WHITE PAPER

Bitdefender®

HOW DO SECURITY SOLUTIONS AFFECT APPLICATION AND DESKTOP VIRTUALIZATION?

DIGITAL WORKSPACE ADOPTION AND USER EXPERIENCE

"When adopting virtual desktop infrastructures or desktop as a service, infrastructure and operations leaders need to prioritize the user experience." - Gartner

Businesses with large office- or task-based workforces, like call centers, are increasingly moving to application and desktop virtualization. In fact, 82% of organizations already use VDI, according to the End User Computing State of the Union Report by VDI Like a Pro.

This is because virtualization technologies, most notably for servers, applications and virtual desktop infrastructure (VDI), offer IT organizations and their end users an array of choices in accessing applications and desktops. They also form the foundation for hybrid, multi-cloud infrastructures that combine private and public cloud services. The collective benefits, including greater business agility, simplified management, and lower costs, have prompted a sweeping IT transformation to digital workspaces.

As organizations adopt digital workspaces, they naturally expect a higher-quality user experience. Unfortunately, traditional endpoint security solutions add latency that degrades the user experience and curbs the benefits of modern, digital workspaces.

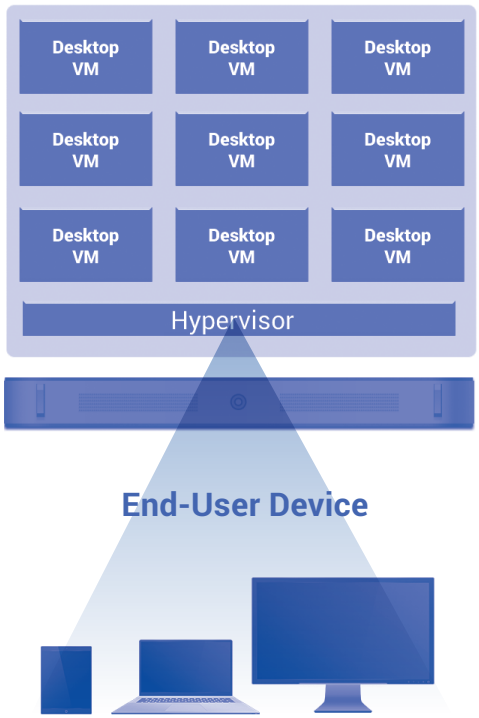

Figure 1: Virtual Desktop Infrastructure

What IT departments need for digital workspace implementations are security and management capabilities natively designed for virtual and cloud environments. Cloud Workload Security (CWS), or Cloud Workload Protection Platforms (CWPPs), address the security management challenges and performance constraints that traditional endpoint security tools create. When IT organizations begin assessing and selecting a CWPP solution, it is critical they determine the right fit and use trusted test methodologies and benchmarking tools like Login VSI for objective, evidence-based evaluation.

SECURITY CHALLENGES FOR VIRTUALIZED ENVIRONMENTS

While virtualized applications and desktops are centralized, they still must be secured. Applications and operating systems in virtual and cloud-based environments are susceptible to exploitation, just as they are in physical deployments. And while traditional security solutions can be used, they present significant challenges for VDI.

Low Virtual-Machine Density

Traditional security creates performance problems in virtualized environments and lowers virtual machine density, also known as consolidation ratios. It treats each virtual machine as an isolated silo, creating significant duplication - from maintaining redundant copies of threat intelligence data to scanning the same objects for malware multiple times.

Latency

Traditional antimalware also causes latency in virtual environments. Boot latency occurs when a traditional antimalware agent must update threat intelligence, engines, and other components. Even after bootup, latency hampers end user's experience, causing slowdowns and jitter in application performance and prompting IT support calls and, worse, churn among customers using such applications.

Management Challenges

Traditional antimalware also poses a variety of management challenges. For example, AV storms occur when traditional security solution agents on each virtual machine try to update or scan at the same time. This overloads the host CPU, memory, networking, and storage, lowering virtual machine performance and sometimes completely exhausting host resources.

Other management challenges stem from a lack of integration between security and virtualization

management solutions. Many VDI environments are extremely dynamic, with virtual machines (VMs) instantiated and destroyed with great frequency. Traditional endpoint security tools lack contextual awareness in these environments, so they struggle to provide the levels of automation and visibility needed.

This leads to gaps in the deployment of security tools to virtual instances and their unique identification (especially in the case of non-persistent VDI). It also creates problems in granular application of appropriate security policies and reporting on security posture. Only native integration with virtualization management solutions, such as VMware vCenter, Citrix XenServer, Nutanix Prism, Amazon Web Services, Microsoft Azure, and Microsoft Active Directory, can meet these management requirements.

Higher Costs

When organizations can't achieve targeted VM densities and low latency performance, application and desktop virtualization projects suffer. Consequently, IT is forced to either acquire additional hardware, driving up cost, or settle for an unsatisfying end-user experience.

