# Bitdefender Security for Virtualized Environments

Now Available in the #1-Ranked MSP Security Suite

Despite the widespread use of virtualization, Managed Service Providers often use highly inefficient security tools that require multiple copies of the antimalware agent on the host computer hardware, one for each virtual machine (VM). This approach suffocates host resources, deteriorates the user's experience, reduces the number of virtual machines that can run on the host and drives some MSPs to leave VMs unprotected.

Bitdefender Security for Virtualized Environments (SVE) was designed from the bottom up for virtualization. Rather than placing a copy of Bitdefender on each virtual machine, SVE uses one VM, turning it into a Security Virtual Appliance (SVA) that protects all other VMs in the host environment. By having only one instance of Bitdefender's antimalware agent running in the virtualized environment instead of many, performance, consolidation ratios, and the user's experience are drastically improved

SVE is now available as an optional billable service module within the Bitdefender MSP Security Suite.
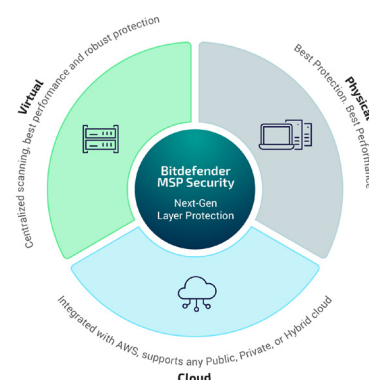
Highlights

- Drastically improves VS/VDI performance and user experience
- Improves application performance
- Unified MSP Security for physical, virtual, and cloud
- Eliminates single points of failure and bottlenecks across virtualized environments

- Full-fledged layered security that includes machine learning, process monitoring, and anti-exploit
- Automates VM security provisioning and eliminates security gaps
- Supports VMware, Citrix, Microsoft, and all other hypervisors

Key Benefits

Best-performing virtualization security

SVE was designed to solve issues related to running AV in a virtualized environment. Our extensive performance testing using LoginVSI proves that SVE has the lowest impact on performance of all major AV solutions, delivering up to 17% better application response times and an increase in VM deployment per physical device (maximized consolidation ratios) of up to 35%.

No compromise, full-fledged layered protection

Bitdefender delivers multiple layers of protection such as machine learning, anti-exploit and continuous process monitoring to maximize protection, while other solutions include only basic technologies to avoid hurting VM performance.

MSP Security for physical, virtual, and cloud

MSPs reduce security monitoring, administration, and reporting efforts and costs with a single dedicated MSP security console (single pane of glass) for physical, virtual, and hybrid cloud environments. Unlike other solutions, Bitdefender supports any hypervisor, is integrated with AWS, and supports all cloud environments.

Highly resilient architecture

The Security Virtual Appliance (SVA) is delivered as a Linux Ubuntu self-configuring hardened virtual appliance. Failover capabilities and load balancing with multiple SVAs ensure optimum performance and protection at all times.

Award-winning security

Bitdefender SVE comes with a powerful mix of security technologies equipped to handle everything from basic malware to the most advanced targeted attacks. In March 2018, Bitdefender won AV-TEST's prestigious Best Protection 2017 and Best Performance 2017 awards, thanks to technologies such as Process Inspector, advanced anti-exploit, award-winning antispam and content filtering, as well as its multi-layered anti-ransomware defense.

The entire arsenal of award-winning Bitdefender threat protection technologies is built into the security engines and embedded into the virtual appliance architecture. With SVE, antimalware protection is more robust than ever, providing leading protection and highly available, instant-on protection for every VM.

Technology overview

Unlike traditional antivirus agents that need to reside on each VM, require constant updates, monitoring and consume significant local resources to operate, Bitdefender's SVE provides the option of delivering antimalware protection using a Security Virtual Appliances (SVA). SVE functions as centralized points of antimalware intelligence, without a traditional security agent installed in each VM. Each VM connects to a Security Server to offload most antimalware functionality, protecting file system, memory, process and registry scanning in both Windows and Linux environments.

SVE uses a multi-layered caching mechanism that contributes to industry-leading performance. First, a local cache is maintained within each VM so objects are scanned only once. Second, a shared cache is maintained at each security server (SVA) so objects scanned on one VM are not scanned on the others. Finally, a series of file block-level caches bring deduplication of scanning down to the level of file chunks, meaning that similar files are not completely rescanned. The net result of these Bitdefender-exclusive technologies is the secret behind the maximized performance that SVE provides.

Central Scan at a glance

For the Security Server to access the file system of each VM, along with memory, registry and running processes and other required features, a communication agent known as Central Scan must be deployed to each VM. The characteristics of Central Scan agent are:

Low system impact:
- Less than 110 MB storage during runtime (including runtime cache)
- 10-20 MB local memory during runtime (on-access scanning)
- Peak CPU load of 1-2%, on a single virtual CPU for on-access scanning

Primary functions:
- Establishes connection to an available authorized Security Server (SVA), allowing local access to file system, registry, memory and processes.
- Switches connection to alternate Security Servers in case of slow response time or sudden unavailability.
- Manages local disinfection, quarantine and process blocking.
- Maintains local cache of scanned items for performance gains.
- Runs as a local service with all administrative privileges removed, guarding against attacks that attempt to shut down protection locally.
- Optionally provides a User Interface inside the VM with desktop pop-up notifications.
- Deployment of Central Scan (available in both a Windows and Linux version) is simple and requires no reboot of the virtual machines. Additionally, deployment of the Security Server does not require a reboot of machines hosting VMs.
- Central Scan can also be baked into templates and VDI images to minimize management overhead.
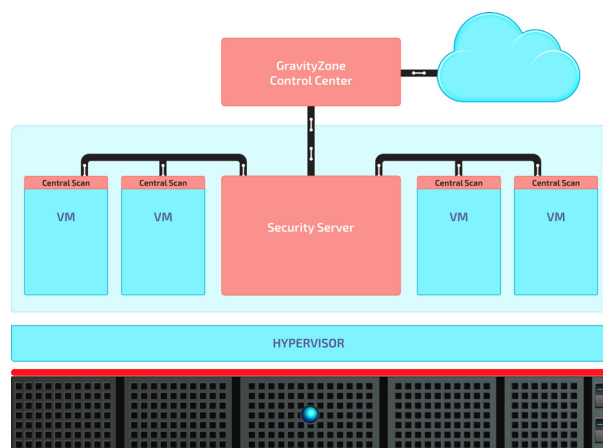
Advanced Architectural Design
- Virtual Machines have no local antimalware scanning engines and definitions, and will always be protected by an available Security Server
- Eliminates the possibility of AV storms
- Multi-level caching across individual VM and Security Server ensures unique files are scanned only once
- Eliminates boot-time performance and security gaps encountered as VMs start
- No single point of failure in the protection, as Central Scan automatically connects or reconnects to an available Security Server, as defined by policy
- Centralized protection without bottlenecks, since Central Scan can automatically switch to another Security Server with a faster response time
- Non-persistent virtual machines are automatically protected and governed by the correct security policy
- Increases VM density, through reduced memory, disk space, CPU and I/O activity
- VMs are always protected by the latest, up-to-date, Bitdefender technologies, even if restored to an older snapshot/backup or if booted after an extended period offline

Try Bitdefender Cloud Security for MSP free by visiting www.bitdefender.com/msp or contact us by phone: (+1) 954 776 6262 x 10116