



MIMOS Trusted Platform (Mi-Trust)

High value information is now the most sought after commodity that must be thoroughly protected. MIMOS Mi-Trust offers reactive security technology to protect the safety of such high value information.

Overview

MIMOS Mi-Trust is a security technology that offers reactive protection for high value information. The reactive security provides protection when and where prevention measures are found insufficient. Mi-Trust is divided into two main core technologies: Mi-Trust Folder Protection and Mi-Trust Fingerprints.

Mi-Trust Folder Protection monitors all activities in the system and guards against activities that affect files under its protection based on the policies that have been set.

In a scenario where an intruder breaks into a website and modifies it, Mi-Trust Fingerprints detects the changes made and provides auto recovery if necessary.

Features

Mi-Trust comprises the following features:

File Integrity Protection

Mi-Trust guards the files under its protection from malicious activities through copy prohibition, delete prohibition, web email attachment prohibition and runtime prohibition based on policy.

Webpage Modification Detection and Auto Recovery Support

Mi-Trust detects unauthorised changes made on the system and auto recovers if necessary.

End-Point Security

Mi-Trust provides data protection over a variety of platforms such as smart devices, servers, PCs and notebooks.

Technology Benefits

The main impacts of Mi-Trust are:

Protection from Unauthorised Sharing

Mi-Trust reactive protection prevents illegal sharing by valid users once a folder is deemed protected in the system.

Real-Time Detection

Mi-Trust provides real-time detection to ensure the integrity of information.

Information Monitoring and Protection

Mi-Trust monitors and protects information to ensure the security and integrity of folders and websites.

Technology Summary

Mi-Trust

A security technology that offers reactive protection for high value information.

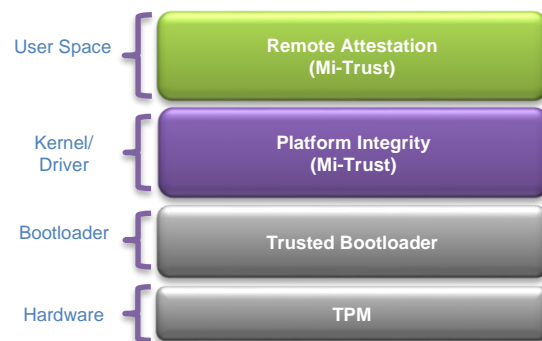
Industries: Enterprise, Government, Defence, Public Safety

Features

- File integrity protection
- Webpage modification detection and auto recovery support
- End-point security

Technology Benefits

- Protection from unauthorised sharing
- Real-time detection
- Information monitoring and protection



MIMOS Mi-Trust components

System Requirements

Mi-Trust	
Windows Security	
Processor(s)	AMD/Intel® Processor X86-64 Architecture 2GHz or higher
Memory	Minimum 4GB of memory
Disk Storage	Minimum 15GB of hard disk space
Operating System	Windows® XP (Service Pack 3) Windows 7 and Windows 8 Windows Server 2003 and 2008
Linux Security	
Processor(s)	AMD/Intel® Processor X86-64 Architecture 2GHz or higher
Memory	Minimum 4GB of memory
Disk Storage	Minimum 15GB of hard disk space
Operating System	Linux® Kernel 2.6.30 and above i386 or i686GNU \Linux
Security Chip	TPM Chip (SLB9635TT1.2)

