Consolidated Assessment

Consolidated Risk Report

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: 07/08/2025

Prepared for: TEL5

Prepared by: TEL5

07/08/2025

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

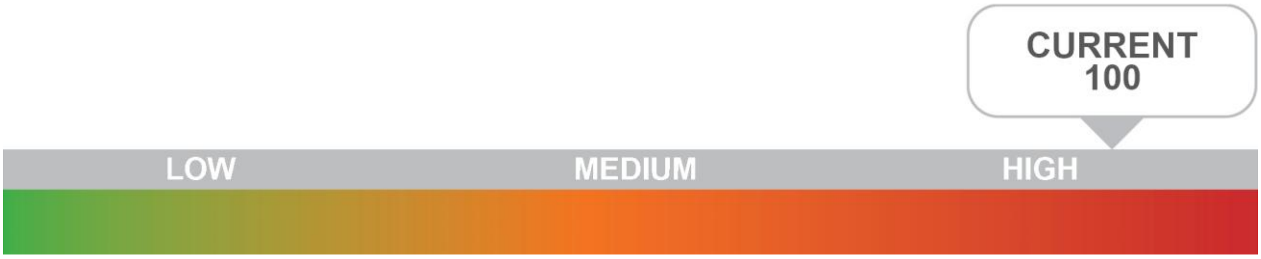
The following discovery tasks were performed.

	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.

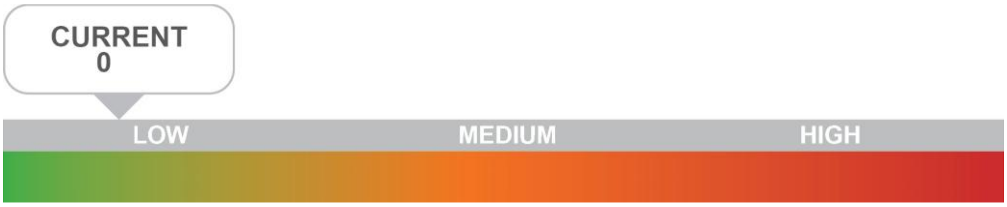
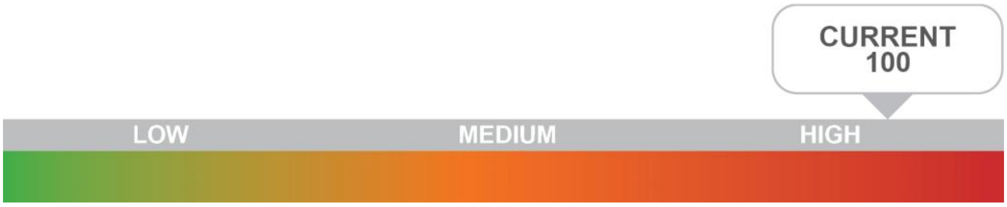
	TASK	DESCRIPTION
Security		
✓	Detect System Protocol Leakage	Detects outbound protocols that should not be allowed.
✓	Detect Unrestricted Protocols	Detects system controls for protocols that should be allowed but restricted.
✓	Detect User Controls	Determines if controls are in place for user web browsing.
✓	Detect Wireless Access	Detects and determines if wireless networks are available and secured.
✗	External Security Vulnerabilities	Performs a detailed External Vulnerability Scan. Lists and 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.

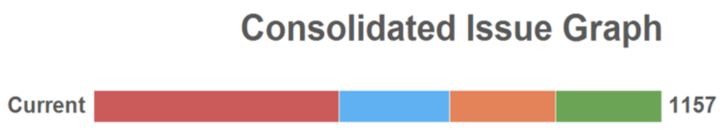


Several critical issues were identified. Identified issues should be investigated and addressed according to the Consolidated Risk Report.

MODULE	RISK SCORE
Network	
Security	

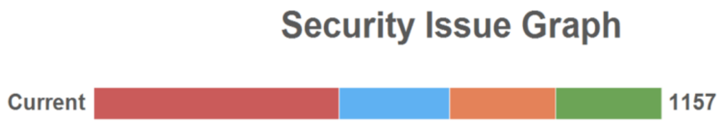
4 - Consolidated Issue Graph

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 (%)

Network Issue Graph
Current
0



5 - Consolidated Issue Summary

5.1 - Network Issue Summary

No issues detected.

