YourIT!
Your Logo Goes Here

Progress Reporting

Client Progress Report

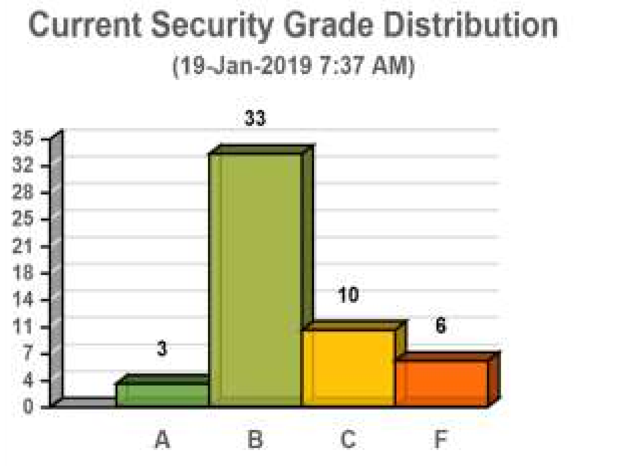
CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited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

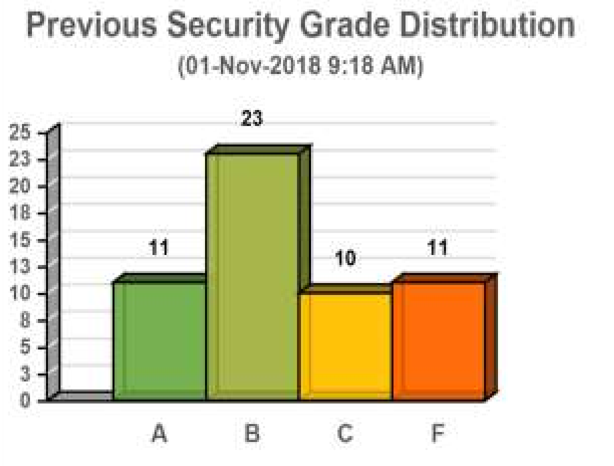
Prepared for:
My IT Client
Prepared by:
YourIT Company

Executive Summary

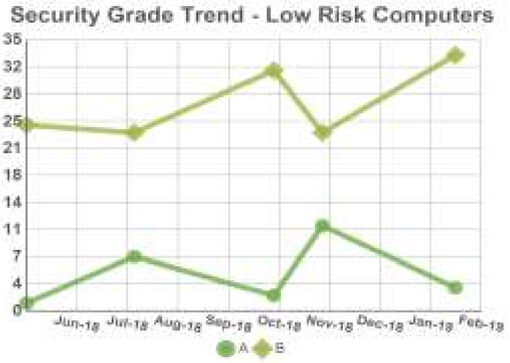
As part of our ongoing services to ensure the health of your business IT, we regularly scan the environment collecting large amounts of data. We use the data to perform network and security assessments to evaluate both overall health of the network as well as individual computers.

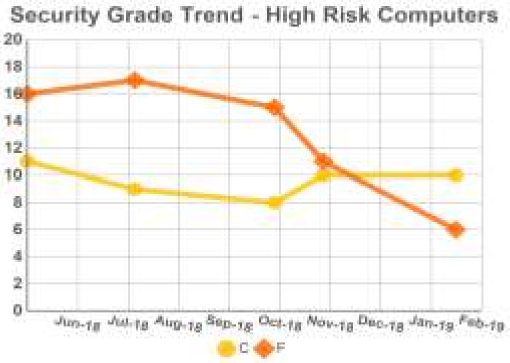
Computers are given a letter grade ('A' through 'F'). Below is the current computer security score breakdown of the IT environment.


Current Security Grade Distribution
(19-Jan-2019 7:37 AM)


Previous Security Grade Distribution
(01-Nov-2018 9:18 AM)

