VMware View Offline Desktops: The Birth of the VDI Bomb?

Alan Murphy, 2008-04-12

About two years ago, I was part of the team at F5 that helped design and build our Technology Center – a fully functioning showcase lab housing all of our products as well as other infrastructure and application partner technologies such as VMware, Microsoft, Dell, etc. My role (besides cable monkey during install week ;) was to define and isolate the security risks associated with guest virtual machines and segmentation (both physical and logical) of the virtual network and working spaces. Probably one of the coolest and most fun projects I've ever been involved in; the Tech Center really is a work of Data Center art.

One of the areas I was most concerned about from the get-go was the portability and availability of guest VMs; customers and partners can bring in their own virtual machines to provide back-end services during their testing time at the TC and we'll run those on our virtual platforms. Now while all of our partners are trustworthy people, we paranoid types know that trust in the security realm is a tough thing to come by, so we needed to create a fully-functional yet safe environment for these VMs to run -- safe for them so there's minimal sharing of resources with other customers and partners that may be visiting, and safe for us since it's our infrastructure. From day one I've been concerned about the check-in/check-out possibilities with virtual machines; it equates to building a secure box that's ready to be racked, and just before you rack it you let a stranger take it home for a week, then that stranger brings it back, you rack, cable, boot, and let it run loose. Scary, huh.

We solved that problem in the Tech Center using extremely tight networking configurations (walled gardens are your friends) via BIG-IP LTM and hardware isolation for our partners and their specific virtual machine environments, with good management on top to make sure everything functions as expected. To date it's been an excellent solution.

Fast forward two years later and meet VMware View: VMware's VDI management solution that, in theory, should lead us down a path of near complete mobile desktop computing which, as a side benefit, should drastically improve desktop security. With one huge exception: Offline Desktops. Still an experimental feature today, Offline Desktops allow an end-user to check out their VDI image (which is a complete VM: OS, apps, everything) and take it with them. Let's say Alice (or maybe Mallory is a better example? ;) is in the office on Tuesday morning running her desktop remotely over the LAN, she checks out her desktop and hops on a plane, works on the flight, and then jumps on the VPN when she's in her hotel and check her desktop back in, changes and all. Rinse. Repeat. Cool idea with huge benefits, but…

The paranoid me writing this blog immediately started locking doors, lowering blinds, checking the lamps for bugs, etc. I see this as a huge security risk: once the desktop is out of the DC and out of IT's control, it's immediately suspect. Just like one of the primary use cases for NAC where external, unknown laptops aren't allowed to jack directly into the corporate network without auth and some level of validation and sanity check, any VDI image checked out via View and then checked back in should be treated as a new, external device, requiring quarantine, inspection, sanitization, re-authentication, the whole ball of wax. The risks are even more severe for VMs that are allowed to leave and re-enter the data center due to shared resources that run those VMs. The risk is no longer limited to a segmented network; it now extends to the entire VDC platform.

Could this simple, highly usable and beneficial feature open the door for VDI Bombs? A Frankensteinian marriage of trojan bombs (plant today, blow up on delivery or at a later time) delivered via VMs and targeted towards the host hypervisor, network, or CPU? Are IT departments going to build sophisticated quarantine environments for VDI VMs that are checked back in, and if so, will those tools be available soon enough to catch these bombs before time runs out? Or maybe this is a perfect opportunity to see VMSafe used as intended. Seems like the check-in/sync operation would be the perfect time to scan the guest kernel, filesystem, VM tools, etc, via VMsafe.

I think a completely mobile virtual desktop is a great idea, even if it just pacifies us until true application virtualization becomes a reality, especially for IT client management. But how much more management and security will be needed in the data center to make this a functional reality? Too much to justify the benefit? We'll see. And while this concern has been around for a while, even when we were planning for somewhat mobile server VMs, VMware is the first company to make this easily accessible to end-users. This scenario is applicable to any virtual machine architecture where VMs can come and go in and out of the data center. This issue is not restricted to just VMware.

A lot to think about as VMs come full circle from end-user desktops with Workstation through the Data Center with ESX and now back to end-users with View, and hopefully a good chunk of that thinking involves security planning for portable VDI images. I already have ideas for bumper stickers: "Stop VDI Bombs!"

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.	F5 Networks	F5 Networks Ltd.	F5 Networks
Corporate Headquarters	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com