Bitdefender

Solution Brief

Security for Virtualized Environments Running Citrix Xen

CITRIX ready

Bitdefender

Virtualization provides organizations with many costs savings and significant business agility. Among the most efficient datacenter operators are service providers, such as Cloud Service Providers (also known as infrastructure-as-a-service) and application-as-a-service providers.

Within traditional businesses, virtualization is powering a shift toward IT as a service. As an organization increases the level of virtualization and takes steps toward creating an internal (private) cloud, operating margins become a primary focus of IT departments. Similarly, cost and operational efficiency represent the primary driver for leveraging external (public) clouds.

Many organizations use the Xen hypervisor, while service providers often use Linux operating systems as they provide attractive cost models and operational flexibility. These organizations excel at increasing operational efficiency through innovative use of virtualization since datacenters are not part of the business, but rather, datacenters are the business.

When creating a highly virtualized datacenter, organizations normally consider the impact on hardware, networking, storage, back-up, and so on. However, they must also consider the impact of endpoint security on the success of their cloud infrastructure projects.

This solution brief describes the often unanticipated impact of endpoint security on operating margins, which must be considered as organizations push virtualization usage toward cloud.

Virtualization security challenges

It is a well-known fact that antivirus software is quite simply a requirement today. Applications and operating systems 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 this type of infrastructures.

Using traditional antivirus solutions can result in specific challenges in a cloud 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- Outdated AV on dormant virtual machines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. All application and user actions performed within a virtual machine instance are evaluated by a security agent within the operating system. This generates significant duplication across the environment, from signature databases to scan results for the same files, which ultimately creates performance issues and lowers virtual machine consolidation ratios.

Boot latency is the direct result of using traditional antimalware in virtualized 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 that in some cases leads to denial of service.

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, especially 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 frequently moved.

Virtual Desktop Infrastructure is an area where organizations encounter most of the challenges listed above. On performance, VDI introduces much higher consolidation ratios than server virtualization. There are far more copies of traditional antimalware agents that require memory, CPU, and storage. This exposes significant performance bottlenecks, making organizations consider having to choose between the success of a VDI project (as measured by ROI) and endpoint security. The highly dynamic nature of VDI deployments also leads to various management issues, as hundreds of VMs are daily instantiated, moved, and destroyed.

Strong Security: organizations seldom question the efficiency of their endpoint security, considering it “good enough” and ignoring the performance implications it triggers. In this context, virtualization must be viewed as an opportunity to evaluate the security strengths of an endpoint security solution. While moving to virtualization-specific solutions, organizations must also consider the strength or level of protection they provide. Many of the

solutions available on the market do not support critical functionality like memory or process scanning of virtual machines, which leaves the company's security posture exposed.

Cross-platform Security for Virtualized Environments

Bitdefender has created Security for Virtualized Environments (SVE) to address the security needs of organizations with highly virtualized environments. The solution centralizes and deduplicates scanning of virtual machines on a hardened Security Virtual Appliance for each host system. In addition to VMware vShield Endpoint 5 integration accommodating agentless protection, SVE leverages unique Bitdefender technologies to protect VMs running on virtualizations platforms such as Xen and Hyper-V.

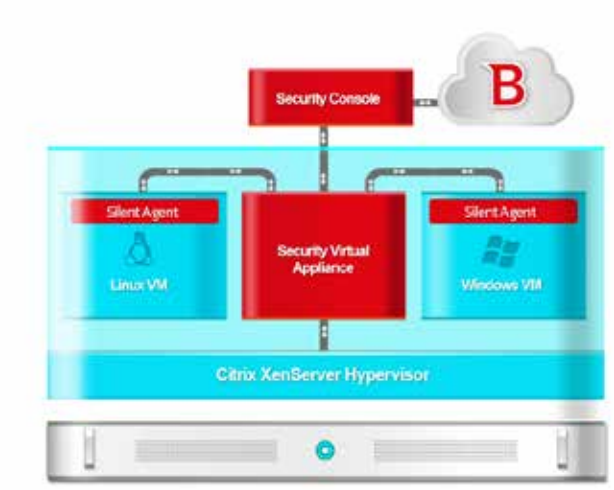

Figure 1: Overview of SVE architecture

Leveraging the pooled nature of virtualization, SVE allows for greater VM density. While traditional solutions require full antivirus clients installed on each virtual machine, Bitdefender delivers a dedicated virtual appliance to perform regular antimalware activities outside the protected guests.

