Solution Paper

Bitdefender®

Virtualization security solutions provide a competitive advantage to service providers – IaaS, PaaS and SaaS

Contents

About this Document

This document is aimed at service providers that host infrastructure or higher-level services (platform, software) as-a-service for end customers.

While there are many business scenarios, this document focuses on providers with a managed security model. Other providers may choose to provide security above the infrastructure as a managed offering, customer-managed option, or as part of a marketplace (https://aws.amazon.com/marketplace/pp/B0096BADNI).

Executive Overview

For service providers that have a virtualized infrastructure, Bitdefender GravityZone delivers the opportunity to maximize profit and increase the service level offered to customers. The solution also provides:

- Relief from AV storms that are encountered if VMs are protected using traditional antivirus technologies.
- Increased revenue and competitive advantages.
- Improved performance and an increase in VM density of 30%, allowing more VMs on each host.
- Customers will experience advantages in having AV as a service, rather than protecting their VM using traditional methods, as they are able to save time and money.
- Security-as-a-service that saves end-customers money when the primary service is not being used.

Introduction

Bitdefender Security for Virtualized Environments (SVE) is seamlessly integrated in a hosting environment that leverages VMware technologies. This provides the optional value-added service of antimalware protection for end customers.

For the hosting provider, this is an additional service to offer end customers, giving the provider additional revenue as either a value-added or optional service. Management can be done by hosting service, or the end customer, depending on the business model. This includes all day-to-day tasks, such as configuring security policies, monitoring the security status, and generating reports. This document focuses on the model that has the provider managing security for customers.

The benefits of such a service include:

- Protection provided by the hosting company, so that end-customers don't need to invest in antimalware licenses from a third party.
- Eliminating the expense of server licenses and maintenance to operate an antimalware administrative console and database.
- Operations and maintenance of security provided by the service provider as a value-add to the service so that customers don't need to procure an additional third-party security management console.
- Remove the need for a bulky, traditional anti-virus agent in each virtual machine, which generates 'AV Storms' due to high consumption of CPU, memory, and storage resources, especially in highly consolidated environments.
- Endpoints are protected by the #1 ranked antimalware, according to independent security experts such as the German AV-Test. http://www.av-test.org/no_cache/en/tests/test-reports/?tx_avtestreports_pi1[report_no]=134185
- Increase the level of high-availability as the antimalware service is provided by the hosting provider will fail-over and load distribution between available instances, removing a traditional single point of failure.

The bottom line is that the end customers obtain a higher level of protection, with no up-front investment and lowered operational costs.

Brief Technology Description

Security for Virtualized Environments (SVE) provides endpoint antimalware protection from one or more Security Virtual Appliances (SVAs), which provide antimalware scanning services. On average, a single SVA per hypervisor is deployed, though often, fewer are required.

Within protected VMs a static piece of software called Bitdefender Tools (BD Tools) is required. BD Tools is extremely lightweight and, being relatively static, doesn't require frequent updates. Using BD Tools, each protected VM connects, via a TCP connection, to an SVA. BD Tools performs the following tasks:

- Connect to the first responding SVA instance that the security policy applied to the VM specifies, while favoring the SVA that is on the same host, if present – providing highly-available resource pools of antimalware protection.
- Provides access to VM memory for scanning at SVA.
- Provides access to the VM Windows registry database for scanning at SVA.
- Provides access to the VM disks for scanning at SVA.
- Maintains a local cache of what has been scanned (pre-populated with standard operating system and application objects).
- Handles encryption of infected files and transfers to quarantine area, according to the security policy.
- Can optionally provide a local graphical user interface with pop-up notification, typically used with virtual desktops and terminal servers.

BD Tools can be installed in VM templates, while existing VMs can have BD Tools installed through a downloadable package for Windows. For Linux, BD Tools is delivered as a scripted installation which will automatically identify the supported Linux distribution, and for real-time file system scanning, identify the correct kernel version.

On Windows, BD Tools also has self-protection mechanisms. This ensures that the service cannot be stopped through administrative privileges or malicious activity.

