McAfee Application Control

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

Advanced persistent threats via remote attack or social engineering make it increasingly difficult to protect your business. McAfee® Application Control software helps you outsmart cyberthugs and keeps your business secure and productive. This centrally managed whitelisting solution uses a dynamic trust model and innovative security features that block unauthorized applications and foil advanced persistent threats (APTs)—without labor-intensive lists to manage. If you have zero tolerance for zero-day threats, take a closer look at McAfee Application Control.

Key Advantages

- Protect against zero-day and APTs without signature updates.
- Uses McAfee Global Threat Intelligence (McAfee GTI) to provide reputation of files and applications within enterprise.
- Strengthen security and lower ownership costs with dynamic whitelisting.
- Efficiently control application access with McAfee® ePolicy Orchestrator® (McAfee ePO™) software's centralized management platform.
- Reduce patch cycles through secure whitelisting and advanced memory protection.
- Enforce controls on connected or disconnected servers, virtual machines (VMs), endpoints, and fixed devices such as point-of-sale terminals.
- Automatically accept new software added through your authorized processes.

McAfee Application Control software provides complete protection from unwanted applications and code—blocking advanced threats without requiring signature updates. It lets you consistently enable the known good, block the known and unknown bad, and properly administer new software. Our dynamic whitelisting trust model reduces costs by eliminating expensive manual support requirements associated with other whitelisting technologies.

One Inventory. No Guesswork.

You don't need to be a detective to find and manage application-related files. Our application inventory feature groups all binaries (EXEs, DLLs, drivers, and scripts) across your enterprise by application and vendor, displaying them in an intuitive, hierarchical format. Applications are classified as well-known, unknown, and known bad. Plus, you can easily search for useful insights, such as applications added this week, uncertified binaries, files with unknown reputations, systems running outdated versions of Adobe Reader, and more to quickly pinpoint vulnerabilities and validate compliance of software licenses.

Help Users Become Part of the Solution

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.

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 software with McAfee Host Intrusion Prevention, McAfee Firewall, and other McAfee security and risk management products. In addition, single-step installation and update of McAfee Application Control deployment

can be done from Microsoft System Center. Furthermore, McAfee ePO software can easily embrace products from McAfee Security Innovation Alliance Partners, as well as your home-grown management applications.

Key Advantages (continued)

- Discover trusted updater policies before having to deploy whitelisting in an enterprise.
- Provide flexibility to desktop users by optionally allowing them to approve new applications.
- Maintain user productivity and server performance with a low-overhead solution.
- Easily protect unsupported legacy systems, such as Microsoft Windows NT, 2000, and XP.
- Integrates with McAfee ePO console for centralized IT management.

Supported Platforms

Microsoft Windows (32-bit and 64-bit)

- Embedded: XPE, 7E, WEPOS, Pos Ready 2009, WES 2009, 8, 8.1 Industry
- Server: 2008, 2008 R2, 2012, 2012 R2
- Desktop: Vista, 7, 8, 8.1

Linux

- RHEL/CentOS 5, 6
- SUSE/openSUSE 10, 11
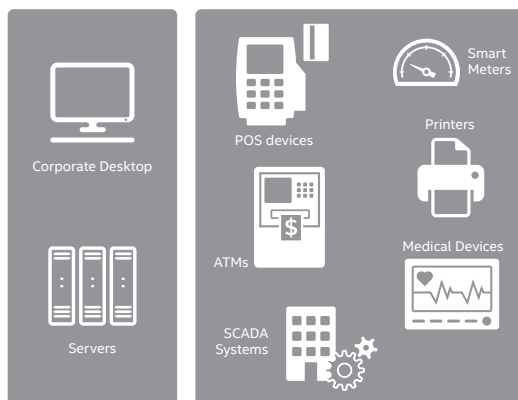- OEL 5, 6
- Ubuntu 12.04

Figure 1. In addition to desktops and servers, McAfee Application Control software extends protection to fixed-function devices to significantly reduce consumer risk.

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 software in pre- or early-production environments without breaking applications. Through McAfee Application Control, admins can use a single policy discovery page for defining policies for observations and self-approval requests.

Powerful Suggestions Are Built In

McAfee Application Control software includes a suggestions interface that recommends new update policies based on execution patterns at the endpoints. It's an excellent way to manage exceptions generated by blocked applications. Simply inspect the exceptions and the details of the blocked application. Then, either approve and whitelist the file or ignore it when the application is meant to be blocked.

Figure 2. Secure update flow.

Protect Legacy Systems

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 software has you covered.

Minimize Patching and Protect Memory

McAfee Application Control software works with McAfee Host Intrusion Prevention to sandbox traffic entering and leaving greylisted applications. This validated countermeasure allows you to delay patch deployment until your regular patch cycle. McAfee Application Control software also prevents whitelisted applications from being exploited via memory buffer overflow attacks on Windows 32- and 64-bit systems.

McAfee GTI Integration: The Smart Way to Deal with Global Threats

McAfee GTI is an exclusive McAfee technology that tracks the reputation of files, messages, and senders in real time using millions of sensors worldwide. McAfee Application Control software uses this cloud-based knowledge to determine the reputation of all files in your computing environment, classifying them as good, bad, and unknown. GTI reputation tracking is able to operate both in secure, isolated environments as well as connected infrastructures. With McAfee GTI integration, you'll know with certainty when any malware has been inadvertently whitelisted.
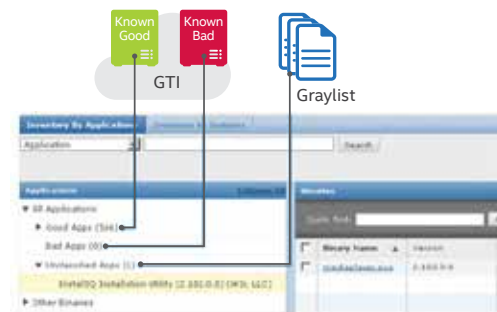
Small Footprint and Overhead

McAfee Application Control is a low-overhead software solution:

- Easy setup and low initial and ongoing operational overhead.
- Negligible memory usage.
- No file scanning that could impact system performance.
- Works in disconnected and in offline mode.
- Requires no signature updates.

Figure 3. McAfee Global Threat Intelligence constantly monitors the reputation of files and senders, allowing automatic blocking of known bad files and greylisting of those with no known reputation.

Next Steps

McAfee Application Control software provides an effective way to block unauthorized applications and code on servers, corporate desktops, and fixed-function devices. This centrally managed whitelisting solution uses a dynamic trust model and innovative security features that thwart advanced persistent threats—without requiring signature updates or labor-intensive list management. Protect systems from unknown, advanced persistent threats with centrally managed whitelisting with McAfee Application Control today.