5.2 - Security Issue Summary

500 Compromised Passwords found on the Dark Web (100 pts each)

Current Score: 100 pts x 5 = 500: 43.22%

Issue: A scan of the Dark Web revealed one or more compromised passwords from your domain. The most recent compromise occurred in 2025.

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.

225 Passwords less than 8 characters allowed (75 pts each)

Current Score: 75 pts x 3 = 225: 19.45%

Issue: Passwords are not required to be 8 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.

Recommendation: Enable enforcement of password length to 8 or more characters.

216 Password history not remembered for at least six passwords (72 pts each)

Current Score: 72 pts x 3 = 216: 18.67%

Issue: Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.

Recommendation: Increase password history to remember at least six passwords.

216 Automatic screen lock not turned on (72 pts each)

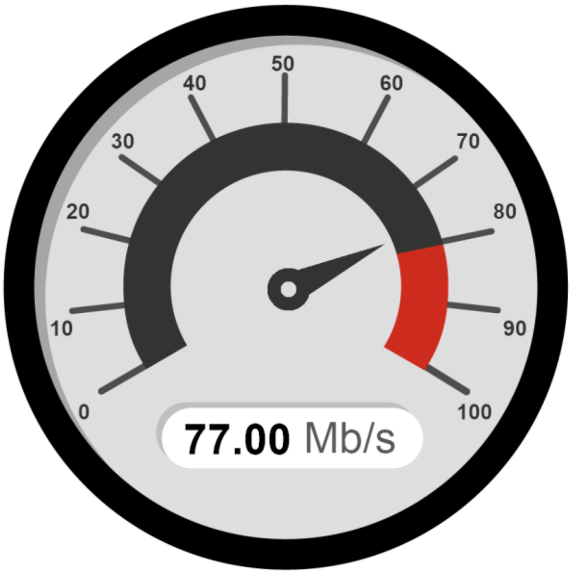
Current Score: 72 pts x 3 = 216: 18.67%

Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.

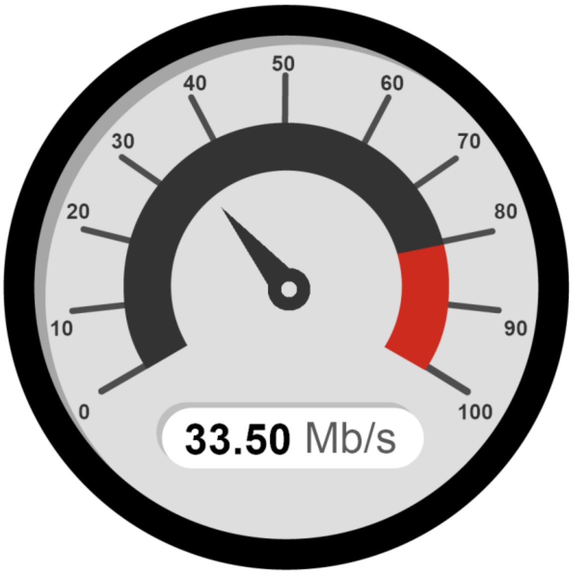
Recommendation: Enable automatic screen lock on the specified computers.

