Bitdefender®

# Getting the most out of your cloud deployment





# Contents

# Introduction

Organizations are under ever increasing pressure to reduce IT costs. One of the cost reduction methods is to move applications into the cloud. Cloud-based computing provides organizations with cost savings over time, instead of the upfront costs associated with traditional datacenter equipment. By moving from a capital expenditure (CAPEX) model to an operational expenditure (OPEX) model, organizations are able to reduce costs associated with hardware and cooling in datacenters. There are other benefits like increased productivity based on reduced administrative burden, a result of the self-service nature of cloud computing, and the ability to almost instantly provision to meet service requirements.

When moving an application into the cloud, there are design considerations that must be taken into account. Cloud computing architecture is quite different compared to traditional physical or virtual environments. For example Amazon Web Services (AWS) persistent storage is disassociated from the Amazon Machine Image (AMI), and virtual machine instances are simply disposable.

One should also take into consideration how applications running in the cloud need to be secured. Virtual machines in a cloud environment are as susceptible to nefarious exploitation – where sensitive data is highly valuable – as physical machines. The same exposure profile exists regardless of the underlying platform (traditional physical, virtualized, private cloud or public cloud). Although traditional security can be used in the cloud, it is neither built, nor optimized for the cloud. This paper outlines the design considerations that must be taken into account when moving an application into the cloud; it will also explore the performance impact traditional antimalware solutions impose in the cloud, affecting the ROI achieved by moving workloads into the cloud.

# Moving your application into the cloud

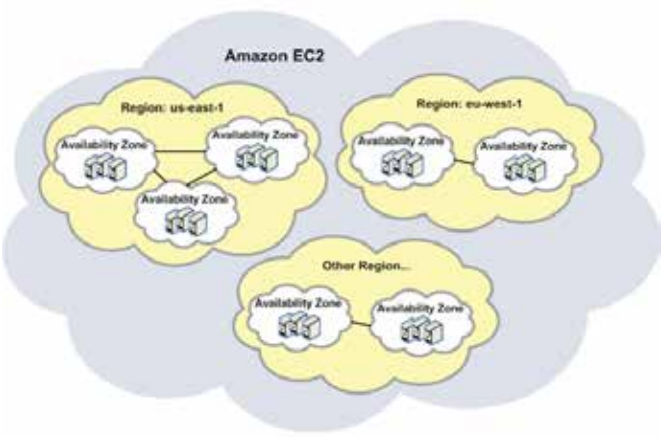



Figure 1: Amazon availability zones

There are many aspects that need to be taken into account when moving an application into the cloud. Two in particular that are explored in this paper are, design for failure and the security of the workload. The widely reported Amazon outage1 last year impacted numerous organizations' quality-of-service. This resulted in loss of revenue, in some cases, severe if most or all of the business relied on being online. A more recent Amazon outage caused by electrical storms and the leap second2 again resulted in services interruptions. Both of the Amazon outages referenced above affected specific availability zones. An availability zone can be compared to a datacenter. If there is an interruption in service in one availability zone, the other zones will continue to service requests as long as the application in question is designed to run across multiple availability zones.

Organizations that designed for failure experienced no impact to their business during the AWS outages. In addition to designing across multiple availability zones and regions, one should consider cross-cloud provider design. In doing so, an organization is not limited or locked into one cloud provider, but diversifies the risk of service interruption across multiple providers. Bandwidth charges across two cloud providers can become expensive and should be taken into consideration, in addition to potential latency issues. Applications implemented in cloud environments must be designed to support and take advantage of architectures, facilitating things like horizontal scaling as an example.

When moving an application into the cloud, there is no need to build from scratch. For example, cloud brokers offer solutions that provide end users with pre-configured environments and templates that are managed within a single pane of glass. Cloud brokers are also exceptional at managing cross-cloud deployments, enabling customers to design applications that run across multiple cloud providers, thus diluting the risk of service failure.

