Enhancing Cloud Security with BizCloud VPE | CSC

CSC BizCloud VPE SERVICE OVERVIEW

CSC BizCloud Virtual Private Edition (VPE) bridges the gap between the public, multitenant CSC CloudCompute™ service and the private, dedicated CSC BizCloud service. BizCloud VPE offers a lower cost entry point into an environment that features a dedicated amount of CPU, RAM and storage capacity without the larger minimum commitment required for a completely dedicated CSC BizCloud.

Generally speaking, security threats to a subscribing organization’s cloud workloads fall into one of two categories: internal threats and external threats. Internal threats most often represent issues arising from multitenancy, and external threats target the exterior security of the hosted cloud environment. CSC BizCloud VPE addresses internal security threats with a multitenant hypervisor-based solution by isolating and dedicating physical and virtual compute, storage and networking resources.

This segregation and dedication is enforced at the physical infrastructure level through the use of a dedicated blade or blades. At the VMware vSphere® layer, this is done with the creation of a dedicated hypervisor cluster component; at the storage layer, with the dedication of an entire logical unit (LUN) or units from the storage array; at the VMware vCloud® Director™ level, with the creation of a dedicated virtual data center and organization virtual data center(s); and at the network layer, with the creation of a dedicated VMware vSphere® Distributed Virtual Switch and VMware vShield™ Edge virtual appliance host segregation.

Although our CSC CloudCompute multitenant environment does not provide direct access to the underlying physical resources, it relies on resource sharing by provisioning multiple enterprise virtual data centers on the same physical hosts and within the same storage boundaries with the use of the VMware vSphere® Hypervisor. Although extremely unlikely, the potential exists for a malicious attack on the shared hypervisor that underlies this multitenant environment. Such an attack could compromise, obstruct or gain access to other virtual machines operating within these physical and logical boundaries. This potential vulnerability causes some companies concern about the prospect of moving workloads into a multitenant cloud. CSC BizCloud addresses these concerns by dedicating 100% of the physical and virtual resources and its supporting infrastructure systems to a single customer; however, some organizations find this dedicated solution to be cost prohibitive due to the minimum monthly commitment, or they are simply not ready to migrate sufficient workloads and applications into a dedicated cloud to justify its higher commitment and cost. CSC BizCloud VPE addresses this possible area of vulnerability through the dedication and segregation of the underlying physical compute and storage resources.
Physical Processors — The hypervisor’s primary function is to arbitrate shared access to the host’s physical CPUs to enable oversubscription of that resource. By dedicating the entire physical host’s processing resources to a particular subscribing customer, successful attempts to exploit the hypervisor surface area cannot result in the compromise of that subscriber’s data from outside their organization.

Physical Memory — The hypervisor is also responsible for managing shared access to the physical memory resources within the host on which it runs. Each virtual machine is granted access to a measure of physical memory capacity that the guest operating system can manage and assign as virtual memory to the requesting application workloads. As with CPU resources, dedicating these physical memory resources prevents malicious activity from being performed by another cloud subscriber that could compromise the hypervisor and potentially allow them to access the memory resources of the virtual machines.

Storage Capacity — Another key function of the hypervisor layer is the management of storage resources, which are typically presented to the hosts in the form of LUNs, representing a segregated allocation of storage from the disk array. Although the hypervisor abstracts the Fiber Channel storage layer through a virtual SCSI adapter, within a multitenant environment the virtual disk devices that hold the subscriber’s data are logically separated from each other by the security controls of the hypervisor’s storage subcomponents. Therefore the potential exists for an exploit to enable access from one virtual machine within a particular LUN or data store. To mitigate this risk, CSC BizCloud VPE dedicates the entire LUN to a single subscribing organization.
To enable segregation and dedication of physical and storage resources within the leveraged virtualization management framework, these resources are logically grouped together to form a dedicated vSphere Cluster. This construct represents the dedicated host or hosts and their associated resource pools and data stores, and serves as the security boundary enabling later segregation within VMware vCloud® Director™. In environments consisting of multiple hosts’ worth of resources in a single cluster, VMware High Availability (HA) and Dynamic Resource Scheduling are also enabled, similar to the CSC CloudCompute clusters, to provide resiliency and automatic resource management across the cluster. CSC maintains a low response/repair/replacement service level agreement (SLA) with the hardware vendors to ensure that in the case of a hardware failure, service can be restored within the BizCloud VPE uptime SLA. This CSC practice offsets the higher downtime potential for subscribing organizations purchasing only a single blade’s worth of capacity, as HA is not available.

Within VMware vCloud® Director™, a virtual data center creates an abstraction of compute and storage virtual resources. A CSC BizCloud VPE Virtual Data Center is a 1:1 mapping to the CPU and memory resources of an entire vSphere ESX cluster. This cluster consists of one or more dedicated ESX hosts and contains the data store(s) seen by those hosts. This dedicated virtual data center can be further divided into multiple organization virtual data centers if that fits the subscribing organization’s needs, but all organization virtual data centers created from this dedicated virtual data center remain segregated from those of other cloud subscribers.

The same VLAN separation that exists within CSC CloudCompute to prevent multiple subscribers from gaining access to the same networks is also carried over to CSC BizCloud VPE to provide network security within the dedicated virtual environment. In both offerings, VMware vCloud® Director™ facilitates the creation of consistent secure VLANs, and the VMware Distributed Virtual Switch enforces the separation of traffic between the different VLANs.

