Bitdefender

Solution Paper

The six most important things to know about VDI/DaaS security

Bitdefender

Executive summary

As virtualization continues to mature, organizations look to virtualizing desktop and laptops. Companies such as Citrix continue to improve management features, while service providers such as Amazon Web Services continue to build and expand desktop-as-a-service offerings. However, virtualization isn't homogeneous. Just as public and private clouds, though related, are very different concepts, as is server and end-user system virtualization.

When x86 virtualization started to gain mainstream acceptance and the return on investment model was proven, the level of server virtualization adoption rose quickly. However, virtualizing desktops/laptops for end-users has consistently lagged behind. The reasons behind this are straightforward:

- Servers stay in the datacenter, whether they're physical or virtual ('cloud bursting' is not yet a reality)
- User experience with servers is accomplished via browsers, not 'hands-on' as is the case with end-user systems; in other words, to the customer, virtualizing a server that they access is transparent (the underlying infrastructure doesn't matter to them), while virtualizing and end-user system creates major changes to end-user experience
- End-user systems have to move from the hands of end-users to datacenters
- The major driver behind server virtualization – COST – is not shared by end-user system virtualization

Drivers of virtualized end-user workspaces

As David K. Johnson at Forrester rightly pointed-out "IT [is] shifting the reasons why they're interested in client virtualization technology. It's no longer about cost and efficiency, it's about employee workstyle flexibility!"[1]. The major drivers behind Virtual Desktop Infrastructure (VDI) adoption have changed; or perhaps the drivers have become more rational. Simply put, pursuing VDI as a cost-saving strategy, from the perspective of hardware and maintenance costs, as the primary driver, will doom VDI projects.

> *IT [is] shifting the reasons why they're interested in client virtualization technology. It's no longer about cost and efficiency, it's about employee workstyle flexibility!*

The problem is the last letter of VDI – **infrastructure**, and the cost associated with it. Where server virtualization was a transformation of datacenters, VDI involves the creation of new parts of a datacenter.

Transforming end-user experience is problematic. The majority of the time, end-users access servers via a browser or dedicated client, which pushes the experience to the end-user system. VDI, on the other hand, pulls the rug out from under that entire experience. End-users still have to access something, but now their access point is via an in-hand tool (tablet, lightweight laptop, etc.) and remote desktop instance. Interaction becomes troublesome (the gestures used to

interact with tablets don't yet translate well… in-fact, something as simple as removing a keyboard has not yet been accomplished!), along with connectivity, customizability, and other aspects of the end-user experience. Simply put, VDI doesn't change just the 'look and feel' of that experience, it changes the comfort zone and the user's behavioral state.

All of these considerations around VDI contrast with server virtualization. Looking back, virtualizing servers seems simple. It leveraged an easy to understand cost benefit (run more server workloads on fewer physical hosts), didn't affect end-users (the web application will look exactly the same), and it provided secondary benefits (flexibility, redundancy, etc.) beyond cost that were difficult to achieve using traditional technology.

This may all sound quite gloomy, but VDI, especially consumed as DaaS, may be experiencing a new push. Architects and other practitioners better understand that VDI is about getting centralized control of data, greater flexibility, not saving costs. Adding to this is the wider acceptance of Bring You Own Device (BYOD), or as the Citrix mantra goes, ***Don't Own Stuff***.

> *DOS – Don't Own Stuff*
> *I hear routinely in customer meetings about their desire to get out of the business of managing on-premise datacenters.*[2]

Virtualizing end-user systems is clearly a different undertaking, with different costs and benefits, than virtualizing servers. What does that mean for endpoint security?

Virtualized end-user systems and endpoint security

As organizations ramped-up efforts to virtualize servers, it revealed areas within datacenters that needed to change. Networking, storage, and the physical servers themselves; everything needed to be refreshed to accommodate virtualization. How datacenters are designed, planned, built, managed, and measured changed. However, the applications running within the endpoints being virtualized do not always make the transition quite as gracefully.

The physical-to-virtual migration is automated to the point that one can direct a tool at a physical system and sit-back whilst the operating system and applications running within are transformed from traditional endpoints to virtual machines. Endpoint security, meaning security that runs within an operating system, has proven to be the primary culprit responsible for performance problems in highly virtualized environments. This is because the physical-to-virtual migration is so smooth – until performance problems were identified as being caused by traditional antivirus products, people simply didn't question the wisdom of assuming that everything running within a VM would be virtualized gracefully.

While virtualizing servers leads to cost-friendly consolidation ratios (that is, the number of servers that can be run on each piece of hardware), those ratios are much lower than those achievable via VDI. Each end-user VM requires far less host resources than a virtualized server, and so many more VDI instances can be run per-CPU, unit of RAM, and so on.