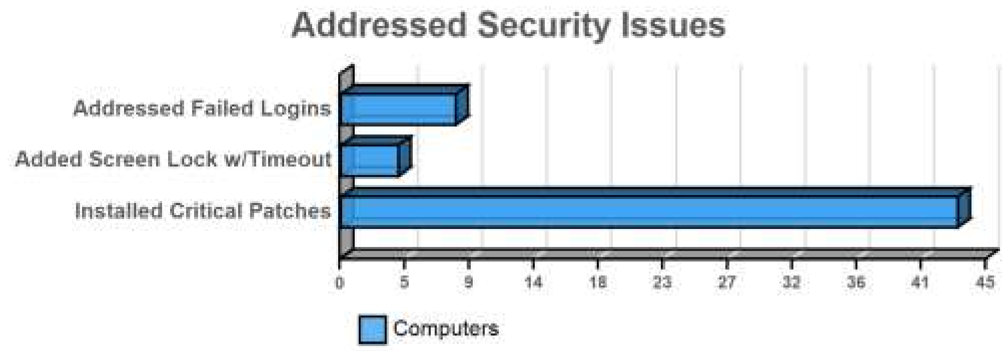
Our goal is "peak performance" of all your computers. To objectively measure how well we are doing, we try to increase the number of computers receiving an 'A' grade over time. Certain factors, like the introduction of new systems, failed updates, or misconfigurations can cause issues and lower scores.


Security Grade Trend - Low Risk Computers


Security Grade Trend - High Risk Computers

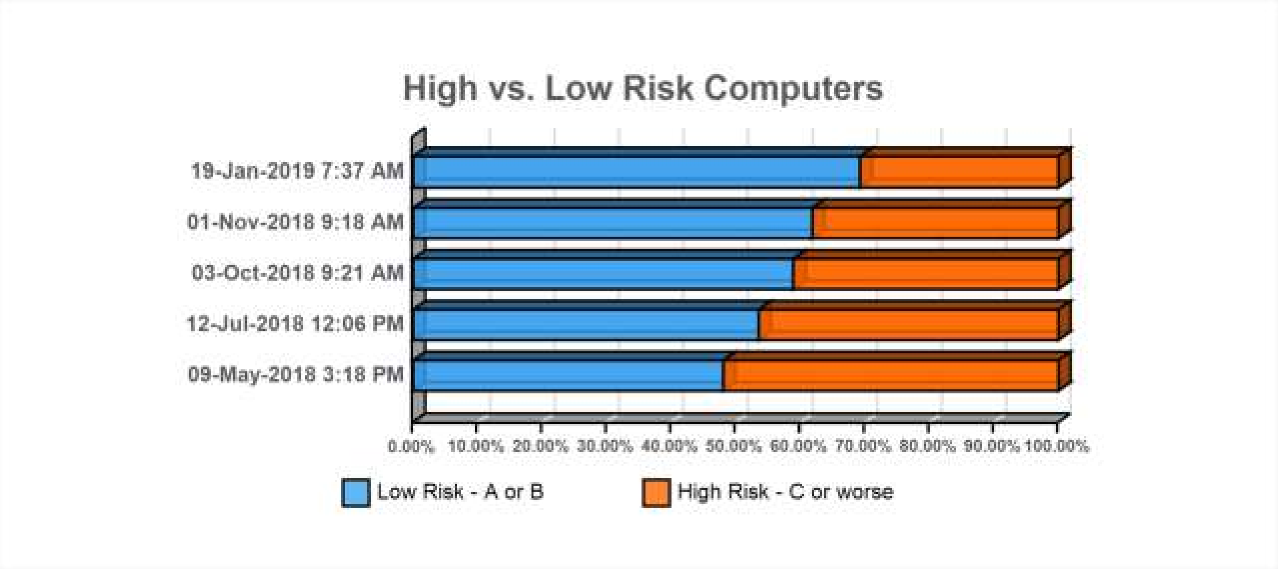
Improvements over the Last Reporting Period

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.


Addressed Security Issues
Addressed Failed Logins
Added Screen Lock w/Timeout
Installed Critical Patches
0
5
9
14
18
23
27
32
36
41
45
Computers

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.