PERFORMANCE TESTING WITH LOGIN VSI

Login VSI, which simulates typical user behavior in VDI environments, is the industry-standard VDI performance benchmarking tool. It measures the total response time of specific user operations performed in a scripted loop. VSImax and Baseline are the most important metrics:

- **VSImax** is the maximum number of VDI sessions attainable on the host without degrading performance. VSImax indicates the achievable levels of virtualization density.
- **Baseline** measures in milliseconds (ms) the response of specific operations performed in the desktop workload with no stress on the system. A low Baseline indicates a better VDI user experience. Very long response times are akin to working with a dynamic web page that takes extended periods to refresh.

These measurements show what is achievable with a given solution stack. The only way to improve results with the same software stack is to add computing power, driving up costs.

With a documented and controlled test harness, Login VSI test results allow IT organizations to better understand the choices they are making, and their potential impact on costs and user experience.

PUTTING SECURITY SOLUTIONS TO THE TEST

Bitdefender used Login VSI version 4.1.32 to test the performance of several security solutions. The test results below indicate how each affects a VDI environment. In this testing, the hardware, virtualization software, and other factors were the same. Only the security solution was changed from test to test.

Figure 2 shows the VSImax of each solution. This is the most straightforward test, representing the number of VDI instances that can run before the user experience degrades below adequate levels. Bitdefender GravityZone SVE Multiplatform enables the highest number of VDI sessions per host, 55% more than the lowest-performing solution tested. Virtualization density (the VSImax score) attainable with Bitdefender is second only to that of a system with no security running (which is, obviously, not recommended).

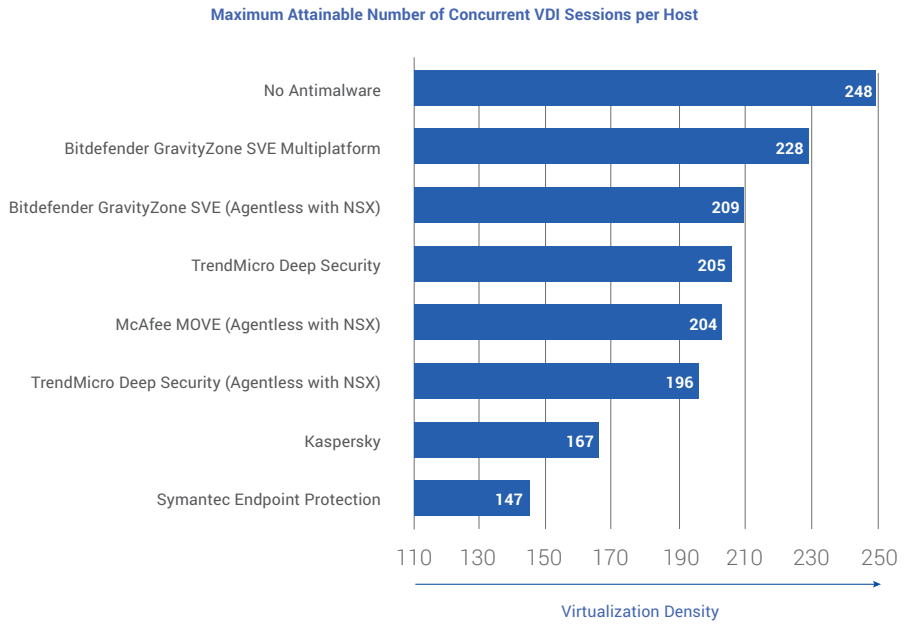

Figure 2: VSImax of each compared solution

Figure 3 outlines Baseline measurement of response times for specific operations performed with no stress on the system. Bitdefender achieves the fastest Baseline response time (36% faster than the lowest-performing competitor), allowing for a better user experience and superior system performance.

