Matrixforce®

Consolidated Assessment

Consolidated Risk Report

Prepared for: Matrixforce
Prepared by: Insight Partners

05/02/2024

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

Scan Date: 04/23/2024

Table of Contents

1 - Consolidated Risk Report Overview

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

The report details the scan tasks undertaken to discover security issues. In addition to the overall Consolidated Risk Score, the report also presents separate risk scores for all IT assessments (Network, Security, Exchange, SQL Server) and compliance assessments (HIPAA and PCI) performed on the network environment. 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.

2 - Consolidated Discovery Tasks

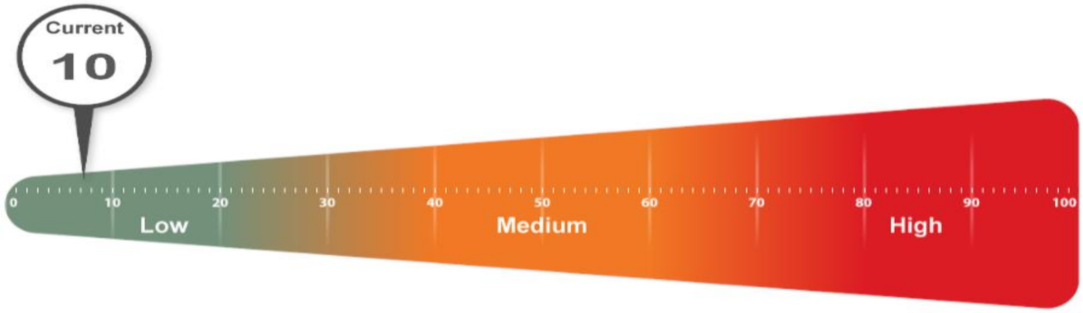
The following discovery tasks were performed.

	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).
✓	Internet Domain Analysis	Queries company domain(s) via a WHOIS lookup.
✓	Missing Security Updates	Identifies computers missing security updates.
✓	System by System Event Log Analysis	Discovers the file 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.
✗	Detect Wireless Access	Detects and determines if wireless networks are available and secured.
✓	External Security Vulnerabilities	Performs a detailed External Vulnerability Scan. Lists and

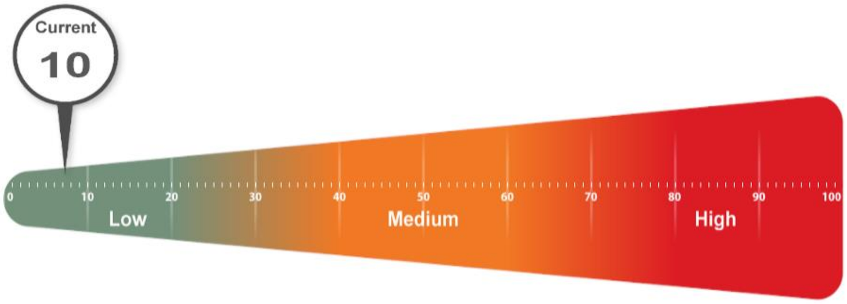
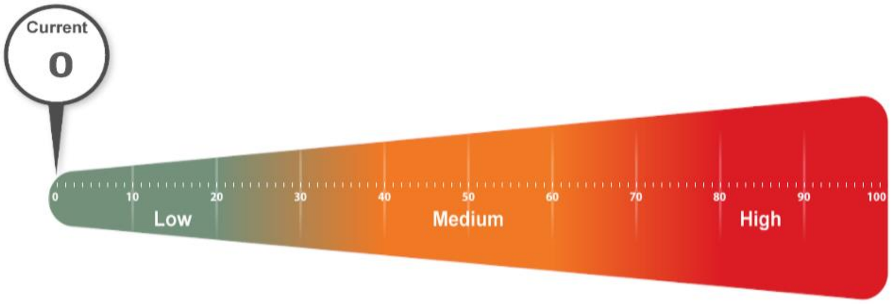
	Task	Description
		categorizes external security threats.
✓	Network Share Permissions	Documents access to file system shares.
✓	Domain Security Policy	Documents domain computer and domain controller security policies.
✓	Local Security Policy	Documents and assesses consistency of local security policies.

3 - Consolidated 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.

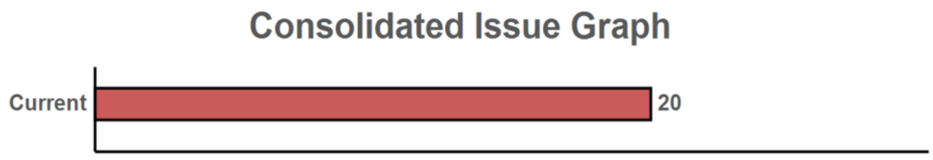


Several critical issues were identified. Identified issues should be investigated and addressed according to the Consolidated Risk Report.