Where CSC BizCloud VPE differs from CSC CloudCompute is with the creation of a dedicated distributed virtual switch per VPE cluster. In the CSC CloudCompute environment, a distributed virtual switch can potentially span an entire vSphere Data Center and all clusters and hosts contained within. This can result in a vShield Edge being deployed on a cluster, for which it carries traffic, that is not dedicated to the subscribing organization — effectively routing traffic through an ESX host that is running virtual machines for other subscribers. Again, although unlikely, this creates the potential for data compromise if a virtual machine on the non-VPE cluster gains access to the vShield Edge appliance that belongs to the VPE subscribing organization. By limiting the distributed virtual switch membership to hosts within the CSC BizCloud VPE subscriber’s dedicated environment, we limit the vShield Edge appliances committed to that subscribing enterprise to running only on the appropriate hosts.
CSC BizCloud VPE does leverage some existing CSC CloudCompute infrastructure systems to cost-effectively provide the service, while still providing complete segregation at the hypervisor level for the subscriber’s virtual machines. In particular, the same VMware vCloud® Director™ and CSC Cloud Store Orchestration instances used by CSC CloudCompute subscribers to provision and modify workloads in the public cloud environment are also used by CSC BizCloud VPE subscribers to manage their dedicated capacity. These systems control vCenter Server instances, which are also leveraged with the CSC CloudCompute environment. Figure 1 provides a comprehensive representation of these leveraged systems.

CSC BizCloud VPE addresses the multitenant vulnerability concerns of many potential enterprise cloud subscribers by providing dedicated blades, dedicated LUN from the storage array, a dedicated virtual data center at the VMware vCloud® Director™ level and a dedicated virtual switch at the network layer, providing vShield virtual application segregation.

The creation of a dedicated distributed virtual switch that only needs to connect to VLANs dedicated to a single subscribing organization also allows for the reduction of the number of VLANs that need to be presented to these dedicated blades within the UCS Service Profile vNIC Templates. This results in a lower number of VLAN ports consumed across the UCS domain.

To capitalize on this benefit, a new network pool must be created for each CSC BizCloud VPE subscribing organization within vCloud® Director™, containing only the number of VLANs required by the VPE subscriber. The resulting VLAN port count reduction potentially can be drastic, especially across UCS domains with a high number of blades.

CSC BizCloud VPE COMPONENTS

SHARED WITH THE CSC CloudCompute PRODUCT

SUMMARY

Attacks on Shared Hypervisor Compromising Customer’s Data
- Dedicate the entire physical host’s processing and memory resources to a single customer
- Presentation and dedication of an entire LUN or data store to only a single customer

Network Sharing
- VLAN separation (same as for CloudCompute) to prevent multiple customers from gaining access to the same networks
- Add a dedicated VMware Distributed Virtual Switch for the client’s VLAN cluster

Workload Segregation
- Resource grouped to form a dedicated vSphere® Cluster serves as a security boundary
- VMware vCloud® Director’s™ Virtual Datacenter segregates and separates resources dedicated to a single BizCloud VPE client
- Further division into multiple group/department virtual data centers, if required by the client
BizCloud VPE delivers cloud privacy for less time, money and commitment than BizCloud, with more security than CloudCompute due to higher levels of resource segregation and almost all competitive private hosted cloud offerings. It delivers these benefits:

- Real cloud experience
- Scale resources up with 20% headroom
- Infrastructure support shifted to external supplier
- Accelerated cycle time for provisioning
- Eliminate HW upgrade process
- No capital expense

It is a lower-cost alternative than a build-it-yourself cloud and requires about half of the minimum commitment required for a BizCloud environment (270GB VRAM for BizCloud VPE vs. 1,917GB VRAM for BizCloud). Except for the ability to implement BizCloud in the client data center, all the other benefits of BizCloud as compared to a do-it-yourself alternative are in play.

---

**BUILD YOUR OWN PRIVATE CLOUD** | **CSC BIZCLOUD** | **CSC BIZCLOUD VPE**

| REDUCED RISK | On-premises solution | ✓ | ✓ |
| Managed risk and security | ✓ | ✓ | ✓ |

| PRESERVED CAPITAL | Capital expense | ✓ |
| Operating expense | ✓ | ✓ | ✓ |

| INCREASED AGILITY AND FLEXIBILITY | Elasticity — dial resources up and down | ✓ | ✓ |
| Pay as you go with standard rate card | ✓ | ✓ | ✓ |
| Chargeback capability | ✓ | ✓ | ✓ |
| Fully managed orchestration capability | ✓ $$$ | ✓ | ✓ |
| Service catalog | ✓ $$$ | ✓ | ✓ |
| Self-service provisioning portal | ✓ $$$ | ✓ | ✓ |

| STANDARDIZED GLOBAL DELIVERY | Standard operating environments | ✓ | ✓ | ✓ |
| Monitoring and management (infrastructure & OS) | ✓ | ✓ | ✓ |
| Single contact for support and maintenance | ✓ | ✓ | ✓ |

| 10 MONTHS $$$$$$ | 10 WEEKS $ | DAYS $ |

---

*BizCloud VPE — added cloud security for less time, money and a lower minimum commitment.*