luminate

Security Controls at the Speed of Cloud Infrastructure

luminate

Software Defined Infrastructure vs Physical One

Software-Defined Infrastructure (SDI) and Software-Defined Data Centers (SDDC) are notions that are encompassing 20+ years of industry development in virtualization of computing, networking, storage, and other IT resources, as well as advancements in management and automation processes and technologies.

Public cloud, particularly Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS), is yet another step in this evolution. Both are delivering a multitude of Software-Defined Components as a service while all the underlying physical infrastructure (or Datacenter) is completely owned by the service provider.

Companies choose to leverage IaaS / PaaS for their IT needs because they want to:

Become more agile,scalable and competitive

Reduce expenses on IT infrastructure and expertise

Deliver IT solutions faster to support business needs

Improve reliability and security

How Traditional Security Solutions are Treating Software Defined Infrastructure

It is very clear, to any reasonable IT professional, that security is an inseparable part of any data center, physical or software-defined. The question, though, is whether the security tools that were defined for physical datacenters are good enough for the software-defined ones.

The traditional approach of the leading vendors of IT Security solutions for physical datacenters is very straightforward – replace “physical” security appliances with “virtual” ones, deployed in IaaS environments, and all the rest remains the same.

Does it work? Is that all that is required from a security vendor?

Lets examine certain aspects of this strategy:

Network Topology – While being deployed in a virtual (Software-Defined) network, and not in a physical one, the traditional topology of separation between internal and external subnets, the creation of DMZs and tight management of open ports between the DMZs and the internal network still applies. It is something that must be planned and executed by network and security experts, incurring costs and complexities.

Deployment and Configuration of Virtual Appliances – While vendors of virtual security appliances create special images optimized for various on-premises and cloud-based hypervisors, deployment of these products in production environments is a multi-step process that requires expertise. Again, there are complexities and delays in deployment.

Managing the Security Policies – After the virtual appliances are deployed and configured, every change in the Software-Defined Infrastructure (and such changes should be frequent, as this is the main reason for using Software-Defined vs Physical) will require manual updates to the security policies, that should be managed via organized change management cycles and carried out by security administrators.

Scalability and Redundancy – The Software-Defined Infrastructure should evolve with high pace. Naturally, any production-grade solution should have the ability to work without a single point of failure. This will require the deployment of redundant virtual appliances or clusters, duplicating the amount of work mentioned above. Solutions based on virtual appliances lack automatic scaling and require planning for peak load, as they do in physical datacenters.

Solutions based on virtual appliances lack automatic scaling and require planning for peak load, as they do in physical datacenters.

Multiple Sites / Locations – All of the challenges described above must be addressed in each location / site. This could multiply the investment of time and effort.

Patching and Updating Virtual Appliances – Virtual or physical, having a self-hosted machine running software in your datacenter puts the responsibility for patching and updating it onto the owner and not onto the vendor. For example, in January 2018, Cisco, a respectable traditional vendor of network security solutions announced a critical vulnerability in its code that required all users of its physical and virtual appliances (approximately 10 different product lines were declared affected) to work hectically to update their owned solutions.

The above list of considerations, while not claiming to be all-inclusive, provides points that are indicative of the virtual appliances approach. It underlines one important principle: trying to treat Software-Defined Infrastructure with the tools that were built for a physical infrastructure is possible, but the outcome will be this: the organization will not benefit from the advantages that the Software-Defined Infrastructure can offer.

Trying to treat Software-Defined Infrastructure with the tools that were built for a physical infrastructure is possible, but the outcome will be this: the organization will not benefit from the advantages that the Software-Defined Infrastructure can offer.

Automation of Deployment and of Traditional Access Policy – Is this enough?

The challenges we listed here have driven the vendors of virtual appliance security solutions to action. This resulted in functional additions to the products and in massive outbound campaigns claiming that such solutions can be adapted to the speed of modernized Software-Defined Infrastructure.

Let's examine the two major functional additions to the products that most of the vendors have introduced, analyzing their impact on the challenges.

1. Deployment Templates for Virtual Security Appliances

The first significant challenge that the traditional vendors targeted was the complexity of the deployment of virtual appliances that required changes in the network topology and allocation of computer and storage resources.

