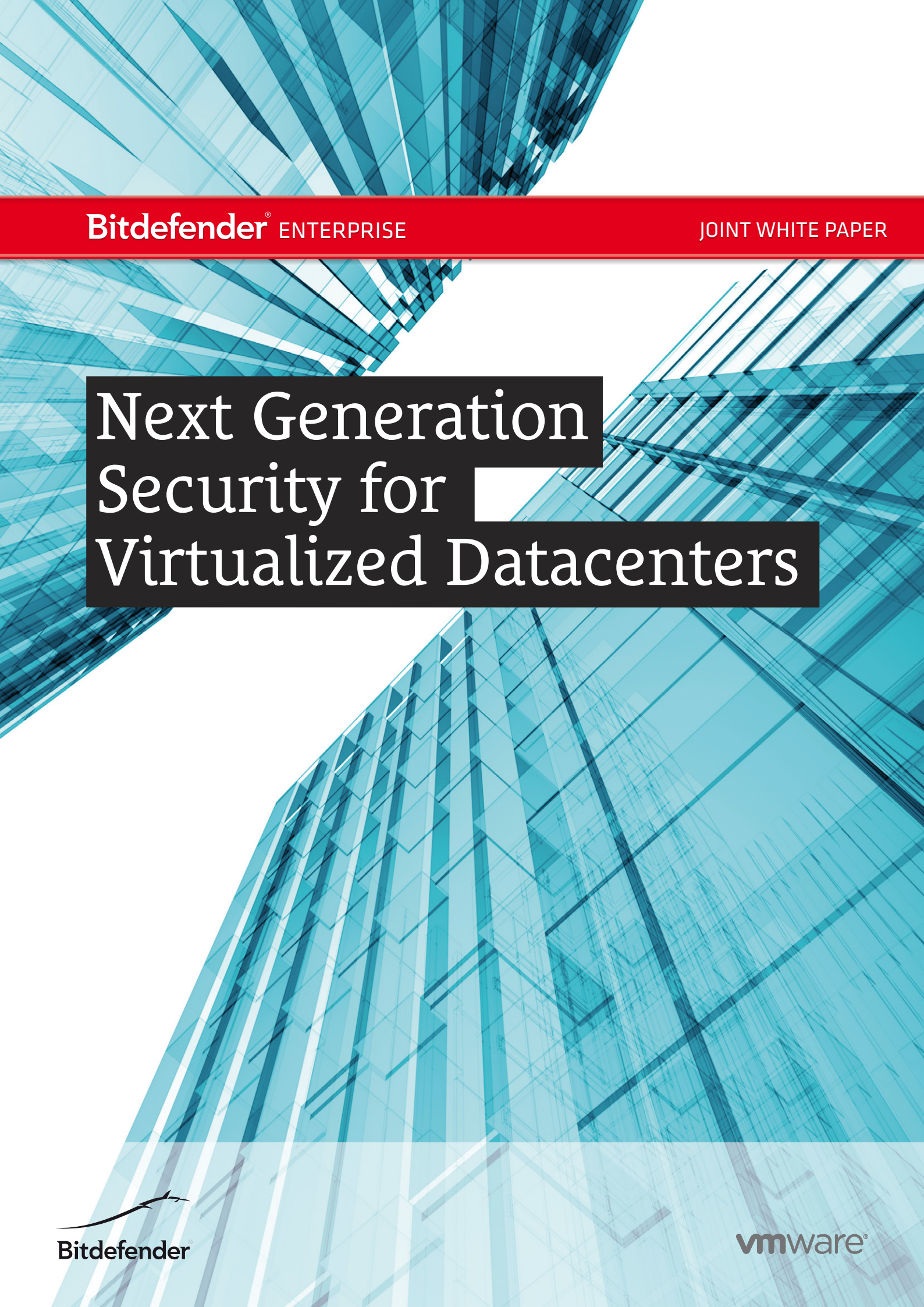

Bitdefender® ENTERPRISE
JOINT WHITE PAPER
Next Generation Security for Virtualized Datacenters
Bitdefender®
vmware®

