Bitdefender

White Paper

The impact of virtualization security on your VDI environment

Bitdefender

Introduction

Virtualization provides organizations with many costs savings and significant business agility. One virtualization technology that many organizations take advantage of is called virtual desktop infrastructure (VDI). VDI empowers employees and employers with many benefits, no matter the size of the organization. One such benefit with VDI is the ability to provide centrally managed desktop environments to employees on any device. In doing so, the organization can rest assured that information is always accessed and managed in a secure fashion – regardless of where the user is accessing information from.

VDI is not for everyone. Yet it does serve a purpose in production environments like call centers that have a high concentration of task-based workers, or to replace large scale office-based desktop deployments. However, as with any environment security should always play a pivotal role and should complement the business environment. With VDI it's no different; security should be seamless, without any effect on the user experience. Designed for physical environments, traditional security can hamper VDI deployments, thus reversing the purpose of adopting virtualization or VDI in the first place – efficiency, flexibility and cost savings.

This paper provides details about performance testing conducted using industry standard tools like Login VSI. The test results show the comparison of four security solutions available on the market today that have been specifically designed for virtualized environments. These test results are aimed to help organizations gain better insight into the sizing requirement and expected performance from their VDI deployments with optimized virtualization security.

What is VDI?

Virtual desktop infrastructure (VDI) is the practice by which a desktop operating system is hosted within a virtual machine. The virtual machine can be hosted in the organizations datacenter or from the cloud. In doing so, the VDI can be accessed from devices like thin clients, refurbished PCs, smart phones, tablets and so on. This provides organizations with the ability to guarantee quality end-user experience, regardless of the device used to connect to the corporate network.

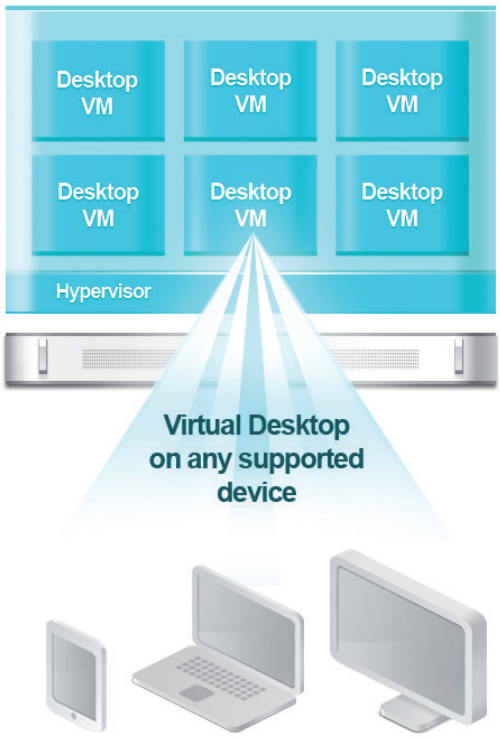

Figure 1: Virtual Desktop Infrastructure

Virtualization security challenges

It is a well-known fact that antivirus software is quite simply a requirement today. Applications running in physical, virtual or cloud-based environments are all susceptible to exploitation. Although traditional security can be used in virtualized environments, it is neither built nor optimized for virtualized environments.

Using traditional antivirus solutions can result in specific challenges in a VDI environment such as:

- Low virtual machine consolidation ratios
- Boot latency
- AV storms
- Outdated AV on dormant virtual machines
- Administrative bottlenecks

Consolidation ratios suffer as a result of using traditional security in virtual environments. Traditional security treats each virtual machine on a silo basis; it is not designed to evaluate all the virtual machine instances in a specific network or group. All application and user actions performed within the virtual machine instance are evaluated by the security agent within the operating system. This silo effect creates significant duplication, from signature databases to scan results for the same files, ultimately creating a performance problem, subsequently lowering virtual machine consolidation ratios.

