RISK REPORT

NETWORK ASSESSMENT

PREPARED FOR [client]

PREPARED BY XMI

[date]

XMI

TABLE OF CONTENTS

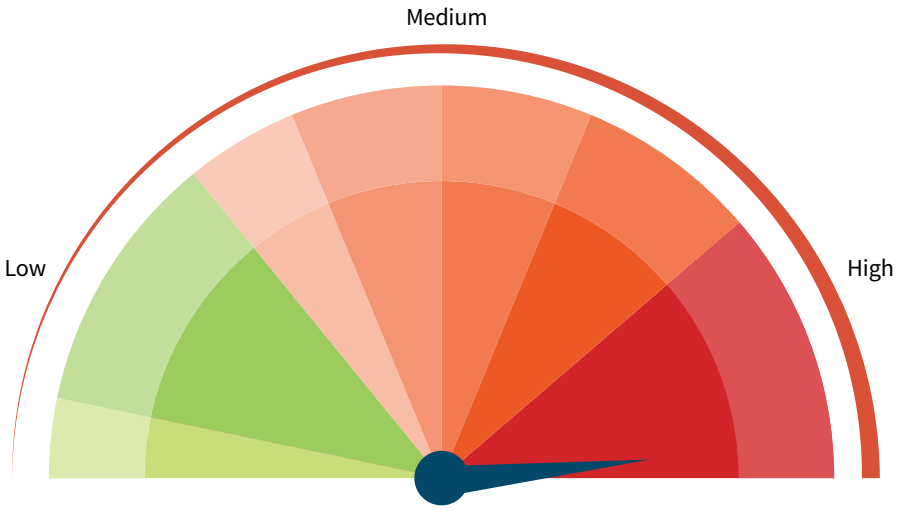
Discovery Tasks

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	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
✓	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 the 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.
✓	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	Discovers the five system and app event log errors for servers.
✗	External Security Vulnerabilities	Lists the 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. 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 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

SCORE	ISSUES DETECTED

460

Operating system in Extended Support (20 pts each)

Current Score: 20 pts x 23 = **460: 43.27%**

Issue: 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.

280

Insecure listening ports (10 pts each)

Current Score: 10 pts x 28 = **280: 26.34%**

Issue: are to be 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.

100

Potential password strength risks (100 pts each)

Current Score: 100 pts x 1 = **100: 9.41%**

Issue: Local account passwords on 1 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 remediating the immediate password issues on the identified systems.

Overall Issue Score

SCORE	ISSUES DETECTED

97

Unsupported operating systems (97 pts each)

Current Score: 97 pts x 1 = **97: 9.13%**

Issue: 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.

68

Potential disk space issue (68 pts each)

Current Score: 68 pts x 1 = **68: 6.4%**

Issue: 1 computer were found with significantly low free disk space.

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

45

Inactive computers (15 pts each)

Current Score: 15 pts x 3 = **45: 4.23%**

Issue: 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, or powered on.

13

User has not logged on to domain 30 days (13 pts each)

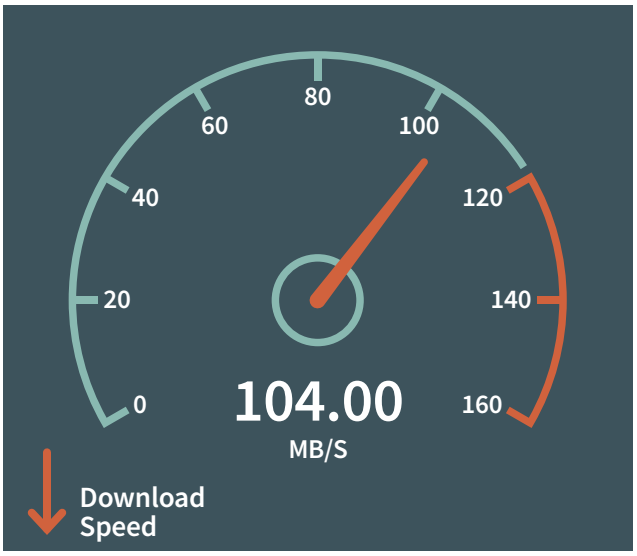
Current Score: 13 pts x 1 = **13: 1.22%**