The problem is that as the endpoint security that runs in each system is virtualized as part of the VM, and it is thereby duplicated across the VMs. If using traditional endpoint antimalware, each and every VM maintains a set of inspection engines, signature and heuristic databases, and everything else associated with endpoint security. The antimalware agents were designed to run on islands of hardware, following the traditional model, not the shared hardware that provides benefits in virtualized environments.

The result is commonly referred to as 'antivirus storms', which include performance bottlenecks due to:

- Scheduled scans during which the antivirus agent in every VM attempts to leverage as much of the hardware resources as are available, quickly exhausting those resources
- Updates during which every antivirus agent must download the latest signature and heuristic engines locally to maintain the latest level of security
- Upgrades during which antivirus engines are modified or reinstalled to maintain the latest level of security
- Inspection of the same objects (files, registry items, and so on) across VMs which are based on the same template, thus sharing single versions of many objects

The management tools of traditional antivirus products present their own problems in virtualized environments. As discussed, flexibility is a key benefit. Part of that is moving VMs between hosts based on load demand, maintenance cycles, etc. It also means being able to instantiate and destroy VMs, especially VDI instances, on a whim. Traditional management tools are built to monitor and control the antivirus client on long-lived, highly static systems. If hundreds, or even thousands, of VMs are created and destroyed daily, these consoles are quickly overwhelmed with orphaned entries.

The six most important things to know about VDI/DaaS security

While not every organization will encounter severe issues with traditional antivirus products when beginning to virtualize servers, every VDI deployment will see problems from the start. In the end, traditional antivirus clients and management tools are ill-suited for virtualized environments. Unfortunately, organizations have found themselves in the position of having to decide if a VDI project will fail, or if VDI instances will be created without endpoint security. Neither prospect is acceptable.

Following the key characteristics of virtualization, an antimalware solution built for virtualized environments should have, at least, the following:

1) Centralized and deduplicated components

The most harmful source of performance problems is the architecture of enforcement systems. In traditional environments, each endpoint was a hardware island, and antivirus clients were designed as such. In virtualized environments, running a full, independent antivirus client in each VM, especially in the case of VDI, will lead to significant performance problems.

Removing scanning components from VMs and moving them to dedicated, Linux-based virtual appliances vastly reduces the performance impact of endpoint antimalware. To perform inspection from a virtual appliance, there must be a method of remote introspection.

Look for a vendor that supports this style of scanning offload on multiple platforms, and across multiple endpoint types and operating systems. It is sometimes not clear exactly what a vendor is offloading, and on which endpoints. While a number of vendors have integrated with VMware vShield Endpoint, it is supported on only ESXi hypervisors, and protects only the file system, and only Windows VMs.

Centralizing scanning results and associated information is also important. For example, if a file is scanned on one VM of a host, there should be no need to scan the same file on any other VM that a virtual appliance protects. It is highly likely that VMs groups run similar workloads (many VDI instances based on one or two templates, for example).

2) Minimal in-VM footprint

While the marketing term ‘agentless’ has gained quite a bit of traction, it is misleading. There must be software in each VM to facilitate remote introspection by a virtual appliance.

As with VMware vShield Endpoint, that software may be bundled with another package (VMware Tools), or be a software package created by the security vendor. Note that with vShield Endpoint, there is no GUI in the protected VMs, and memory and process scanning is not supported. There are available additional software packages supplied by security vendors to deliver functionality layered on top of vShield Endpoint. In some cases, the security vendor may have a package that entirely replaces vShield Endpoint.

While the marketing term ‘agentless’ has gained quite a bit of traction, it is misleading. There must be software in each VM to facilitate remote introspection by a virtual appliance.

The least amount of functionality that is required for effective remote introspection should be present in each VM. The goal is to centralize as much as possible, reducing the updates/upgrades required at the VM. However, some functionality should be kept in the VM. Antimalware requires only certain blocks of a file. This inspection is based on the file type and other information, which can be identified only after

unpacking. Therefore, it makes sense to include engines that unpack and repack files within each VM. If unpacking is performed on the virtual appliance, entire files must be passed across the network to the virtual appliance.

3) Demonstrable performance improvement

As the saying goes, “trust, but verify”. Look for performance information that is based on industry standard tools, such as Login VSI (http://www.loginvsi.com/). One-off, commissioned test results based on custom tools are often misleading. If possible, attempt to verify performance information in your own environment. Above all, verify the scanning offload model in practice, as some vendors will market as though offloading is supported across environments, while support is actually limited to ESXi hypervisors and Windows VMs, thus requiring a heavy traditional antivirus agent in any configuration outside of their narrow support matrix.