Introduction

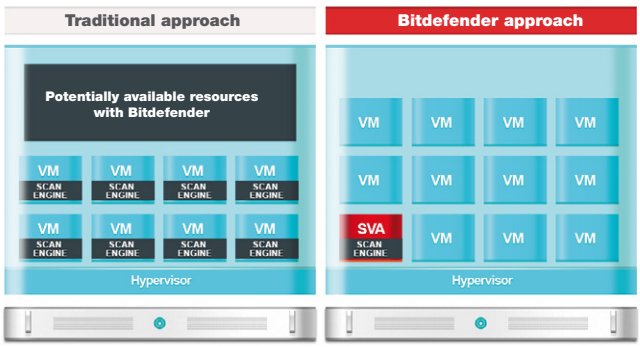
In recent years, virtualization has gradually become a game-changing strategy for the IT industry worldwide and is now a tried and true approach for corporate computing environments. Since its emergence as a consolidating technology, it has continued to drive tremendous operational benefits, which help increase IT productivity and accelerate business agility. Virtualization lowers various equipment and maintenance-associated costs, while also providing higher availability, density and automation rates across data centers.

To accelerate the business benefits enabled by virtualization, companies must not overlook security. However isolated and self-contained, virtual containers are still vulnerable to increasingly sophisticated malicious attacks carried out by dedicated networks of cybercriminals. The larger the virtualized environment, the more challenging it can become to efficiently secure virtual machines, mainly because of their dynamic nature: they can be moved from one host to another, remain dormant or offline for extended periods of time. In addition to providing context-aware protection, security tools must also ensure optimized utilization of resources for improved performance in the virtualized environment.

Limitations of legacy security models

The need for adaptable, context-aware security software is even more critical, as organizations embrace cloud computing offerings. Although not the best practice, organizations are still deploying typical endpoint antivirus solutions designed for physical platforms, in a hasty transition from physical to virtual environments.

Lacking virtualization awareness and optimization, these traditional solutions have proved inefficient and are resource intensive when running on virtual machines. With heavy agents installed on each virtual machine, endpoint security software can cause massive degradation of service during periodic maintenance or scanning processes.



One example of such performance spike is the resource contention condition or AV storm, which occurs when multiple virtual machines residing on the same host are using the server's CPU and memory resources during concurrent scanning. Apart from the impacted production efficiency, such performance hits also affect the pooling capacity expected from virtualized servers.

Agentless security with VMware vShield™ Endpoint

As the global leader in virtualization and cloud infrastructures, VMware delivers enterprise-ready solutions, which provide the key for business success. Embraced by hundreds of renowned companies worldwide, VMware's approach accelerates the transition to cloud computing, while ensuring faster provisioning, higher availability and better manageability. At the same time, VMware improves performance of VM security with vShield Endpoint 5.

Designed to streamline resource utilization and provide cost-effective security tools for virtualized datacenters, VMware vShield Endpoint provides the EPSEC API for integrated security. This modern concept facilitates a number of technological benefits that help transcend the performance limitations of physical security, while significantly reducing system requirements. To eliminate the need for locally-installed antivirus agents, the EPSEC drivers offload key antivirus functions to a dedicated secure virtual appliance. Critical physical resources are thus deduplicated so that virtual machines will no longer have to compete for disk and memory resources of the host during simultaneous scanning or virus signature

The vShield Endpoint Advantage

- Streamlines download of antivirus updates and antimalware file events to a hardened SVA
- Improves VM performance through secure offload mechanisms
- Maximizes VM consolidation ratios by minimizing the antivirus footprint

The following scenario illustrates the difference in cost efficiency between vShield-integrated solutions and legacy antivirus software, from a storage allocation perspective. With agentless security, system administrators can easily allocate storage capacity per physical host instead of VM, because there is no antivirus footprint installed locally on each virtual machine, hence no storage impact. Calculations involve 4,000 virtualized servers on 400 physical hosts, where the price per TB of SAN is $6,000.

SAN Allocation with Legacy AV	4 TB (4,000 VMs * 1 GB per VM)
SAN Allocation with vShield Endpoint	1.2 TB (400 hosts * 3 GB per host)
Legacy AV – Associated Costs	$24,000 (4 TB * 6,000)
vShield Endpoint – Associated Costs	$7,200 (1.2 * 6,000)
Cost savings with vShield Endpoint	$16,800 (24,000 – 7,200)

Note: *SAN allocation with vShield Endpoint of 3 GB includes: 2 GB for SVA and 1 GB for the Security Console.*

Common security gaps occurring with legacy security are also eliminated due to the tight integration between Security for Virtualized Environments by Bitdefender and vShield™ Endpoint.