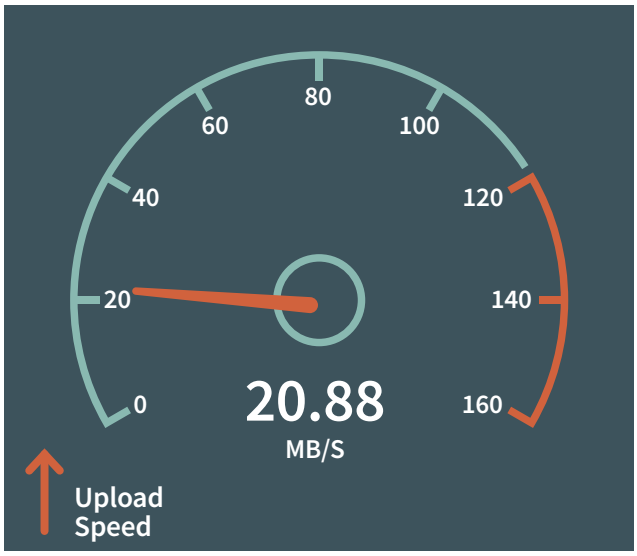
Issue: Users that have not logged in in 30 days could be from A user that has not logged in for an extended period of time could be a former employee or vendor.

Recommendation: Disable or remove user accounts for users that have not logged on to active directory in 30 days.

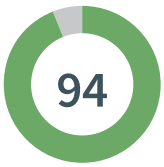
Back to TOC ▶

Internet Speed Test Results



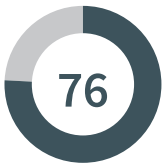


Asset Summary: *Total Discovered Assets*



Computers

Windows



Web Servers

Printers

Exchange Servers

MX Records

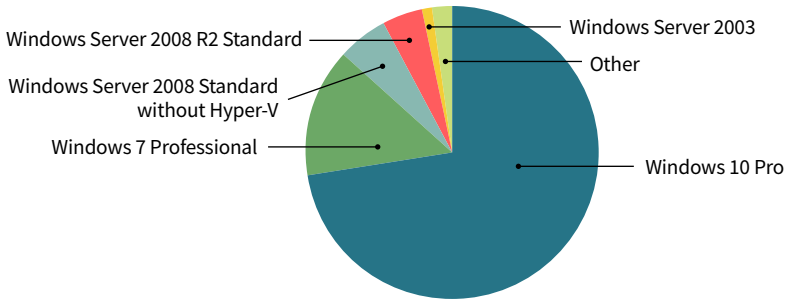
0 Linux
0 Mac OS
0 MS S-QL Servers

Back to TOC ▶

Asset Summary: *Active Computers*

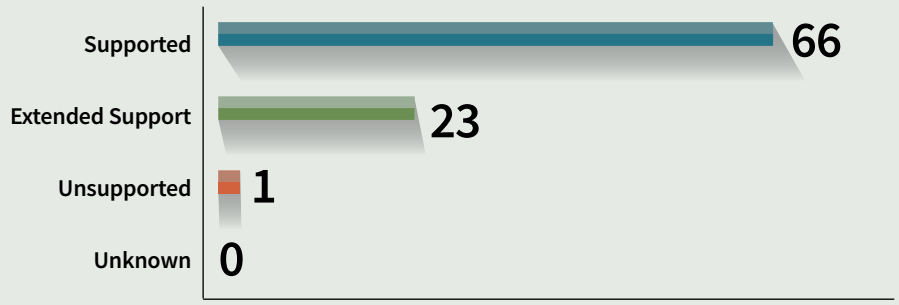
Active Computers are defined as computers that were either actively responding at the time of the scan or have checked in with Active Directory within the past 30 days.

Active Computers by Operating System
Total (91)



	Operating System	Total	Percent
Top Five	Windows 10 Pro	66	72.5%
	Windows 7 Professional	13	14.3%
	Windows Server 2008 Standard without Hyper-V	5	5.5%
	Windows Server 2008 R2 Standard	4	4.4%
	Windows Server 2003	1	1.1%
	TOTAL - TOP FIVE	**89**	**97.8%**
Other	Windows Server 2008 Enterprise without Hyper-V	1	1.1%
	Windows Server 2012 R2 Standard	1	1.1%
	TOTAL - OTHER	**2**	**2.2%**
	OVERALL TOTAL	**91**	**100%**

