DATA SHEET

# Trellix Malware Analysis

## Analyze attacks with 360-degree visibility

## Highlights

- Performs deep forensic analysis through the full attack lifecycle using the Trellix IVX engine
- Streamlines and batches analysis of suspicious web code, executables, and files
- Reports in depth on system-level OS and application changes to file systems, memory, and registries
- Offers live-mode or sandbox-mode analysis to confirm zero-day exploits
- Generates threat intelligence dynamically for immediate local protection via integration with the Trellix Central Management System
- Includes Trellix malware detection technologies to optimize incident response prioritization
- Supports Windows, MacOS X and CentOS environments

## Overview

As cybercriminals tailor attacks to penetrate a specific business, user account, or system, your organization needs easy-to-use forensic tools to help you rapidly address targeted malicious activities.

Trellix Malware Analysis is a forensic analysis solution that gives your security analysts hands-on control over powerful auto-configured test environments. There, you can safely execute and inspect malware, zero-day, and advanced persistent threat (APT) attacks embedded in web pages, email attachments, and files.

### Assess OS, browser, and application attacks

Malware Analysis uses the Trellix Intelligent Virtual Execution (IVX) engine to provide your in-house analysts with a full 360-degree view of an attack—from the initial exploit to callback destinations and follow-on binary download attempts.

Through a preconfigured, instrumented Microsoft Windows, MacOS X and Linux virtual analysis environment, the IVX engine fully executes suspicious code to allow deep inspection of common web objects, email attachments, and files. Malware Analysis uses the IVX engine to inspect single files or batches of files for malware and tracks outbound connection attempts across multiple protocols.

## Spend time analyzing, not administering

Malware Analysis frees your administrators from time-consuming setup, baselining, and restoration of the virtual machine environments used in manual malware analysis. With built-in customization and granular control over payload detonations, Malware Analysis enables forensic analysts to arrive at a comprehensive understanding of the attack that's suited to your enterprise's requirements.

## Choose live analysis or sandbox modes

Malware Analysis offers two analysis modes: live and sandbox. Your analysts can use the live, on-network mode for full malware lifecycle analysis with external connectivity. This allows Malware Analysis to track advanced attacks across multiple stages and different vectors. In sandbox mode, the execution path of particular malware samples is fully contained and visible in the virtual environment.

In both modes, you can generate a dynamic and anonymized profile of the attack that can be shared through the Trellix Central Management System to other Trellix solutions. The malware attack profiles generated by Malware Analysis include identifiers of malware code, exploit URLs, and other sources of infections and attacks. Malware communication protocol characteristics are shared to provide dynamic blocking of data exfiltration attempts across your organization's Trellix deployment via Trellix Dynamic Threat Intelligence (DTI).

## Enable customization with YARA-based rules

Malware Analysis supports importing custom YARA-based rules to specify byte-level rules and quickly analyze suspicious objects forthreats specific to your organization.

## Stay connected with a global malware protection network

Malware Analysis can share malware forensics data with other Trellix solutions, block outbound data exfiltration attempts, and stop known inbound attacks. Threat data from Malware Analysis can be shared via the DTI cloud to protect against new emerging attacks.

With preconfigured IVX engines eliminating the need for tuning heuristics, Malware Analysis saves your administrators setup time and configuration issues. This solution also helps threat researchers analyze advanced targeted attacks without adding network and security management overhead.

## Table 1. Technical specifications

| | AX 5600 |
|---|---|
| Performance* | Up to ~10,000 analyses per day. |
| OS support | Microsoft Windows/Apple Mac OS X/CentOS |
| Network interface ports | 2x 10/100/1000 BASE-T ports |
| IPMI port (rear panel) | Included |
| Keypad | Not available |
| DB15 VGA ports (rear panel) | Included |
| USB ports (rear panel) | 2 X USB2.0 , 2 X USB3.2 |
| Serial port (rear panel) | 115,200 bps, no parity, 8 bits, 1 stop bit |
| Drive capacity | 2 x 4 TB HDD, RAID 1, 3.5 inch, FRU |
| Enclosure | 1RU, fits 19 inch rack |
| Chassis dimensions (WxDxH) | 17.2in (437mm) x 19.98in (507 mm) x 1.7in (43 mm) |
| DC power supply | Not available |
| AC power supply | Redundant (1+1), FRU, 400W with Input 1100-240VAC / 6.0 – 3.0A \| 200-240VDC / 3.4-3.2A, 50-60 Hz IEC60320- C14 inlet |
| Power consumption maximum | 300 watts |
| Thermal dissipation maximum | 1024 BTU/hr |
| MTBF | Coming soon |
| Appliance alone/As shipped weight | 24 lbs (10.8 kg)/37 lbs (16.7 kg) |
| Safety certifications | EN IEC 62368-1:2018+A11:2020 |
| EMC/EMI certifications | EN 55032:2015/A11:2020, EN 55035:2017/A11:2020,EN 61000-3-2:2014, EN 61000-3-3:2013 |
| Regulatory compliance | RoHS: Directive 2011/65/EU |
| Operating temperature | 5°C - 35°C (41°F - 95°F) |
| Operating relative humidity | 8% - 90% (non-condensing) |
| Operating altitude | 0 to 5000ft |

*Note: Performance numbers are based on default analysis times when using Malware Analysis, but will vary depending on the system configuration and traffic profiles being processed.

To learn more about Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com