Boot latency is the result of using traditional antimalware in virtual environments. When a virtual machine is started, the security solution must download its latest antivirus engine signatures, as well as the latest software updates. This update process alone can take anywhere between 5 to 12 seconds, which creates a window of opportunity for malicious intent.

AV storms occur when the traditional security solution agents installed on each virtual machine attempt to perform an update or a scheduled scan at the same time. In doing so, the host CPU, memory and IOP are overloaded, resulting in poor virtual machine performance and in some cases total host failure.

Outdated AV on dormant virtual machines brings the management of traditional antimalware security solutions full circle. Antimalware agents installed on dormant virtual machines can only be updated when the virtual machine is started, which results in boot latency issues and potentially AV storms, leaving the VM unprotected by the most current engine signature files.

Management of traditional security solutions can become tedious; this is especially the case in larger deployments. Each time a new traditional agent is installed, it is registered to the security management console, for administration. When a virtual machine is deleted or dormant, the traditional agent still remains registered with the security console and the only way to remove that entry is manually. This can become a laborious, mundane task, especially for large organizations where virtual machines are constantly on the move.

Choosing the right virtualization security solution

Bitdefender used the Login Virtual Session Indexer, (Login VSI) to test how the four virtualization security solutions available on the market today impact a VDI environment. These results can be used in deciding the sizing requirements for a VDI environment when deploying virtualized security.

Login VSI is an industry standard VDI benchmarking tool that simulates typical user behavior in VDI environments. The tool measures the total response time of several specific user operations being performed within a desktop workload in a scripted loop. There are three values in particular that are important to note the baseline, VSImax # VDI, and VSImax Dynamic.

1. The baseline is the measurement of the response time of specific operations performed in the desktop workload, which is measured in milliseconds (ms).

2. The VSImax # VDI is the maximum number of VDI sessions attainable on the host before experiencing degradation in host and VDI performance.

3. VSImax Dynamic is calculated based on the response times consistently being above a specific threshold. These thresholds are dynamically calculated on the baseline response time of the test.

A low baseline depicts better user experience, resulting in applications responding faster in the VDI environment.

Figure 3 outlines the test results of Security for Virtualized Environments (SVE) by Bitdefender compared to the three virtualization security products currently available on the market. There are a number of things to note:

1. The other three virtualization security solutions rely on VMware vShield Endpoint integration. Although SVE supports the same vShield Endpoint integration, it is not limited to only supporting environments that are using VMware vShield Endpoint. Bitdefender SVE has been purpose built and optimized for any virtualized environment. Figure 2 shows SVE for VMware vShield Endpoint and SVE Multi-platform version.

2. Security for Virtualized Environments (SVE) has the lowest Login VSI response times compared to its competitors, which results in better desktop workload performance and user experience.

3. As a result of SVE having the best response times, organizations using SVE are also able to achieve higher number of VDI sessions as compared to competitive security solutions.

4. With SVE one is able to attain at least 20 extra sessions compared to the nearest competitor. As a result; this equates to lower VDI costs due to less hardware being needed to host the same amount of VDI sessions.

