INCREASE VDI SCALABILITY WITH TRAPS

Thin clients and X terminals had limited success in the '90s. As a result, people turned to virtual desktops – virtual copies, or "images," of desktop environments – stored on a central server, also known as a virtual desktop infrastructure, or VDI. Centralized control of desktop images reduces costs and improves security.

Instead of running on endpoints, virtual desktop images run in a central virtual environment, such as those from VMware, Citrix or Microsoft. Each desktop runs as a virtual machine and can use one or more virtual CPUs depending on user needs. To reduce variation and multiple versions, a "golden" image is used across many desktops and can be deployed easily as new ones are added.

The use of virtual desktops ranges from allowing expansion beyond the physical limitations of a desktop screen to enabling on-demand desktop access from any device, anywhere. Virtual desktops also reduce the time required to provision new devices and help cut costs associated with desktop management and support. However, if the golden image contains unpatched software or vulnerable applications, the problem becomes magnified and replicated across all virtual desktops.

Securing VDI With Antivirus

Traditionally, securing a VM has required installing an antivirus product on each instance, with some major implications for performance and scalability.

Testing shows that traditional AV architectures generally have a CPU resource impact of up to 40 percent in their default configuration. To optimize for VDI, users may turn off security features, such as heuristics, severely limiting the antivirus product's ability to stop unknown attacks.

Although it is recommended that the VDI golden image be regularly scanned, not many teams do so. This leaves users reliant on scheduled antivirus scans to catch any attacks.

AV signatures can be up to 500MB, and memory and CPU consumption of antivirus products is 35–50 percent, even with limited security functions enabled. This means the number of virtual desktops per core has to be reduced by around 40 percent on average to accommodate the usage, wasting memory and CPU resources.

Traps: The Alternative to Securing VDI

Palo Alto Networks® Traps™ advanced endpoint protection does not rely on signatures, scanning or behavior-based detection to identify attacks. It has an observed CPU utilization of less than 0.1 percent and a lightweight structure, which add up to some significant benefits for use on virtual machines:

- The lightweight Traps agent minimizes impact on server resources. A minuscule footprint on disk, memory and CPU preserves more resources to run VDI.
- High performance can be achieved without turning off any features, all while providing multiple methods of protection.
- Each Traps instance sits in the VM and protects each desktop instantly from known and unknown threats without depending on signatures or scanning.
- Traps protects the VMs and golden image, reducing the risk of imaging compromised virtual desktops.
- Traps licenses are allocated from a pool of licenses rather than assigned on a per-user basis. As an image comes up, a Traps license is distributed. As the image comes down, the license is placed back into the pool.
- Customers using Palo Alto Networks firewalls, whether on-premises or in the cloud, can automatically detect and block new attacks Traps discovers.

As organizations deploy VDI for improved efficiency and optimization, their endpoint security should enhance, rather than hinder, that optimization. Traps provides up to 39 percent lower costs per desktop, 60 percent more users per server and 66 percent more VMs per core in addition to protecting against malware, exploits and ransomware through coordinated enforcement with cloud and network security.

To learn more about Traps, read the Traps overview.

© 2018 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at http://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.