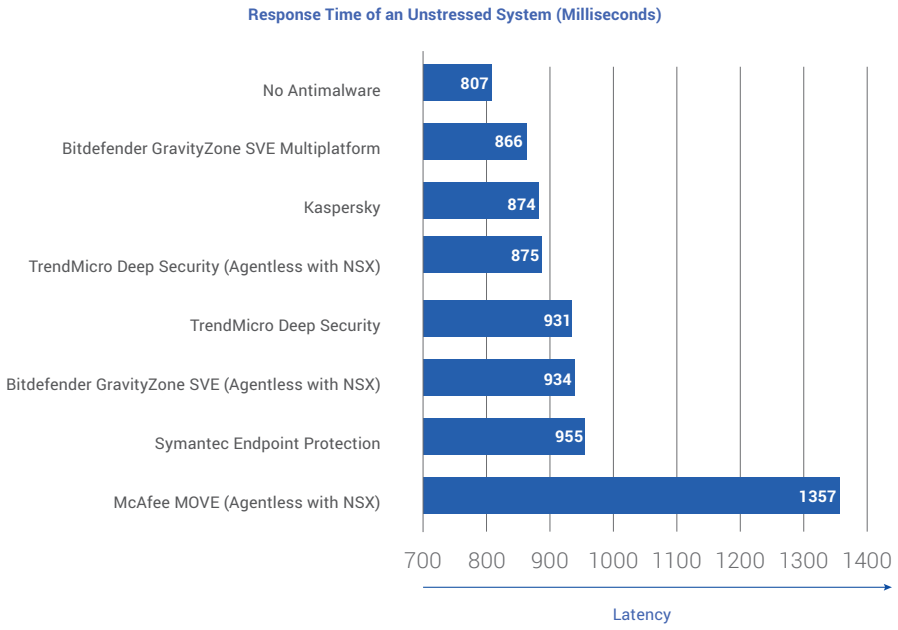

Figure 3: Test results for Baseline measurement

TEST METHODOLOGY

This performance study using Login VSI included Bitdefender software as well as solutions by other vendors.

All security solutions were installed and tested in the same environment, in a minimum default installation with antivirus and antimalware features activated. The performance metrics and values used are standard runtime performance parameters provided by Login VSI software, as described in its official documentation:

- VSImax Metrics, Baseline, and Average are calculated using the methodology published by Login VSI for version v4.1.32: https://www.loginvsi.com/documentation/index.php?title=Login_VSI_VSImax
- VSImax parameters (VSI Timers, VSI Index) are computed automatically by Login VSI using the methodology described in this article: https://www.loginvsi.com/blog/login-vsi/481-calculating-maximum-virtual-desktop-capacity-vsimax-explained
- The Login VSI workload profile configuration used in our testing is “Power Worker”. The description of this profile is provided here: https://www.loginvsi.com/documentation/index.php?title=Login_VSI_Workloads#Power_Worker

TEST ENVIRONMENT

Hardware Configurations	**(1) Dell R730xd server** • **CPU:** 2 x Intel e5-2680 • **Memory:** 386 GB RAM DDR4 • **Storage Controller:** Perc H700 • **Local Storage:** 12x Samsung 860 PRO in RAID 0 • **Network:** 2 x 10 GBE interfaces
Compute Platform Software	**VMware vSphere** • ESXi hypervisor version 6.5.0 6765664 • vCenter Server version 6.5.0 Build 8024368 • NSX Manager version 6.4.1 8599035
VM Hardware Configurations (VDI Image)	• CPU: 2 vCPUs allocated, no reservation • 1408 MB RAM, no reservation, no limits • 100GB single disk, thin provisioning
VDI Orchestration	Citrix XenDesktop version 7.15
Guest OS Image Software	• Windows 7 SP1 x64 build 7601 (up-to-date patches as of 10/1/2018) • VMware Tools version 10.1.7.10279 • Default page file configuration • Image optimized for VDI workloads using VMware VDI Optimization Tool, including: 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
Testing Scan Policy	• Scan all files • Scan network files • Exclude archives from scanning • Exclude mail archives from scanning

SELECTING THE RIGHT SOLUTION

Choosing the best security solution for a virtualized application and desktop environment can determine the success or failure of a project. Success leads to a high-quality end-user experience, while failure prompts support calls, lost revenue, and the need for additional hardware.

A security solution in an application and desktop virtualization environment must have the least impact possible. It must facilitate end-user productivity and meet high user expectations for speedy boot-ups, logins, and application response.

Bitdefender GravityZone Security for Virtualized Environments (SVE) is an all-encompassing security solution built specifically to protect virtual and cloud workloads.

Compared to other security solutions, GravityZone SVE offers:

- Improved application response time and end-user experience
- Increased VM density
- Greater flexibility in choice of hypervisor and cloud platforms
- Comprehensive protection for files, memory, processes, and registry.

> "Because GravityZone has lightened the load on our servers so much, performance support tickets have practically disappeared. When they occasionally come in, we no longer trace root cause to security.
>
> [Plus, with GravityZone] virtualization density improved by up to 30 percent, eliminating the need for additional infrastructure"
>
> – Mentor, a Siemens Business

1 Define and Prioritize the User Experience to Succeed with VDI and DaaS, Gartner

2 Mentor Fires Up Datacenter Transformation With Next-Gen Security, https://download.bitdefender.com/resources/files/News/CaseStudies/study/204/Bitdefender-Business-CaseStudy-MentorGraphics-creatent154-210x297-en-EN-GenericUse.pdf

Bitdefender®

www.bitdefender.com

Bitdefender is a global cybersecurity leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for the smart connected home, mobile users, modern businesses and their networks, devices, data centers and Cloud infrastructure. Today, Bitdefender is also the provider of choice, embedded in over 38% of the world's security solutions. Recognized by industry, respected by vendors and evangelized by customers, Bitdefender is the cybersecurity company you can trust and rely on.

Bitdefender-Business-WhitePaper-VSI-CREA3420-letter-en_US