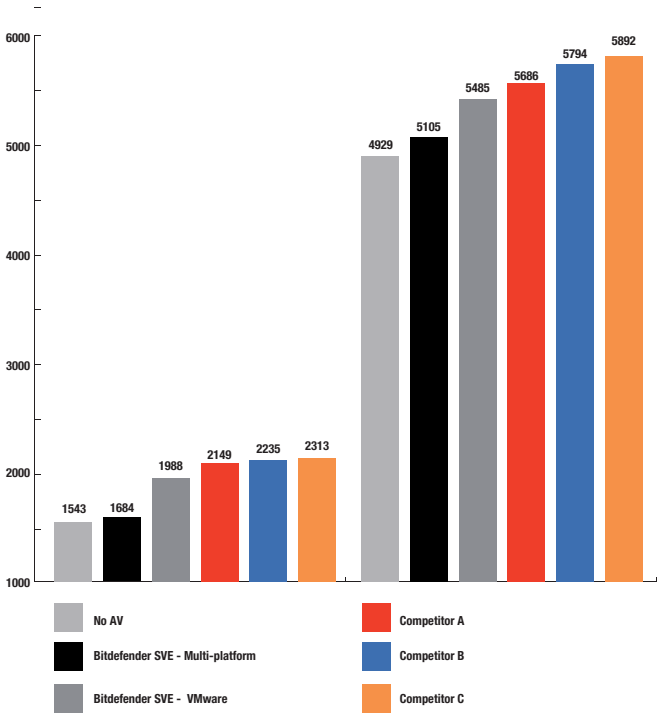

Figure 2: Login VSI – response times

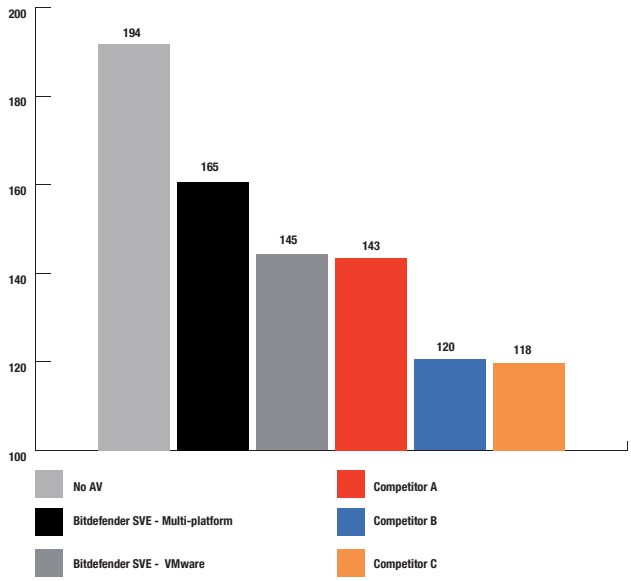

Figure 3: Login VSI – Max number of VDI sessions

Conclusion

It has already been proven, security is paramount to ensure that organizations' applications and data remain safe. However, security should not hamper the business in any way. Choosing the right security solution can mean the difference between additional capital outlay on

more hardware and frustrated employees and wasted productivity. In a VDI environment, the security solution implemented needs to have the least possible impact – lower waiting times for applications to open will result in better employee productivity and consequently in fewer helpdesk calls.

Security for Virtualized Environments is an all-encompassing security solution, specifically built for any virtualized infrastructure. When SVE is deployed in a VDI environment, it supports the highest number of VDI sessions achievable compared to any other virtualization security solution available on the market.

When compared to other virtualization security solutions, using SVE in a VDI environment results in:

- Improved cost savings.
- Improved application response time.
- Increased number of VDI sessions.
- Flexibility of using any hypervisor.

Appendix

Testing methodology

The following example illustrates how the baseline(ms) is calculated:

Activity	Result (ms)	Weight (%)	Weighted Result (ms)
Refresh document (RFS)	160	100%	160
Start Word with new doc (LOAD)	1400	33.3%	467
File Open Dialogue (OPEN)	350	100%	350
Start Notepad (NOTEPAD)	50	300%	150
Print Dialogue (PRINT)	220	200%	440
Replace Dialogue (FIND)	10	400%	40
Zip Document (ZIP)	130	200%	230
Baseline			**1837**