6 - Internet Speed Test Results

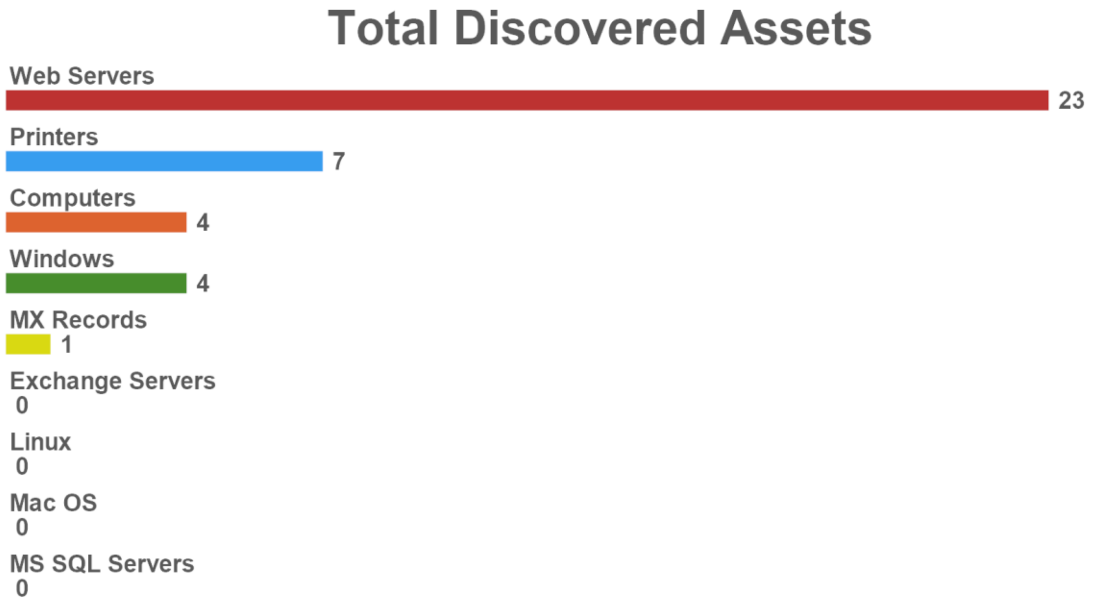
Download Speed: **77.0 Mb/s**



Upload Speed: **33.5 Mb/s**

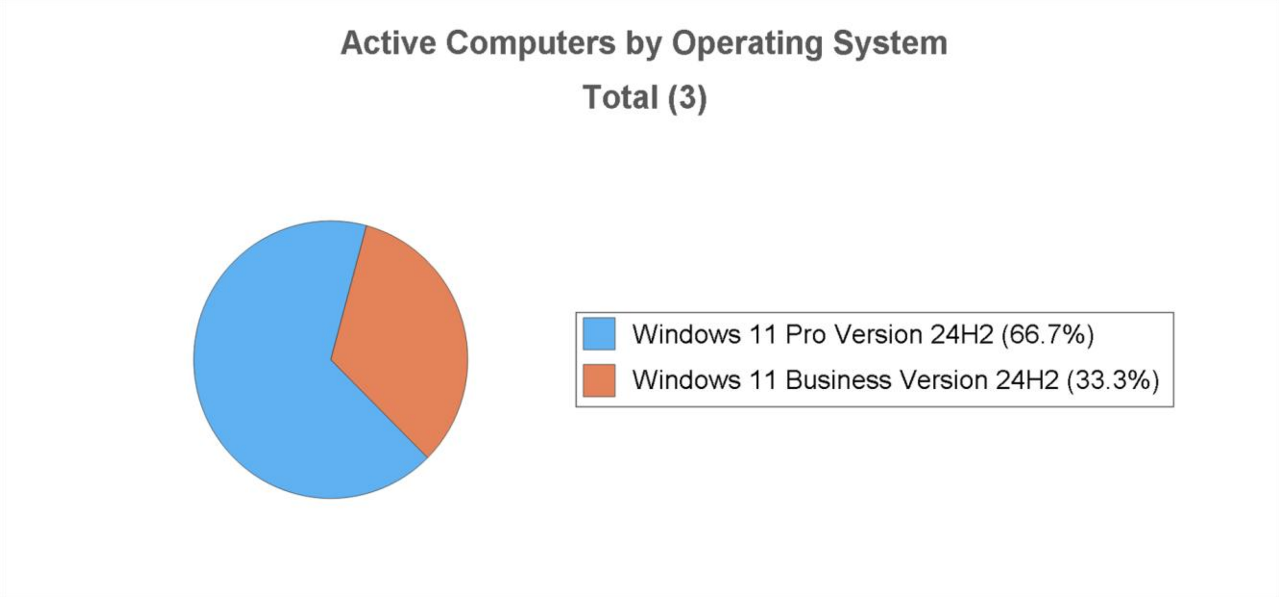


7 - Asset Summary: Total Discovered Assets



8 - Asset Summary: Active Computers

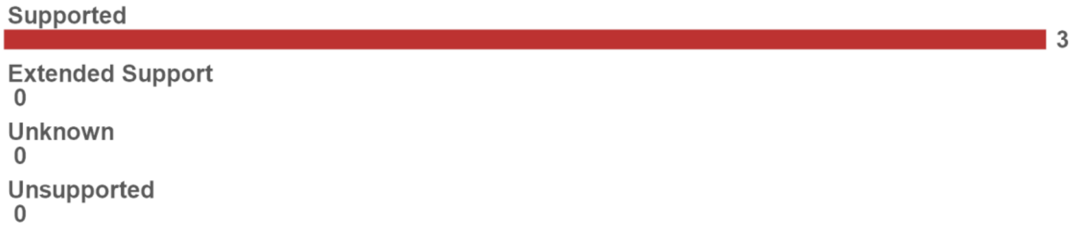
Active Computers are defined as computers that were either actively responding at the time of the scan or have checked in with Active Directory or Microsoft Entra ID within the past 30 days.



