

McAfee Deep Defender

Security beyond the OS to expose and eliminate covert threats

Key Points

- Kernel-level behavioral monitoring exposes and removes unknown threats, including rootkits, to preempt zero-day malware
- First-of-its-kind integration with Intel resides between the memory and OS to perform real-time memory and CPU monitoring
- Managed with McAfee ePO software for efficient deployment, centralized policy management, improved threat visibility, and unified reporting
- Removes low-level threats that traditional OS-based protection cannot detect, lowering re-imaging and remediation costs and enhancing overall security
- Stealthy malware is escalating: McAfee Labs™ identifies nearly 110,000 new unique rootkits each quarter

“One of the most important things to understand about stealthy malware like that in Stuxnet and Zeus is that it truly owns the computers it takes over. Through rootkits that operate at the user and kernel and firmware levels, malware can hide, replicate, protect itself against being overwritten, and deactivate antivirus and other defenses.”

—David Marcus, McAfee Labs, and Thom Sawicki, Intel, *The New Reality of Stealth Crimeware*, <http://www.mcafee.com/stealthcrimeware>

Stealthy malware has become a cybercrime tool of choice, with more and more new and unknown malware using cloaking techniques such as rootkits. Criminals rely on this low-level code to evade operating system (OS)-based protections. McAfee® Deep Defender™ helps you fight back with a new generation of hardware-assisted security enabled by McAfee® DeepSAFE™ technology. This behavioral monitoring of real-time kernel operations reveals and removes advanced, invisible attacks. Integrated with McAfee ePolicy Orchestrator® (McAfee ePO™) software and McAfee Global Threat Intelligence™ (McAfee GTI™), McAfee Deep Defender makes it easy to extend system security beyond the operating system (OS) to preempt covert zero-day threats.

Enterprise endpoints are easy prey for stealthy malware that can maneuver around antivirus and other operating system-based defenses. Criminals design this low-level malware to exploit the inherent security weaknesses of the OS, hiding its presence so that the system appears normal as it boots up.

The invisible malware is free to spread infection, deactivate countermeasures, and steal network credentials or confidential information. Restoration for compromised endpoints requires full re-imaging, which takes IT and end-users away from productive tasks for hours per event.

Beyond the operating system

McAfee and Intel have teamed up to defeat these attacks with hardware-enabled protection that operates between the CPU and the OS, protecting components that reside in physical memory. McAfee Deep Defender gains a trusted view of the drivers and other software as they operate and can detect and clean threats that load before, during, and after the OS.

Real-time memory and CPU monitoring

McAfee Deep Defender utilizes McAfee DeepSAFE® technology, a memory software layer executing in VMX-root mode, to provide real-time kernel memory and CPU event protection with minimal performance impact.

This low-level visibility allows McAfee Deep Defender to recognize evasive techniques employed by stealthy malware and gives administrators a real-time view of memory processes, enabling configurable block or deny actions. If a rootkit or stealth malware is active, McAfee DeepSAFE will catch the attempt to modify the kernel.

True zero-day protection

McAfee Deep Defender requires no prior knowledge of the rootkit to detect its existence. Instead, McAfee Deep Defender identifies its malicious behavior, providing true zero-day protection.

McAfee Deep Defender protects before a rootkit has a chance to conceal malware. Its kernel and memory protection includes:

- Preventing and logging write attempts to the system's interrupt descriptor table (IDT) and the system service dispatch table (SSDT)
- Stopping changes to the processor system transitioning table
- Preventing modifications to the direct kernel object manipulation (DKOM) list and threads
- Eliminating malicious attachments to kernel mode drivers
- Prohibiting malicious inline hooking to kernel code sections along with key device drivers

System Requirements and Specifications

- Supports Intel® Core i3, i5, and i7 processors
- Supports Windows 7; 32- and 64-bit
- 2 GB RAM (32-bit) or 4 GB RAM (64-bit)
- Managed by McAfee ePO software 4.5 or higher
- Intel Virtualization Technology (VT) enabled in BIOS
- Internationalized and localized for deployment worldwide

Tested for compatibility with the following McAfee products:

- McAfee VirusScan Enterprise 8.7 or higher
- McAfee Application Control 5.x
- McAfee Endpoint Encryption for PC 5, 5.2.6, 5.2.9, and 6.1
- McAfee Host DLP 9.x
- McAfee Host Intrusion Prevention 8.x
- McAfee Network Access Control 3.2

- Stopping malicious modifications to drivers' import address table (IAT) hooking
- Preventing malicious modifications to kernel export address table (EAT)
- Stopping malicious I/O calls from device drivers
- Detecting malicious changes to drivers' dispatch routines

Detects and deletes known and unknown threats, leveraging McAfee GTI

McAfee Deep Defender will report, block, quarantine, and remove known and unknown malware in the kernel. Your existing McAfee VirusScan® Enterprise anti-malware leverages the unclocking capabilities of McAfee Deep Defender to cleanse the affected user-mode components completely.

For suspected or unknown malware, McAfee Deep Defender sends a fingerprint of the code to the McAfee GTI network to report and confirm its identity. The fingerprint of confirmed malware joins the McAfee GTI database to extend immediate protection to other McAfee GTI-enabled endpoints, including other endpoints at your site.

Centrally managed with McAfee ePO

McAfee Deep Defender lets you strengthen your existing protections without adding management or administration overhead. PCs and laptops running McAfee endpoint software today can deploy McAfee Deep Defender enterprise-wide on supported systems using existing McAfee ePO agents and management infrastructure.

The familiar McAfee ePO console makes it simple to develop policies for McAfee Deep Defender real-time memory actions. Once you have installed McAfee Deep Defender, your McAfee ePO dashboards and reports provide visibility into hidden threats.

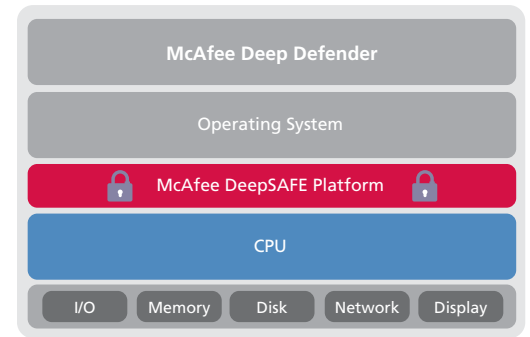


Figure 1. McAfee Deep Defender gains a new vantage point on threats by utilizing the McAfee DeepSAFE technology that resides between the CPU and OS.

Start decloaking stealthy malware today

Defenses that only operate within the OS cannot detect or expose the advanced evasion techniques at the disposal of today's sophisticated cyber criminals. McAfee Deep Defender complements traditional endpoint security with vital, incremental protection against these threats.

Adoption is easy, since McAfee Deep Defender takes advantage of the centralized and convenient McAfee ePO management environment and enhances the protection offered by the McAfee VirusScan anti-malware engine and McAfee GTI network.

Learn more at www.mcafee.com/deepdefender.