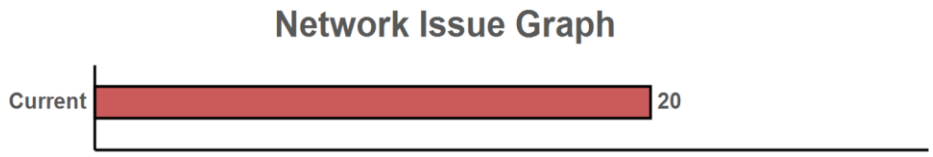
Module	Risk Score
Network	
Security	

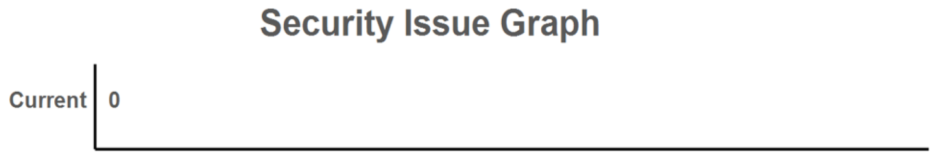
4 - Consolidated Issue Graph

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





5 - Consolidated Issue Summary

5.1 - Network Issue Summary

	Insecure listening ports (10 pts each)
20	***Current Score:*** 10 pts x 2 = 20: 100%
	Issue: Computers are 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 often 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. See Listening Ports sheets in Excel Export for details.

	Operating system in Extended Support ~~*(20 pts each)*~~
0	***Current Score:*** ~~20 pts x 0 = 0: 0%~~
	Issue: Computers are using an operating system that is in Extended Support. 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.~~
	Exception Explanation: False positive, Servers are 2019 and above. Workstations running windows 10/11.

	Inactive computers ~~*(15 pts each)*~~
0	***Current Score:*** ~~15 pts x 0 = 0: 0%~~
	Issue: Computers have 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, logged into by authorized users, or powered on.~~
	Exception Explanation: These accounts in question are secondary administrative accounts subject to regular security checks and password changes.

5.2 - Security Issue Summary

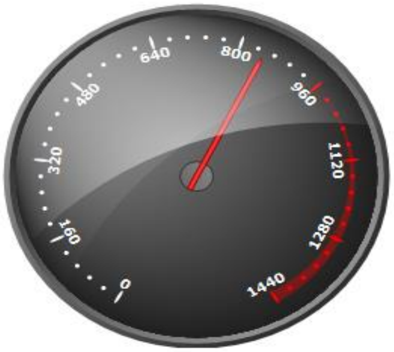
	Compromised Passwords found on the Dark Web ~~*(100 pts each)*~~
0	***Current Score:*** ~~100 pts x 0 = 0: 0%~~
	Issue: A scan of the Dark Web revealed one or more compromised passwords from your domain. The most recent compromise occurred in 2024.
	Recommendation: ~~Ensure the compromised passwords are no longer in use. We recommend having all users reset their password as the extent of the compromise is difficult~~

	~~to assess. Only the first 5 per domain are listed here.~~
	Exception Explanation: These passwords have all been changed as a part of routine operations.

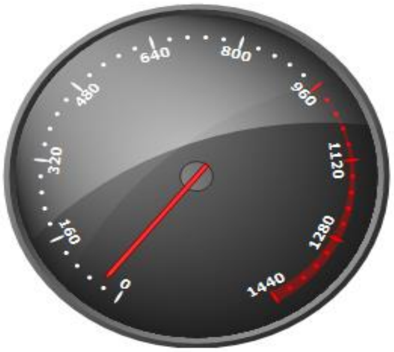
	Automatic screen lock not turned on *~~(72 pts each)~~*
0	***Current Score:*** ~~72 pts x 0 = 0: 0%~~
	Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.
	Recommendation: ~~Enable automatic screen lock on the specified computers.~~
	Exception Explanation: Screen lockout is configured through a different mechanism