	OPERATING SYSTEM (TOP FIVE)	TOTAL	PERCENT
🟦	Windows 11 Pro Version 24H2	2	66.7%
🟧	Windows 11 Business Version 24H2	1	33.3%
	Total - Top Five	**3**	**100%**

OPERATING SYSTEM (OTHER)	TOTAL	PERCENT
Total - Other	**0**	**0%**
OVERALL TOTAL	3	100%

Operating System Support

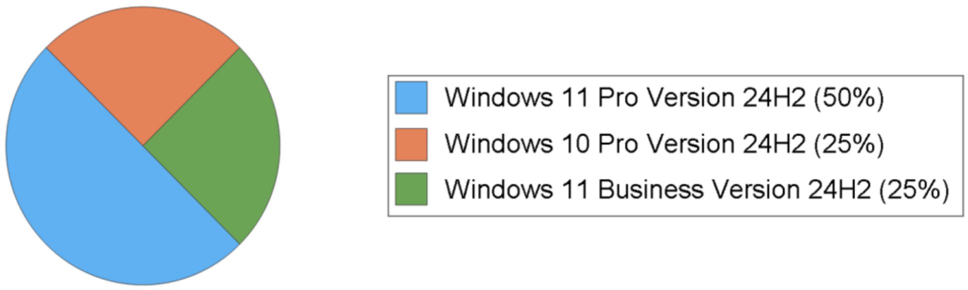

Supported
3
Extended Support
0
Unknown
0
Unsupported
0

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) or Microsoft Entra ID.

Total Computers by Operating System

Total (4)