Comparison between traditional AV agent and Bitdefender Tools (non-vShield Endpoint version)

	Traditional AV agent	Bitdefender Tools
Size on disk	Around 1 GB	less than 100 MB
Memory allocation	100-300 MB	10-15 MB
CPU usage	High	Almost none
I/O activity	Massive as many tasks are repeated for each VM.	Reduced drastically by multi-level caching (only unique files across all protected VMs are scanned)

The deployment is monitored and controlled at the management console, GravityZone Control Center. The management components are based on a virtual appliance. Each instance can act in one or more of four server roles:

1. Database
2. Web console
3. Communication
4. Update

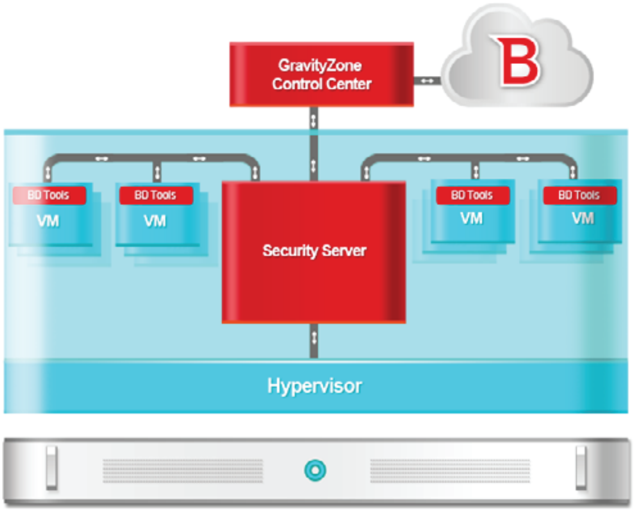

Figure 1: All roles can be installed on a single appliance or distributed over several appliances for high availability.

Scanning Routines

The scanning traffic between BD Tools and SVA does not require passing complete files. The following diagram helps illustrate how scanning is performed:

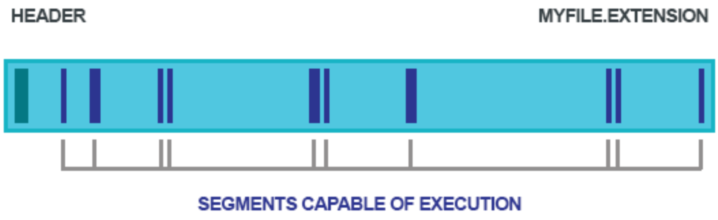

Figure 2: Representation of a file with segments, or blocks, that are important for scanning

The first 16 KB contain header information, which identifies the file type, and other information. It is always the first segment passed to the engine at an SVA for scanning. The scanning engine determines which further segments are required.

To use the example of a Microsoft Word file, the text area does not pose a threat. For instance, including a batch script in this section of the file is not dangerous, as it cannot be executed either directly from the file executable or another executable process reading the file. A command such as format c: /y would be relatively harmless. On the other hand, segments of a Word file, such as the macro area, are scanned.

The parts of the file required for scanning are sent by BD Tools to an SVA in segments.

Optionally the scanning traffic can be encrypted using SSL, with a minor resource impact on both the VMs and SVA engines for the encryption/decryption process. The encryption activation is managed through security policies and can be activated or deactivated on individual machines, groups of machines, or resource pools.

Port allocations and traffic description

The following table contains information on the port usage for the different Bitdefender objects needed in the solution:

GravityZone (GZ) administrative solution consists of 4 different server roles. The roles can be placed on individual GZ virtual appliances; database, web console, communication- and update server role.

Network Communication Requirements by Role

The following table provides information about the required TCP connections that are either initiated or received by different components of GravityZone management cluster.

Component	Direction	Port	Source / Destination	Description
Web Console role	Inbound	80	Any	Admin Web Console, redirect to 443
		443	Any	Admin Web Console
		4369, 6150	Communication Server	RabbitMQ Messaging
	Outbound	27017	Database Server	Database Access
		389	Domain Controller	AD Integration
		443	vCenter Server	vCenter Integration
		443	lv2.bitdefender.com my.bitdefender.com	License Validation
		4369, 6150	Communication Server	RabbitMQ Messaging
Communication Server Role	Inbound	8443	Any	Agent Management Traffic
		4369, 6150,	Web Server	RabbitMQ Messaging
	Outbound	27017	Database Server	Database Access
		4369, 6150	Web Server	RabbitMQ Messaging
Database Server Role	Inbound	27017	Any	Database Access
	Outbound	N/A	N/A	N/A
Update Server Role	Inbound	7074	Any	Update Publishing
	Outbound	80	upgrade.bitdefender.com download.bitdefender.com	Update Download
		7074	Other local update server	Update Download

