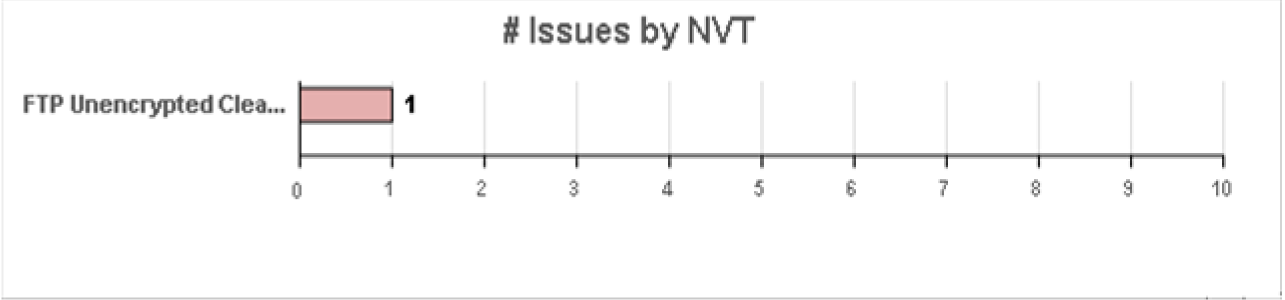
External Vulnerabilities



Host Issue Summary

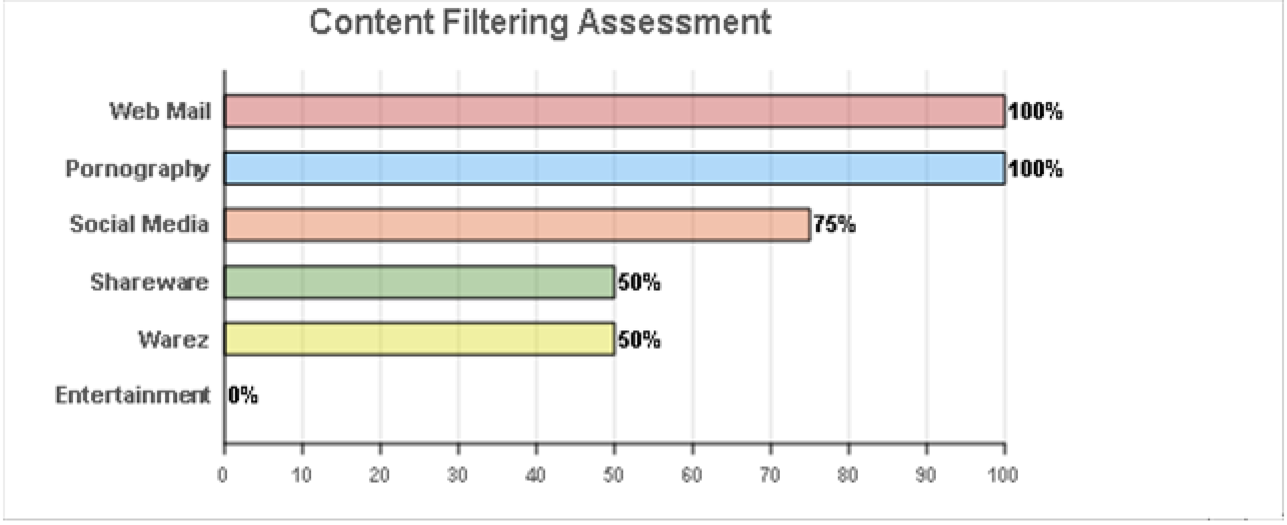
Host	Open Ports	High	Med	Low	False	Highest CVSS
97.72.92.49 (97-72-92-49-static.atl.earthlinkbusiness.net)	3	0	1	0	0	4.8
Total: 1	3	0	1	0	0	4.8



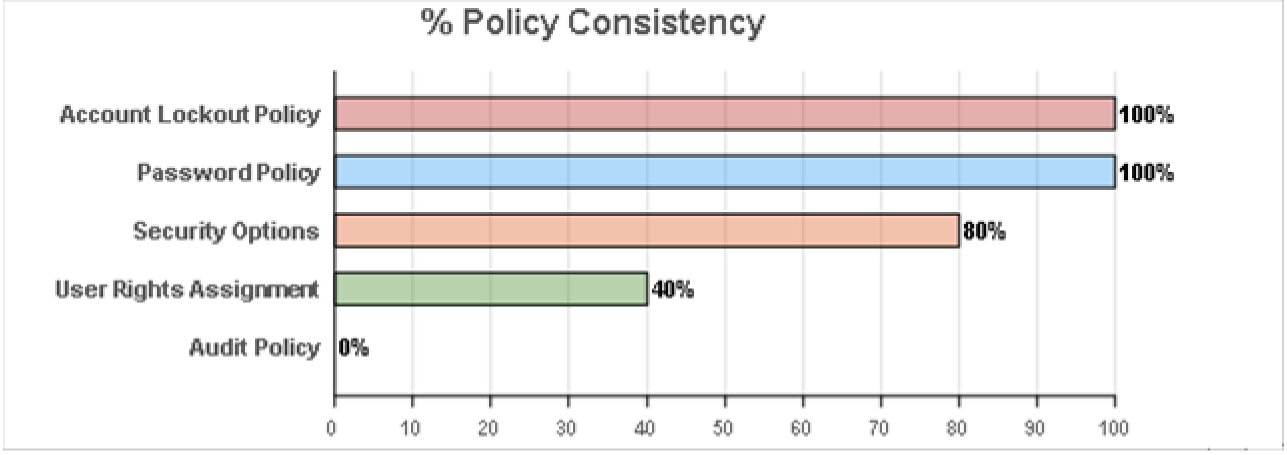


Issue	Count
FTP Unencrypted Cleartext Login	1

Unrestricted Web Content



Local Security Policy Consistency


% Policy Consistency
Account Lockout Policy
Password Policy
Security Options
User Rights Assignment
Audit Policy