[1] Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region – Source: http://aws.amazon.com/message/65648/

[2] Storms, leap second trigger weekend of outages – Source: http://www.information-age.com/channels/the-cloud-and-virtualization/news/2110828/storms-leap-second-trigger-weekend-of-outages.thtml

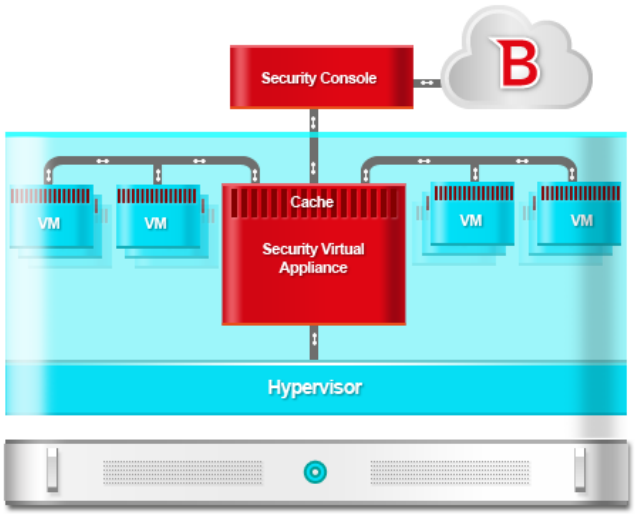
There are also many online resources and system integrators that can assist in deploying an application in the cloud. Designing an application to run in a highly available configuration is paramount in the cloud, as service failure is inevitable. One aspect of the design is security; poor or badly implemented security will not only result in sensitive information exploitation, but can also cause poor quality of service. Although cloud providers have multiple security measures, it is ultimately the responsibility of the application owner to implement security solutions that are appropriate for the application.

# Securing your application in the cloud

When moving an application into the cloud, one must consider all facets of security that were implemented in physical environments. Although cloud providers create separation between tenants, it is still up to the tenant to secure the workload against malicious intent.

One organization that provides recommendations on application security in the cloud is the Cloud Security Alliance. In the CSA "Security Guidance for Critical Areas of Focus in Cloud Computing" version 3.03, there are eight domains dedicated to operating in the cloud that provide exceptional guidance.

Domain 13 of the CSA Security Guidance deals with virtualization – one of the key elements in cloud computing. This leads to the second aspect to be explored when moving applications into the cloud - securing the workload. Regardless where a workload runs, whether a physical, virtual or a cloud computing environment, it must be secured. As explained in domain 13 of the CSA Security Guidance, using security software that is designed for physical environments in virtual environments may result in severe performance degradation of both the host and the virtual machine.




In cloud environments, the concern of physical host performance may not necessarily be an issue to a tenant, but the performance of the virtual machine certainly is. If the security solution employed negatively impacts system performance, the result is the need to run larger virtual machine instance sizes – at additional cost – so that the application runs optimally. The difference could mean an increase in additional cost of 8-32 cents per hour4 respectively. It would therefore be wise to evaluate security solutions that have been purpose-built and optimized for virtualized environments.

# Traditional security pitfalls

In AWS, virtual machine templates known as Amazon Machine Images (AMIs) are used to instantiate multiple copies of virtual machine instances from a single AMI. Traditional security can technically be employed in a cloud environment, but at what cost? When making a decision about security, there are a few aspects that should be taken into consideration, including:

### Security gaps

In cloud-based infrastructures such as AWS, agent-based antimalware solutions will at one time or another become outdated due to the dormancy of a virtual machine in an offline state – the AMI. When a virtual machine instance of the AMI 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.

### Duplication

Due to the nature of applications running in the cloud, virtual machines are instantiated and terminated based on demand. In many cases, multiple virtual machine instances are instantiated from a base image and applications are installed to the image via startup scripts, which

[3] Security Guidance for Critical Areas of Focus in Cloud Computing – source: https://cloudsecurityalliance.org/research/security-guidance/

[4] http://aws.amazon.com/ec2/pricing/

provide the customization for that application environment. These virtual machine instances need to be secured from malware. With traditional antivirus, an agent containing the antivirus engine signatures runs on each virtual machine instance in order to provide adequate protection. This duplicates the effort of installing the traditional agent on each virtual machine instance every time one is instantiated and creates a significant management burden.

### Management

Each time a new traditional agent is installed, it is registered to the security management console, for administration. When a virtual machine instance is terminated, 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 if the organization is terminating and instantiating virtual machine instances on a daily basis to handle the peaks and troughs of demand.

### Licensing

Traditional security is normally licensed per user or per virtual machine, however in the cloud the number of virtual machine instances and users fluctuates based on demand. Organizations must therefore estimate their peak number of virtual machines or users, and license traditional security accordingly. Why pay for what is not used? Traditional antivirus licensing does not accommodate the hourly consumption-based model.

