

## Advanced Threat Protection

Designed to work with other products, a central system to verify files.

---

McAfee



### Features

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.

### Description

Designed to work with other products, a central system to verify files. Works with: 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 McAfee Advanced Threat Defense protects against advanced malware, including zero-day

and advanced persistent threats, providing the strongest advanced threat protection available. Advanced targeted attacks are designed to defeat security systems through approaches that either confuse or evade defenses. McAfee Advanced Threat Defense detects targeted attacks and connects with existing defenses, converting threat intelligence into immediate action and protection. Unlike traditional sandboxes, it provides multiple analysis engines to broaden detection and expose evasive threats. As part of the Security Connected platform, McAfee Advanced Threat Defense is tightly integrated with other Intel Security solutions—from network to endpoint—enabling instant sharing of threat intelligence across the entire infrastructure to enhance zero-day threat protection, reduce time from detection to containment, and aid investigation to remediate post-attack.

## Specification

ATD-3000 – 30 VMs, Form factor 1U Rack-Mount  
ATD-6000 – 60 VMs, Form factor 2U Rack-Mount  
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.

## Links

[Data Sheet](#) [Solution Brief](#) [Product Guide 3.6.2](#)

[Best practices to avoid being compromised by file infectors](#)

[Best practices to avoid being compromised by Worms](#)

[Bank Case Study](#)

[ExpertCenter](#)

---

**Sweden**

Cognosec Nordic AB  
Birger Jarlsgatan 12  
114 34 Stockholm  
Sweden  
Tel +46 (0)8 400 170 00  
sales.se@cognosec.com

**UK & Ireland**

Cognosec Limited  
3rd Floor  
The News Building  
3 London Bridge Street  
London SE1 9SG  
UK  
Tel +44 (0)20 3870 1539  
sales.uk@cognosec.com

**Germany**

Cognosec GmbH  
An der Welle 4  
60322 Frankfurt  
Germany  
Tel +49 (0)69 7593 8490  
sales.de@cognosec.com

**Austria**

Cognosec GmbH  
Castellezgasse 16/2  
1020 Vienna  
Austria  
Tel +43 (0)1 212 2020  
sales.at@cognosec.com

**UAE**

Cognosec DMCC  
2202 Indigo Icon Tower  
Cluster F  
Jumeirah Lakes Towers, Dubai  
UAE  
Tel +971 (0)4 451 1552  
sales.dxb@cognosec.com

Copyright © 2017 Cognosec Limited. All rights reserved.