TrustedDesktop

Comprehensive endpoint security solution and efficient desktop management

Today´s information systems still lack in efficient protection against both outsider and insider threats. Targeted malware attacks and data leakages are the most visible examples of these increasing threats. Thus, time has come for a more comprehensive approach to endpoint security. Today, IT infrastructures are shared, distributed, and heterogeneous. They extend into cloud computing. 360° security concepts have become essential, yet they should not add extra complexity or limitations in use.

TrustedDesktop provides an all-new level of protection both against attacks from outside and against data leakages from inside. Rohde & Schwarz Cybersecurity is first to comprehensively implement the notion of trustworthy systems as a fundamental concept for IT infrastructures.

Solution

TrustedDesktop is a secure virtualized desktop solution with practicable information flow control. Its basic principle is the strong isolation of critical applications and corporate workflows as well as the reliable enforcement of security policies.

Its innovative technology enables a comprehensive and auditable lifecycle protection of all enterprise data. The overall system guarantees that protected information is only processed by trustworthy components. Thus, any data leakage by malicious or accidental errors is prevented efficiently.

At the same time, the TrustedObjects Manager (TOM) combines a system-wide security policy management with an easy to use deployment, configuration and provisioning system for the entire infrastructure, including networks, clients and desktop images.

Architecture

The core component of TrustedDesktop is the TURAYA™ SecurityKernel. The SecurityKernel virtualizes different operating systems into individual isolated areas (compartments) running in parallel on the same client machine. Every compartment can be allocated independently to a Trusted Virtual Domain (TVD), each spanning a distributed, but closed virtual processing area. Data leaving a compartment is seamlessly encrypted and can only by accessed in a local or remote compartment that belongs to the same TVD. This concept is revolutionary as it enables for the first time an efficient information flow control for enterprise systems working with legacy operating systems. This is made possible by the SecurityKernel technology along with the integration of Trusted Computing technology. TrustedDesktop provides many security and functional features, enhancing the enterprise security and increasing the efficiency of workflows:

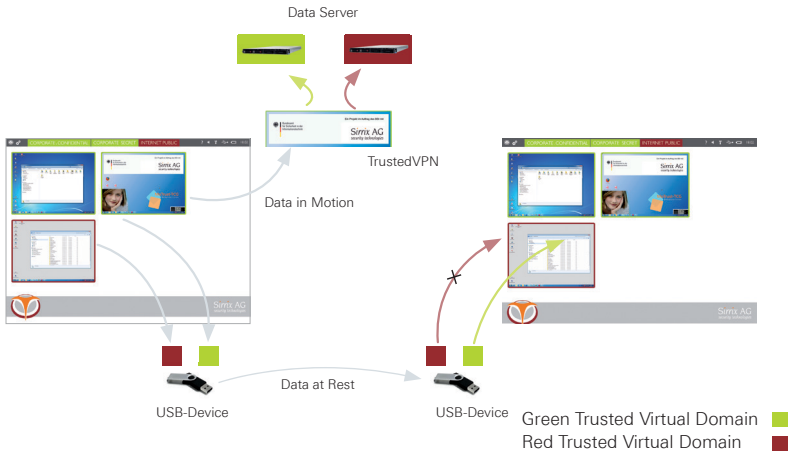
- Comprehensive data leakage prevention with transparent file en-cryption. The solution transparently encrypts data leaving a secured compartment. This includes transparent encryption of data on remov- able storage (USB, HDD) or data stored on remote locations (NFS, SMB). Thus, it provides offline transport capabilities for

TrustedDesktop

exchanged data. A transfer of unencrypted data between different TVDs is only possible if explicitly allowed by the security policy.

- An intelligent VPN client enables secure links between compartments belonging to the same Trusted Virtual Domain and to dedicated networks.
- Full harddisk-encryption, sealed to the TPM security chip: In contrast to other solutions, the encryption key is never seen by the operating system and thus, no viruses, trojan horses or other malware can leak or change sensitive key material.

TrustedDesktop is based on a Security Kernel with the Trusted Platform Module (TPM) acting as a hardware anchor for full system integrity. The solution withstands even physical attacks like malicious code injection or attempts to steal sensitive key material.



Features

Basic characteristics

TrustedInfrastructure

- System-wide data containment based on
- Trusted Virtual Domains (TVDs)
- Cross-platform Information Flow Control
- Supports clients (TrustedDesktop), servers (TrustedServer) and networks (TrustedVPN)

TrustedDesktop Client

- Support of multiple, strongly isolated Virtual Machines, belonging to different Trusted Virtual Domains (TVD).
- Based on Turaya™ Security Kernel
- Secure bootstrap and system integrity, enabled by hardware-based TPM module
- Trusted GUI with Secure Clipboard function for a local policy enforcement
- Transparent File Encryption for local and remote storage devices
- Full hard disk encryption with secure bootstrap ensuring system integrity
- Integrated VPN Client for cross-plattform communication
- Printing allowance controlled by TVD
- Smartcard-based user authentification
- Access to periphal devices (e.g. camera, microphone)
- controlled via TVD policy

TrustedObjects Manager

- Centralized infrastructure and security policy management for clients, networks, servers and virtual machines (trusted objects)
- Centralized infrastructure management
  Registration and authentication of all trusted objects
  Remote attestation of integrity for all trusted objects
  Provisioning of certified compartment images
- System-Wide Security Policy Management based on TVDs
  Information Flow Allowances between TVDs
  Network access control and firewall rules within TVDs
  User & Role based policies
- Web-based GUI for authorized administrators
- Fully integrated PKI solution
- Ready-to run appliance, integrates hardware security module (TPM or HSM module)

Rohde&Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 89 4129-206 000
cybersecurity@rohde-schwarz.com
www.cybersecurity.rohde-schwarz.com

3607577732
3607.5777.32 01.00 PDP 1 en July 2016