Data Sheet

McAfee Application Control for Desktops

Improve protection, gain application visibility, and reduce patching cycles without impacting enterprise desktop performance.

Desktops pose formidable security challenges for corporate IT staff—complicated in no small part by end users inadvertently downloading malicious software. But the real problem is the new types of advanced persistent threats (APTs) constantly targeting users. APTs use social networking and other attack methods to dupe users into loading untrustworthy utilities, extensions, and applications. As a part of the Intel® Security product offering, McAfee® Application Control for Desktops adds a vital layer of security—beyond antivirus—to protect standardized, IT-controlled desktop systems while keeping users and IT staff productive.

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 the 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.
- 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 applications, block the known and unknown bad, and properly administer new software.

Improve Protection

Effective desktop management requires the use of a standardized, IT-controlled operating environment. Securing these systems also involves best practices for antivirus, intrusion protection, and other technologies to block viruses, worms, Trojans, spam, adware, spyware, and other known malware.

But what about unknown threats? Polymorphic malware, APTs, and zero-day threats are often delivered under the guise of legitimate applications. The best way to address these threats is to limit access to applications that are known to be trustworthy through application whitelisting. That's why McAfee believes the best strategy for endpoint security is the perfect blend of anti-malware scanning and dynamic application control. McAfee Application Control for Desktops uses a unique, centrally managed dynamic whitelisting trust model that reduces costs by eliminating expensive end-user support requirements associated with other whitelisting technologies.

McAfee GTI integration: The smart way to deal with global threats

McAfee GTI is an exclusive McAfee technology that tracks the reputations of files, IPs, and websites in real time using millions of sensors worldwide. McAfee Application Control software uses this cloud-based knowledge to determine the reputations of all files in your computing environment, classifying them as good, bad, and unknown. With McAfee GTI integration, you'll know with certainty when any malware has been inadvertently whitelisted.

intel Security

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
Ubuntu 12.04

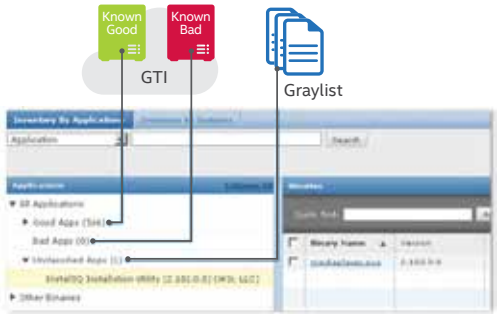

Figure 1. McAfee GTI constantly monitors the reputation of files, allowing blocking of known bad files and greylisting of those with no known reputation.

One Inventory, No Guesswork

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. This feature is great for quickly pinpointing vulnerabilities and validating compliance of software licenses.

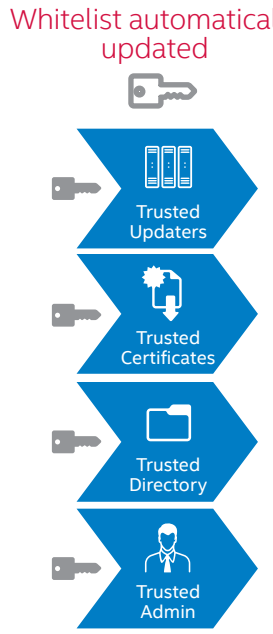

Figure 2. Secure update flow.

Gain Visibility of Application Usage

Watch and learn in observation mode
Observation mode helps you discover policies for dynamic desktop environments prior to whitelist activation. It lets you gradually deploy McAfee Application Control software—and discover new trusted updaters—without disrupting 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 for Desktops software includes a suggestions interface that recommends new update policies based on execution patterns at the endpoints. In addition, you can choose flexible policies for different users who may require higher controls or less oversight.

Help Users Become Part of the Solution with User Self-Approvals

Sometimes users need access to applications that are not yet corporate-approved. In these instances, users install new software without waiting for an IT approval.

IT inspects these self-approvals and creates enterprise-wide policies to either ban the application or permit it on all systems. Users who cannot self-approve will 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.

Figure 3. Users attempting to install unapproved applications are presented with a Self-Approval Request box, including notification that their request is pending IT staff approval. Upon approval, applications are easily added to the whitelist, avoiding future requests.

Reduce Patch Panic

McAfee Application Control for Desktops works with McAfee Host Intrusion Prevention to prevent remote memory-based threats. This validated countermeasure allows you to delay patch deployment until your regular patch cycle.

McAfee ePO Software: Security Management Through a Single Pane of Glass

McAfee ePO software consolidates and centralizes management, providing a global view of enterprise security—without blind spots. This powerful security management platform integrates McAfee Application Control for Desktops 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 homegrown management applications.

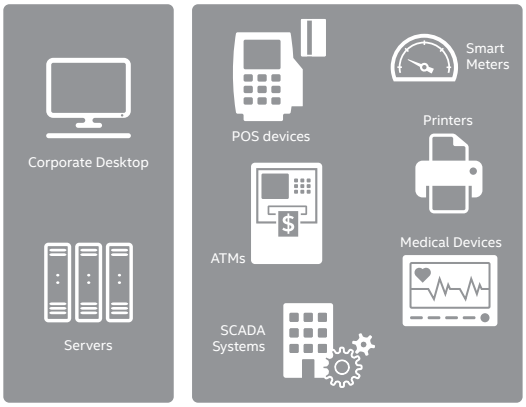

Figure 4. In addition to desktops, McAfee Application Control software is available to protect servers and fixed-function devices to significantly reduce risk for a wide variety of applications.

Next Steps

McAfee Application Control for Desktops provides an effective way to block unauthorized applications and code on corporate desktops and notebooks. 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.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com