Network Detective

Prepared For:

Customer

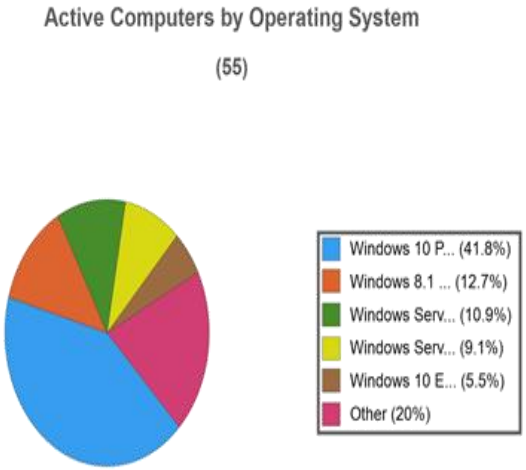
Prepared By:

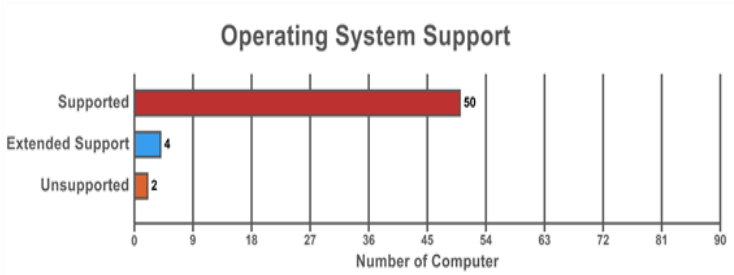
The Cassid Group

Agenda

- Environment
- Risk and Issue Score
- Issue Review
- Next Steps

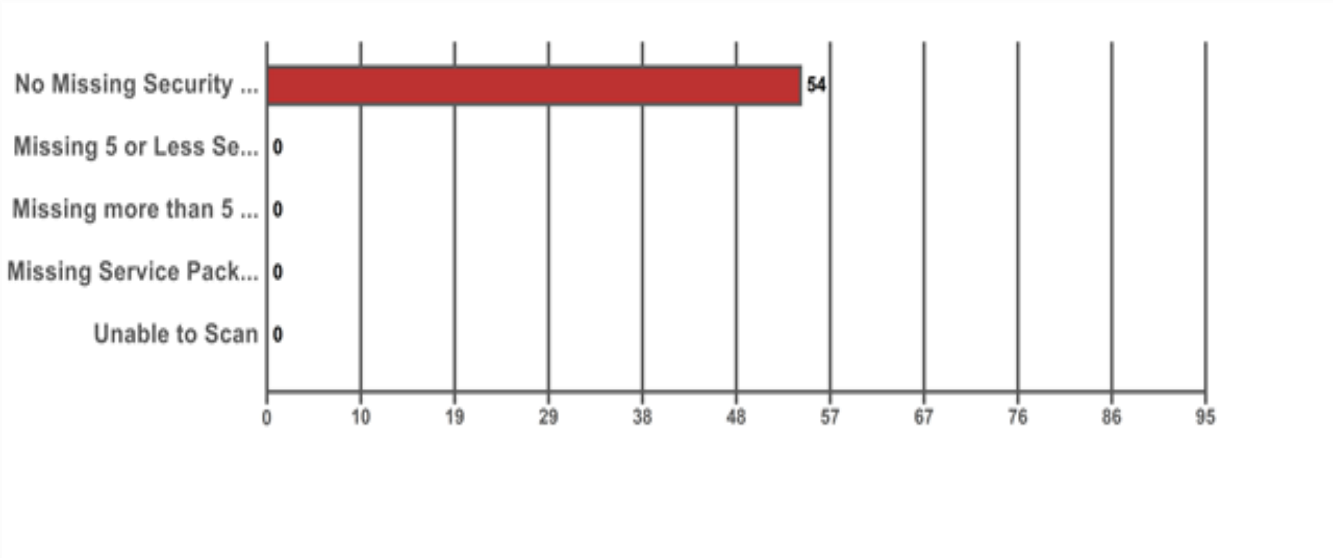
Environment - Overview





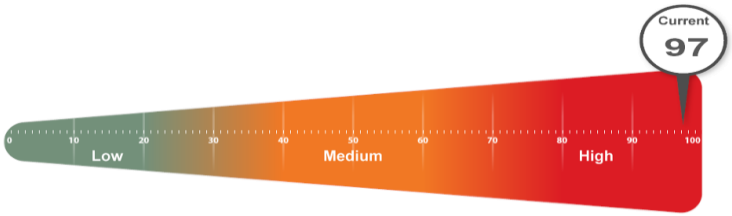
Domain	
Domain Controllers	1
Number of Organizational Units	17
Users	
# Enabled	74
Last Login within 30 days	33
Last Login older than 30 days	41
# Disabled	59
Last Login within 30 days	0
Last Login older than 30 days	59
Security Group	
Groups with Users	39
# Total Groups	74
Computers in Domain	
Total Computers	144
Last Login within 30 days	55
Last Login older than 30 days	89

Environment - Patching



Risk and Issue Score

Risk Score



Issue Score

Issue Review

Unsupported operating systems (97 pts)
Issue: 2 computers 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.

Issue Review

Anti-spyware not installed (94 pts)
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.

Issue Review

Anti-virus not installed (94 pts)
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.

Issue Review

Lack of redundant domain controller (85 pts)
Issue: Only one domain controller was found on the network. There is a heightened risk of business downtime, loss of data, or service outage due to a lack of redundancy.
Recommendation: Evaluate the risk, cost, and benefits of implementing a redundant Domain Controller.

Issue Review

User password set to never expire (80 pts)
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.

Issue Review

Potential disk space issue (68 pts)
Issue: 4 computers were found with significantly low free disk space.
Recommendation: Free or add additional disk space for the specified drives.

Issue Review

Operating system in Extended Support (20 pts)
Issue: 4 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.

Issue Review

Inactive computers (15 pts)
Issue: 89 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, or powered on.

Issue Review

User has not logged on to domain 30 days (13 pts)
Issue: 41 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.

Issue Review

Un-populated organization units (10 pts)
Issue: Empty organizational units (OU) were found in Active Directory. They may not be needed and can lead to misconfiguration.
Recommendation: Remove or populate empty organizational units.

Issue Review

Insecure listening ports (10 pts)
Issue: 20 computers 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.

Next Steps

- Agree on List of Issues to Resolve
- Present Project Estimates and Costs
- Establish Timelines
- Set Milestones
- Get Signoff to Begin Work