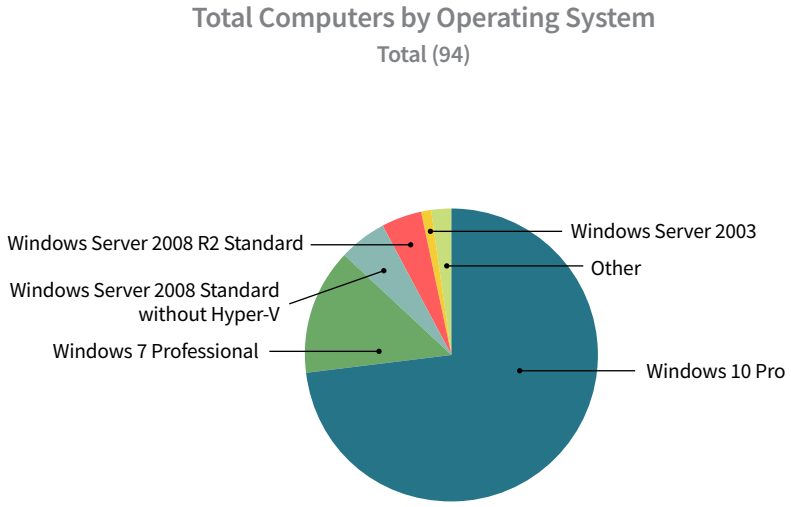
Operating System Support
(Number of computers)



Back to TOC ▶

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).

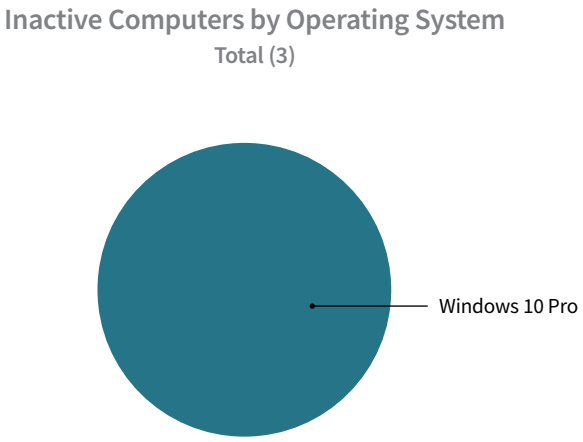


	Operating System	Total	Percent
Top Five	Windows 10 Pro	69	73.4%
	Windows 7 Professional	13	13.8%
	Windows Server 2008 Standard without Hyper-V	5	5.3%
	Windows Server 2008 R2 Standard	4	4.3%
	Windows Server 2003	1	1.1%
	TOTAL - TOP FIVE	**92**	**97.9%**
Other	Windows Server 2008 Enterprise without Hyper-V	1	1.1%
	Windows Server 2012 R2 Standard	1	1.1%
	TOTAL - OTHER	**2**	**2.2%**
	OVERALL TOTAL	**94**	**100%**

Back to TOC ▶

Asset Summary: *Inactive Computers*

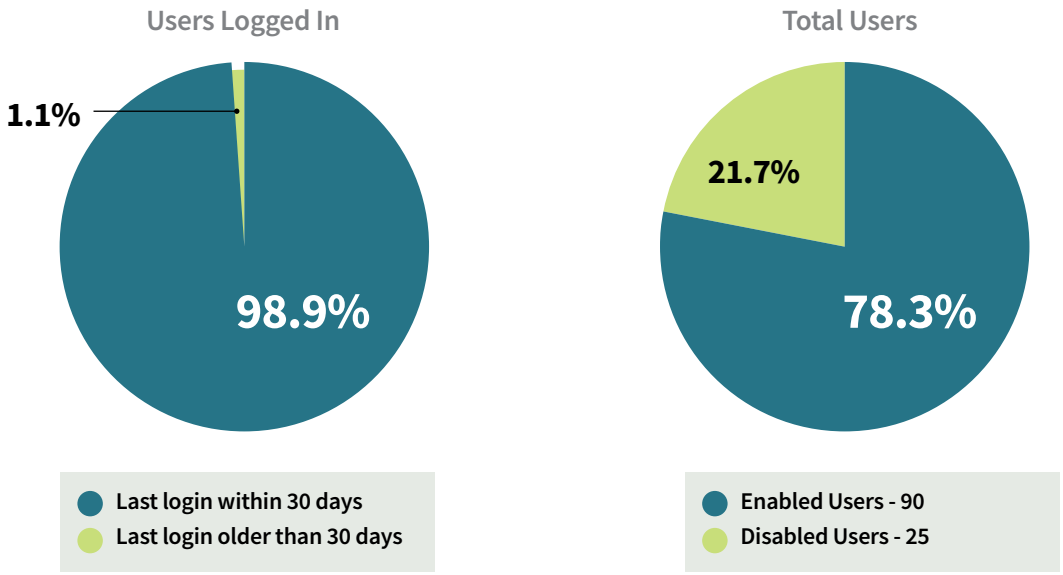
Inactive computers are computers that could not be scanned or have not checked into Active Directory in the past 30 days.

