Defendpoint Windows Client Release Notes

Software Version: 5.1.149.0 SR1

Document Version: 1.1

Document Date: May 2018

Chapter 1 - Release Notes

For this release, Microsoft Office 2016 should be at version 16.0.6001.1038 or later. Please see Avecto KB article https://connect.avecto.com/community/articles/en_US/Support_KB_Article/Required-Microsoft-Update-for-Office-2016-when-using-Defendpoint-v4-3-118-and-above and Microsoft KB article: https://support.microsoft.com/en-gb/kb/3104401 for more information.

- **New Features** detailed below
- **Bug Fixes** detailed below

You need to restart all endpoints managed by Defendpoint after upgrading to this version of Defendpoint to ensure policy is correctly applied.

1.1 - New Features

72507 - Added support for Trusted Application Protection (TAP) DLL audit events for endpoints being managed by iC3 version 2.0 and above. The following TAP DLL audit events are now sent to iC3 2.0 and above from the endpoint:
706 - Passive Event
716 - Blocked
720 - Canceled

1.2 - Bug Fixes

77416 - Hardened the security for the Defendpoint hook load mechanism by removing the reliance on global mutexes. This does not affect the management of, or the user experience of, Defendpoint. This addresses CVE-2017-16245.

75951 - Hardened security by migrating the Defendpoint Application Control feature from user mode to kernel mode. This does not affect the management of, or the user experience of, Defendpoint. This addresses CVE-2017-16246.

54821 - Added support for Swedish in the on-demand options to 'Run as' and 'Run as administrator'.

72106, 72539, 74152 - Application rules are now correctly applied when an application is run from a network path.

73972 - Anti-tamper has been improved to protect the Defendpoint client from a WMIC uninstall.

76474 - All events are now correctly forwarded and displayed in iC3 irrespective of time-zone.

80880 - Improved the reliability of command line parsing for batch files. As part of this change we have hardened our approach to matching for batch files. When using the 'start' command line switch, Defendpoint does not match any rules for subsequent batch files. This is in line with the existing '\K' command line switch functionality.

81499 - Added a check to ensure computer level environment variables cannot be overridden by user defined environment variables. This addresses CVE-2018-10959 reported by the Lockheed Martin Red Team.

Chapter 2 - Supported Operating Systems

- **Privilege Management/Application Control Support** detailed below
- **Content Isolation** detailed below

2.1 - Privilege Management/Application Control Support

These platforms are supported with the latest service pack or update is applied.

Platforms
- Windows 7
- Windows 8 and 8.1
- Windows 10 builds 1507, 1607, 1703, and 1709
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

2.2 - Content Isolation

These platforms are supported with the latest service pack or update is applied.

Platforms
- Windows 7
- Windows 8 and 8.1
- Windows 10 builds 1507, 1607, 1703, 1709
- Windows Server 2008 R2
- Windows Server 2012 and 2012 R2
- Windows Server 2016

Primary Application Support
- Internet Explorer 8+
- Google Chrome
- Microsoft Office Word 2007/2010/2013/2016
- Microsoft Office Excel 2007/2010/2013/2016
- Microsoft Office PowerPoint 2007/2010/2013/2016
- Microsoft Office Outlook 2007/2010/2013/2016
- Adobe Reader 10+
- Zip Archivers (Winzip, WinRAR, Windows Compressed Folders)

If you are upgrading Defendpoint you may need to update your workstyles to incorporate newly supported features/applications.

Chapter 3 - Prerequisites

- **Defendpoint Client** detailed below
- **Defendpoint Activity Viewer** detailed below

3.1 - Defendpoint Client

- .NET Framework 2.0 (Required to run PowerShell audit scripts)
- Micosoft SQL Server Compact 3.5 SP2
- The McAfee Agent must be installed if you are installing the Defendpoint client with switch EPOMODE=1

3.2 - Defendpoint Activity Viewer

- Microsoft SQL Server Compact 4.0
- Microsoft .NET Framework 4.0 Client

Notes

The executable version of the client package includes all necessary prerequisites (excluding .NET Framework 2.0), and automatically installs them as necessary.