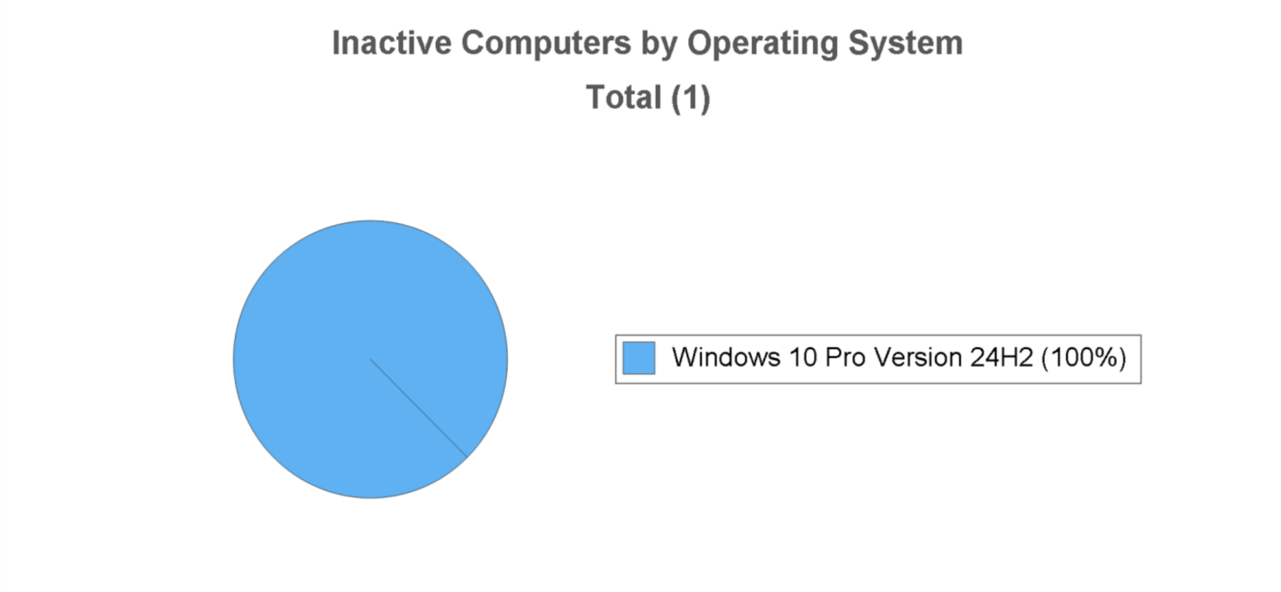


	OPERATING SYSTEM (TOP FIVE)	TOTAL	PERCENT
🟦	Windows 11 Pro Version 24H2	2	50%
🟧	Windows 10 Pro Version 24H2	1	25%
🟩	Windows 11 Business Version 24H2	1	25%
	Total - Top Five	**4**	**100%**

OPERATING SYSTEM (OTHER)	TOTAL	PERCENT
Total - Other	**0**	**0%**
OVERALL TOTAL	4	100%

10 - Asset Summary: Inactive Computers

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



	OPERATING SYSTEM (TOP FIVE)	TOTAL	PERCENT
🟦	Windows 10 Pro Version 24H2	1	100%
	Total - Top Five	**1**	**100%**

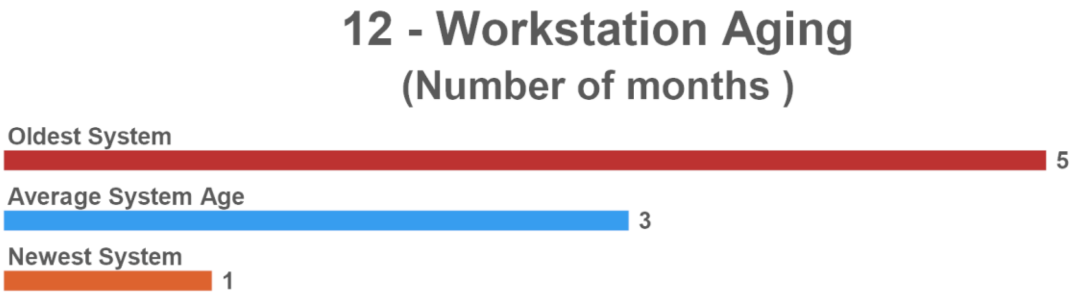
OPERATING SYSTEM (OTHER)	TOTAL	PERCENT
Total - Other	**0**	**0%**

OVERALL TOTAL	1	100%

11 - Server Aging

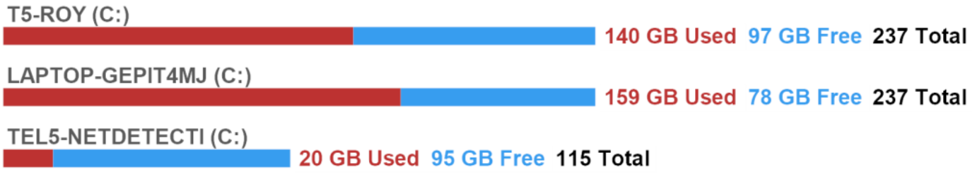
No Server Aging data could be determined.