### Performance

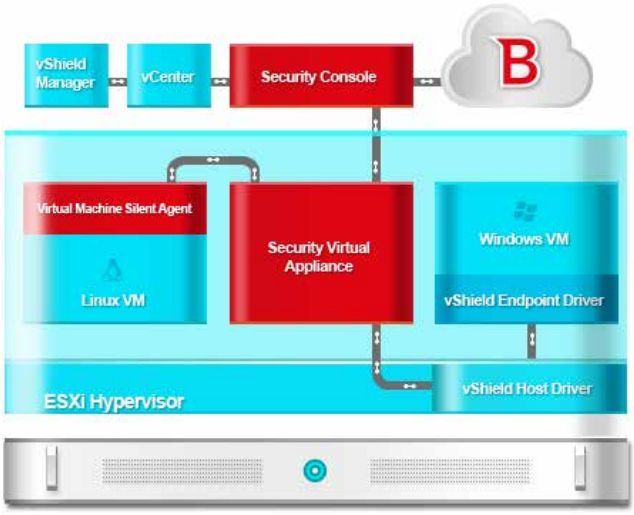
Traditional security treats each virtual machine on a silo basis; it is not designed to evaluate all the virtual machine instances in a specific network or availability zone as a group. All application and user actions performed within the virtual machine instance are evaluated by the security agent within the instance. This silo effect creates significant duplication, from signature databases to scan results for the same files, ultimately creating a performance problem. This performance impact should be estimated based on the nature of the application running in the cloud and the size of the virtual machine instance used to meet service requirements.

## Purpose-built cloud security

An alternative to legacy antimalware solutions is to take advantage of security solutions that are specifically built for virtualization and cloud-based architectures. Such solutions help mitigate the issues outlined earlier in this paper.

Security for Virtualized environments (SVE) by Bitdefender enables customers to gain higher consolidation ratios and better virtual machine performance in the private or public cloud. This is achieved through patent-pending optimization technologies from Bitdefender that streamline the antimalware processes and reduce resource utilization on each virtual machine instance.

Bitdefender implements centralized scanning by offloading much of the antimalware functionality from each virtual machine instance to dedicated hardened Security Virtual Appliances (SVA). This approach optimizes both on-access and on-demand scanning processes while de-duplicating critical computing resources. To achieve this, a silent agent optimized specifically for virtual environments is installed on each virtual machine instance. The silent agent removes the security pitfalls discussed earlier, as described in further detail below.




### Security gaps reduced

The silent agent does not include scan engines or signature files like traditional agent-based security. With no antivirus engine signatures or scanning engine updates required on each virtual machine, the security gap is reduced. This is achieved because all of the scanning is offloaded to the SVA.

When deploying the silent agent in an AWS EC2 environment there are a couple of deployment options:

## Flexible deployment

While building an AMI, the Bitdefender silent agent can be installed along with other applications in the AMI. When multiple instances are spun up from an AMI with Bitdefender silent agent installed, each of the instances is protected and listed in the SVE Security Console with the policies that have been configured to the parent AMI applied.

## Automatic deployment

When managing cloud deployments with tools offered by RightScale for example, the instances used will be derived from base AMIs with applications installed at startup as they are needed. In doing so, one is able to automate the server build in a controlled and reproducible fashion. Bitdefender offers the ability to add auto-deploy tags when instantiating an instance so that the silent agent is installed at startup.

## Integrated intuitive management

SVE integrates with many AWS APIs. One result is that virtual machine instance status information that is available in the AWS management console is replicated in the SVE management console. In the event that an instance is terminated, it is removed from the SVE console. However any events associated with the terminated instance are stored for logging and reporting purposes.

## Cost of cloud security reduced

Cloud computing users are accustomed to the pay-as-you-grow utility-based licensing. Traditional antivirus does not accommodate for this type of licensing, which is prohibitive to cost savings associated with cloud computing. Licensing costs are an important part of choosing which security solution to implement based on the license model that best fits one's business needs. Bitdefender SVE provides this flexibility. Customers can choose to use SVE SaaS with the hourly consumption-based model or for a lower fixed monthly subscription, customers can deploy SVE in AWS to protect a fixed number of virtual machines.

In a recent paper "Scalability and economics of XenApp on Amazon Cloud"5, by Citrix, there is an example of the hourly cost per user without security for XenApp being hosted in AWS. As a test, Bitdefender used the example of 65 XenApp user sessions for a small organization hosting XenApp on AWS. The test includes the impact of adding security while providing at least 65 user sessions. Our results are included in this whitepaper.