6 - Internet Speed Test Results

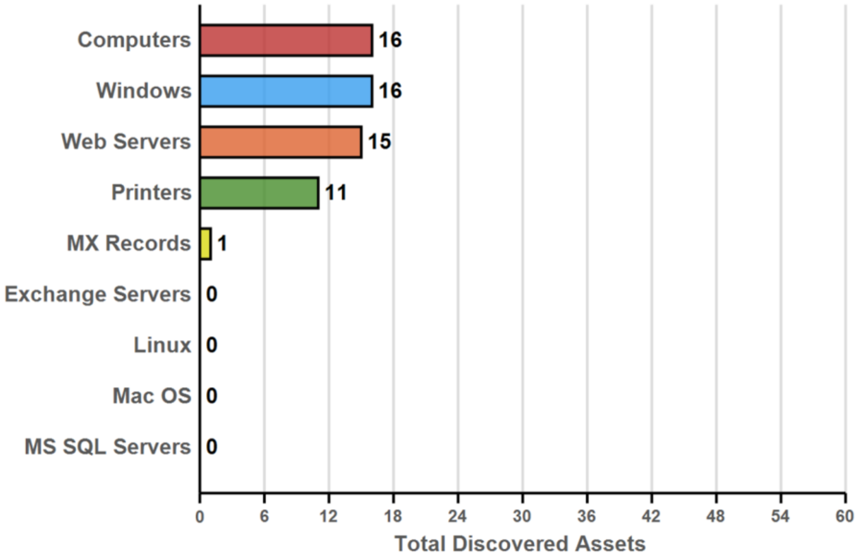
Download Speed: **845.6 Mb/s**



Upload Speed: **41.1 Mb/s**

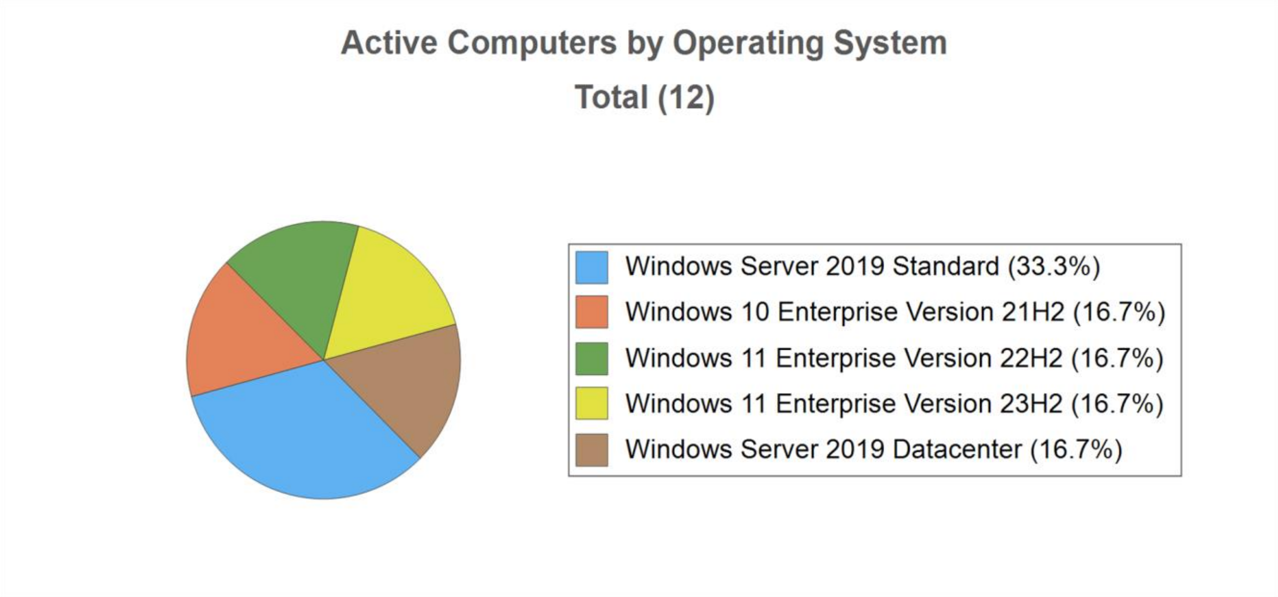


7 - Asset Summary: Total Discovered Assets

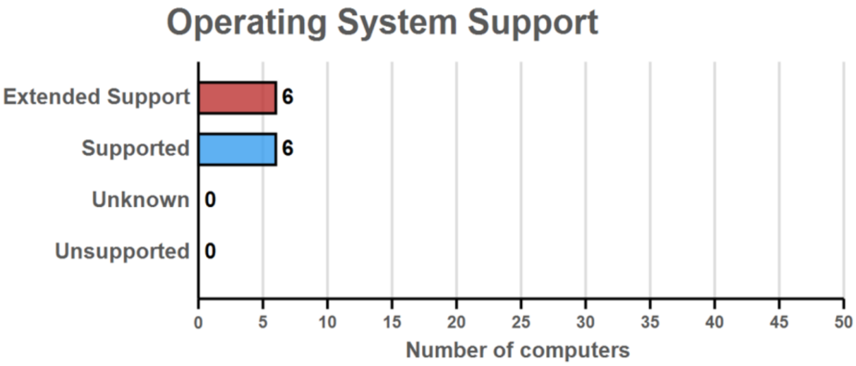


8 - Asset Summary: Active Computers

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.

