YourIT!
Your Logo Goes Here

Progress Reporting

Client Progress Report

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.óó Global

Prepared for:
My IT Client
Prepared by:
YourIT Company

Executive Summary

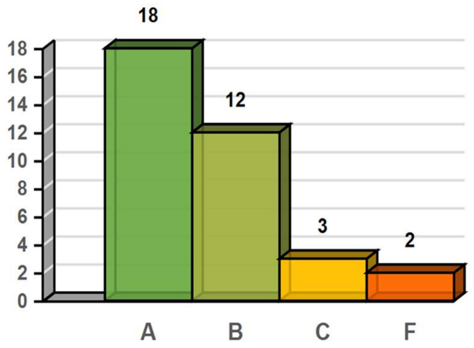
As part of our ongoing services to ensure the health of your business IT, we regularly scan the environment collecting large amounts of data. We use the data to perform network and security assessments to evaluate both overall health of the network as well as individual computers.

Computers are given a letter grade ('A' through 'F'). Below is the current and previous computer security score breakdown of the IT environment.

There has been a **significant increase** in the number of low risk computers from 25 to 30.

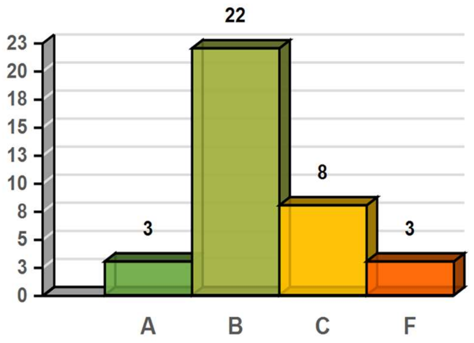
Current Security Grade Distribution

2020/04/20



Previous Security Grade Distribution

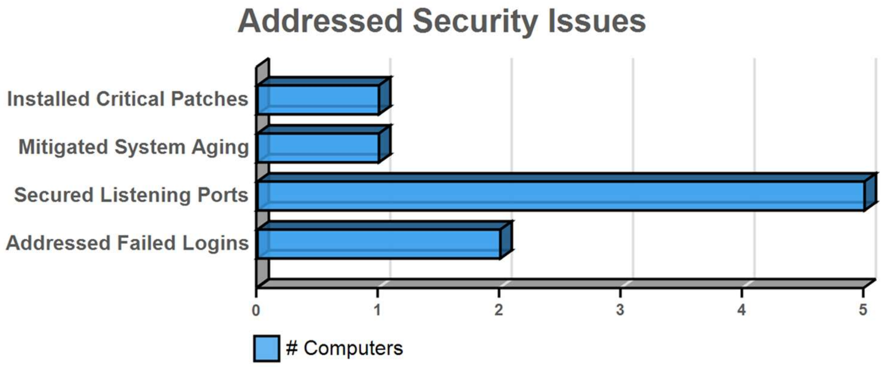
2019/10/02



Our goal is "peak performance" of all your computers. To objectively measure how well we are doing, we try to increase the number of computers receiving an 'A' grade over time. Certain factors, like the introduction of new systems, failed updates, or misconfigurations can cause issues and lower scores.

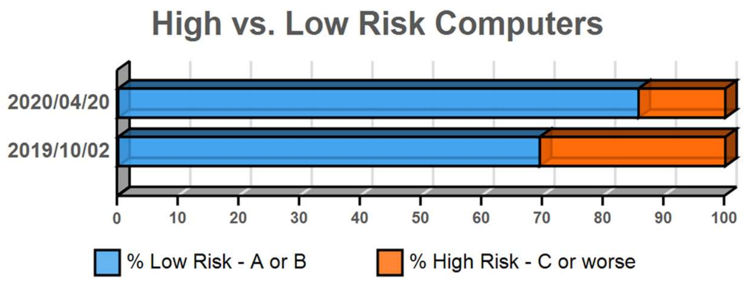
Improvements over the Last Reporting Period

On an ongoing basis we proactively identify potential IT issues before they can impact the performance and availability of your computer network and, consequently, your business as well. Since the last assessment, several security issues were found and remediated. Below is a summary of the addressed issues.



