SierraVDI

Protect sensitive data by sandboxing virtual application instances

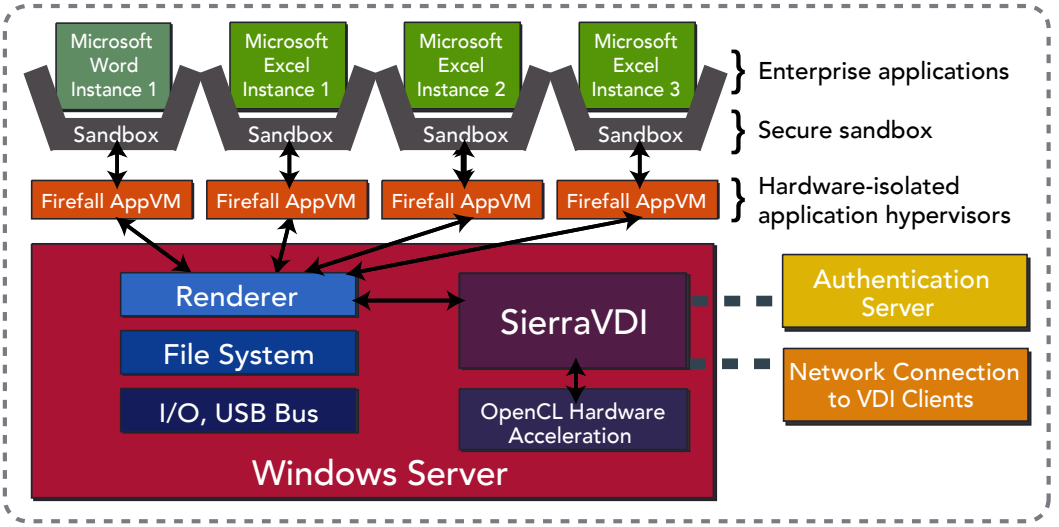
Virtual desktop infrastructure (VDI) has revolutionized the way that IT provisions and manages applications. VDI has automated application deployment, reduced capital costs, and enabled users to access applications from any device and any location. But wait; thereės a catch. Unfortunately, most VDI solutions today expose businesses to malware infections and data theft.

Security risks in traditional VDI deployments

Attackers can easily infiltrate VDI servers to monitor, manipulate or steal data. They can trick virtual desktop users into opening malicious files such as spreadsheets which install malware on host servers. In addition, virtual desktop users can inadvertently download malware from virtually hosted web browsers, like Microsoft Explorer, to VDI servers. Alternatively, malicious insiders can initiate VDI sessions and intentionally install rootkits on VDI servers. Without proper security controls, hackers can easily compromise VDI services.

Hardware-isolated protection against attack

SierraVDI not only delivers high-performance virtualized desktop services, it also offers built-in security and isolation through Sierrawareės innovative Firefall application VMs. The Firefall VM 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. By sandboxing each application instance with a hardware-isolated hypervisor, SierraVDI prevents targeted attacks and zero-day threats.



The SierraVDI architecture features Firefall virtualization technology and sandbox containers to secure each application instance.

Features and Benefits

- Increase productivity by enabling fast, easy access from employee-owned devices
- Automate and centralize application provisioning and management
- Increase security by centrally hosting critical business applications
- Ensure business continuity by replicating services in redundant data centers
- Enable remote or field employees to work anytime and anywhere
- Allow partners to securely access business applications
- Improve user experience with multimedia and USB redirection
- Leverage H.265 encoding to improve performance and application density

sierraware