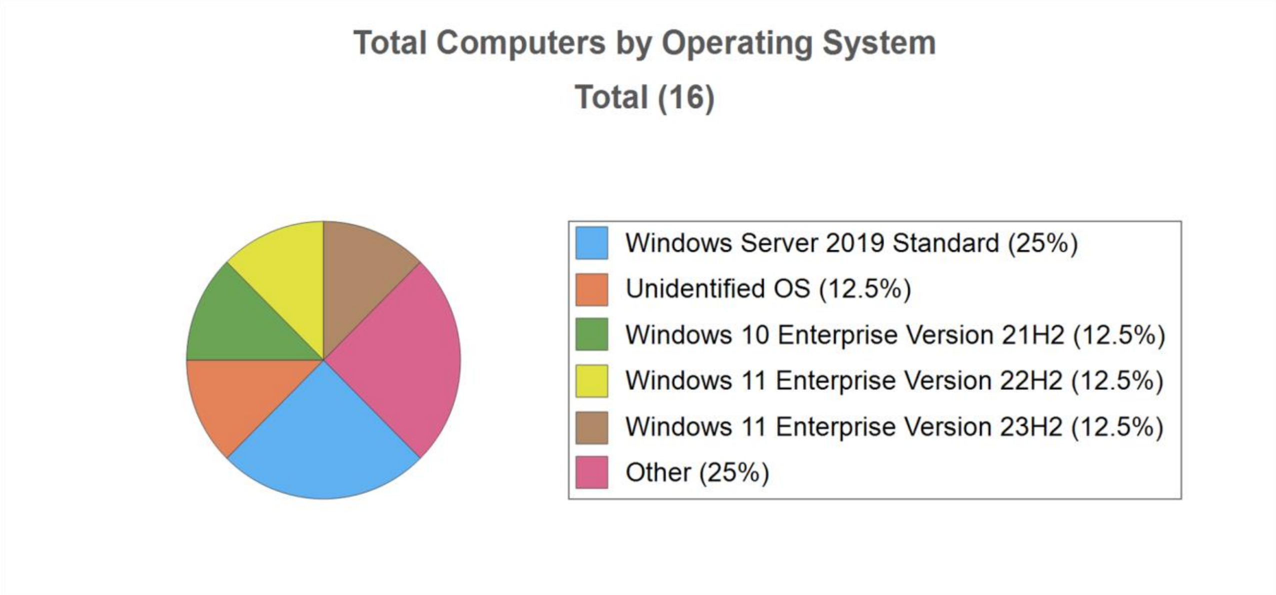


	Operating System	Total	Percent
	Top Five		
🟦	Windows Server 2019 Standard	4	33.3%
🟧	Windows 10 Enterprise Version 21H2	2	16.7%
🟩	Windows 11 Enterprise Version 22H2	2	16.7%
🟨	Windows 11 Enterprise Version 23H2	2	16.7%
🟫	Windows Server 2019 Datacenter	2	16.7%
	Total - Top Five	**12**	**100%**
	Other		
	Total - Other	**0**	**0%**
	Overall Total	**12**	**100%**


Operating System Support
Extended Support
6
Supported
6
Unknown
0
Unsupported
0
0
5
10
15
20
25
30
35
40
45
50
Number of computers

9 - Asset Summary: All Computers

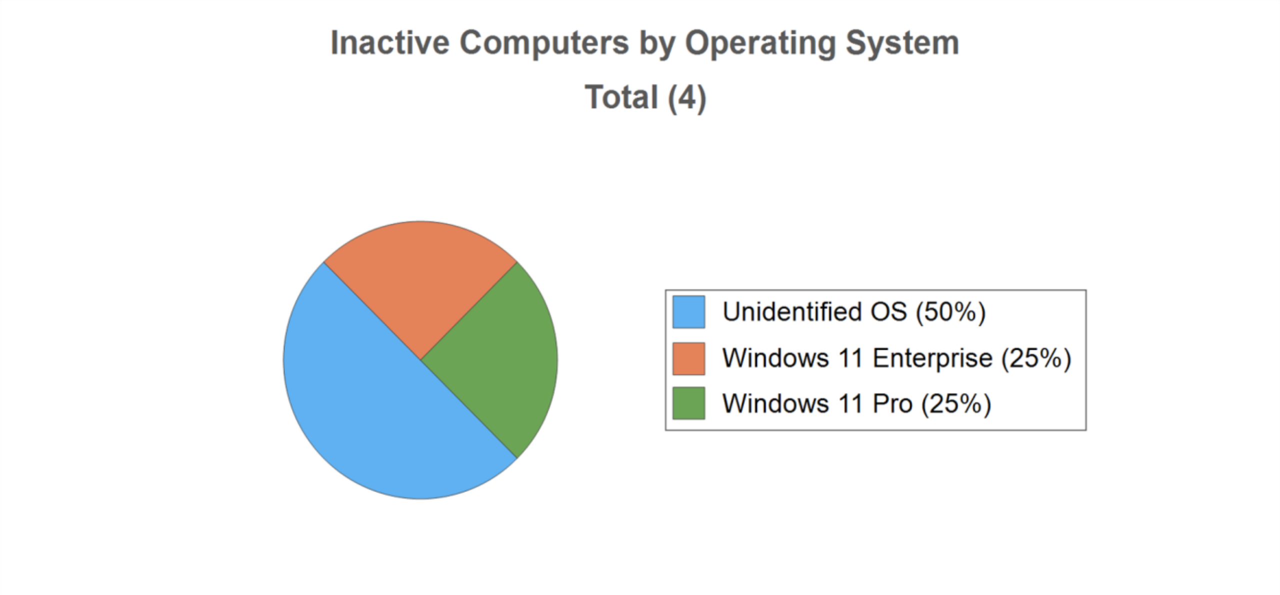
The list of all computers includes computers that may no longer be active but have entries in Active Directory (in a domain environment).



