

“Desktop security done right”

User friendly virtualization solutions to guard against malware and malicious attacks

The vision consists of products based on virtualization solutions which could assist in guarding against malware and malicious attacks while still being easy and intuitive to use and install.

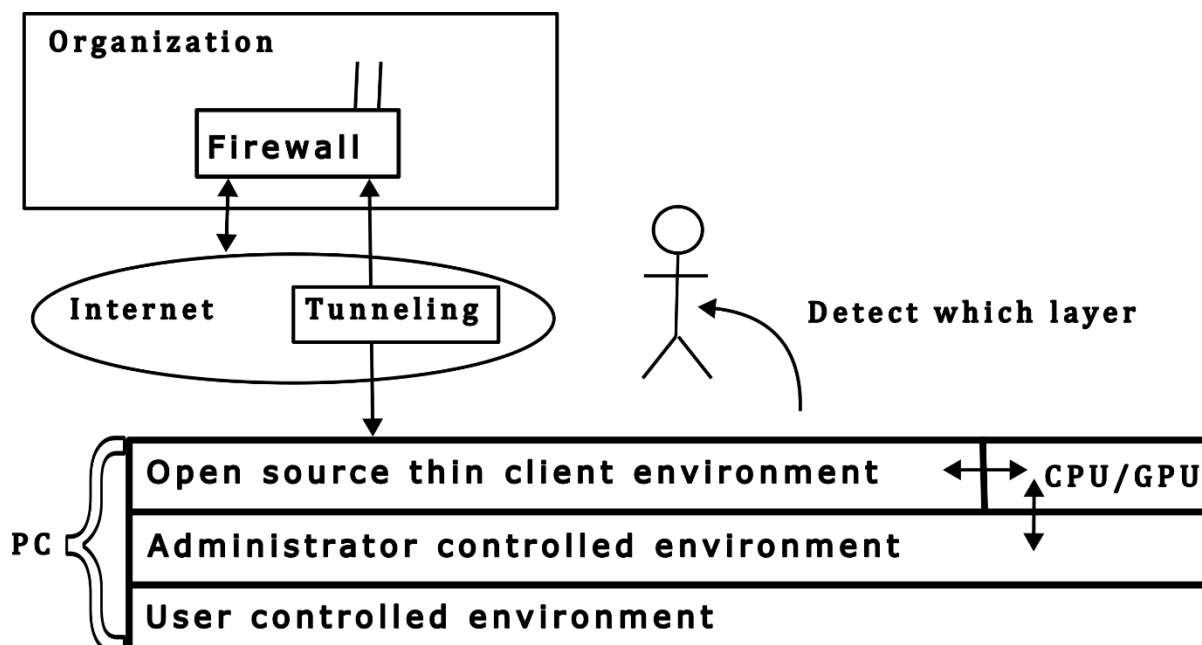


Figure: Three-layered security approach with firewall

Remote Application Access Station

One product has already been created. It is a product which can be used by organizations which want users to be able to install software while still having the benefits from administrator-controlled environments on their local machines. The user interface allows users to install and use applications on virtual machines by using them as remote applications. It is designed to work as similar as possible to the approach used for installing and handling applications by the local operating system.

RAAS Server and RAAS Client have already been created for Windows and RAAS Client should be ported to Linux, Macintosh and Chromebook, starting with Linux.

New Product suggestions

The current product suggestions could all benefit from forwarding of devices, CPU and GPU capabilities to a virtual machine. All the candidates attempt to isolate a closed source operating

system with closed source applications in different ways by placing it in a virtual machine on an open source operating system with open source applications which contains the hypervisor.

The product plans for each of the candidates are all rather elaborate, but they are summarized in the following sections.

Utility Firewall

This is a dual operating system configuration where both operating systems can be used simultaneously where the closed source operating system and applications is run in a virtual machine behind a white listed firewall. The firewall is placed on an open source operating system running the hypervisor and the closed source software should not be able to manipulate it. Internet can still be accessed through the open source operating system.

Note: Firewall in its simplest form is to tunnel in behind an organisations firewall.

Administrator Desktop

This configuration uses a closed source operating system and applications in a virtual machine and a open source operating system for the hypervisor for a dual operating system configuration where both operating systems can be used simultaneously. Administrators can use this utility if they want to restrict access to their infrastructure only to open source operating systems and applications but still want to use a closed source operating system with closed source applications in their everyday work. Similar to Utility Firewall but without the white listed firewall.

Note: A solution can still be to tunnel in behind an organisations firewall, but the firewall does not need to be white listed.

Thin Client Extension

This configuration uses one closed source operating system within a virtual machine and an open source operating system for the hypervisor. It differs from the previous products by viewing one operating system at a time and switch viewing and input between them. The closed source operating system is used for daily work while the open source operating system functions as a thin client when necessary, preventing any malware on the closed source operating system from accessing inputs or outputs when used as a thin client.

Note: To tunnel in behind an organisations firewall is optional but not mandatory for this solution.

Firewall Extension

This configuration uses one closed source operating system within a virtual machine and an open source operating system for the hypervisor. The open source operating system contains a firewall which the closed source operating system and applications should not be able to manipulate. The firewall could be accessed over the network and users should not need to interface with the open source operating system directly. Everyday work can be performed on the closed source operating system with the firewall running in the background.

Note: Firewall in its simplest form is to tunnel in behind an organisations firewall.

Technologies

We will use Kernel-based Virtual Machine (KVM), we will use FreeRDP, we will use Nautilus.