12 - Workstation Aging

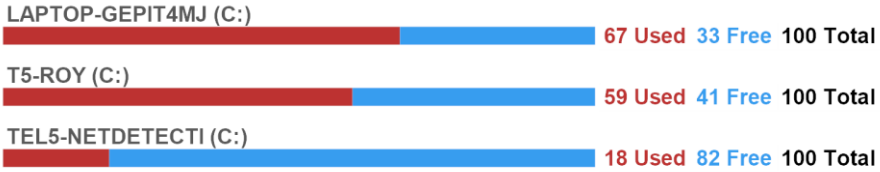


13 - Asset Summary: Storage

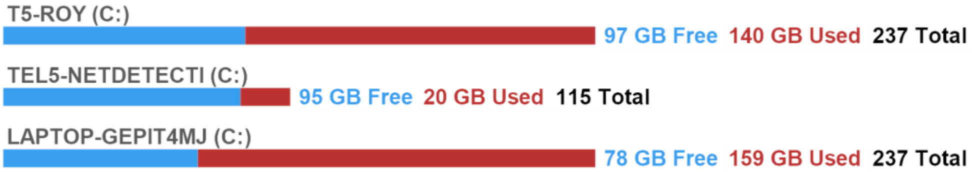
Top 10 Drive Capacity



Top 10 Drive % Used

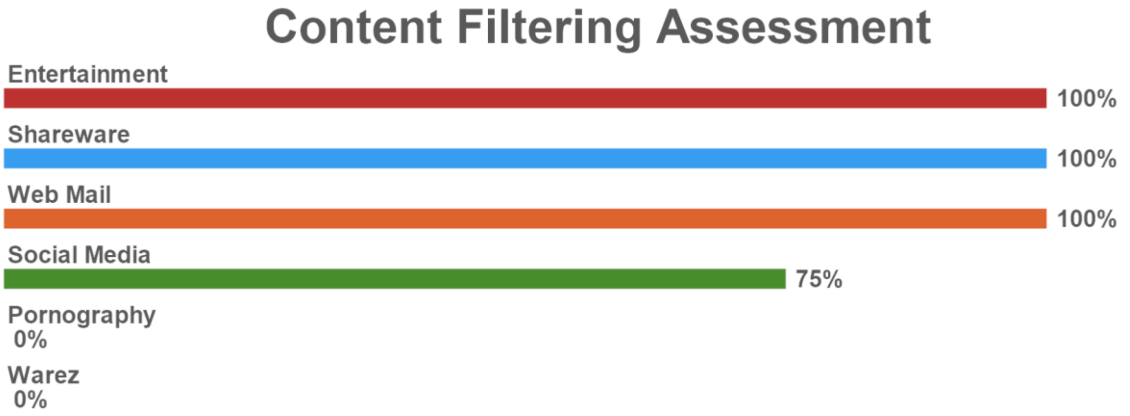


Top 10 Drive Free Space

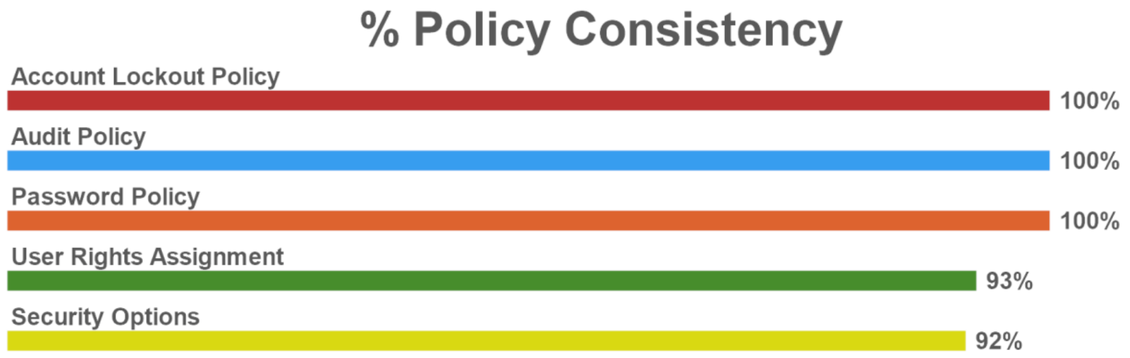


14 - Unrestricted Web Content

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.



15 - Local Security Policy Consistency



16 - 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
varun@tel5.com.au	Ade*********	02/17/2025	id theft forum
varun@tel5.com.au	Ade*********	12/17/2024	id theft forum
nick@tel5.com.au	003*************************** ******************************* ******************************* ******************************* *************	09/28/2024	id theft forum
sarah@tel5.com.au	003*************************** ******************************* ******************************* ******************************* ******************************* **************	09/28/2024	id theft forum
info@tel5.com.au		03/24/2024	id theft forum