McAfee Advanced Threat Defense

Detect advanced targeted attacks.

McAfee® Advanced Threat Defense—part of the Intel Security® product offering—enables organizations to detect advanced targeted attacks and convert threat information into immediate action and protection. Unlike traditional sandboxes, it includes additional inspection capabilities that broaden detection and expose evasive threats. Tight integration between Intel Security solutions—from network to endpoint—enables instant sharing of threat information across the environment, enhancing protection and investigation.

McAfee Advanced Threat Defense Key Differentiators

Tight Intel Security solution integration

- Close the gap from encounter to containment and protection across the organization.
- Streamline workflows to expedite response and remediation.

Powerful analysis capabilities

- Utilize strong unpacking for better, more complete analysis.
- Combine advanced static code and dynamic analysis for more accurate detection with unparalleled analysis data.

Centralized malware analysis

- Cost-effectively reduce the number of required devices across the network through shared analysis.
- Simplify deployment.

Our technology has transformed the act of detection by connecting advanced malware analysis capabilities with existing defenses—from the network edge through the endpoint—and sharing threat intelligence with the entire IT environment. By sharing threat intelligence among management, network, and endpoint systems, our solutions immediately shut down command-and-control communications, quarantine compromised systems, block additional instances of the same or similar threats, assess where damage may have occurred, and take action.

McAfee Advanced Threat Defense: Detect Advanced Threats

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 on 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 by catching known malware, the addition of full static code analysis to sandboxing broadens protection against highly camouflaged, evasive threats. It provides detailed malware classification information including assessment of similarity with known malware families leveraging code reuse. Sandbox evasion techniques such as delayed or contingent execution paths, often not executed in a dynamic environment, can be detected through unpacking and full static code analysis.

Malware writers use packing to change the composition of the code or to hide it in order to evade detection. Most products cannot properly unpack the entire original (source) executable code for analysis. McAfee Advanced Threat Defense includes extensive unpacking capabilities that remove obfuscation, exposing the original executable

Integrated Solutions

- **McAfee Active Response**
- **McAfee Application Control**
- **McAfee Enterprise Security Manager**
- **McAfee ePolicy Orchestrator software**
- **McAfee Network Security Platform**
- **McAfee Threat Intelligence Exchange**
- **McAfee Web Gateway**

code. It enables static code analysis to look beyond high-level file attributes for anomalies, analyzing all the attributes and instruction sets to determine the intended behavior.

Together, static code and dynamic analysis provide a complete, detailed evaluation of suspected malware.

Target-specific sandboxing increases detection accuracy

Targeted attacks looking for environment variables or custom applications can often evade sandbox detection. To counter this, McAfee Advanced Threat Defense supports customized images for analysis. Each organization determines not only which operating systems and applications will best suit their environment, but also which versions. This enables organizations to analyze threats under the conditions of the actual host profile, rather than a generic image, and provides a more accurate risk assessment.

Because an organization may have multiple host profiles operating in the same network, McAfee Advanced Threat Defense queries McAfee ePolicy Orchestrator® (McAfee ePO™) software to determine the hosts' operating system and list of applications. It then analyzes suspect files under the conditions of the target host.

Enhance protection

Finding advanced malware is important. But if all a solution can do is provide a report or signal an alert, administrators are still left with massive amounts of work, and the network is still unprotected.

Tight integration between McAfee Advanced Threat Defense and security devices—from the network edge through the endpoint—enables integrated security devices to take immediate action when McAfee Advanced Threat Defense convicts a file as malicious. This tight and automated integration between detect and protect is critical.

McAfee Advanced Threat Defense can integrate in two ways, direct with select security solutions or through McAfee Threat Intelligence Exchange.

A direct integration enables Intel Security solutions to immediately take action on files convicted by McAfee Advanced Threat Defense. They can immediately incorporate threat intelligence into existing policy enforcement processes and block additional instances of the same or similar files from entering the network.