	Operating System	Total	Percent
	Top Five		
🟦	Windows Server 2019 Standard	4	25%
🟧	Unidentified OS	2	12.5%
🟩	Windows 10 Enterprise Version 21H2	2	12.5%
🟨	Windows 11 Enterprise Version 22H2	2	12.5%
🟫	Windows 11 Enterprise Version 23H2	2	12.5%
	Total - Top Five	**12**	**75%**
	Other		
🟥	Windows Server 2019 Datacenter	2	12.5%
🟥	Windows 11 Enterprise	1	6.2%
🟥	Windows 11 Pro	1	6.2%
	Total - Other	**4**	**25%**
	Overall Total	**16**	**100%**

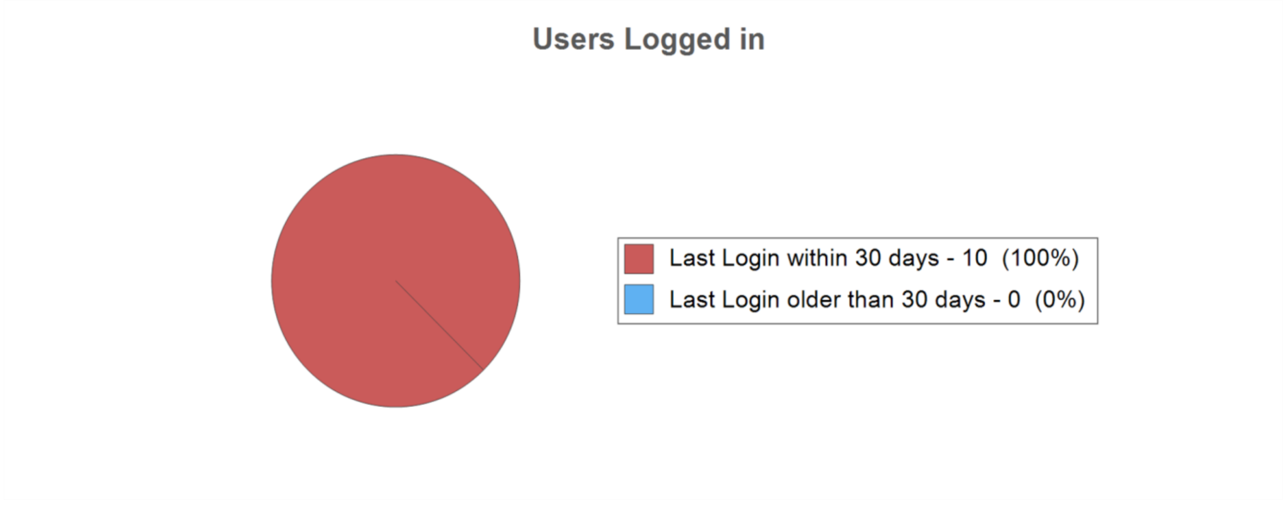
10 - Asset Summary: Inactive Computers

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

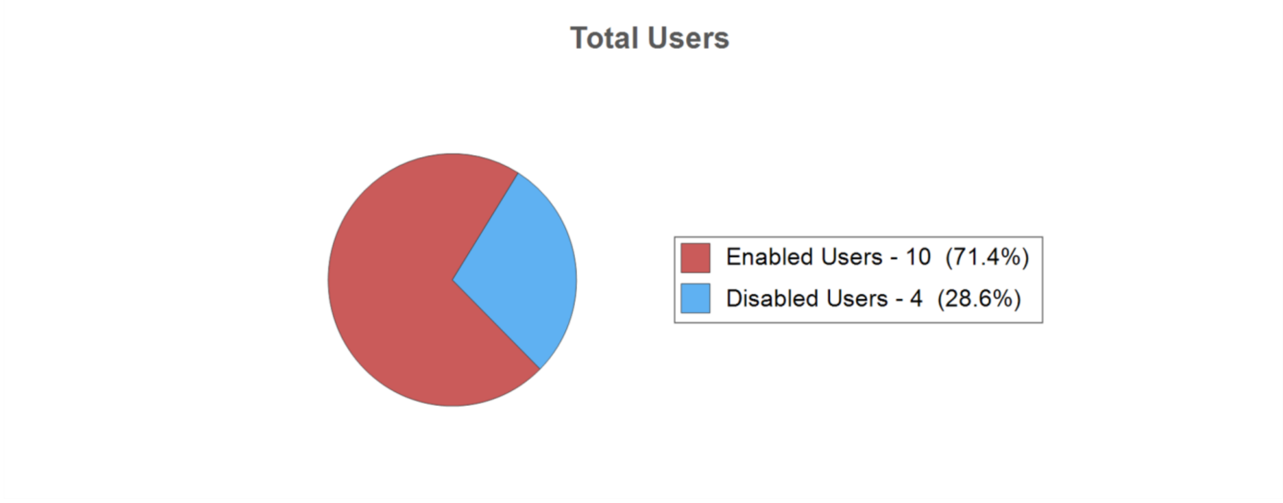


	Operating System	Total	Percent
	Top Five		
🟦	Unidentified OS	2	50%
🟧	Windows 11 Enterprise	1	25%
🟩	Windows 11 Pro	1	25%
	Total - Top Five	**4**	**100%**
	Other		
	Total - Other	**0**	**0%**
	Overall Total	**4**	**100%**