Report Card

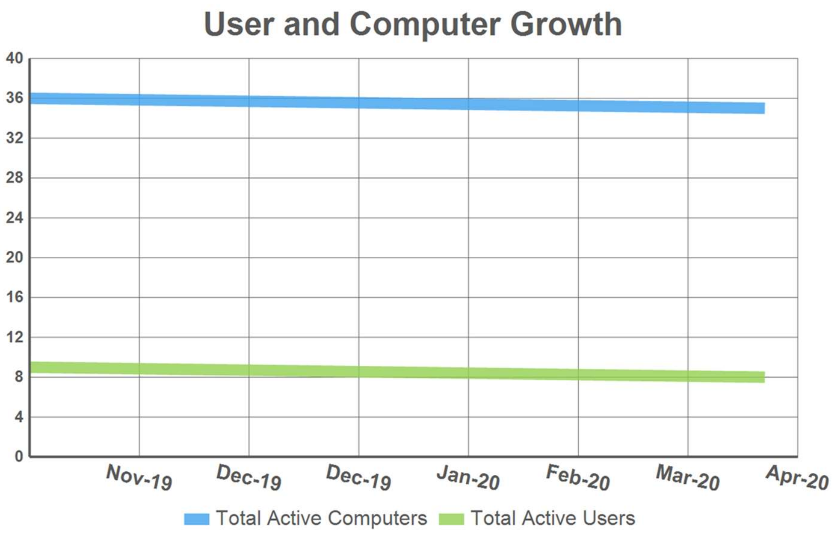
Devices discovered on the network are assigned an overall score, as well as a specific score for each of the assessment categories detailed below. The scores are represented as color-coded letter grades ('A' through 'F'). Where there is not enough information to determine a grade, a gray box with "N/A" is displayed. The rubric at the end of this report lists the criteria used to determine the grade for each category. * Note that because the overall grade is a composite of available grades, it may be skewed in cases where all security data could not be gathered.



Top 10 High Risk Computers

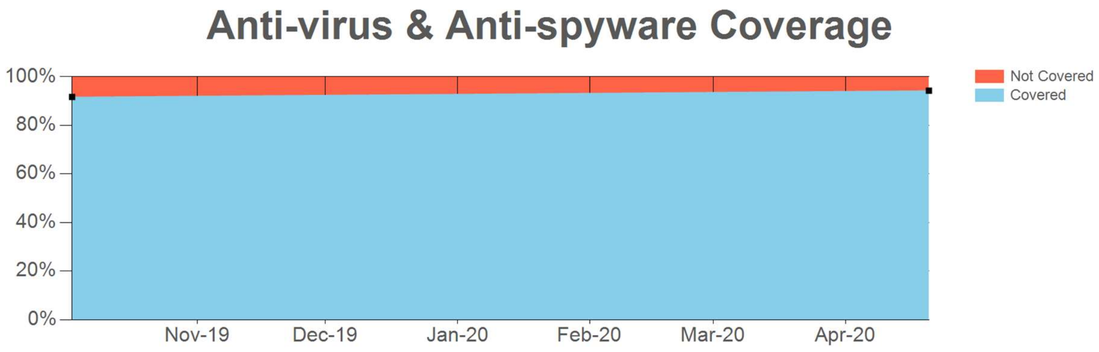
Computer	Overall Grade	Anti-virus	Anti-spyware	Local Firewall	Missing Critical Patches	Insecure Listening Ports	Failed Logins	Network Vulnerabilities	Screen Lock with Timeout	System Aging	Supported OS
MYCO\NV-GIS (172.16.2.127)	**F**	F	F	A	N/A	A	A	N/A	N/A	A	A
MYCO\FILESERVER1 (172.16.2.148)	**F**	F	F	A	N/A	A	A	N/A	N/A	A	A
MYCO\FILESERVER2 (172.16.2.121)	**C**	B	A	A	N/A	A	A	N/A	N/A	A	F
MYCO\NV-PRINTSVR (172.16.2.159)	**C**	B	A	A	N/A	A	A	N/A	N/A	A	F
MYCO\NV-STORE1 (172.16.2.231)	**C**	A	B	A	N/A	A	A	N/A	F	A	A
MYCO\NV-AUTOMATE (172.16.2.62)	**B**	A	A	A	A	A	A	N/A	F	A	A
MYCO\RSTRSVR (172.16.2.37)	**B**	B	B	A	N/A	N/A	A	N/A	N/A	A	A
MYCO\NV-CAMA (172.16.2.229)	**B**	A	B	A	N/A	A	B	N/A	N/A	A	A
MYCO\NV-DV (172.16.2.29)	**B**	A	B	A	N/A	A	A	N/A	N/A	A	A
MYCO\NV-GPSTEST (172.16.2.68)	**B**	A	B	A	N/A	A	A	N/A	N/A	A	A