| Instance type | Compute units | RAM (GB) | vCPUs | East Coast Cost per hr | User Sessions | Cost per hr per user |
|---|---|---|---|---|---|---|
| Standard small | 1 | 1.7 | 1 | $0.115 | 0 | N/A |
| Standard medium | 2 | 3.7 | 2 | $0.230 | 5 | $0.0460 |
| Standard large | 4 | 7.5 | 2 | $0.460 | 9 | $0.0511 |
| Standard extra large | 8 | 15 | 4 | $0.920 | 18 | $0.0511 |
| Micro 32-bit or 64-bit | 1 | 0.613 | 1 | $0.030 | 0 | N/A |
| High-memory extra large | 6.5 | 17.1 | 2 | $0.570 | 17 | $0.0335 |
| High-memory double extra large | 13 | 34.2 | 4 | $1.140 | 33 | $0.0345 |
| High-memory quadruple extra large | 26 | 68.4 | 8 | $2.280 | 65 | $0.0351 |
| High-CPU medium | 5 | 1.7 | 2 | $0.285 | 2 | $0.1425 |
| High-CPU extra large | 20 | 7 | 8 | $1.140 | 23 | $0.0495 |
| Cluster compute quadruple extra large | 33.5 | 23 | 16 | $1.610 | 85 | $0.0189 |
| Cluster compute eight extra large | 88 | 60.5 | 32 | $2.970 | 150 | $0.0198 |
| Cluster GPU quadruple extra large | 33.5 | 22 | 16 | $2.600 | 85 | $0.0306 |

Figure 2: AWS Compute costing per hour - Scalability and economics of XenApp on Amazon Cloud

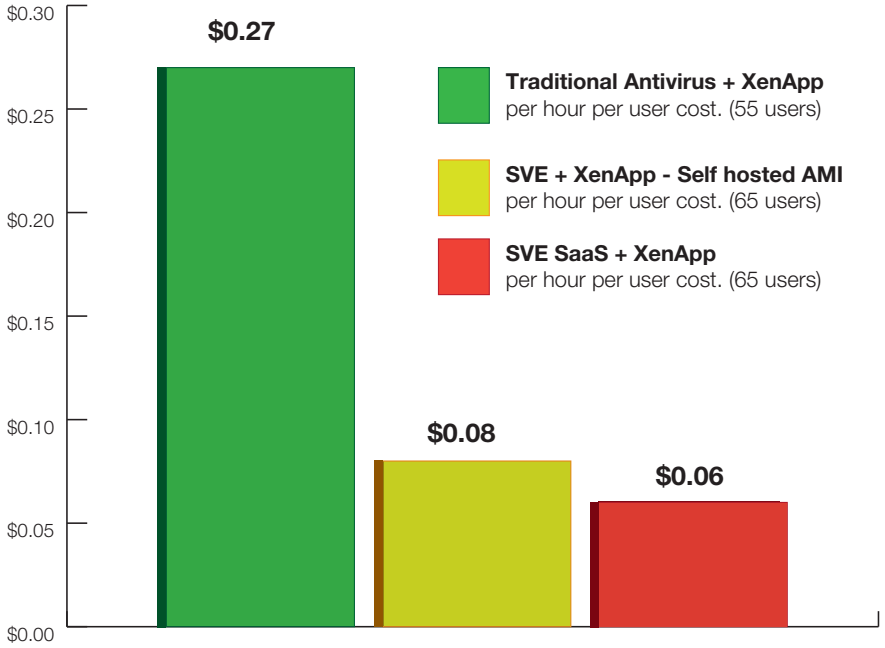
According to the Login VSI performance testing, – before any applications or antivirus is installed – to support at least 65 user XenApp sessions, an AWS virtual machine instance type high-memory quadruple extra-large will be required.

[5] Scalability and economics of XenApp on Amazon Cloud – Source: http://community.citrix.com/download/attachments/173117739/Citrix_XenApp_on_AWS_Sizing_Economics_Whitepaper_050912.pdf

Using the same industry standing Login VSI tools to benchmark the impact of security in a VDI environment, Bitdefender installed traditional antivirus on the instance type high-memory quadruple extra-large; the result was that only 55 user XenApp sessions are achieved.

Due to offloading antimalware scanning ability that Security for Virtualized Environments (SVE) employs; supporting 65 user XenApp sessions requires no increase in AWS virtual machine instance size hosting XenApp in AWS. This equates to less capital outlay for AWS monthly costs compared to using traditional antivirus solutions.

The following graph illustrates the testing results using an AWS high-memory quadruple extra-large virtual machine instance to host XenApp. It outlines the difference between hourly pricing that one could expect when using SVE compared to traditional antivirus. The illustration also details the different pricing models offered by Bitdefender to suit customer needs.