For instance, this security model helps prevent boot latency security gaps because the antivirus engines and database reside within the Security Virtual Appliance (SVA), which never goes offline. Typically, scan engines take up to 12 seconds to load, during which time virtual machines are potentially exposed to any threat.

Locally-installed antimalware agents represent another exploitable breach. Most attacks succeed when carried out on unpatched operating systems with outdated virus signatures. Moreover, the antimalware agents can themselves become the target of stealth malicious software trying to evade security checks or even to disable core functions of the antivirus program. Such risks are completely mitigated with the vShield-integrated model.

The Security Virtual Appliance and vShield Endpoint components form a robust set of software, which implements centralized scanning capabilities while dropping the antivirus footprint on each virtual machine. In this single-instance or agentless security model, the connection between the tamperproof Linux-based appliance and the protected virtual machines is intelligent and interactive, leaving nothing to chance.

Resource-effective security for virtualized datacenters

In response to these limitations of the traditional security approaches, **Security for Virtualized Environments by Bitdefender** provides highly-optimized protection with minimal resource requirements, which helps prevent any usage bottlenecks. Addressing even the most demanding performance requirements, Bitdefender provides virtualization-smart security, without hampering the shared computing and storage pools.

The world-class level of security, as well as the overall simplicity and flexibility provided by Security for Virtualized Environments, make it perfectly suitable for any type of virtualized infrastructure. While accommodating silent protection and highly-optimized scanning traffic, Bitdefender's solution scales to the datacenter's capacity and ultimately boosts business production by ensuring improved consolidation ratios.

Bitdefender takes further advantage of the VMware extensible solutions by integrating the Security Console with the vCenter server, a powerful management tool for vSphere-based infrastructures. This combination creates a tightly-controlled line of defense across the datacenter and facilitates increasing visibility over the entire protected area, while dynamically paving the way to cloud computing models.

Extending VMware vShield for comprehensive security

Process and Memory Scan

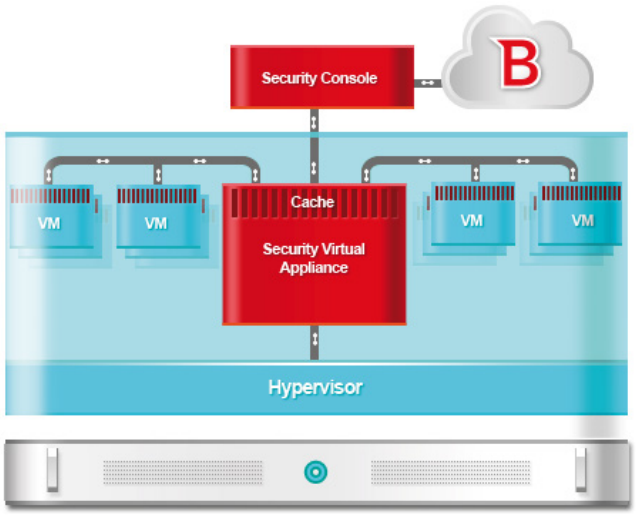
Security for Virtualized Environments not only highlights the VMware advantage, but also strengthens VM security by enabling process and memory scanning inside the Silent Agent component. With dormant VMs susceptible to sophisticated rootkit injections, memory and process scans are even more important than in physical environments. Together with the SVA-contained antimalware activity, these local scans ensure full protection at a VM level without overloading Silent Agent's light footprint.

Cross-Platform Support

To further leverage the complexity and specificity of each datacenter, Bitdefender adds value to any virtualization project by offering a comprehensive package adapted to any virtualization technology. On the guest side, the minimal system requirements are combined with extended support across multiple platforms, including Windows, Unix and Solaris.