McAfee Advanced Threat Defense convictions appear in the integrated products' logs and dashboards as if the entire analysis had been completed onboard, streamlining workflows and enabling administrators to efficiently manage alerts by working through a single interface.

Integration with McAfee Threat Intelligence Exchange extends McAfee Advanced Threat Defense capabilities to additional defenses including McAfee Endpoint Protection and enables a broad range of integrated security solutions to access analysis results and indicators of compromise. If a file is convicted by McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange immediately publishes threat information via a reputation update to all integrated countermeasures within the organization.

McAfee Threat Intelligence Exchange-enabled endpoints can block patient-zero malware installations and provide proactive protection if the file appears in the future. McAfee Threat Intelligence Exchange-enabled gateways can prevent the file from entering the organization. Additionally, McAfee Threat Intelligence Exchange-enabled endpoints continue to receive file conviction updates when off-network, eliminating blind spots from out-of-band payload delivery.

Find and correct compromised systems

To remediate an attack, organizations need comprehensive visibility with prioritized, actionable intelligence to make better decisions and respond appropriately. McAfee solutions work together to provide organizations exactly what they need.

McAfee Enterprise Security Manager consumes and correlates detailed file reputation and execution events from McAfee Advanced Threat Defense and other security systems to provide advanced alerting and historic views for enhanced security intelligence, risk prioritization, and real-time situational

awareness. With indicator of compromise data from McAfee Advanced Threat Defense, McAfee Enterprise Security Manager will look back up to six months to hunt for indications of these artifacts in any network or system data it has retained. It can reveal systems that have previously communicated with newly identified malware sources. McAfee Enterprise Security Manager provides a clear understanding of risk so immediate corrective actions—interactive or automated—are taken. Tight integration with McAfee Endpoint Protection, McAfee Threat Intelligence Exchange, and McAfee Active Response optimizes security operations response and efficiency with visibility and action such as issuing new configurations, implementing new policies, removing files, and deploying software updates that can proactively mitigate risk. Informed action is easily taken when infected endpoints across the network are automatically identified by McAfee Active Response and listed in McAfee Advanced Threat Defense reports.

Deployment

McAfee Advanced Threat Defense is a centrally deployed, advanced malware analysis appliance that seamlessly fits into your existing McAfee security investment. McAfee Advanced Threat Defense acts as a shared resource between multiple Intel Security devices, cost-effectively scaling across the network.

Security operations centers and malware analysts can also use Advanced Threat Defense for investigation.

McAfee Advanced Threat Defense offers numerous, advanced capabilities including:

- User interactive mode: Enables analysts to interact directly with malware samples.
- Extensive unpacking capabilities: Reduces investigation time from days to minutes.
- Full logic path: Enables deeper sample analysis by forcing execution of additional logic paths that remain dormant in typical sandbox environments.
- Sample submission to multiple virtual environments: Speeds investigation by determining which environment variables are needed for file execution.
- Detailed reports from disassembly output to graphical function call diagrams and embedded or dropped file information: Provides critical information for analyst investigation.

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

McAfee Advanced Threat Defense Specifications	**ATD-3000**	**ATD-6000**
Form factor	1U Rack-Mount	2U Rack-Mount
Detection	**ATD-3000/ATD-6000**	
File/media types supported	PE files, Adobe files, MS Office Suite files, Image files, Archives, Java, Android Application Package	
Analysis methods	McAfee Anti-Malware, GTI reputation: file/URL/IP, Gateway Anti-Malware (emulation and behavioral analysis), dynamic analysis (sandboxing), static code analysis, custom YARA rules	
Supported OS	Win 8 (32-bit/64-bit), Win 7 (32-bit/64-bit), Win XP (32-bit/64-bit), Win Server 2003, Win Server 2008 (64-bit); Android All Windows operating system support available in: English, German, Italian, Japanese, and Simplified Chinese.	

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