

Privilege Management for Windows and Mac 5.5

(formerly Avecto Defendpoint)

New and Updated Features (November 2019)

BeyondTrust [Privilege Management for Windows and Mac](#) (formerly Defendpoint) reduces the risk of privilege misuse by assigning privileges only to authorized tasks that require them, controlling application and script usage, as well as logging, monitoring, and reporting on privileged activities. By providing fine-grained control over privileged access, IT protects users while improving the efficiency of least privilege management.

PMWM 5.5 includes improvements to existing features, as well as a brand-new capability to BeyondTrust's market leading Privilege Management for Mac.

[Please see the release notes](#) for additional details on these important enhancements.

NEW FEATURE HIGHLIGHTS

Mac - Homebrew/Shell Script Support

Brand new to PMWM 5.5 is support for Homebrew and Shell Scripts. This innovative feature provides important capabilities for developers and sysadmins on Mac, who need to execute scripts, or use applications like Homebrew that execute scripts, when logged in as a non-admin user.

Through Shell Script support, all Sudo commands executed by Shell Scripts are fully audited by PMWM through BeyondInsight, Privilege Management Console (formerly iC3), McAfee ePolicy Orchestrator, and also audited to the local Syslog, giving a complete and actionable audit trail of all Sudo activity, and the script that the Sudo command originated from.

Enterprises can now empower developers and sysadmins by allowing them to execute Shell Scripts and use applications like Homebrew while logged in and protected by a standard user account, dramatically increasing security for your organization without reducing productivity.

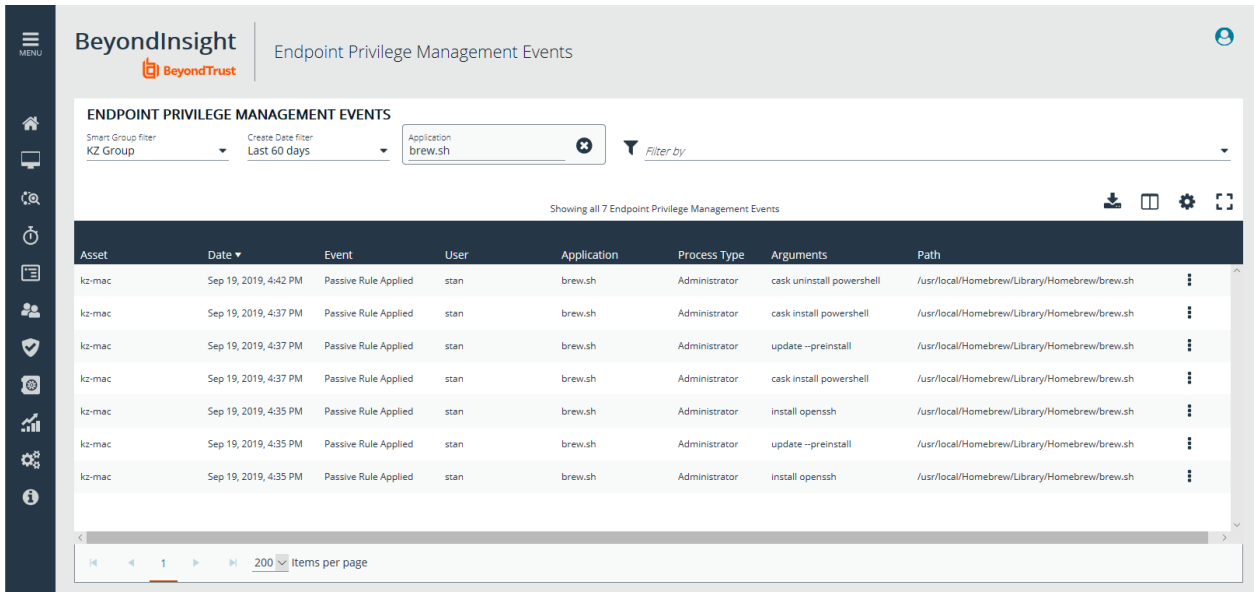


Figure 1: BeyondInsight – Full auditing and transparency of script commands and arguments

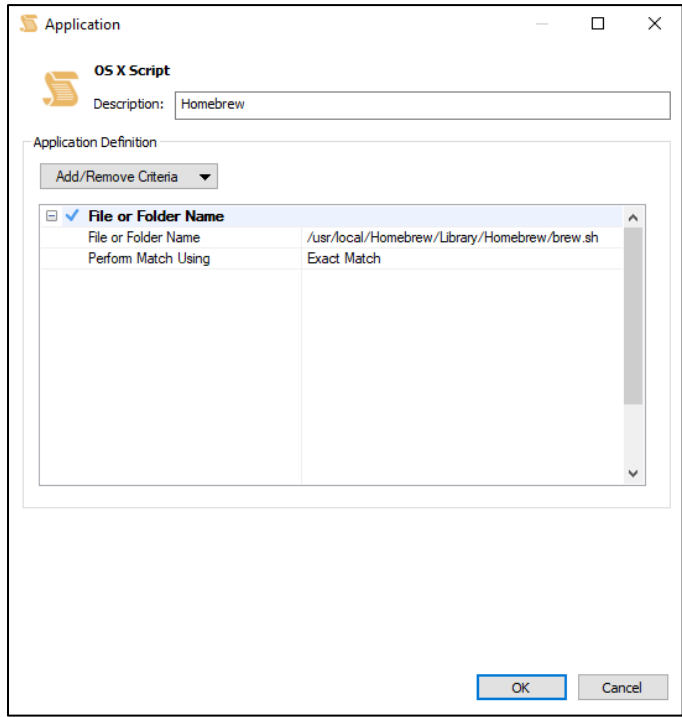


Figure 2: PMWM – Adding a rule that authorizes Sudo commands for the Homebrew script

Windows – Enhanced protection for Open/Save file dialogs

PMWM brings a feature enhancement to file dialog protection by ensuring that File Open/File Save dialogs cannot be used to run applications with child inheritance. This enhancement ensures that applications run in this way by users will not match as a child rule, and therefore not inheriting the same elevation rights as it's parent process.

New Platform Support

Support for the following platforms has been added in this release:

- Windows 10 19H2
- Windows Server 2019 Core
- macOS 10.15 Catalina