ENSURING SECURE CONTENT PROTECTION SOLUTIONS

TrustVDI

Protect sensitive data by end-to-end sandboxing

Features and Benefits

- Enable remote employees to work anytime and anywhere
- Increase security by sandboxing end-to-end entities for VDI
- Compatible with existing VDI framework and is easy to deploy

The most secured VDI framework we known in industry

The Need for Securing VDI

Virtual desktop infrastructure (VDI) has revolutionized the way that IT provisions and manages applications. With VDI, your business is borderless. It gives employees the freedom to work from anywhere while cutting IT costs.

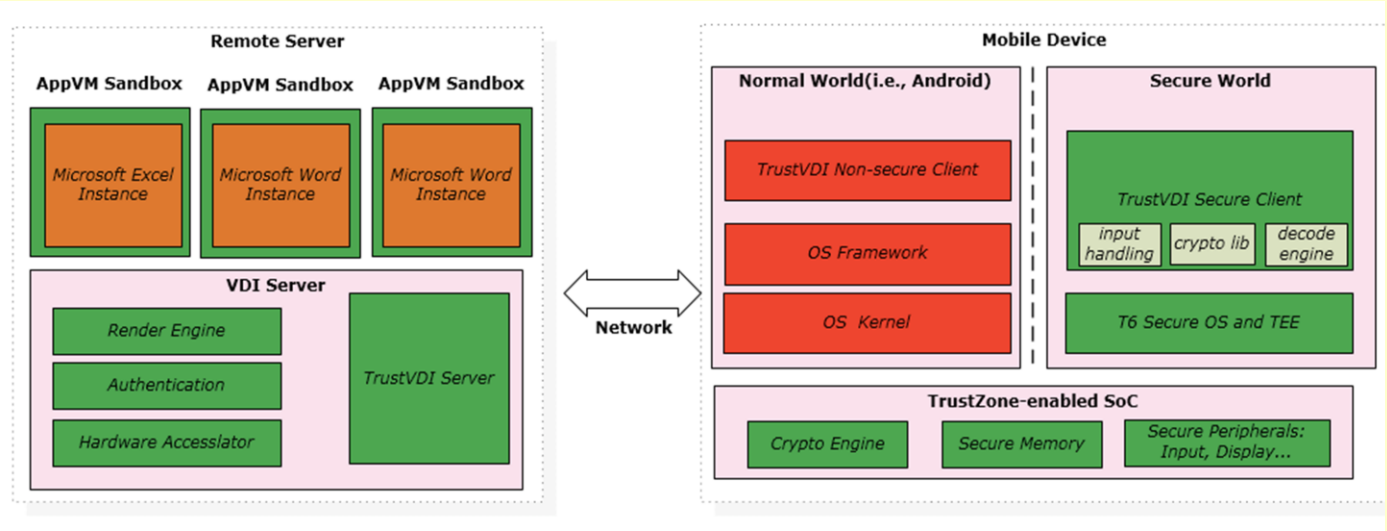
Unfortunately, most VDI solutions today expose businesses to malware infections and data theft. Existing approaches to securing sensitive data of VDI are through either a set of predefined policies or online auditing,

Attackers can easily infiltrate VDI servers or clients to monitor, manipulate or steal data. Without proper security controls, hackers can easily compromise VDI services and steal sensitive data.

Hardware-assisted Sandboxing against Attacks

TrustVDI not only delivers high-performance virtualized desktop services, it also offers built-in security and isolation through TrustKernel's appVM and Trusted Execution Environment (TEE). The appVM sandbox is a light weight virtualized container, which provides a flexible isolation while maintaining high performance. By using TrustKernel's TEE, TrustVDI protects its client with a strong security guarantee and removes the commodity software stack out of its TCB. A hardware-assisted end-to-end sandboxing mechanism in TrustVDI prevents most of known attacks against VDI.

TrustVDI Architecture



AppVM-based Isolation in TrustVDI Server

The appVM sandboxing mechanism provides an invisible shield around each application instance, preventing application users from installing malware on the underlying operating system or from accessing other application instances. TrustVDI Server achieves its high performance through hardware-assisted accesslation.

TrustVDI is secured by its design nature and existing security enhancing mechanism such as policy enforcement could still be applied

TrustZone-based Isolation in TrustVDI Client

TrustVDI client is protected by hardware isolated mechanism called TrustZone and by using TrustKernel's TEE, most of modern malware and attacks could be prevented. The TrustVDI client is incrementally deployable and requires little modification on existing VDI client.

Learn More

For more information, please visit http://trustkernel.org or email contact@trustkernel.org.

About TrustKernel

Founded in 2013 and headquartered in Shanghai, TrustKernel is focused on next generation mobile and server security solutions and tries to provide these available solutions to end users. TrustKernel's defined goal is to deliver fast and simple IT security solutions for mobile, embedded devices and server to our customers and partners.