

Extend McAfee Total Protection for Endpoint with HBGary Active Defense

Advanced threat detection and post-exploitation analysis system for targeted attacks

McAfee Compatible Solution:
HBGary Active Defense and
McAfee ePO 4.6.

Targeted attacks and advanced persistent threats (APTs) continue to transform the computer security landscape. Sophisticated cyber adversaries want your intellectual property, confidential information, financial data, and money. If your network is connected to the Internet, it can be compromised.

HBGary Active Defense™ represents an additional and complementary line of defense to McAfee® security solutions for your endpoints. It is the next-generation enterprise threat detection software solution to detect advanced, unknown malware, APTs, and exploitation tools without signatures or prior knowledge of the threat, on disk or in all physical areas of memory. When an APT is found, Active Defense scans your environment for targeted breach indicators to determine the full extent of the infection.

Extend McAfee Total Protection for Endpoint

To effectively combat enterprise threats, and the people behind them, threat intelligence is required. Leveraging HBGary's core Digital DNA technology, Active Defense extends the capabilities of McAfee Total Protection™ for Endpoint by providing a new and complementary method for host malware detection.

Active Defense with Digital DNA works with McAfee® ePolicy Orchestrator® (McAfee ePO™) software to proactively or reactively identify compromised Microsoft Windows computers throughout the enterprise. Malware and suspicious binaries and their underlying behavioral traits are reported with color-coded alerts on the McAfee ePO console.

Expand Detection of Unknown Threats without Signatures

Traditional security tools detect known threats via signatures. Criminals can bypass detection using new malware variants. To combat this targeted, customized malware, HBGary offers behavioral detection for significantly better security against both zero-day and targeted threats.

Active Defense monitors host physical memory, raw disk, and live operating systems across the enterprise, and provides an unprecedented view of host-level threats. Instead of requiring a unique signature for every new malware sample, Active Defense uses a behavior analysis approach that flags binaries that act like malware. This approach is complementary to McAfee Global Threat Intelligence™ reputation service, our on-demand, real-time cloud-based malware protection for known and unknown threats.

Detection Using Automated Offline Analysis of Physical Memory and Executables

Like an MRI body scan, physical memory reveals everything running on a computer, including APTs and rootkits. All malware must reside in memory to execute on the CPU, so offline memory analysis is the only way to truly and completely assess what is running on a computer. Digital DNA creates an image of physical memory and reconstructs all digital objects running, including the operating system and programs. After reconstruction, Digital DNA examines the entire operating system, including the kernel, and validates that no code is executing to thwart the detection system. Digital DNA reveals the underlying behaviors of every running program and assigns color-coded alerts to help analysts determine if it is safe or malicious.

Supported Platforms for the Joint Solution

- Windows 2008 Server
- Windows 7
- Windows Vista
- Windows 2003 Server
- Windows XP
- Windows 2000 Server
- Windows 2000

Reporting Output

Reports can be exported in several formats including PDF, XLS, CSV, HTML, ASCII, and RTF

Active Defense with Digital DNA with McAfee ePolicy Orchestrator

McAfee users deploy Active Defense with Digital DNA via their existing McAfee ePO enterprise infrastructure, increasing the value derived from current hardware, software, and network communications. The Active Defense agent can be throttled at three different levels to control host system impact. Your staff can use Active Defense with Digital DNA with little or no training to gain endpoint security visibility. Malware threats are automatically displayed on the web-based McAfee ePO dashboard console. Behavioral traits provide quick threat metadata, and historical alerts are centrally reported and correlated.

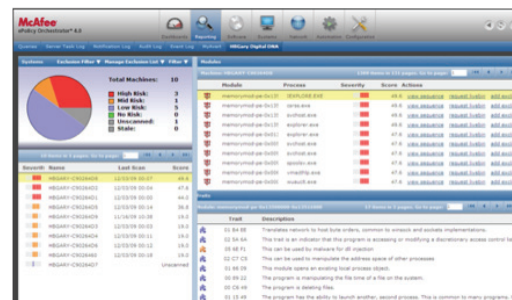


Figure 1. HBGary dashboard in McAfee ePO software.

Responder Professional

Once malware is detected by Active Defense with Digital DNA, you can use HBGary’s Responder Professional, a stand-alone workstation tool, for a deeper level of analysis of a computer’s memory and its malware.

With a mouse click, you can automatically extract malware from a remote computer’s memory and safely transfer it over the network to Responder Pro for deep static and dynamic analysis, reverse engineering, and reporting. Responder Pro allows your incident response team to quickly understand cyberthreats to help bolster network defenses. Responder Pro is also used for physical memory forensics.

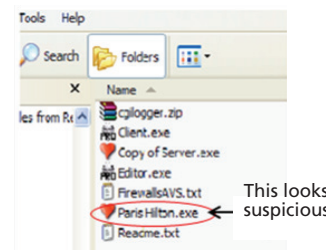


Figure 2. Identify in-memory threats.

About HBGary Active Defense and Responder Software

HBGary, Inc. is a McAfee Security Innovation Alliance Partner that delivers enterprise host malware detection and analysis solutions that provide customers with actionable threat intelligence. Co-founded in 2003 by renowned security expert Greg Hoglund, HBGary has expertise in Windows internals, software reverse engineering, rootkit techniques, offensive computer network attacks, and countermeasures. Software products include Active Defense for host-level detection and critical threat intelligence across enterprise and Responder Pro for post-exploitation forensic analysis. <http://www.hbgary.com>.

About McAfee ePolicy Orchestrator software

McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.



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

McAfee, the McAfee logo, ePolicy Orchestrator, McAfee ePO, McAfee Total Protection for Endpoint, and McAfee Global Threat Intelligence are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2011 McAfee, Inc. 36905brf_hbgary_1011