The Defendpoint Client executable installer automatically installs Microsoft SQL Server Compact 3.5 SP2. If you do not wish to use the Activity Viewer, and do not wish for this prerequisite to be installed, we recommend you install the Defendpoint Client MSI installation.

Chapter 4 - Version History

4.1 - 5.1.95.0 GA

4.1.1 - New Features

69356 - Added a new 'Uninstaller' Application Type. This feature allows end users to uninstall applications from machines managed by Defendpoint.

73305 - Added Support For Windows 10 version 1709.

4.1.2 - Bug Fixes

37022, **51595**, **70376**, **76273** - You can now run applications as a different user when you have a policy in place to elevate applications that have generated a UAC prompt.

54257, **54734**, **73099** - These bugs have been addressed by the new uninstall capability in this release using the native Windows Programs and Features functionality.

74360, **74387** - Compatibility issues between Docker for Windows and Defendpoint have been resolved.

74595, **74596**, **74827** - Defendpoint now correctly elevates 'Windows PowerShell (Admin)' from the start menu when an application rule is in place that targets it.

74598 - Information is now correctly audited from files that have been run from a network share.

74659, **74660** - You can now use the on-demand rule to elevate Device Manager from the Control Panel.

74663, **74666** - MSIs with child processes are now correctly elevated according to Defendpoint policy when using the '/qn' command line switch.

74751 - Fixed an issue that caused attributes to be missing within MSI audit events.

76388 - Added an engineering setting to the Defendpoint Client that allows specific processes to be excluded in the event that incompatibilities with Defendpoint are encountered. For more information, please refer to Avecto Support.

76353 - Fixed an issue that caused the Windows Store application to crash if it was elevated using Defendpoint with Windows 10 build 1709.

76786 - Fixed an issue that caused Internet Explorer to open minimized on the task bar.

4.2 - 5.0.102.0 GA

4.2.1 - New Features

61293 – Added a new QuickStart template for Defendpoint configuration. This is a best practice configuration consisting of three layers of workstyles with different levels of flexibility.

67887 – Added the ability to show and hide Sandboxing specific controls in the Policy Editor.

67890, **68472** – Added two new templates for Trusted Application Protection (TAP); High Flexibility and High Security. These provide additional protection for applications (such as document readers and web browsers) that are commonly used to deliver malware. These templates automatically prevent untrusted executable, script and DLL payloads from being executed from web pages and documents.

4.2.2 - Enhancements

68711 – There have been several branding updates throughout the product.

68974 – Defendpoint works when Windows Control Flow Guard is enabled.

73544 – Defendpoint can now match on the Avecto Zone Identifier.

4.2.3 - Bug Fixes

39857, **48539**, **55970** – Defendpoint now correctly displays information in the event viewer when Media from Netflix or Amazon Video is blocked because 'mfpmp.exe' isn't allowed to execute due to policy.

69319 – Fixed signature verification checks for remote PowerShell scripts.

74642 - Conflicts between Defendpoint and Hyper-V have been resolved so that virtual machines start correctly.

71665 - Fixed an issue that caused Internet Explorer to fail to run sandboxed on a clean installation of Windows 10.

72815 – The SQL Server Express service now starts correctly.

61231, **72989**, **67147** – Wildcards in the 'Does not match publisher' criteria are now correctly matched for applications.

4.2.4 - Known Limitations

There are two circumstances in which the Avecto Zone Identifier is not applied by Avecto when the user downloads a file from the browser:

- Files that are compressed in a zip file. The zip file itself is tagged with the Avecto Zone Identifier tag.
- Files that are downloaded directly to a mapped network drive. The Avecto Zone Identifier tag is applied when you save the file to your local drive first before moving it to a mapped network drive.

This means that you cannot match on the Avecto Zone Identifier tag in the above scenarios.