WHITE PAPER

Security Controls at the Speed of Cloud Infrastructure

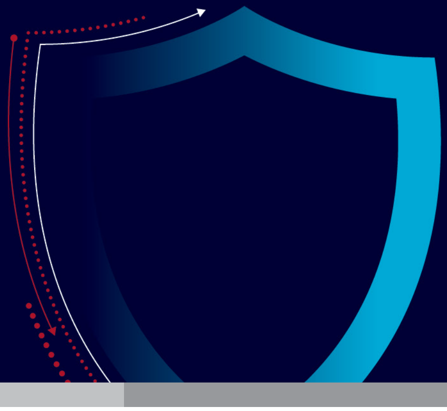


TABLE OF CONTENTS

Software-Defined Infrastructure Versus A Physical One

Software-defined infrastructure (SDI) and software-defined data centers (SDDC) are notions 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.

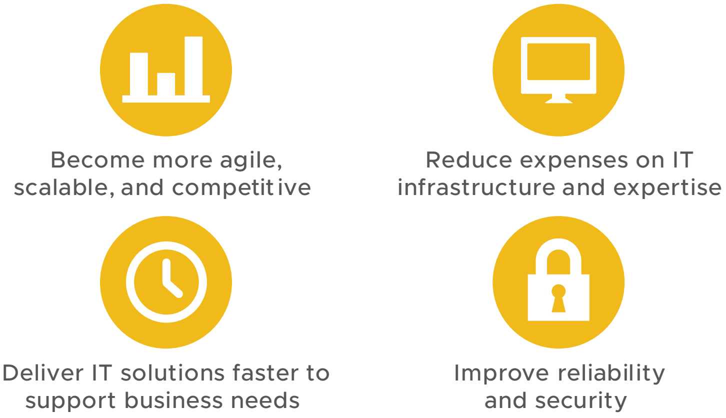
Public cloud, particularly infrastructure as a service (IaaS) and platform as a service (PaaS), is yet another step in this evolution. Both are delivering a multitude of software-defined components as a service while all the underlying physical infrastructure or data center is completely owned by the service provider.

Traditional Security Solutions for Software-Defined Infrastructure

Security is an inseparable part of any data center, whether physical or software defined. The question, though, is whether the security tools that were defined for physical data centers are good enough for the software-defined ones.

The traditional approach of the leading vendors of IT security solutions for physical data centers 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's required from a security vendor?

Figure 1: Why Companies Choose to Leverage IaaS/PaaS for IT Requirements


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

Examining 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 Security Policies

After the virtual appliances are deployed and configured, every change in the SDI (and such changes should be frequent, as this is the main reason for using software-defined vs. physical) requires manual updates to the security policies. These changes should be managed by organized change management cycles and carried out by security administrators.

SOLUTIONS BASED ON VIRTUAL APPLIANCES LACK AUTOMATIC SCALING AND REQUIRE PLANNING FOR PEAK LOAD, AS THEY DO IN PHYSICAL DATA CENTERS

Scalability and Redundancy

The SDI 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 data centers.

Multiple Sites/Locations

All of the challenges described above must be addressed in each site or location. This could easily multiply the investment of time and effort.

Patching and Updating Virtual Appliances

Virtual or physical, having a self-hosted machine running software in your data center puts the responsibility of patching and updating on the owner and not 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 ten different product lines) 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 the important principle that trying to treat SDI with tools that were built for a physical infrastructure may be possible, but the outcome will be this: the organization will not benefit from the advantages of SDI.

Automation of Deployment and Traditional Access Policy: Is It Enough?

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

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

INFRASTRUCTURE AS CODE TEMPLATES OFTEN REQUIRE DEEP UNDERSTANDING AND MODIFICATIONS PRIOR TO BEING DEPLOYED IN PRODUCTION ENVIRONMENTS, RESULTING IN NO INITIAL TIME SAVINGS

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 SDI 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 does not change the picture drastically, as the virtual security appliance still requires a lot of maintenance work (updates, upgrades, policy lifecycle, topology changes, and so on) 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.

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 how to act based on a wide variety of parameters and 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.

SDI 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 SDDC 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. The costs of deploying solutions in each and every location and maintaining the security appliance lifecycle do not change a bit.

The Solution: Certified Elastic Service, Software-Defined Security Controls

The true solution to the challenge is in adopting the same mentality to security as was adopted to the infrastructure. Put in basic terms, the notion of an orchestrated SDDC means: Someone or something can manage my data center resources better than my team can 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 reach a set of solution requirements modeled on the challenges in the traditional model, as presented above:

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.

- **Network topology:** Network topologies in SDDCs should not have any impact on the operations of our security services.
- **Deployment and configuration:** Consuming application-level services in modern SDDCs 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 that the organization relies on 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 SDDC 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 your organization's ability to benefit from the adoption of cutting-edge IT technologies.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

Copyright © 2025 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.
All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

SED-SDI-SDDC-WP101 March 4, 2025