Bitdefender

Solution Brief

AWS and the use of Gaming strategies: imitation and reality

Bitdefender

Getting in the game

A popular genre of video games is real-time strategy (RTS). In these games, the player must find and extract resources and use those resources to create things. The first in-game units created help the player gain more resources to build more units. The player can then start building increasingly complicated weapons to totally annihilate other players (victory!), and likewise defenses to prevent other players from annihilating the player (not losing!). The strategic component is in balancing between increasing resource production, and building weapons and defense.

If we consider building and delivering killer AWS applications as weapons, those weapons require resources such as an infrastructure to support Windows and Linux servers. Delivering applications that are better than the competitors', and delivering and scaling faster results in victory.

Amazon Web Services is an RTS player's dream; all-but infinite and instant resource availability. However, in the drive to victory, the defensive mechanisms that prevent defeat at the hands of others – security - cannot be left out of a winning AWS build strategy. **Failing to address basic security can lead to embarrassing failures, and ultimately losing more than just a game.**

Assumptions of protection

Amazon Web Services builds tend to be led by technical operations (developer-operations, or DevOps) teams with a primary focus on delivering an application in as little time as possible. The flexibility and agility of AWS provides these teams with many tools for taking an application from concept, though development and testing, to production release very quickly. However, as with many public cloud providers, the responsibility for security assumed by the provider has clear limits set-out.

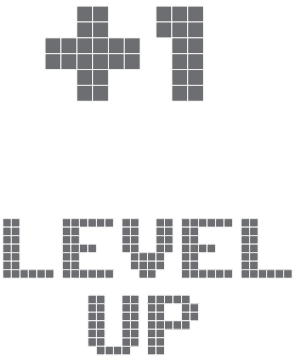
The rapid build capabilities are the direct result of using on-demand public cloud. The DevOps are effectively bypassing many of the hurdles that are associated with creating and deploying applications within an established, internal datacenter. In exceptional cases, internal IT groups are not able to deliver as much infrastructure, with as much functionality, as quickly as one can on AWS. Add to this, another branch of IT traditionally associated with slowing projects is security. With public cloud, **DevOps are hesitant to involve security teams until after-the-fact, especially if security teams can only attempt to bolt-on traditional security tools that are built to run in on-premise datacenters.**

Avoid traditional bolt-on

Every DevOp knows that when setting-up a Windows endpoint, there are certain basics that must be addressed before allowing a system to run production workloads. Two of the most basic requirements are: controlling network access, which AWS provides via firewall configuration, and endpoint anti-malware, which is the responsibility of the AWS user.

Using the same endpoint anti-malware as-is, used in an internal datacenter, can be problematic. A **traditional security solution is not integrated with AWS, and so deployment will be a laborious, ongoing, task. The management console is not built to handle endpoints on AWS, and yearly per-endpoint licensing makes no sense in the usage-based world of AWS. Finally, each instance will require a full anti-malware client.** Instance resources will go to hosting antimalware. Ultimately, running the smallest possible instance for an app or a service is less expensive than using an unnecessarily powerful instance. Throwing traditional anti-malware into that efficient and flexible environment can require more powerful and expensive instances to do the same job.

Additional security controls, such as network IDS, storage encryption, web application firewalls, and other perimeter and storage security may be appropriate when public cloud usage reaches a certain threshold. However, the primary goals of DevOps are focused on rapid delivery with streamlined cost models. Implementing these costly and complex solutions should be considered stand-alone projects so that they are decoupled from the immediate primary goals.



Winning the game with resource-efficient defense

In the gaming world, RTS encapsulates building and defending, ensuring what is built has the greatest chance of victory. However, concentrating solely on resources, some that come at a premium, will take your eye off the wider game and put you at risk.

The Bitdefender AWS Security-as-a-Service is built for the economics of the AWS environment, offering several key advantages over traditional antimalware solutions. The overall aim of the solution is to provide robust endpoint antimalware that will not slow the AWS build or saddle the result with high costs that threaten the viability of using AWS. Bitdefender accomplishes this in the following ways.

No new instances required

In every AWS build, resources usage must be well-managed. **While the available infrastructure resources are all-but finite, financial resources to use the infrastructure is anything but infinite.** Security that demands one, two, or even five virtual machines in a datacenter is acceptable; it's not a big investment. However, if a handful of instances on AWS is required to run a security solution, it's a problem. A simple management instance will need to be run even if only a single instance is being protected.