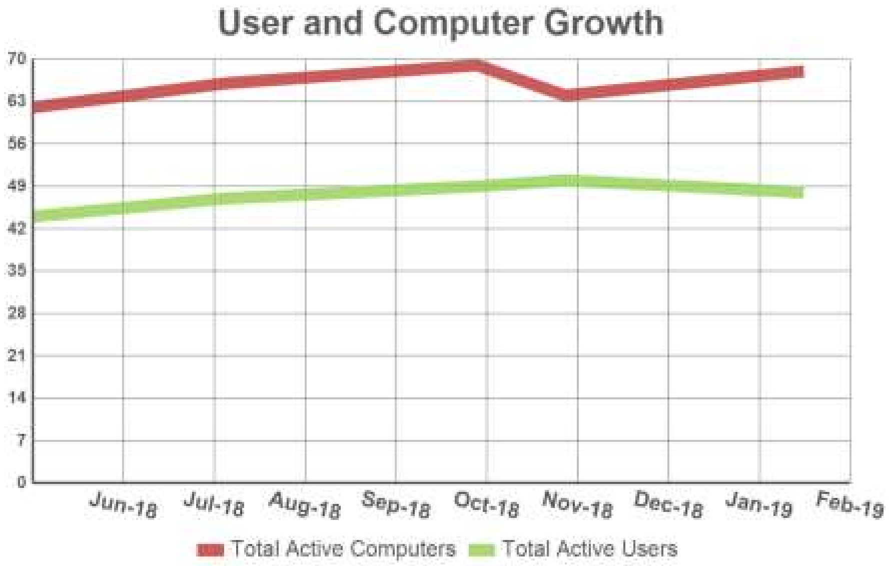


Top 10 High Risk Computers

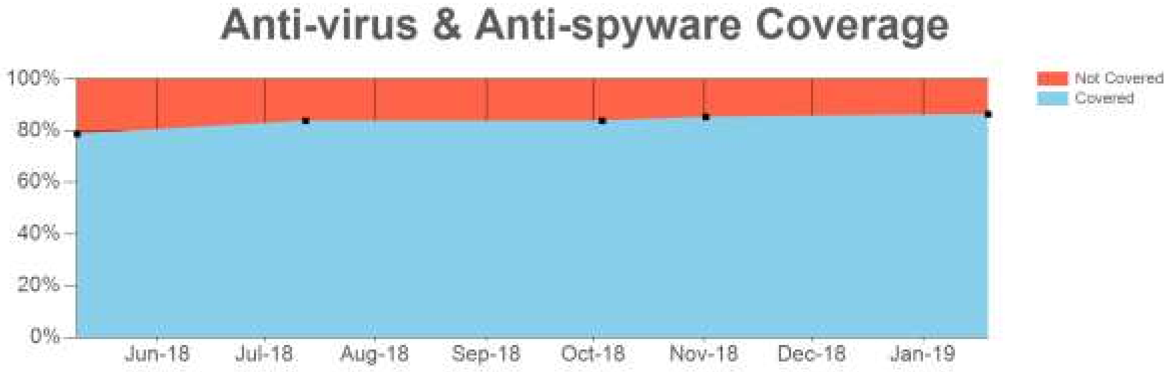
Computer	Overall Grade	Anti-virus	Anti-spyware	Local Firewall	Missing Critical Patches	Insecure Listening Ports	Failed Logins	Network Vulnerabilities	Screen Lock with Timeout	System Aging	Supported OS
MYCO\NV-GIS (172.16.2.127)	**F**	F	F	C	A	A	F	N/A	A	F	F
MYCO\FILESERVER1 (172.16.2.148)	**F**	F	F	C	A	A	B	N/A	A	C	F
MYCO\FILESERVER2 (172.16.2.121)	**F**	F	F	C	A	A	A	N/A	A	C	F
MYCO\NV-PRINTSVR (172.16.2.159)	**F**	F	F	C	A	A	A	N/A	A	B	F
MYCO\NV-STORE1 (172.16.2.231)	**F**	F	F	C	A	A	F	N/A	A	A	A
MYCO\NV-AUTOMATE (172.16.2.62)	**F**	A	A	C	N/A	A	A	N/A	F	C	F
MYCO\RSTRSVR (172.16.2.37, 172.16.2.107)	**C**	A	A	C	N/A	A	B	N/A	N/A	C	F
MYCO\NV-CAMA	**C**	B	B	A	A	A	A	N/A	A	F	F

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
(172.16.2.229)											
MYCO\NV-DV (172.16.2.29)	**C**	F	F	C	A	A	A	N/A	A	A	A
MYCO\NV-GPSTEST (172.16.2.68)	**C**	F	F	C	A	A	A	N/A	A	A	A