Adapted Architecture for non-VMware Environments

In non-VMware environments, Security for Virtualized Environments by Bitdefender extends security to make it comprehensive by incorporating patent-pending technologies, which perform similarly to vShield Endpoint. Due to its remarkable scalability, the Bitdefender solution acts as a key enabler for improved resource consolidation, enabling significant savings in operational expenditures and resource consumption. Created on a highly-optimized architecture, Security for Virtualized Environments provides every organization with a set of reliable security tools able to maximize the return on VDI investment, without compromising consolidation ratios.



vmware Bitdefender

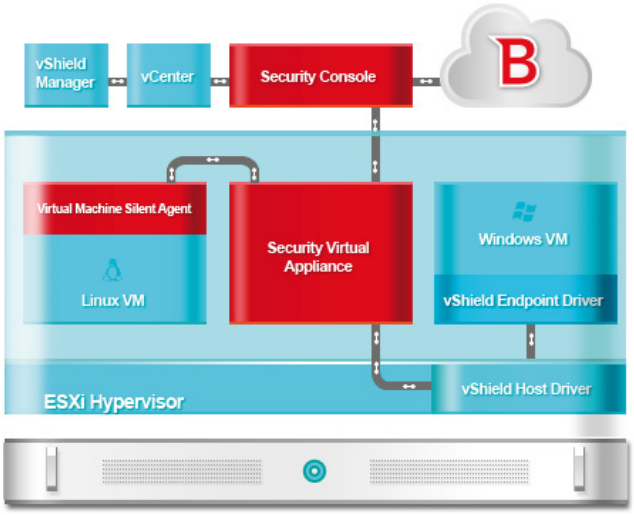
Main components of Security for Virtualized Environments

Bitdefender delivers a simplified package based on an innovative architectural framework comprising of:

Security Virtual Appliance (SVA): A dedicated security machine running on a hardened Linux server installed on each host. It is the single, centralized location for Bitdefender's scanning engines and signature updates. Connected to the protected guests through vShield EPSEC drivers, SVA supports scheduled, on-access and on-demand scanning, and thus deduplicates the antivirus-associated load. It is made up of four modules, which plug directly in vShield Endpoint: powerful scanning engines, signatures database, scan managers and smart cache mechanisms.

Silent Agent: A lightweight in-guest component, which displays notifications for local security events and facilitates process and memory scanning on the protected virtual machines. It has a very small footprint (up to 4 MB of disk and 6 MB of memory) and can be automatically deployed on Windows, Linux or Solaris guest systems.

Security Console: An intuitive web-based interface acting like a security hub for the virtualized environment. Integrated with VMware vCenter server for enhanced visibility, the console is the central point of management and monitoring for the protected VMs. Bitdefender Security Console enables deployment of the Security Virtual Appliances and Silent Agents, centralized quarantine, policy enforcement throughout the virtualized datacenter, advanced reporting of the security status on the dashboard and on-demand, scheduled or recurrent reporting.



Conclusion

Best-of-breed Security, No Bells and Whistles

As more and more corporations virtualize their infrastructures, security best practices must not be overlooked. The adoption of legacy solutions has proven inefficient due to the architectural differences between physical and virtual environments. Specifically, traditional software solutions have not passed the performance test when running on virtual machines. While being heavily wasteful in resource utilization, they can cause undesirable performance hits like resource contention.

Security for Virtualized Environments by Bitdefender addresses all the virtualization-specific challenges by providing simplified and comprehensive security for even the most demanding and heterogeneous datacenters.

Partnering with VMware, the world-leader in virtualization technologies, Bitdefender delivers a highly-optimized solution, closely integrated with vShield 5. Strengthened by the vShield Endpoint components, Bitdefender implements centralized scanning within a hardened Linux-based Security Virtual Appliance. While unobtrusively defending virtual machines with the lightweight Silent Agent, the solution goes beyond VMware's area of protection by ensuring process and memory scan capabilities. Additionally, it covers an extended range of operating platforms, including Windows, Unix and Solaris, in environments powered by any virtualization technology.

About Bitdefender

Bitdefender is a global company that delivers security technology in more than 200 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.

About VMware

VMware is the leader in virtualization and cloud infrastructure solutions that enable businesses to thrive in the Cloud Era. Customers rely on VMware to help them transform the way they build, deliver and consume Information Technology resources in a manner that is evolutionary and based on their specific needs. With 2011 revenues of $3.77 billion, VMware has more than 350,000 customers and 50,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com.

Bitdefender