Table 2: GravityZone management cluster communication ports

When deploying the GravityZone management cluster and Security Servers, administrators must place the virtual appliance network interface in a network segment or VLAN in which:

The Web Server role is allowed access to Bitdefender Cloud Services

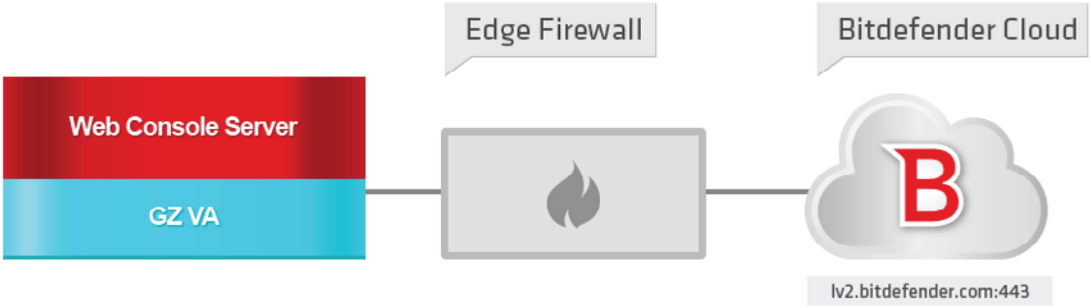

Figure 3: Internet communication required by Web Server role

The Update Server role is allowed access to Bitdefender Cloud Services

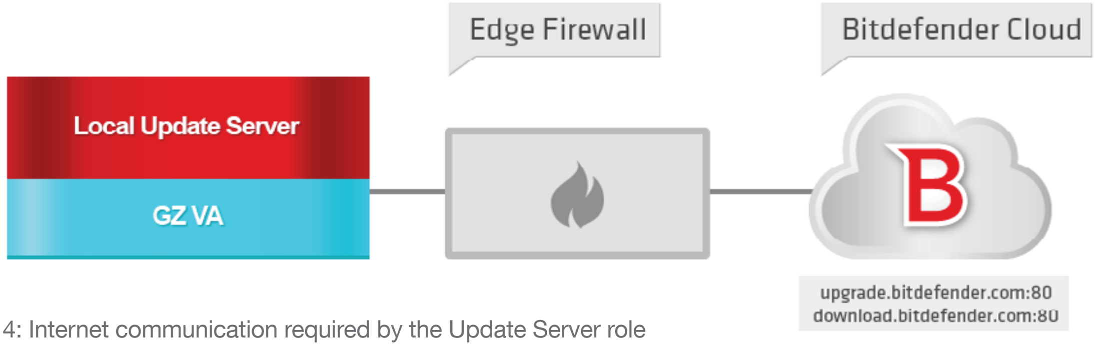

Figure 4: Internet communication required by the Update Server role

Each GravityZone virtual appliance is allowed to connect with each other. The following image presents the network communication required by the GravityZone management cluster

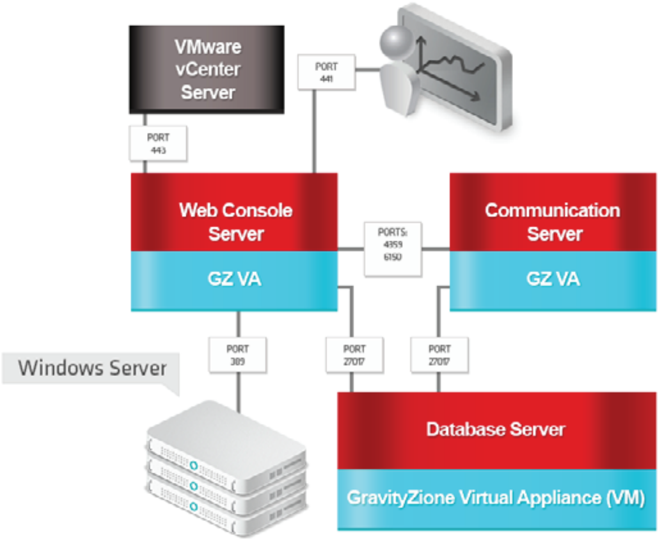

Figure 5: Internal network traffic within the GravityZone management cluster

Each Security Server is allowed to connect with the Communication Server role and Update Server role; Each instance of Bitdefender Tools is allowed to connect with Security Servers and Update Server role.