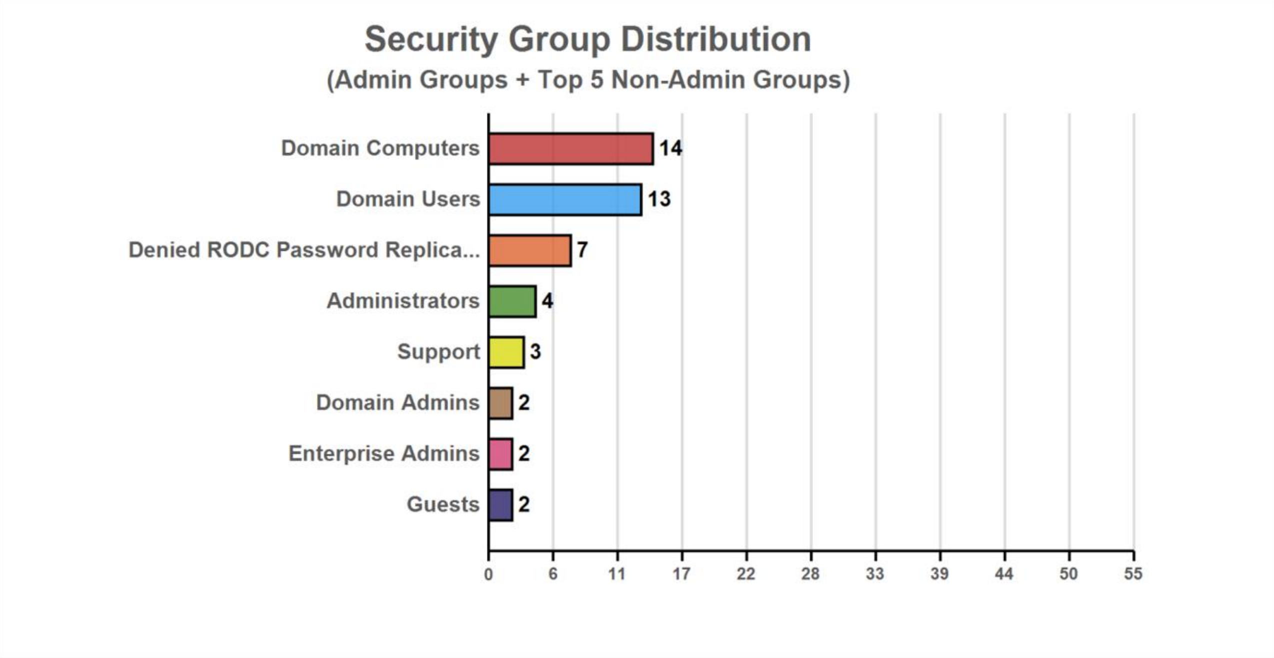
11 - Asset Summary: Users



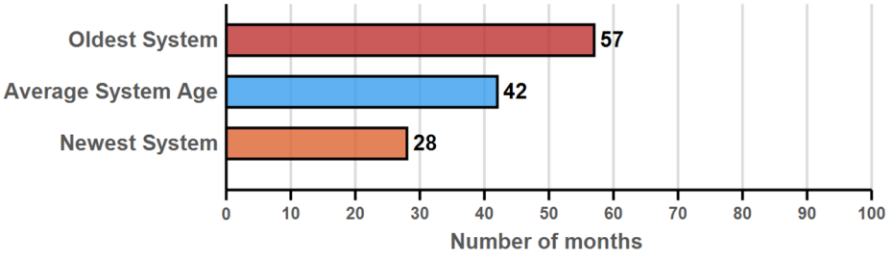
Users Logged in



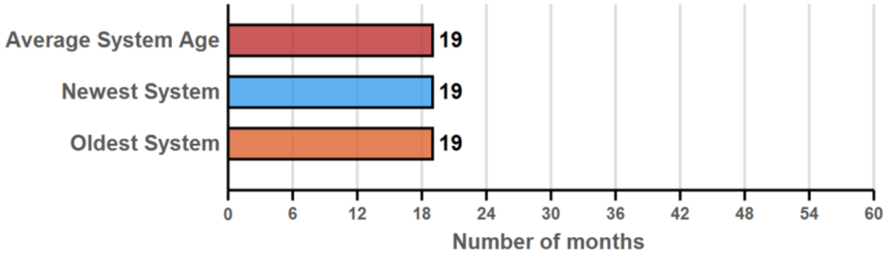
Total Users


Security Group Distribution
(Admin Groups + Top 5 Non-Admin Groups)
Domain Computers
14
Domain Users
13
Denied RODC Password Replica...
7
Administrators
4
Support
3
Domain Admins
2
Enterprise Admins
2
Guests
2
0
6
11
17
22
28
33
39
44
50
55