4) Management integration

Traditional endpoint antimalware integrated with Active Directory. While that integration must still be included when dealing with traditional endpoints, integration with virtualization management systems is the new standard. These include vCenter and XenServer as the two most common examples, while integration with Amazon Web Services for protecting Amazon Machine Images, or other public cloud consoles, may be also be necessary.

Integration should be able to handle creation and deletion of VMs, allow security policy to be applied based on grouping (groups of VMs, Resource Pools, etc.), and generally ensure that management tasks performed in the virtualization management console are reflected in the security management console.

5) Support for a wide variety of environments

Although VMware ESXi dominates enterprise environments today, the wider market is far more varied. For example, Citrix solutions such as XenDesktop and VDI-in-a-Box support the management of VMs running on Xen, ESXi, and Hyper-V. When pursuing a VDI deployment, an enterprise with an existing VMware-centric datacenter may be likely to expand the ESXi base to include VDI managed by Citrix. However, a mid- or small-sized organization may prefer to use Hyper-V or open-source Xen for cost savings, and because they don’t have a VMware deployment.

Service providers who are building DaaS offerings may also turn to alternative hypervisors such as Xen or KVM for cost reasons.

While there will be a variety of scenarios today, no organizations wishes to be dependent on a single infrastructure vendor. To realize this, using security vendors who support a wide variety of environments is important.

6) Coverage of multiple endpoint types

Addressing endpoint antimalware in virtualized environments is important, especially in the case of VDI. However, introducing a new stand-alone console as a point-solution is not advisable. Vendors should be capable of building monitoring and control of virtualized environments in the same console that is used to manage traditional and mobile endpoints. While the ability to roll-up logs to a central reporting console is good, it does not necessarily centralize control. Be wary of solutions that require multiple control points for a single environment for reasons of either functionality or, quite commonly, scale. Prefer solutions that have modular management consoles that are capable of scaling, while maintaining redundancy, across all of your endpoints, no matter how large and/or distributed your environment is.

The Bitdefender approach to protecting VDI

Bitdefender has taken a multi-faceted approach to protecting VDI deployments. Centralized and deduplicated scanning offload is central to the protection mechanism, while providing a robust and scalable management console ties together VDI, server virtualization, traditional endpoints, and mobile endpoints.

The GravityZone security management solution architecture is based not on traditional client-server architecture, but rather, on cloud technologies. Beginning with the persistent data store, Bitdefender leverages MongoDB (https://www.mongodb.org/), a non-relational, high-performance and massively scalable datastore.

GravityZone is delivered as a single virtual appliance that is imported to an environment. The appliance is cloned as many times as needed, with each instance playing one or more discreet roles, such as datastore or web-based management console, within a single deployment. With built-in redundancy, including software load-balancers, a single deployment scales-out horizontally and across geographies.

GravityZone has three primary protection modules that are licensed separately, while managed (insight and control) from the same web-based console. These modules are Security for Endpoints (for traditional endpoints), Security for Virtualized Environments, and Security for Mobile Devices.

Security for Virtualized Environments (SVE) provides centralized and deduplicated scanning offload across a wide variety of environments. While integrated with VMware vShield Endpoint, many customers take advantage of Bitdefender unique offloading technology that covers:

- ESXi, Xen, Hyper-V, KVM, and other hypervisors
- Integration with vCenter and XenServer
- Windows and Linux, servers and end-user systems
- Memory and process scanning, in addition to real-time file system protection

Due to this wide support matrix, SVE was the first security solution to gain Citrix Ready (http://blogs.citrix.com/2012/11/26/bitdefender-is-citrix-ready/) status for VDI-in-a-Box, and other Citrix solutions.

For more information about GravityZone and Security for Virtualized Environments, including a free trial, refer to:

- http://enterprise.bitdefender.com/solutions/gravityzone/
- http://enterprise.bitdefender.com/solutions/gravityzone/virtualization-security.html

1. David K Johson's post: http://blogs.forrester.com/david_johnson/13-04-01-has_vdi_peaked_a_change_in_the_adoption_drivers_sheds_new_light_and_new_life)
2. http://blogs.citrix.com/2013/07/08/top-5-scenarios-for-xendesktop-on-windows-azure/

About Bitdefender

Bitdefender is a global company that delivers security technology in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning security technology, for businesses and consumers, and is one of the top security providers in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has created the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with some of the world's leading virtualization and cloud technology providers.

Bitdefender

BDE-180414-SP_KS-DaasVDI-en_EN