Graph 1: Cost per user XenApp session with Antivirus

As shown in graph 1, there are two key values that require attention:

- Traditional antivirus reduces the application performance – the maximum number of user sessions was reduced from 65 to 55.
- The cost of traditional antivirus compared to SVE increased by at least 22% more per user per hour.
- The per user costs include the cost of hosting the traditional antivirus management console on a small instance on AWS. The SVE self-hosted AMI costs include the costs of hosting the SVE scan appliance and management console on AWS.

What is not included, and still needs to be added in the traditional antivirus cost, is the cost of bandwidth to update each of the traditional agents running on the virtual machine instance. Moreover, traditional antivirus licensing is normally based on fixed monthly or annual amounts paid on fixed number of endpoints. SVE provides the licensing flexibility cloud users are accustomed to.

It is a well-known fact that antivirus is quite simply a requirement on systems today. The testing performed by Login VSI in the Citrix paper "Scalability and economics of XenApp on Amazon Cloud" shows that traditional antivirus and application virtualization impacts XenApp response time. In Login VSI terms, the response time is measured to illustrate the maximum number of user sessions one is able to achieve on a specific system hosting XenApp. In the case of the Login VSI testing, traditional antivirus will impact the number of user sessions, resulting in 15% (55 user sessions compared to 65 user sessions) less user sessions compared to no impact on the number of user sessions when using SVE.

Security for Virtualized environments (SVE) by Bitdefender is purpose-built for virtualized environments. It is designed and optimized from the ground up to provide the best performance possible with the least impact, while maintaining a high level of security assurance.

# Built-in intelligence

Security for Virtualized Environments employs a unique patent-pending intelligent caching mechanism and whitelisting of common operating system files and applications. This process significantly improves the scanning performance of virtual machines, and is updated on a continuous basis. This is achieved through two layers of caching that the solution utilizes, one of which is a self-learning cache that is built into SVA. The silent agent employs a local cache that is prepopulated based on its environment variables, and in doing so, it offloads scanning of only what is required while excluding objects that are safe.


Figure 3: Scanning architecture overview

# Conclusion

When moving an application into the cloud, using traditional security results in adverse effects that negatively impact the business. It is imperative to use security solutions that have been purpose-built for virtualized environments. Using traditional antivirus solutions in the cloud will result in diminished system performance with increased costs. This results in lower or no cost savings, severely reducing the value of moving an application into the cloud.

Security for Virtualized Environments is architected specifically for both the private and public cloud. The solution isolates the scanning service from virtual machine instances that are protected, removing many of the virtualization security challenges outlined earlier. Additionally, the increased performance gains achieved from the patent-pending intelligent caching mechanisms that SVE employs are updated on a continuous basis. This results in higher cost savings due to the drastically reduced impact SVE has on each of the virtual machine instances compared to traditional security.

# Appendix

## About Login VSI

As VDI and HVD are getting more and more established as end-user infrastructure technologies, performance emerges as one of the key-issues in these centralized environments. Organizations that are researching or implementing these new infrastructures want to make the right decisions about vendors, products and capacity. After implementation they are looking for ways to predict the effect that infrastructure changes may have on overall performance.

Login Virtual Session Indexer (Login VSI) is a vendor independent benchmarking tool to objectively test and measure the performance and scalability of centralized Windows desktop environments such as Server Based Computing (SBC) and Virtual Desktop Infrastructure (VDI). Both leading IT-analysts and IT-vendors recognize and recommend Login VSI as the de-facto industry standard benchmarking tool for SBC and VDI.

Login VSI can be used to test virtual desktop environments like Citrix XenDesktop and XenApp, Microsoft VDI and RDS (Terminal Server), VMware View, Quest vWorkspace and other VDI/SBC solutions.

- Customers of Login VSI use the tool for different purposes:
- Benchmarking: Make the right decisions about different infrastructure options based on tests.
- Load-testing: Gain insight in the maximum capacity of your current (or future) hardware environment.
- Capacity planning: Decide exactly what infrastructure is needed to offer users an optimal performing desktop.
- Change Impact Analysis: To test and predict the performance effect of every intended modification before its implementation.

Infrastructure vendor organizations that are committed to continuous improvements in the field of performance and scalability use Login VSI as an objective benchmark to test, compare and improve the performance and scalability of their solutions. They publish the results in technical white papers (for an overview please visit www.loginvsi.com) and present the results on conferences. Login VSI is also used by end-user organizations, system integrators, hosting providers and testing companies.

Login VSI is the standard tool used in all tests that are executed in the internationally acclaimed Project Virtual Reality Check (for more information visit www.projectvrc.com).

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

BD-Business-May.14.2015-TK#: 70585