Centralized scanning eliminates the need to install a full, traditional antimalware client on each VM. This saves hundreds of megabytes of storage for each VM, along with the CPU, memory, and network resources required to maintain individual traditional antimalware agents. Intelligent caching mechanisms further improve performance by ensuring that files duplicated across VMs (such as operating system files) are not scanned more than once.

To ensure complete visibility and ease the administration effort, SVE is integrated with Citrix XenCenter and VMware vCenter. SVE further integrates with Amazon Web Services to provide cloud-centric antimalware delivered as a service for Amazon EC2 users worldwide.

When investigating the available technology, it is important to consider virtualization platform and operating system support. SVE offers flexibility in both areas, within a single solution. From one management console, Windows and Linux VMs running on Xen, vSphere, Hyper-V, and KVM, can be protected without full antimalware agents in each VM. This hypervisor-agnostic approach is important today, and may be even more important in the future as organizations embrace emerging cloud technology. The extreme flexibility of the SVE technology was proven by its presence on the Amazon AWS Marketplace at its launch.

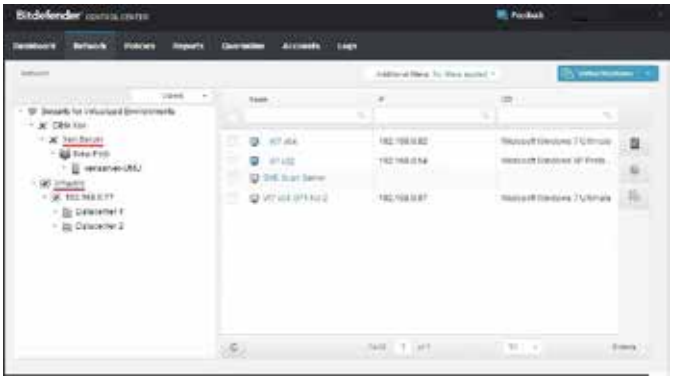

Figure 2: Unique control center for Citrix and VMware

Deployment is as simple as importing two virtual appliances. Security Console is the management console that covers an entire environment. A single Security Virtual appliance is imported to each physical host. Both are Linux-based virtual appliances that require minimal configuration. The simplified deployment process means that even the largest environments are protected quickly.

With Amazon Web Services, protected instances are centrally managed from the intuitive Bitdefender Security Console due to close integration with Amazon EC 2 API sets. It provides users with a unified view of the security state across all AWS regions, acting as a single point of control for configuring and reporting on the security activity within the cloud. To further streamline the administrative effort, the solution enables automatic deployment of the antimalware protection through AWS instance tagging.

Finally, SVE is the only virtualization-centric security solution able to scan processes and memory of virtual machines. This, combined with Bitdefender consistently top-ranked anti-malware capabilities, means that security need not be sacrificed when considering performance. If performance problems caused by security can hamper virtualization success, security concerns caused by virtualization may also limit virtualization momentum in an organization.

Conclusion

Organizations today are increasing the scope of virtualization projects. While initial projects certainly gain from increased returns delivered by solutions like Security for Virtualized Environments (SVE), the move to heavier use of virtualization likewise increases the gains provided by SVE. As the drive toward infrastructure as a service, via an internal or external cloud, becomes more common, the strategies that the most successful service providers employ must be adopted.

Choosing the right endpoint security is an important strategy of all virtualization projects from the perspectives of performance and security. The key characteristics of endpoint security in virtualized environments include the ability to centralize and deduplicate scanning at a virtual appliance, providing these benefits across multiple hypervisors and operating systems, together with management integration. The primary goals are to provide strong security while minimizing the resource use of security across environments and easing the management overhead.

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®