

McAfee Application Control

Reduce risk from unauthorized applications to control endpoints, servers, and fixed devices.

Advanced persistent threats (APTs) via remote attack or social engineering make it increasingly difficult to protect your business. McAfee® Application Control helps you outsmart cybercriminals and keeps your business secure and productive. Using a dynamic trust model and innovative security features such as local and global reputation intelligence, real-time behavioral analytics, and auto-immunization of endpoints, this McAfee solution immediately thwarts APTs—without requiring labor-intensive list management or signature updates. If you have zero tolerance for zero-day threats, take a closer look at McAfee Application Control.

Intelligent Whitelisting

McAfee Application Control prevents zero-day and APT attacks by blocking execution of unauthorized applications. Using our inventory feature, you can easily find and manage application-related files. It groups binaries (.EXEs, DLLs, drivers, and scripts) across your enterprise by application and vendor, displays them in an intuitive, hierarchical format, and intelligently classifies them as well-known, unknown, and known-bad applications. Using whitelisting, you can prevent attacks from unknown malware by allowing only known-good whitelisted applications to run.

Implement the Right Security Posture

As users demand more flexibility to use applications in their social and cloud-enabled business world, McAfee Application Control gives organizations three options to maximize their whitelisting strategy for threat prevention as illustrated here.



Figure 1. Three ways to maximize your whitelist strategy.

Key Advantages

- Protect against zero-day and APTs without signature updates.
- Take advantage of McAfee Global Threat Intelligence and McAfee Threat Intelligence Exchange to provide global and local reputation of files and applications.
- Strengthen security and lower ownership costs with dynamic whitelisting that automatically accepts new software added through your trusted channels.
- Efficiently control application access with McAfee® ePolicy Orchestrator® (McAfee ePO™) software, a centralized platform for management of McAfee security solutions.
- Reduce patch cycles through secure whitelisting and advanced memory protection.
- Keep systems current with the latest patches using trusted updaters.
- Enforce controls on connected or disconnected servers, virtual machines, endpoints, fixed devices such as point-of-sale terminals, and legacy systems such as Microsoft Windows XP.

Powerful, Built-In Suggestions

Using inventory search and pre-defined reports, you can quickly find and fix vulnerability, compliance, and security issues in your environment. You can discover useful insights, such as recently added applications, uncertified binaries, files with unknown reputations, systems running outdated versions of software, and more to quickly pinpoint vulnerabilities and validate compliance of software licenses.

Complete and Fast Response

Whitelisting is enhanced with global threat intelligence from McAfee Global Threat Intelligence (McAfee GTI), an exclusive McAfee technology that tracks the reputation of files, messages, and senders in real time using millions of sensors worldwide. McAfee Application Control uses this knowledge to determine the reputation of files in your computing environment, classifying them as good, bad, and unknown.

When deployed with McAfee Threat Intelligence Exchange, an optional module sold separately, McAfee Application Control updates the whitelist based on local reputation intelligence to combat threats instantly. Using McAfee Threat Intelligence Exchange, McAfee Application Control coordinates with McAfee Advanced Threat Defense to dynamically analyze the behavior of unknown applications in a sandbox and automatically immunizes endpoints from newly detected malware.

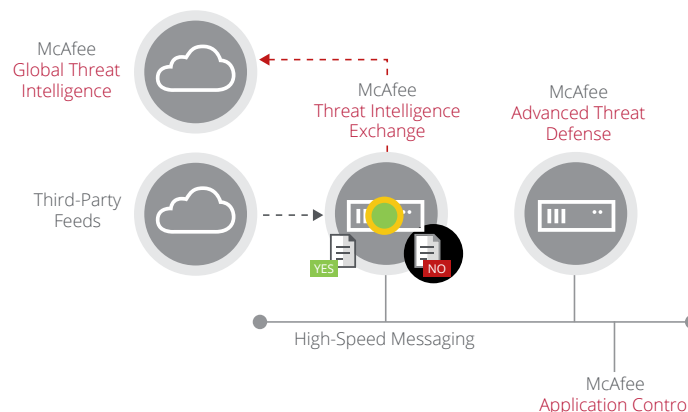


Figure 2. McAfee GTI constantly monitors the reputation of files and senders. When deployed with McAfee Threat Intelligence Exchange, McAfee Application Control automatically updates the whitelist based on local reputation intelligence and can coordinate with McAfee Advanced Threat Defense if more information on a file is needed.