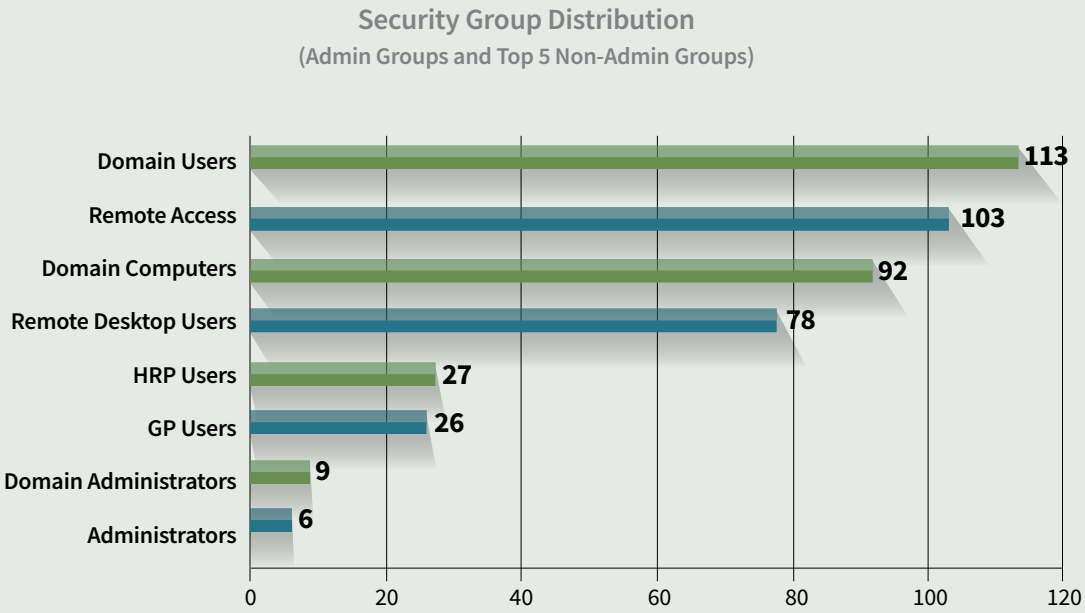


	Operating System	Total	Percent
Top Five	Windows 10 Pro	3	100%
	TOTAL - TOP FIVE	**3**	**100%**
Other	**TOTAL - OTHER**	**0**	**0%**
	OVERALL TOTAL	**3**	**100%**