Changes and Trends



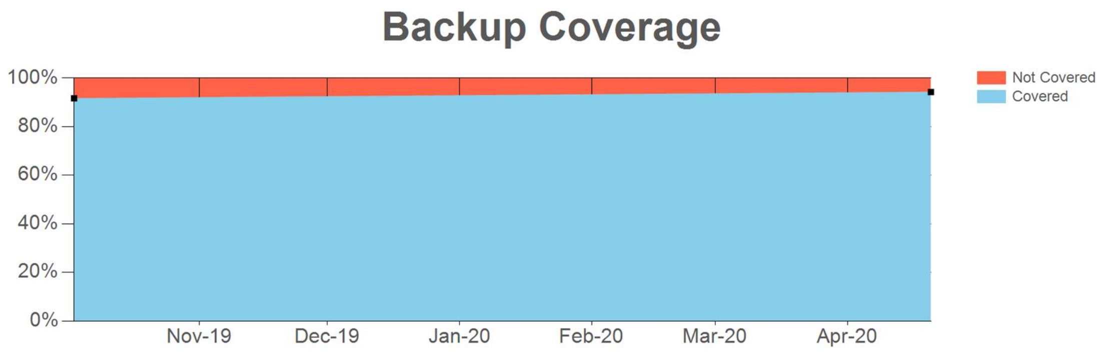
Anti-virus & Anti-spyware

Maintaining maximum anti-virus and anti-spyware coverage is one of the best practices for ensuring a secure and available IT infrastructure. Over time, we track coverage based on which systems have anti-virus and anti-spyware to ensure maximum coverage and minimize risk through coverage gaps.



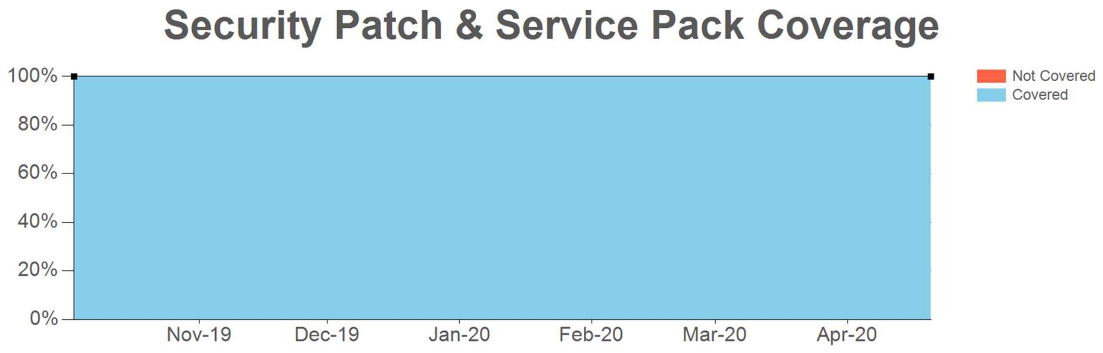
Backup

In the event of an irreparable issue on any computer, the ability to recover is dependent on having proper backups. Some systems should be backed up regularly due to criticality. It is not always necessary to backup all systems but ensuring maximum coverage of local backup agents is one way to mitigate recovery risks.



Security Patch & Service Packs

Proper patch management is a critical component of ensuring the security and availability of your servers and workstations. The chart below tracks the percentage of systems that have had all critical security patches and service packs installed.



Technical Findings

Score Card Improvement Detail

Computer	Previous Grade	Current Grade	Improved Factors
MYCO\ABARKETT-HP	B	A	Failed Logins
MYCO\RSTRSVR	B	A	Missing Critical Patches
MYCO\RSTRSVR-2	B	A	Failed Logins
MYCO\LINETTE-HP308	B	A	Insecure Listening Ports
MYCO\MARKMSI	C	A	Insecure Listening Ports System Aging
MYCO\DBISCOEACER	B	A	Insecure Listening Ports System Aging
MYCO\NV-DV	B	A	Screen Lock with Timeout
MYCO\NV-GPSTEST	B	A	Insecure Listening Ports System Aging
MYCO\NV-SPOOLYZ240	B	A	Screen Lock with Timeout
MYCO\ABARKETT-HP	B	A	Screen Lock with Timeout

