Attachment 1

Functional Checklist – Malware Ransom Ware

		Y/N
1)	Software must support both Windows workstation and server operating systems.	
2)	Software / System must provide continuous monitoring, cyber threat hunting and optional reporting and/or preventative actions.	
3)	Software / System should be a fully integrated system that includes malware, ransom ware, internal user monitoring, reporting and prevention.	
4)	Provides a fully integrated system to capture metadata of user interactions with data/files/folders.	
5)	Provides a fully integrated system to collect critical Active Directory events, like logon events and group changes, and telemetry from DNS servers, web proxies, VPN concentrators, and permissions/access control list information.	
6)	Provides a fully integrated system to create detailed audit logs of changes by a suspected hack or internal user allowing the assessment of possible damage quickly. Provide a method to query for all the access activity by any user over any time period to identify all the files or emails they accessed and changes made.	
7)	Provides a fully integrated system to analyze activity information captured as outlined in 4 and 5 above. When the system detects a meaningful deviation from normal behavior, the software will signal that an attack may be underway and can report and automate preventative responses. ** On an attached sheet –**Labeled Function 7** describe a) How the software identifies activity outside the norm b) What is reported c) What is the software's automatic response may be	
8)	Provides a fully integrated system to detect ransom ware that starts encrypting files on accessible file systems. The system should notify IT and shut down the compromised accounts. ** On an attached sheet –**Labeled Function 8** describe a) How the software identifies encrypting activity b) What and how is the activity reported to IT c) How and what accounts will be automatically shut down.	

9) Provides a fully integrated system to examine analyzes file system permissions, user and group relationships, and activity to find overly broad access. The software should also provide the ability to recommend changes to reduce access; additionally the software should allow for the option of making recommended changes. ** On an attached sheet –**Labeled Function 9** describe a) How the software identifies overly broad access b) Defined the structure of what is reported c) Describe the scripting or other method of making changes to access	
10) The software should identify sensitive data content across all file systems and recommend changes to access of shared files and/or servers. Optionally at the direction of Gordon County IT the software can change access of sensitive data. ** On an attached sheet –**Labeled Function 10** describe a) How the software identifies sensitive data b) Defined the structure of what is reported c) Describe the scripting or other method of making changes to access	