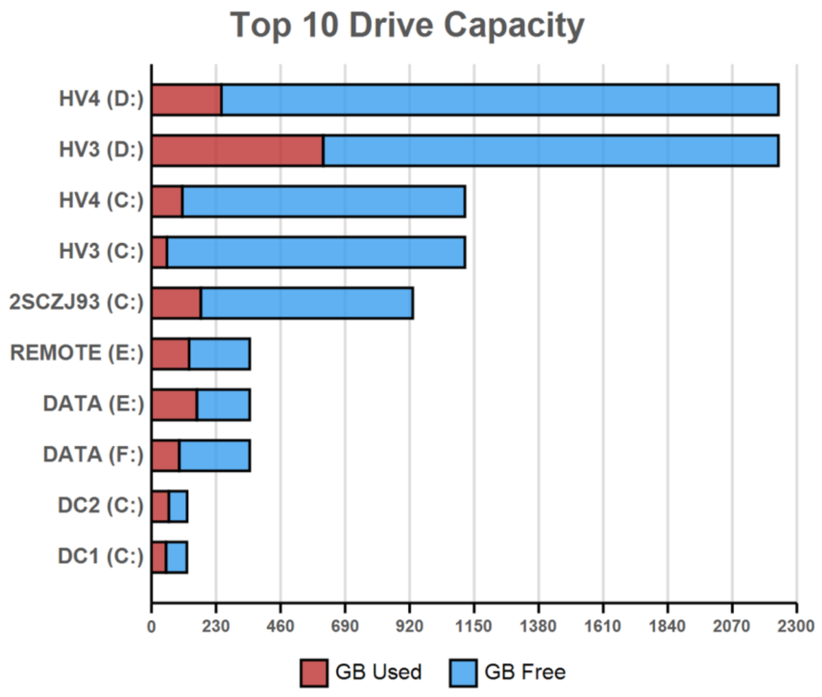
12 - Server Aging

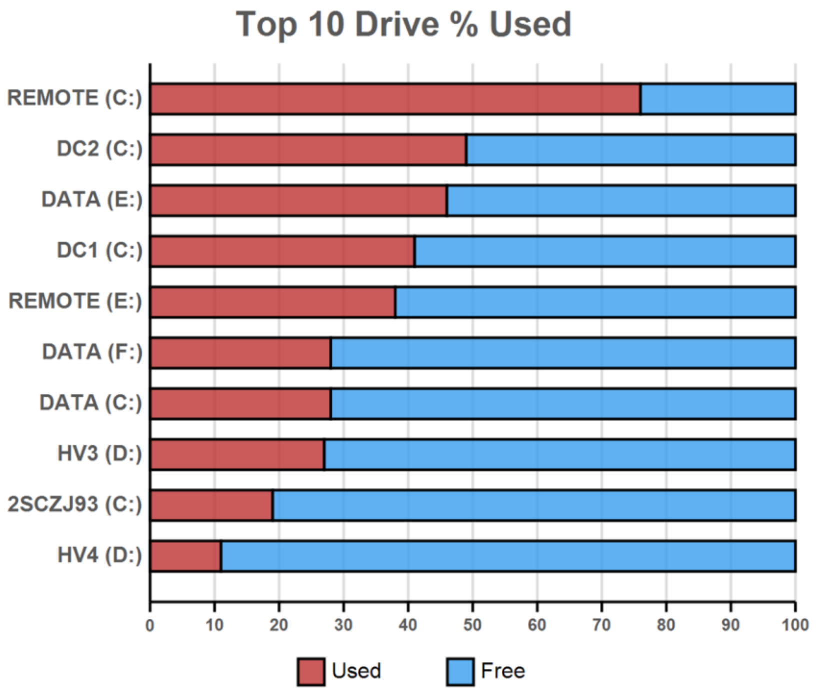


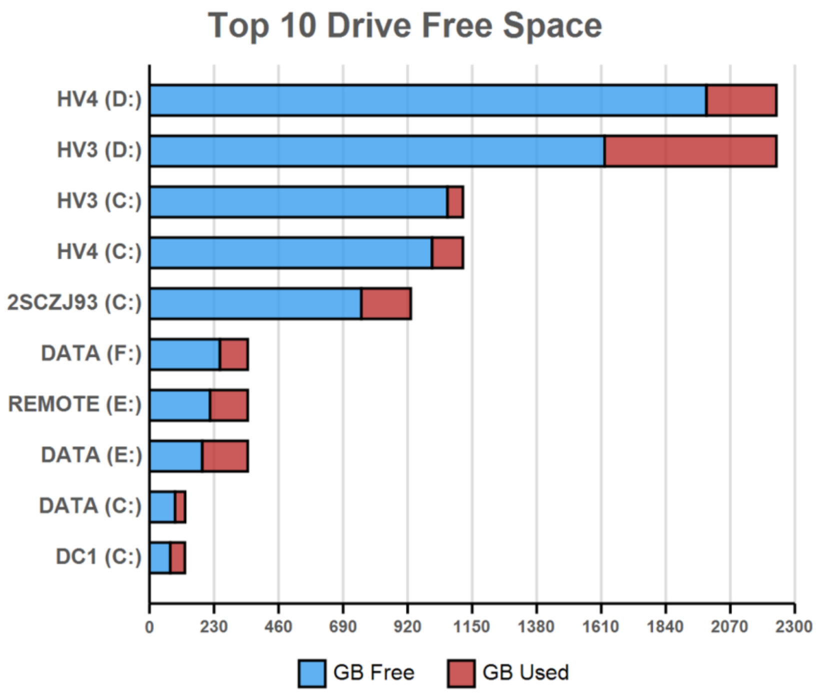
13 - Workstation Aging



14 - Asset Summary: Storage



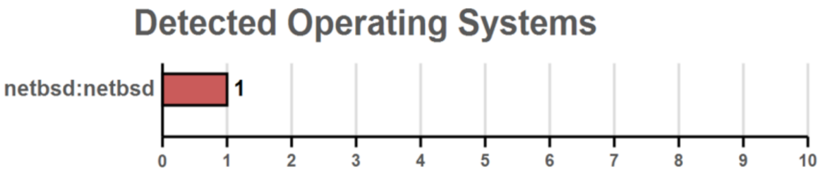



Top 10 Drive Free Space
HV4 (D:)
HV3 (D:)
HV3 (C:)
HV4 (C:)
2SCZJ93 (C:)
DATA (F:)
REMOTE (E:)
DATA (E:)
DATA (C:)
DC1 (C:)
0
230
460
690
920
1150
1380
1610
1840
2070
2300
GB Free
GB Used

15 - External Vulnerabilities

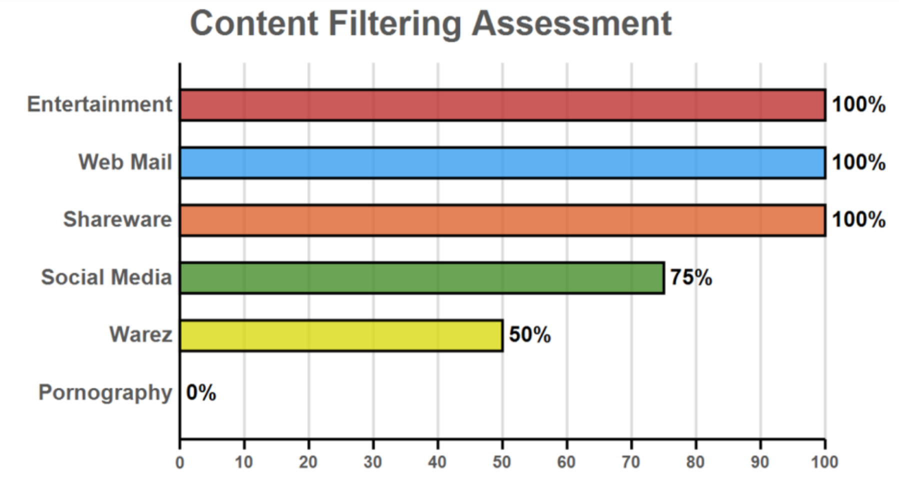
Host Issue Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
[redacted]	0	0	0	0	0	0.0
Total: 1	0	0	0	0	0	0.0

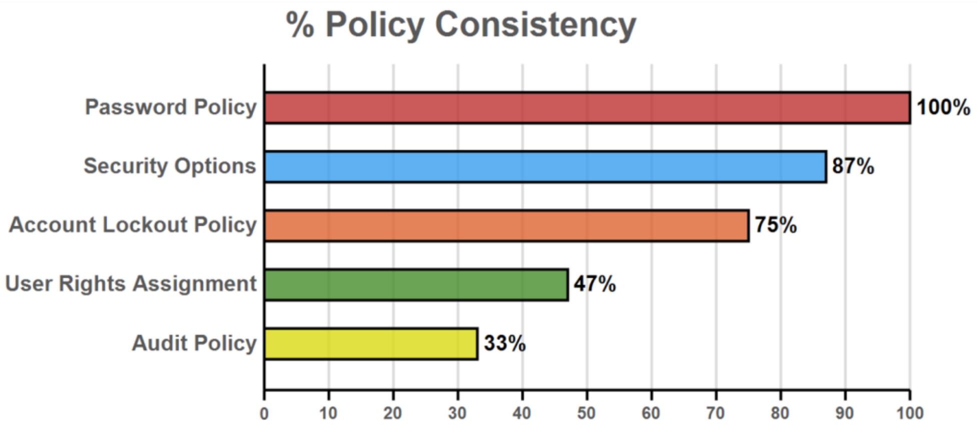


16 - Unrestricted Web Content

The assessment examined whether computers employ web content filters. The percentages below represent the number of potentially unsafe websites that are unrestricted by content category. A higher score indicates that users have unrestricted access to multiple websites that may pose a security threat. *Note that this data does not reflect the actual browsing activity of employees or users on the network.



17 - Local Security Policy Consistency



18 - Dark Web Scan Summary

The following results were retrieved using a preliminary scan of the Dark Web using ID Agent (www.idagent.com).

Only the first 5 per domain are listed here.

Email	Password/SHA1	Compromise Date	Source
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]