Bitdefender requires no new instances. The management console is hosted on AWS by Bitdefender. It is always available, whether you are protecting one, two, or two-thousand instances. Also, you don't pay for the management console – you pay for protecting instances.

Over 80% more affordable than competitive solutions

The advantage of a well-executed AWS build becomes apparent mid-to-late project. During early stages, costs are closely monitored while the full scope of AWS automation capabilities is not yet realized. If a security solution adds significantly to costs, a project will fail. During the early stages, don't go with the 'same-old' – because it will impact your strategy. Instead, you can invest in security that is delivered at streamlined prices. **After-all, a primary driver of moving to AWS is to take advantage of low per-unit costs that result from the economies of scale, so choosing a security solution that doesn't have the right cost-model is a mistake. This is a deceptively simple early choice that is critical to long-term success.**

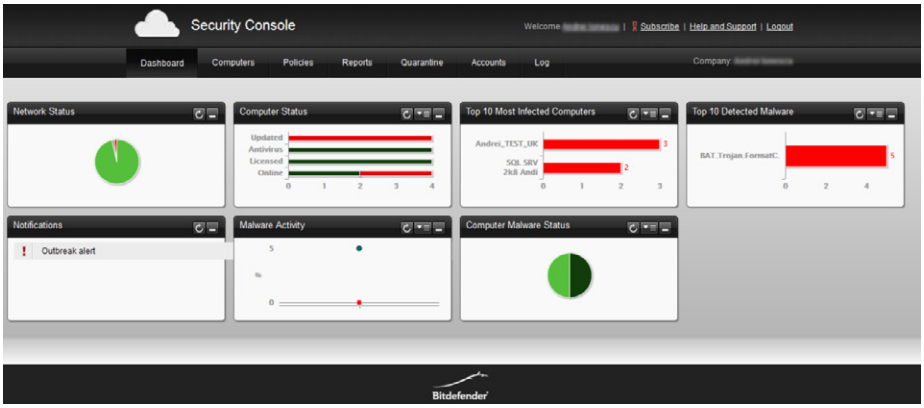
Billed hourly, per instance. Integrated with Amazon's Flexible Payment System (FPS)

A great advantage of AWS is that you pay for only the instances you are using, and the cost is hourly. When an instance is stopped or deleted, costs disappear. If your application has slow times and busy times, your AWS costs will scale with your usage. If using traditional security, you're paying for your peak usage number of instances, and paying for a month or a year, because traditional solutions are licensed per endpoint for a month or year at a time. Bitdefender AWS SaaS is tied directly to instance usage; you pay an hourly fee for each running instance. To make payment and tracking even more convenient, the solution is integrated with Amazon's Flexible Payment System so that you receive a single invoice.

Smallest footprint available

In AWS, larger, more powerful instances cost more. It makes sense to use as much of the available resources as possible of any instance size for serving and application workload before moving to the next larger instance. **Adding a heavy, full antimalware agent doesn't make sense since it robs resources from the application. You should be paying an antimalware vendor to help secure your instances, not for the privilege of installing bloated antimalware agents and then paying for the resources for that agent to run!** The Bitdefender solution

takes advantage of scanning offload that centralizes scanning at Security Virtual Appliances, which Bitdefender hosts on AWS. **As with the management console, you don't pay for the resources that the Security Virtual Appliances use to protect instances, you pay only for the protection of your instances.** All that is left in protected instances is a very small agent that has minimal resource requirements so that your instances both protected and free to dedicate resources to your application, not ours.



Conclusion

Bitdefender AWS Security-as-a-Service is built specifically for helping DevOps teams achieve their goals. **Security cannot be omitted from any AWS build strategy, but security must not create cost, performance, a time impediments that can make the cure as bad as the disease.** The unique, AWS-integrated architecture of the solution gives DevOps a valuable tool to address endpoint security without creating new headaches.

Visit https://amazon.bitdefender.net/register to get a free, full-feature, 30-day trial. Since no new instances need to be created and configured, getting a trial going is simple and easy. There is no downside!

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®

amazon web services™ | solution provider