The way to handle such things in this world of Software-Defined Infrastructure is by using Configuration Automation or Infrastructure as Code Templates, developed with such technologies as AWS CloudFormation, HashiCorp Terraform or CAPS tools (Chef, Ansible, Puppet, SaltStack). The first "move" of the traditional solution vendors was to adopt these technologies to overcome the obstacles in deploying virtual appliances and to partition the software-defined networks.

While this may reduce the complexity of the initial deployment, it doesn't change the picture drastically, as the virtual security appliance still requires a lot of maintenance work (updates, upgrades, policy lifecycle, topology changes, etc.) throughout its lifecycle.

Additionally, quite often, the provided templates require deep understanding and some modifications prior to being deployed in the production environments, so even the initial time saving isn't that significant.

Infrastructure as Code Templates often require deep understanding and some modifications prior to being deployed in the production environments, resulting in no initial time saving.

2. Integration with Hypervisor/Orchestrator Infrastructure, Security Policies Automation

The second "target" for the virtual security appliance vendors was to make the policy management less manual-labor-intensive by integrating with SSDI/ Hypervisor APIs.

A security policy is the "intellect" of the security solution, directing it on how to act based on a wide variety of parameters, enforcing the security checks that the organization requires. The challenge in the Software-Defined environments is that, unlike in the physical environments, these variables constantly change. Network topologies, the amounts and designation of computing resources are very flexible, sometimes orchestrated by automatic mechanisms rather than by operators. Having a static security policy to address them is just not an option.

Software-Defined Infrastructure solutions provide Application Programming Interfaces (APIs) for integration that can expose the dynamic topology at any

given moment. A natural step that all policy-driven security solutions took was to integrate with these APIs and allow their static security policies to relate to abstract terms, such as “Logical Groups” or “Tags” used to classify resources by the Software-Defined Datacenter infrastructure, rather than static terms such as “IP Addresses” or “Networks”.

The impact of this functionality on the TCO of the virtual security appliance is somewhat tangible, but the benefit can only be felt in very particular cases when the Software-Defined resources remain relatively static. Costs of deploying solutions in each and every location and maintaining the security appliance lifecycle don’t change a bit.

Software-Defined resources change constantly, and a static security policy simply cannot address them. Only when they remain relatively static can virtual security appliance answer the challenge.

The Solution
Certified Elastic Service, Software-Defined Security Controls

We believe that the true solution to the challenge is in adopting the same mentality to security as was adopted to the infrastructure. Put in layman’s terms, the notion of an orchestrated Software-Defined datacenter means – “Someone or something can manage my datacenter resources better than my team would do it manually. Therefore, we will rely on this management as a service and focus on delivering our systems within this infrastructure, according to our requirements”.

If we extend this thinking to security (all aspects of it, starting with deploying security solutions in our infrastructure and replacing all the labor-intensive organizational processes) we will reach a set of solution requirements.

Here is such a list of requirements, modelled on the challenges in the traditional model.

Network Topology – Network topologies in Software-Defined Datacenters should not have any impact on the operations of our security services.

Deployment and Configuration – Consuming application-level services in modern Software-Defined Datacenters does not require any deployment in the traditional sense of the word. Consuming such complex services as Databases, Artificial Intelligence or Data Warehousing is done by simple logical Software-Defined operations in the modern infrastructure, and security should not be any different.

Managing the Security Policies – Security policies should be logical, completely abstracted from the network topology, dealing with entities like user and service identity, data type and device / location risk. Defining policy in such terms makes it much closer to the actual business objectives, and ensures that it is auditable and understandable by non-technical role players.

Scalability and Redundancy – Scalability and redundancy of a service you are consuming should not become your concern. Any service the organization relies upon should undergo certifications for its ability to scale up to the enterprise grade demands. In other words, since when did the scalability of SalesForce, the most widely used CRM, become a concern for its users?

Multiple Sites / Locations – If your infrastructure is not bound to specific sites, your abstract business-oriented security policy should be exactly the same. In the modern world, more and more businesses are international. The geographical boundaries of providing goods and services have been removed by global trade laws, demanding that the IT infrastructure follows. So should the security.

Patching and Updating Virtual Appliances – Similar to the notion of scalability and redundancy: when consumed as a service, security infrastructure should not require any patches or updates.

To sum up our approach, we believe that the native solution for security challenges in the Software-Defined Datacenters should follow exactly the same requirements as any other Infrastructure as a Service component. Otherwise, it will not be a native match for the architecture, and it will negatively impact on the ability of the organization to benefit from the adoption of cutting edge IT technologies.