No Impact on Business Continuity

To avoid interference with business continuity, new applications are automatically allowed based on application reputation. For unknown applications, a suggestions interface recommends new update policies based on execution patterns at endpoints. This is an excellent way to manage exceptions generated by blocked applications. After inspecting exceptions and details of the blocked application, simply approve and whitelist the file or ignore it to block the application.

Key Advantages (continued)

- Allow new applications based on application rating or self-approval for improved business continuity.
- Maintain user productivity and server performance with a low-overhead solution.
- Easily protect legacy systems and modern technology investments.

Supported Platforms

Microsoft Windows (32-bit and 64-bit)

- Embedded: XPE, 7E, WEPOS, POSReady 2009, WES 2009, 8, 8.1 Industry, 10
- Server: 2008, 2008 R2, 2012, 2012 R2
- Desktop: NT, 2000, XP, Vista, 7, 8, 8.1, 10

Linux

- Red Hat/CentOS 5, 6, 7
- SUSE/openSUSE 10, 11
- Oracle Enterprise Linux 5, 6, 7
- Ubuntu 12.04

DATA SHEET

Help Users Become Part of the Solution

For unknown applications, McAfee Application Control provides IT with multiple ways to enable users to install new applications:

- **User notifications**—Users can receive informative pop-up messages explaining why access to unauthorized applications is not allowed. These messages prompt users to request approvals via email or helpdesks.
- **User self-approvals**—Users with this privilege can install new software without waiting for an IT approval. IT can inspect these self-approvals and create enterprise-wide policies to either ban the app or permit the app on all systems.

Keep Your Systems Up-to-Date

We understand that keeping your systems current with the latest patch is important. That's why we offer a Dynamic Trust Model to automatically update your systems without impacting business continuity. Keep your systems up to date using trusted users, certificates, processes, and directories. McAfee Application Control also prevents whitelisted applications from being exploited via memory buffer overflow attacks on Microsoft Windows 32- and 64-bit systems.

Get Advanced Execution Control

For enhanced protection, McAfee Application Control lets you combine rules based on file name, process name, parent process name, command line parameters, and user name. You can use advanced execution control to stop attacks that bypass file input/output (I/O), block interactive mode for system interpreters, and prevent exploitation by system tools. Plus, you get the stronger and more robust SHA-256 algorithm for creating policies.

McAfee ePolicy Orchestrator Software: A Single Pane of Glass

McAfee ePO software consolidates and centralizes management, providing a global view of enterprise security—without blind spots. This award-winning platform integrates McAfee Application Control with McAfee Host Intrusion Prevention, and other McAfee security products, including anti-malware for blacklisting. Single-step installation and update of McAfee Application Control deployment can be done from Microsoft System Center as well.

Watch and Learn in Observation Mode

Observation mode helps you discover policies for dynamic desktop environments without enforcing a whitelisting lockdown. It lets you gradually deploy McAfee Application Control in pre-production or early-production environments without breaking applications. Through McAfee Application Control, administrators can use a single policy discovery page for defining policies for observations and self-approval requests.

DATA SHEET

Protect Legacy Systems and Recent Technology Investments

Need to protect older operating systems, such as Microsoft Windows NT, 2000, and XP? Although Microsoft and other security vendors don't support these legacy systems, McAfee Application Control has you covered. Plus, McAfee Application Control supports your latest operating systems, such as Microsoft Windows 10.

Next Steps

For more information, visit <http://www.mcafee.com/us/products/application-control.aspx> or call us at 1 888 847 8766, 24 hours a day, seven days a week.



2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC.
2183_1216
DECEMBER 2016