McAfee

Together is power.

McAfee Advanced Threat Defense

Detect advanced malware

McAfee® Advanced Threat Defense enables organizations to detect advanced, evasive malware 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 security solutions—from network and endpoint to investigation—enables instant sharing of threat information across the environment, enhancing protection and investigation. Flexible deployment options support every network.

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 across the ecosystem, integrated security solutions work together to immediately shut down command-and-control communications, quarantine compromised systems, block additional instances of the same or similar threats, assess impact, investigate, 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 analysis engines such as antivirus signatures, reputation, and real-time emulation with dynamic analysis (sandboxing) to analyze actual behavior. Investigation continues with

in-depth static code analysis that inspects file attributes and instruction sets to determine intended or evasive behavior and assesses similarity with known malware families. A final step in the analysis, McAfee Advanced Threat Defense specifically looks for malicious indicators that have been identified through machine learning via a deep neural network. Combined, this represents the strongest advanced malware security protection on the market and effectively balances the need for both in-depth inspection and performance. While lower analytical intensity methods such as signatures and real-time emulation benefit performance by catching more easily identified malware, the addition of in-depth static code analysis and insights gained through machine learning to sandboxing broadens detection of highly camouflaged, evasive threats. Malicious indicators that may not execute in a dynamic environment can be identified through unpacking, in-depth static code analysis, and machine learning insights.

McAfee Advanced Threat Defense Key Differentiators

Broad solution integration
- Integration with existing McAfee solutions, third-party email gateways and other products supporting open standards
- Close the gap from encounter to containment and protection across the organization
- Streamline workflows to expedite response and remediation
- Enable automation

Powerful analysis capabilities
- Combine in-depth static code analysis, dynamic analysis, and machine learning for more accurate detection with unparalleled analysis data
- Advanced features support the SOC and enable investigation

Flexible, centralized deployment
- Reduce cost with centralized deployment that supports multiple protocols
- Flexible deployment options support every network

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

Together, in-depth static code, machine learning, and dynamic analysis provide a complete, detailed evaluation of suspected malware. Unparalleled analysis output produces summary reports that provide broad understanding and action prioritization, and more detailed reports that provide analyst-grade data on malware.

Enhance protection

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 different ways: direct with select security solutions, through McAfee Threat Intelligence Exchange, or through McAfee Advanced Threat Defense Email Connector.

A direct integration enables security solutions to 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.

McAfee Advanced Threat Defense Email Connector enables McAfee Advanced Threat Defense to receive email attachments for analysis from an email gateway. McAfee Advanced Threat Defense analyzes files in the

Integrated Solutions
- McAfee Active Response
- McAfee Advanced Threat Defense Email Connector
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator® software
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
  - McAfee Application Control
  - McAfee Endpoint Protection
  - McAfee Security for Email Servers
  - McAfee Server Security
- McAfee Web Gateway
- Bro Network Security Monitor
- TAXII (Trusted Automated eXchange of Indicator Information)

attachments and returns a verdict to the forwarding email gateway within the header of the message. The email gateway can then take policy-based action, such as deleting or quarantining the attachment, preventing the malware from infecting and spreading into the internal network. An offline mode enables email with attachments to be delivered to the end user while being scanned by McAfee Advanced Threat Defense. The email gateway does not wait for a verdict on the attachment. Administrators view attachment scanning results through McAfee Advanced Threat Defense or McAfee Threat Intelligence Exchange. For enhanced detection at the email server, McAfee Advanced Threat Defense integrates with McAfee Security for Email Servers through McAfee Threat Intelligence Exchange.

Threat-sharing to enhance and automate investigation

To investigate and remediate an attack, organizations need comprehensive visibility with actionable intelligence to make better decisions and respond appropriately. McAfee Advance Threat Defense produces in-depth threat intelligence that is easily shared across your entire environment to enhance and automate investigations. Support for McAfee Data Exchange Layer (DXL) and REST application programming interfaces (APIs) facilitates integrations with other products and widely used threat-sharing standards, such as Structured Threat Information eXpression (STIX)/ Trusted Automated eXchange of Indicator Information (TAXII) further enables organizations to create, support, and expand a collaborative security ecosystem.

Within a McAfee ecosystem, 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. 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.

Advanced capabilities support investigation

McAfee Advanced Threat Defense offers numerous, advanced capabilities including:

- **Configurable operating system and application support:** Tailor analysis images with select environment variables to validate threats and support investigation.
- **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 and memory dumps to graphical function call diagrams and embedded or dropped file, user API logs, and PCAP information:** Provides critical information for analyst investigation.

- **Bro Network Security Monitor integration:** Deploy Bro sensor to a suspected network segment to monitor and capture traffic and forward files to McAfee Advance Threat Defense for inspection.

Deployment

Flexible advanced threat analysis deployment options support every network. McAfee Advanced Threat Defense is available as an on-premises appliance or a virtual form factor, with support for both private and public cloud with availability in the Azure Marketplace. All form factors act as a shared resource between multiple McAfee solutions, cost-effectively scaling and reducing cost.

McAfee Advanced Threat Defense Specifications

Physical form factor	ATD-3100 1U Rack-Mount	ATD-6100 1U Rack-Mount
Virtual form factor	v1008, v1016, v3032, v6064 ESXi 5.5, 6.0, 6.5 Hyper-V Windows Server 2012 R2, Windows Server 2016	v1008, v1016, v3032, v6064 ESXi 5.5, 6.0, 6.5 Hyper-V Windows Server 2012 R2, Windows Server 2016

Detection

File sample types supported	PE files, Adobe files, MS Office Suite files, Image files, Archives, Java, Android Application Package, URLs
Analysis methods	McAfee Anti-Malware, GTI reputation: file/URL/IP, Gateway Anti-Malware (emulation and behavioral analysis), dynamic analysis (sandboxing), in-depth code analysis, custom YARA rules, machine learning: deep neural network
Supported OS	Win 10 (64-bit), Win 8.1 (64-bit), Win 8 (32-bit/64-bit), Win 7 (32-bit/64-bit), Win XP (32-bit/64-bit), Win Server 2016, Win Server 2012, Win Server 2012 R2, Win Server 2008, Win Server 2003, Android Windows operating system support available in all languages.
Output formats	STIX, OpenIOC, XML, JSON, HTML, PDF, text
Submission methods	Point product integrations, RESTful APIs, manual submission, and McAfee Advanced Threat Defense Email Connector (SMTP)

Learn More

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

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