Bitdefender Tools: Network Requirements

The following table provides information about the required TCP connections that are either initiated or received by endpoint components:

Component	Direction	Port	Source / Destination	Description
Bitdefender Tools	Outbound	7081	Security Server	Scanning Traffic
		7083	Security Server	Scanning Traffic over SSL
		8443	Communication Server	Management Traffic
		7074	Update Server	Update Download
		443	Web Server	Package Download During Deployment Operation
	Inbound	N/A	N/A	N/A
Security Server	Outbound	7074	Update Server	Update download
		8443	Communication Server	Agent management
	Inbound	7081	Any	Scanning Traffic
		7083	Any	Scanning Traffic over SSL

Table 7: Security Server communication ports

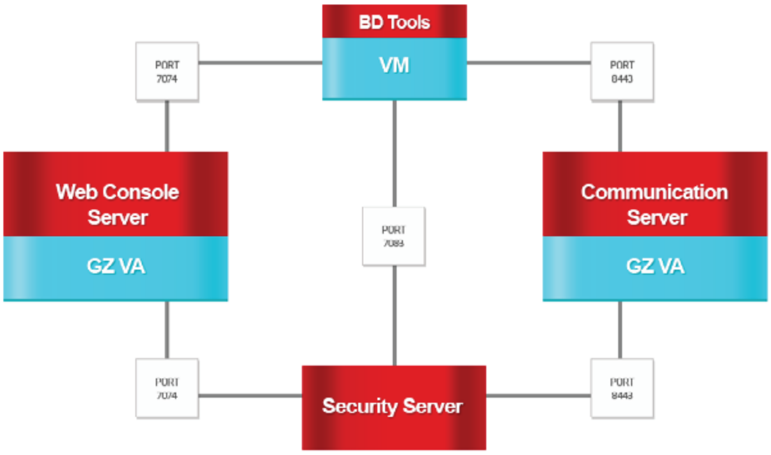

Figure 6: Internal network connections required by SVE components

Network administrators can create a new VLAN dedicated to GravityZone and route this VLAN to allow communication to all other VLANs in which protected physical systems or VMs are residing into.

If intermediary network traffic filtering devices are active between network segments or VLANs in which Bitdefender components are placed in, the filtering rules must be changed to allow communication on the ports mentioned in Table 2. If the virtual appliances are deployed in different VLANS, those VLANS must be routed to allow network communication as described in Table 2 and Table 7.

For SVE vShield (the BD Tools requirements change)

The following table provides information about the required TCP connections that are either initiated or received by SVE Security Server integrated with vShield Endpoint.

Component	Direction	Port	Source / Destination	Description
Security Server	Inbound	48651	Any	Linux VM scanning traffic
	Outbound	7074	Update Server	Update download
		8443	Communication Server	Agent management

Table 9: Security Server communication ports

When deploying the Security Server, administrators must place the virtual appliance management network interface in a network segment or VLAN in which:

Each Security Server is allowed to connect with the Communication Server role and Update Server role; Each instance of Bitdefender Tools is allowed to connect with Security Servers and Update Server role

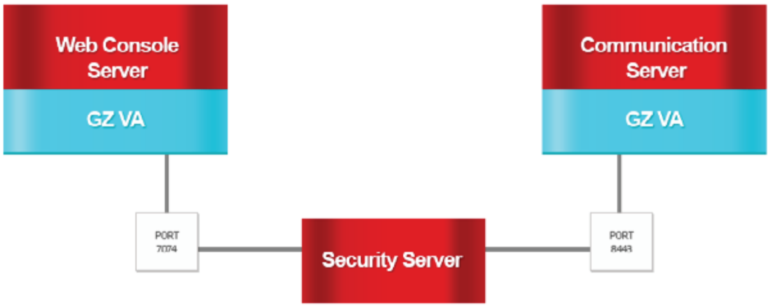

Figure 7: Internal network connections required by Security Server

Note: For protecting Linux VMs, Bitdefender Tools needs to be installed on each target VM. Each instance of Bitdefender Tools deployed on Linux needs to be allowed to connect with the Security Server on the respective host on port 48651, as indicated in Table 9