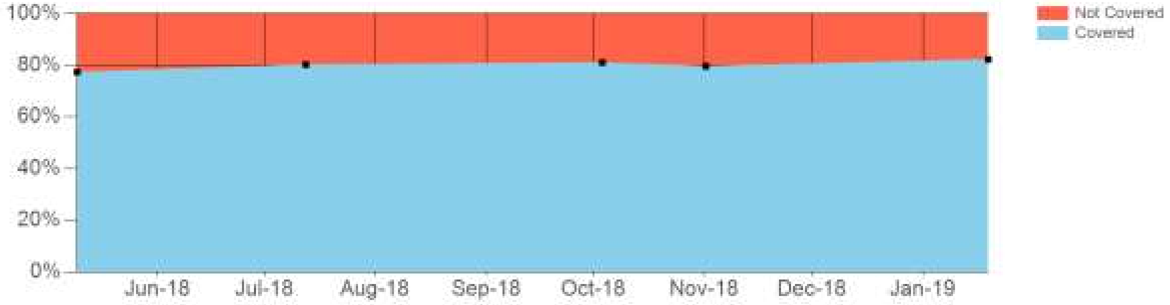
Changes and Trends



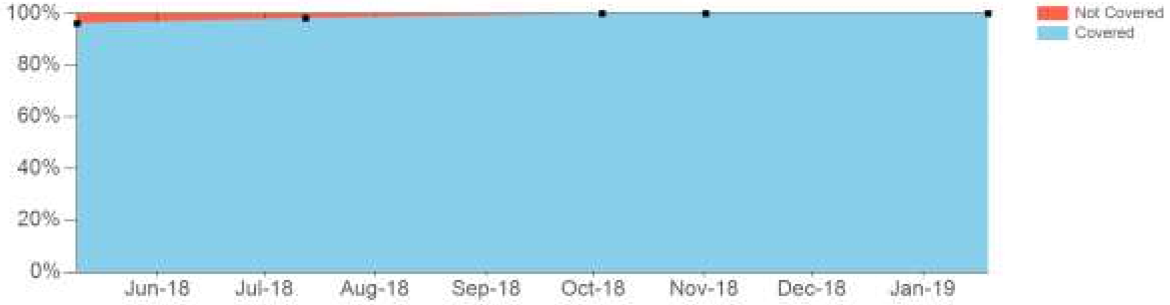
Coverage Metrics



Backup Coverage



Security Patch & Service Pack Coverage



Technical Findings

Score Card Improvement Detail

Computer	Previous Grade	Current Grade	Improved Factors
MYCO\ABARKETT-HP	C	B	Missing Critical Patches
MYCO\RSTRSVR	F	C	Failed Logins
MYCO\DBISCOEACER	C	B	Missing Critical Patches Screen Lock with Timeout
MYCO\LINETTE-HP308	F	C	Missing Critical Patches Failed Logins
MYCO\MARKMSI	C	B	Missing Critical Patches Failed Logins Screen Lock with Timeout
MYCO\NV-DV	F	C	Missing Critical Patches
MYCO\NV-GPSTEST	F	C	Missing Critical Patches
MYCO\SPOOLYZ240	C	B	Missing Critical Patches Failed Logins

Added and Removed Computers

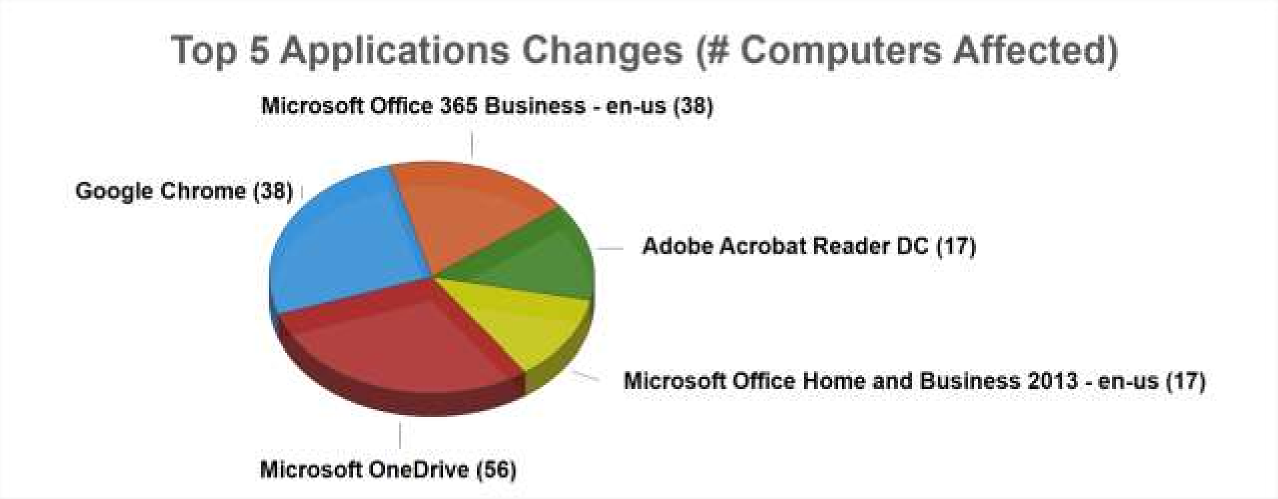
5 computers were added since the last assessment.

