McAfee Advanced Threat Defense

Advanced detection for stealthy, zero-day malware

McAfee addresses three key requirements needed to solve today's advanced malware problem: *Find*, *freeze*, and *fix*. McAfee® Advanced Threat Defense *finds* advanced malware and integrates with McAfee network products to *freeze* the threat while McAfee Real Time software initiates *fix* or remediation actions.

McAfee Advanced Threat Defense Key Differentiators

Tight McAfee solution integration

- Streamlines detection and protection across multiple channels and expedites response and remediation.

Powerful advanced malware analysis capabilities

- Strong unpacking enables better, more complete analysis.
- Advanced static code and dynamic analysis together provide more accurate detection with unparalleled analysis data.

Broad operating system support

- Analyze threats under the same conditions as the actual host profile, reducing the chances of missed malware or false positives.

Centralized malware analysis

- Shared analysis instance simplifies deployment and reduces the number of required devices across the network.

McAfee Advanced Threat Defense: *Find* Advanced Malware

McAfee Advanced Threat Defense detects today's stealthy, zero-day malware with an innovative, layered approach. It combines low-touch antivirus signatures, reputation, and real-time emulation defenses with in-depth static code and dynamic analysis (sandboxing) to analyze actual behavior. Combined, this represents the strongest advanced malware security protection in the market and effectively balances the need for both protection and performance.

While lower analytical intensity methods such as signatures and real-time emulation benefit performance, the addition of full static code analysis to sandboxing provides detailed malware classification information and broadens protection against highly camouflaged, evasive threats and allows identification of associated malware leveraging code re-use. Delayed or contingent execution paths, often not executed in a dynamic environment, can be detected through unpacking and full static code analysis.

Packing changes the composition of the code or hides it to evade detection. Most products cannot properly unpack, but it is the only way to reveal the original (source) executable code for analysis. McAfee Advanced Threat Defense includes extensive unpacking capabilities that remove obfuscation, exposing the original executable code. It enables static code analysis to look beyond high-level file attributes for anomalies and to reverse engineer the code, analyzing all the attributes and instruction sets to determine the intended behavior.

Since advanced and targeted attacks are often designed to evade detection when sandboxing is attempted, McAfee Advanced Threat Defense includes comprehensive techniques to ensure the most code execution possible during dynamic analysis.

Together, static code and dynamic analysis provide a complete evaluation and detailed information such as behavior summary, malware severity, malware family associations, execution paths, and percentage of code executed during dynamic analysis.

Target-specific sandboxing increases detection accuracy

McAfee further advances *find* capabilities by giving administrators the ability to upload and analyze objects through a collection of custom virtual machines or gold images. This enables organizations to analyze threats under the conditions of the actual host profile within the organization, rather than a generic image, providing a more accurate risk assessment.

Because an organization may have multiple host profiles (gold images) operating in the same network, McAfee Advanced Threat Defense queries McAfee ePO software to determine the hosts' operating system and list of applications, only analyzing suspect files under the conditions of the target host.

Freeze the threat

Finding advanced malware is important. But if that is all a solution can do—provide a report on advanced malware that has already infected an organization—administrators are left with massive amounts of work and the network is still unprotected.

Tight integration between McAfee Advanced Threat Defense and network security devices, such as McAfee Network Security Platform, McAfee Email Gateway, or McAfee Web Gateway, enables immediate action when McAfee Advanced Threat Defense convicts a file as malicious. This tight and automated integration between *find* and *freeze* is critical.

McAfee network security solutions immediately block any other copies of this file coming into the network, without the need to send it on for further analysis. In addition, McAfee Network Security Platform can quarantine an infected host, preventing the spread of malicious activity in the network.

Initiate *fix*: From a single host to an entire network of machines

To *fix* an attack, coordination with endpoint solutions to remediate any damage done to the host is needed. Due to the stealthy nature of advanced malware, administrators must be able to look across all endpoints, assess where similar damage occurred, and take action. This is not simply searching for a specific malicious file (for example, file search across all endpoints). Looking for specific changes (for example, DLL or configuration changes) done to the host is also necessary to ensure you really *fix* the problem. After all, good malware does its best to hide its tracks.

Initiate *fix* with McAfee Real Time

From a central console, administrators can *fix* discovered issues related to malware found by McAfee Advanced Threat Defense within seconds. Immediate corrective action can be taken on all (or a subset) of the endpoints by simply clicking a button to target action to those machines. Corrective action can include:

- Kill the application or process.
- Delete/Modify/Create registry keys.
- Delete/Modify/Create file and/or directory.

Deployment

McAfee Advanced Threat Defense can be deployed either as a stand-alone malware appliance or one that seamlessly fits into your existing McAfee network security investment (McAfee Network Security Platform, McAfee Email Gateway, or McAfee Web Gateway). Files are sent directly from an existing network security device to McAfee Advanced Threat Defense, which is deployed as a proxy in the network. McAfee Advanced Threat Defense acts as a shared resource between multiple McAfee network devices, cost-effectively scaling across the network.

For information or to start an evaluation of McAfee Advanced Threat Defense, contact your McAfee representative or visit www.mcafee.com/atd.

McAfee Advanced Threat Defense Specifications	ATD-3000	ATD-6000
Form Factor	1U Rack-Mount	2U Rack-Mount
Performance	Up to 150,000 objects per day	Up to 250,000 objects per day
Detection	ATD-3000/ATD-6000	
File/media types support	PE files, Adobe files, MS Office Suite files, Archives, Java	
Analysis methods	McAfee Anti-malware, GTI file reputation, Gateway Anti-malware (emulation and behavioral analysis), dynamic analysis (sandboxing), static code analysis	
Supported OS	Win 7 (32-bit/64-bit), Win XP; Win Server 2003, Win Server 2008 (64-bit); Android	

McAfee
An Intel Company

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

61050ds_atd_0414_kg