Added and Removed Computers

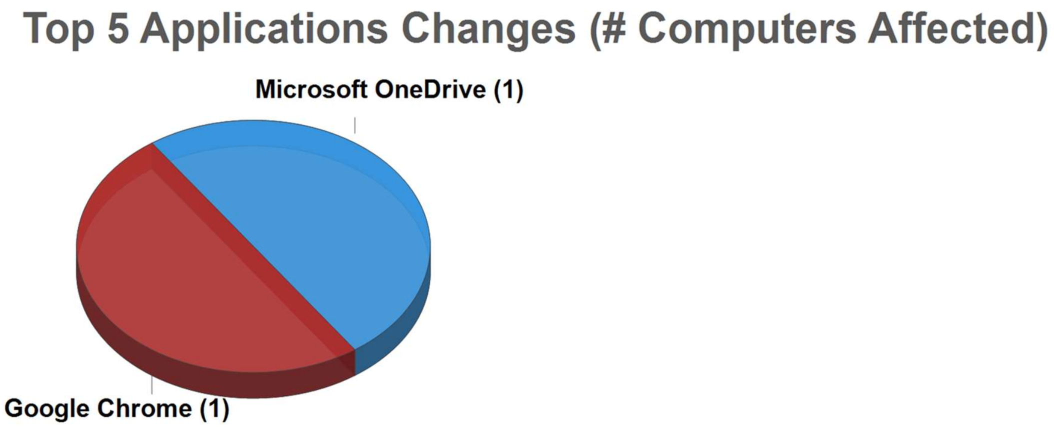
1 computers were added since the last assessment.

Type	OS	Count	Computer Name
Member Workstation	Windows 10 Enterprise	1	MYCO\GEORGEMSI

2 computers were removed since the last assessment.

Type	OS	Count	Computer Name
Member Server	Windows Server 2012 Standard Evaluation	1	MYCO\INV-EXC
Member Server	Windows Server 2016 Standard	1	MYCO\2003MICKEY

Application Changes



0 applications were installed since the previous assessment.

1 applications were updated since the previous assessment.

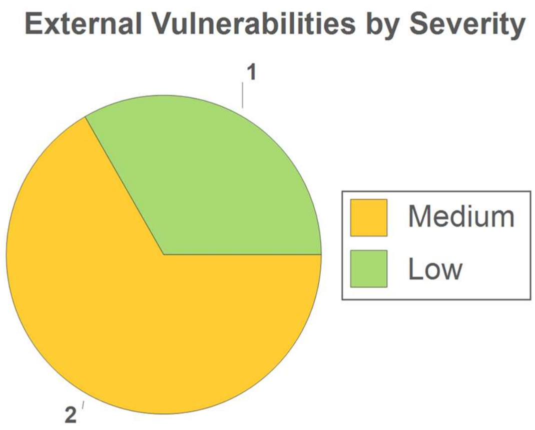
1 applications were removed since the previous assessment.

Major Application	Action	# Computers	% Computers
Google Chrome	Updated	1	25%
Microsoft OneDrive	Removed	1	25%

External Vulnerabilities Details

Security threats to your computer network are an ongoing problem that get worse (not better) over time. Hackers invent new ways to try to exploit your business daily. That's why we take a proactive approach to security and perform continuing vulnerability scans using Common Vulnerability Scoring System (CVSS) which is a recognized industry standard for assessing the severity of computer system security vulnerabilities. CVSS assigns severity scores to vulnerabilities, allowing us to prioritize responses and resources according to threat. Scores range from 0 to 10, with 10 being the most severe. Here's what we uncovered since the last report and what we've done to defeat the bad guys from destroying your business.

Host	Open Ports	High	Med	Low	False	Highest CVSS
205.215.132.27 (60.32.109.215.209.in-addr.arco)	2	0	2	1	0	5.0
Total: 1	2	0	2	1	0	5.0



Top 5 External Vulnerabilities Found

IP Address	Port	External Vulnerability Description	CVSS Score	Risk Factor	Count
67.18.7.89	443/tcp (https)	**Vulnerability:** This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services. **Solution:** The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.	5	Medium	1
67.18.7.89	443/tcp (https)	**Vulnerability:** This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the	4.3	Medium	1

IP Address	Port	External Vulnerability Description	CVSS Score	Risk Factor	Count
		alternative would be to fall back to an even more insecure cleartext communication. **Solution:** The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.			
67.18.7.890		**Vulnerability:** The remote host implements TCP timestamps and therefore allows to compute the uptime. **Solution:** To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.	2.6	Low	1