Performance

Testing with the industry-standard Login VSI demonstrates an increase in VM density of thirty-percent, when comparing SVE performance against traditional AV technologies. Results are available in a joint whitepaper with Login VSI, (The impact of virtualization security on your VDI environment), http://businessresources.bitdefender.com/white-paper-impact-of-virtualization-security-on-vdi that demonstrates the performance advantages provided by SVE. As the SVA caches observe the environment over time, a more complete cache is built, quickly increasing performance with time.

Another component of the performance gain is based on two primary principles of virtualization: centralization, and deduplication. The SVE solution abstracts endpoint antimalware to a single scanning service at an SVA. Doing so centralizes antimalware effort such that only one system must be updated with the latest antimalware engines, definitions, and so-on. Deduplication of scanning effort is achieved by having a view across the virtualized infrastructure. If an object is scanned on a particular VM the result of that scan is maintained in the SVA cache.

Performance is achieved by:

- The two-tier local where one tier is based on a hash of the local object – and the long-lived cache of said objects is pre-trained - and a second cache that is dynamic , expiring entries that are no longer accessed.
- BD Tools has packages (packers and unpackers, compress and deflate, process enumerator) that are updated from time to time – these updates are rare compared to the signature and heuristics databases that are maintained only on Security Virtual Appliances. BD Tools main service, update service, GUI and other components get also get occasional upgrades.
- Files are unpacked, packed, deflated and compressed locally in the VM if the agent must analyze the content. We do cache these types of files, repeating the scanning only if the file is modified. The reverse operation – pack and compress happens only if we rebuild the original file after a successful clean-up, which is a rare circumstance.
- The communication channel from BD tools to the SVA is encrypted using SSL.

Flexibility

- BD Tools can be configured to use multiple SVAs. The priority is given by the order specified in a list of SVAs in each security profile. If an SVA doesn't respond, or is overloaded or under-loaded, BD Tools switches to the next one in the list. BD Tools preferentially use an SVA on the same host, if present.
- The on-demand process and registry scans the memory pages of all running processes on a VM. They are enumerated and dumped to disk, then the SVA engine scanning the memory starts to request chunks of data (usually containing code since the engine is looking to intercept rogue code that may reside in memory).
- The generic disinfection engine also resides in the VM – this one is called whenever cleaning of an infection in a file, memory, or registry, is needed.

Management

If customers prefer to manage their own security, giving them control over individual security policies, reports and monitoring, they must have access to the GravityZone Control Center.

Conclusion

By providing endpoint security as a value-add, service providers can gain:

- Competitive advantage and differentiation
- More efficient datacenters, thereby increasing margins
- Remove a barrier to adoption of services
- A streamlined experience for end-customers wary of hidden costs and hurdles

For both customers and providers, the advantages of centralizing and deduplicating endpoint antimalware are clear. For providers, running the most cost-efficient datacenters possible, while providing a compelling service and cost model to new and potential customers, is the business. Bitdefender understands this, and has designed GravityZone to help providers and customers alike operate virtualized datacenters without the bottlenecks that are associated with traditional anti-virus products.

Beyond security for virtualization, providers may also wish to take advantage of additional GravityZone modules to invite customers to secure mobile devices and traditional, physical endpoints. This can help providers expand services beyond their own datacenters, gaining a footprint on customer-owned devices to further enhance relationships.

Bitdefender®

Bitdefender delivers security technology in more than 100 countries through a cutting-edge network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced market-leading technologies for businesses and consumers and is one of the top security providers in virtualization and cloud technologies. Bitdefender has matched its award-winning technologies with sales alliances and partnerships and has strengthened its global market position through strategic alliances with some of the world's leading virtualization and cloud technology providers.

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com