PARABLU

# PARABLU TECH NOTE – Security Software white-listing & exclusions

Last updated on: February 26, 2021

## ABSTRACT

Parablu's Endpoint agent has components that execute with elevated privileges, these components are required to be explicitly whitelisted or marked trusted for various security solutions deployed on the desktop. If there is a security solution deployed that has components like –

1. Antivirus
2. Application Protection
3. Exploit Detection/Advance Threat protection
4. Firewalls

If any third-party application locks BluVault application files or folders which contain configuration or logs, it may result in corruption or unexpected behaviour. Then appropriate whitelisting, exceptions, exclusions and trust relationships need to be established accordingly. This is standard practice for most commercial grade backup solutions.

# Antivirus Exclusions

It is important that installation and configuration folders belonging to the BluVault endpoint agent as well as specific executables are added as exclusions in Antivirus settings.

# For WINDOWS:

## EXCLUSIONS

Please exclude/whitelist the following paths in Antivirus admin control:

C:/Users/<userprofile>/AppData/Roaming/ParaBlu/
C:/Program Files (x86)/ParaBlu/
C:/Program Files (x86)/ParaBlu/Snapshots

Similarly, exclude the specific paths and files names mentioned below.

# Path & Conf files

C:/Parablu_EPA

ParabluConfig.conf

# Exe

Parablu_EPA.exe

unins000.exe

ParaLib.exe

BluSync.exe

# VBS

OuickAccess.vbs

hideCommand.vbs

# BAT

InstallParaBluSvc.bat

enableFirewall.bat

DeletePbluService.bat

ParabluInstaller.bat

# Services

ParaBluSvc

VSS (Volume Shadow Server)

# For MAC:

## EXCLUSIONS

Please exclude/whitelist the following path in Antivirus admin control:

/Users/<user profile>/.ParaBlu

/Users/<user profile>/ParaBlu

/Applications/Parablu_EPA.app

/Applications/Parablu_EPA

# Files

Parablu_EPA.dmg

# VSS: Disable On-Demand or Real Time scanning

Antivirus or third-party encryption programs may sometimes lock actively used files or folders of other applications. Specifically, anti-virus programs are known to lock files while running a real time or on-access scan which could result in severely slowing down backup operations and causing high i/o usage on the system being backed up.

On Windows systems, BluVault creates a software snapshot or a VSS (Volume Shadow Service) volume which it uses to read files from.  This ensures a consistent copy of data and allows BluVault to safely backup files even if they are in use by an application.  This software snapshot is like a point-in-time picture of the actual Windows drive or volume and is discarded after the backup is complete.  Several antivirus solutions by default also perform on-demand or real-time scanning on Volume Shadow Service volumes.  It is important to turn this OFF to not have them interfere with the backup process.  Please note that it is perfectly OK to allow scheduled antivirus scanning of the VSS volumes – it is only on-demand or real-time scanning that needs to be disabled.

# Service Whitelisting

BluVault also has a service component which runs as a Windows service under auspices of the Service Control Manager.  It is important that this service be white-listed as a known application, so it is not shutdown or uninstalled by anti-virus application.  Not having this service run could impact BluVault's ability to auto-update the end point agent, backup files that are in use, etc.