1. **VsiMax Dymanic (ms):**
   The formula for the dynamic threshold is: Avg. Baseline Response Time x 125% + 3000. As a result, when the baseline response time is 1800, the VSImax threshold will now be 1800 x 125% + 3000 = 5250ms.
2. **VsiMax # VDI:**
   When the response (ms) of all the sessions is above VsiMax Dymanic (ms) the “Maximum number of logged on sessions” (VsiMax # VDI) has been reached “End of test”
3. **Number of machines:**
   Before starting the actual tests, a number of VDIs are started waiting for VSI Login to login to the environment. 220 virtual machines are started at the beginning of each test run. This is performed to better mimic production environments where login may fail. Therefore, the number of “standby VDIs” is larger than the “logged on VDIs” and it has to be a constant value to make the test number of VDIs the same for all test runs.
4. **Test Timeframe:**
   The testing tool (Login Vsi Tool) launches sessions, there has to be some delay between the launched sessions. This value is set before testing to calibrate LoginVSI for the environment.
   The “Timeframe” value is the total time allocated for launching all 220 sessions. The testing tool will logon a user every 16 seconds. This means it must finish logging in all users within 3600 seconds.
5. **Heavy workloads:**
   The heavy workload utilizes higher memory and CPU consumption because more applications are running in the background. This workload simulated a power user. Once a session has been started the heavy workload will repeat every 12 minutes. During each loop the response time is measured every 2 minutes.
   - The heavy workload opens up to 8 apps simultaneously.
   - Type rate is 130ms per character.
   - 40 seconds of Idle time to simulate real-world users.

   Each loop will open and use the following:
   - Outlook 2007/2010, browse 10 messages.
   - Internet Explorer, one instance is left open (BBC.co.uk), one instance browses to Wired.com, Lonelyplanet.com and heavy flash app gettheglass.com.
   - Word 2007/2010, one instance to measure response time, one instance to review and edit document.
   - Bullzip PDF Printer & Acrobat Reader, the word document is printed and reviewed to PDF.
   - Excel 2007/2010, a very large randomized sheet is opened.
   - PowerPoint 2007/2010, a presentation is reviewed and edited.
   - 7-zip: using the command line version the output of the session is zipped.
6. **OS description:**
   - Windows 7 X86 SP1, updated
   - Defragmenter disabled
   - Search indexer disabled
   - Windows update disabled
   - Scheduled tasks disabled
   - Firewall disabled
   - Windows defender disabled
   - Web proxy auto-discovery disabled
   - Themes disabled
   - Superfetch disabled
   - Application experience disabled
   - Offline files disabled
   - Security center disabled
   - Machine debug manager disabled
   - Error reporting disabled
   - 1172 RAM allocated with no reservation
   - 1 VCPU allocated with no reservation
   - Pagefile set static to 2x RAM

About Login VSI

As VDI and HVD are becoming more and more established as end-user infrastructure technologies, performance emerges as one of the key-issues in these centralized environments. Organizations that are researching or implementing these new infrastructures want to make the right decisions about vendors, products and capacity. After implementation they are looking for ways to predict the effect that infrastructure changes may have on overall performance.

Login Virtual Session Indexer (Login VSI) is a vendor-independent benchmarking tool to objectively test and measure the performance and scalability of centralized Windows desktop environments such as Server Based Computing (SBC) and Virtual Desktop Infrastructure (VDI). Both leading IT-analysts and IT-vendors recognize and recommend Login VSI as the de-facto industry standard benchmarking tool for SBC and VDI.

Login VSI can be used to test virtual desktop environments like Citrix XenDesktop and XenApp, Microsoft VDI and RDS (Terminal Server), VMware View, Quest vWorkspace and other VDI/SBC solutions.

Customers of Login VSI use the tool for different purposes:

- **Benchmarking:** Make the right decisions about different infrastructure options based on tests.
- **Load-testing:** Gain insight in the maximum capacity of your current (or future) hardware environment.
- **Capacity planning:** Decide exactly what infrastructure is needed to offer users an optimal performing desktop.
- **Change Impact Analysis:** To test and predict the performance effect of every intended modification before its implementation.

Infrastructure vendor organizations that are committed to continuously improving the field of performance and scalability use Login VSI as an objective benchmark to test, compare, and improve the performance and scalability of their solutions. They publish the results in technical white papers (for an overview please visit www.loginvsi.com) and present the results at conferences. Login VSI is also used by end-user organizations, system integrators, hosting providers and testing companies.

Login VSI is the standard tool used in all tests that are executed in the internationally acclaimed Project Virtual Reality Check (for more information visit www.projectvrc.com).

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®