

Trend Micro™

Dynamic Threat Analysis System

Detection, Identification, and Analysis of Advanced and Targeted Threats

Minimizing the risk and impact of Advanced Persistent Threats and other targeted attacks requires state-of-the-art threat detection and the ability to efficiently conduct a deep forensic analysis of captured malware. Threat analysts and security specialists want to answer questions such as: What is the nature and behavior of this threat? How is it controlled? What is the risk? What can I do to protect my enterprise from successful attack?

Trend Micro Dynamic Threat Analysis System (DTAS) is a malware identification and analysis platform that uses sandboxing and other advanced methods to provide detection, detailed exploration, simulation and full forensic analysis of suspected malware captured by the Trend Micro Threat Management System (TMS) or submitted directly by a security specialist.

In addition to deep forensic analysis, DTAS acts as an adjunct “sandbox” detection engine used by TMS to examine suspicious files and executables. If the sandbox execution does detect malware, standard TMS alarming, reporting and automatic mitigation functions are initiated.

DTAS is part of the Trend Micro Real-Time Threat Management portfolio, a set of integrated products and services designed to provide real-time protection against advanced threats via network-wide visibility and control, actionable threat intelligence, and timely vulnerability protection.

DTAS FEATURES & FUNCTIONS

DTAS is composed of one or more Dynamic Threat Analyzers managed by a Dynamic Threat Analysis Manager. Each Dynamic Threat Analyzer is a network-resident appliance that can execute up to 24 simultaneous sandbox test and analysis environments. The Dynamic Threat Analysis Manager presents an intuitive graphical interface that includes:

- Threat execution and evaluation summary
- In-depth tracking of malware actions and system impact
- Identification of malicious destinations and command and control servers
- Exportable forensic reports and PCAP files
- Generation of complete malware intelligence for immediate local protection
- Manual submission of suspect files

Dynamic Threat Analysis System

- **DETECTION**
- **IDENTIFICATION**
- **FORENSIC ANALYSIS**
- **ACTIONABLE INSIGHT**