Type	OS	Count	Computer Name
Member Workstation	Windows 10 Pro	5	MYCO\GEORGEMSI MYCO\MICKEYHPZ240 MYCO\PA19AD03 MYCO\PA19AD04 MYCO\PA19BD05

8 computers were removed since the last assessment.

Type	OS	Count	Computer Name
Member Server	Windows Server 2008 R2 Standard	1	MYCO\NV-EXCH
Member Workstation	Windows 10 Pro	6	MYCO\2003MICKEY MYCO\JENLENOVOMTM157 MYCO\NNEILLHPZ230-PA MYCO\NV-COMMERCIAL MYCO\SHELMSPRODSKHP MYCO\SISSYL-HP
Member Workstation	Windows 7 Professional	1	MYCO\TA-TRAINING1-HP

Application Changes



45 applications were installed since the previous assessment.

18 applications were updated since the previous assessment.

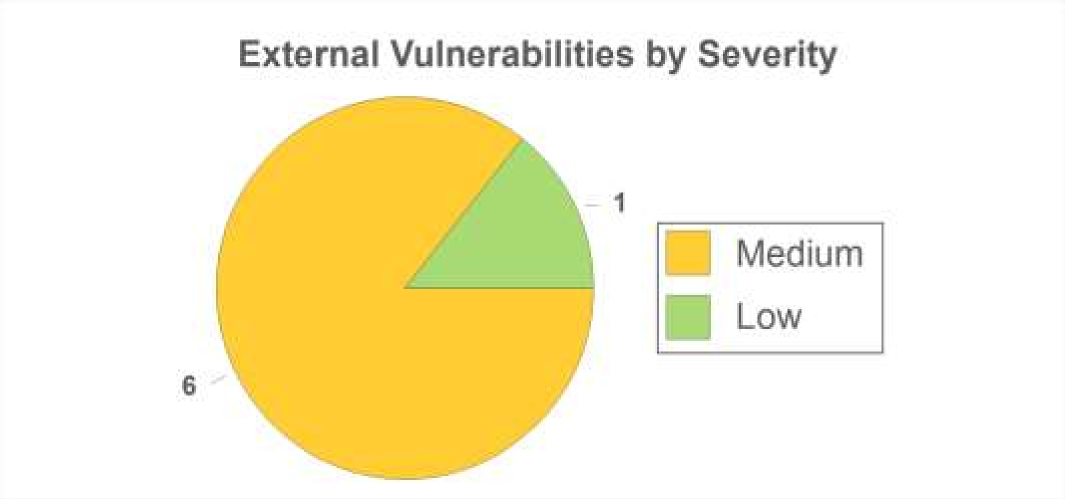
44 applications were removed since the previous assessment.

Major Application	Action	# Computers	% Computers
Google Chrome	Updated	38	81%
Microsoft Office 365 Business - en-us	Installed	38	81%
Microsoft OneDrive	Installed	29	62%
Adobe Acrobat Reader DC	Updated	17	36%
Microsoft Office Home and Business 2013 - en-us	Removed	17	36%
Microsoft OneDrive	Updated	15	32%
Microsoft OneDrive	Removed	12	26%

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)	0	0	0	0	0	0.0
67.18.7.89 (67-18-7-89.atl.business.net)	3	0	6	1	0	5.0
Total: 2	3	0	6	1	0	5.0



Top 5 External Vulnerabilities Found

IP Address	Port	External Vulnerability Description	CVSS Score	Risk Factor	Count
67.18.7.89	80/tcp (http)	**Vulnerability:** The application is missing the 'httpOnly' cookie attribute **Solution:** Set the 'httpOnly' attribute for any session cookie.	5	Medium	1
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

IP Address	Port	External Vulnerability Description	CVSS Score	Risk Factor	Count
67.18.7.89	443/tcp (https)	**Vulnerability:** It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system. **Solution:** It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.	4.3	Medium	1
67.18.7.89	443/tcp (https)	**Vulnerability:** This host is prone to an information disclosure vulnerability. **Solution:** Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+	4.3	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 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.	4.3	Medium	1