Back to TOC ▶

Asset Summary: *Users*

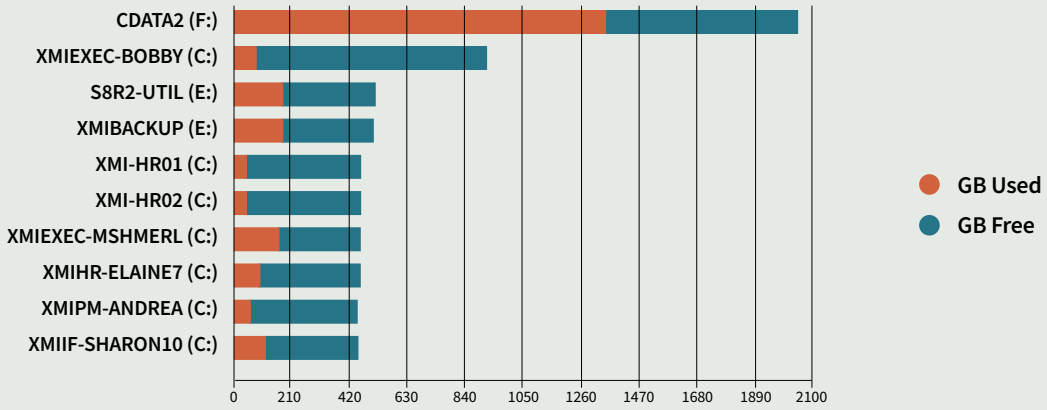




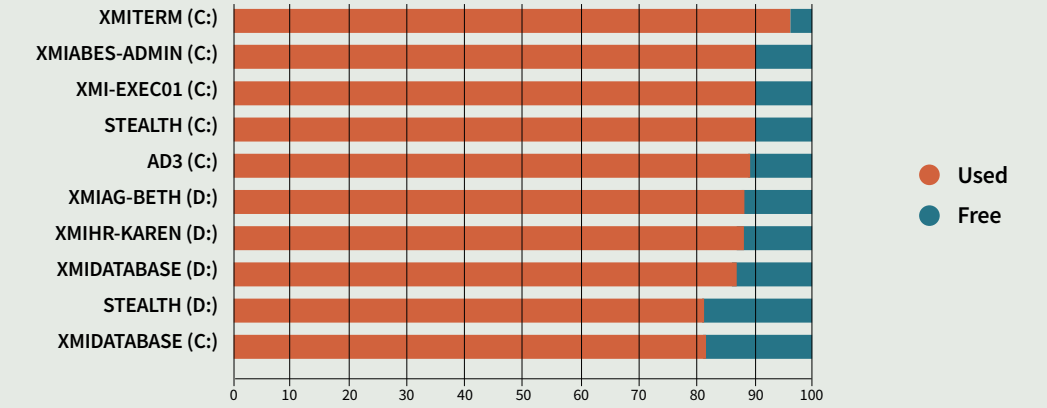
Back to TOC ▶

Asset Summary: *Storage*

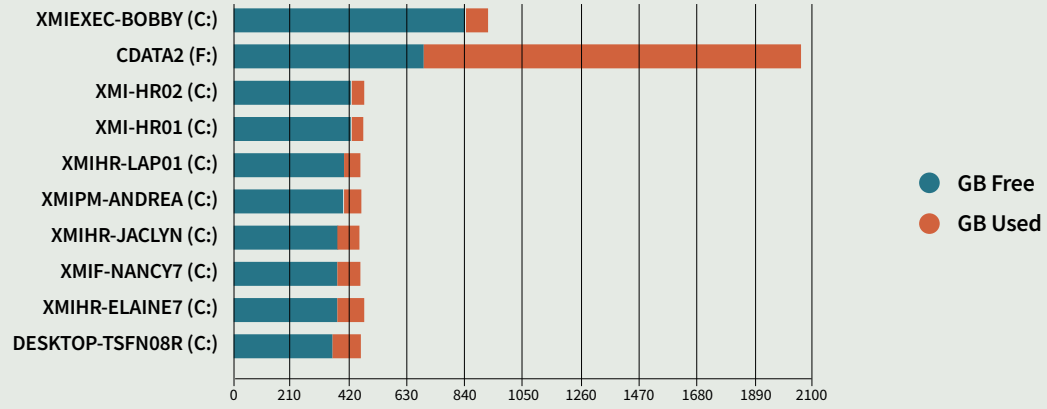
Top 10 Drive Capacity



Top 10 Drive % Used

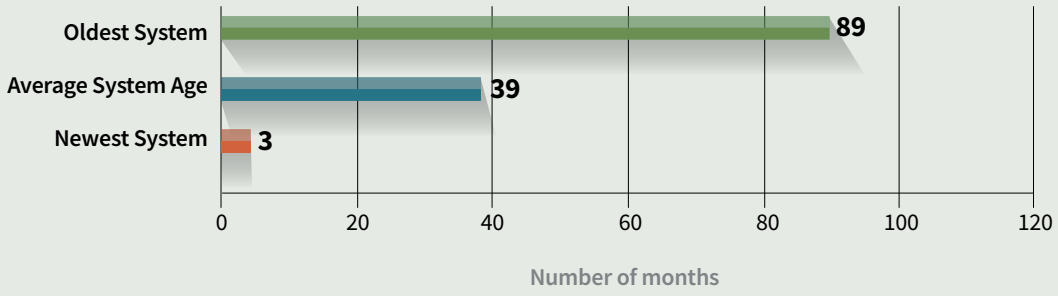


Top 10 Drive Free Space

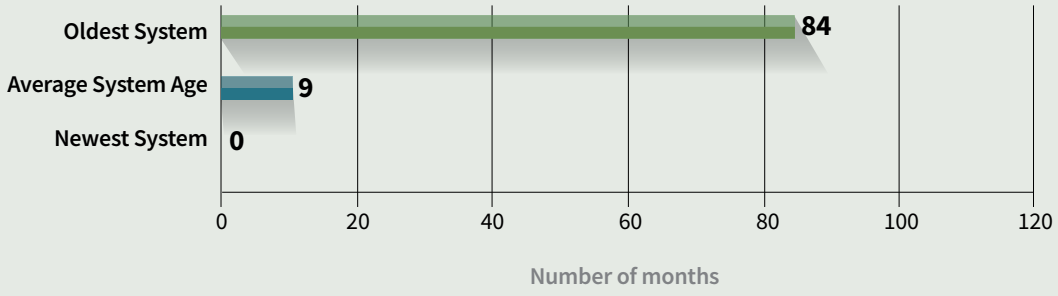


Back to TOC ▶

Server Aging



Workstation Aging



Back to TOC ▶