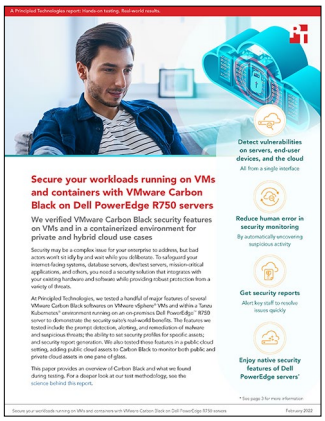

The science behind the report:

Secure your workloads running on VMs and containers with VMware Carbon Black on Dell PowerEdge R750 servers

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report Secure your workloads running on VMs and containers with VMware Carbon Black on Dell PowerEdge R750 servers.

We concluded our hands-on testing on January 14, 2022. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on December 10, 2021 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

System configuration information

Table 1: Detailed information on the system we tested.

System configuration information	Dell PowerEdge™ R750
BIOS name and version	Dell 1.3.8
Non-default BIOS settings	None
Operating system name and version/build number	VMware ESXi™ 7.0.3, build 18825058
Date of last OS updates/patches applied	11/20/2021
Power management policy	Maximum Performance
Processor	
Number of processors	2
Vendor and model	Intel® Xeon® Platinum 8168
Core count (per processor)	28
Core frequency (GHz)	2.00
Stepping	6

System configuration information	Dell PowerEdge™ R750
Memory module(s)	
Total memory in system (GB)	1,024
Number of memory modules	16
Vendor and model	Samsung M393A8G40AB2-CWE
Size (GB)	64
Type	PC4-25600R
Speed (MHz)	3,200
Speed running in the server (MHz)	2,933
Storage controller	
Vendor and model	Dell PERC H755N Front
Cache size (GB)	8GB
Firmware version	52.16.1-4074
Local storage	
Number of drives	6
Drive vendor and model	Dell Ent NVMe AGN MU U.2 1.6TB
Drive size (GB)	1,600
Drive information (speed, interface, type)	NVMe™
Network adapter	
Vendor and model	Intel Ethernet 25G 2P E810-XXV OCP
Number and type of ports	2 x 25GbE
Cooling fans	
Vendor and model	Foxconn PIA060K12Q
Number of cooling fans	6
Power supplies	
Vendor and model	PWR SPLY, 1400W, RDNT, LTON
Number of power supplies	2
Wattage of each (W)	1,400

How we tested

Preparing the local VMware environment

1. On the Dell PowerEdge R750 server, install VMware ESXi 7.0.3, build18825058.
2. In your environment, install VMware vCenter appliance 7.0.3, build1 8778458.
3. Create one small auxiliary VM to run Ubuntu 21.04.

Installing end-user VMs in the VMware and AWS Environments

We created nine VMs on our VMware environment that Carbon Black would later add as business assets. Each VM had 2 vCPUs and 4 GB of vRAM. The VMs ran the following operating systems:

Platform	OS
Microsoft Windows	Windows 8.1 Windows 10
Windows Server	Windows Server 2016 Windows Server 2019 Windows Server Core 2020
Linux Server	Ubuntu 18.10 Ubuntu 2004 CentOS 7 Red Hat Enterprise Linux 8.4

We created two Linux instances on AWS that had could access the public internet. The instances ran Amazon Linux 2 and Ubuntu 20.04.

Creating the Kubernetes clusters in the local VMware environment

We created two Kubernetes Clusters in the local VMware environment using Tanzu Kubernetes Grid (TKG).

1. On the auxiliary VM, install the prerequisites for TKG v1.4.0, and install the tanzu and kubectl utilities (v1.21.2+vmware.1).
2. Using the mgmt-cluster.yaml file below, create the TKG management cluster:

```
tanzu management-cluster  create  --f ./mgmt-cluster.yaml  -v 5
```

```
# MGMT template mgmt-cluster.yaml
    CLUSTER_NAME: mgmt
    CLUSTER_PLAN: dev
    INFRASTRUCTURE_PROVIDER: vsphere
    ENABLE_CEIP_PARTICIPATION: true
    ENABLE_AUDIT_LOGGING: true
    CLUSTER_CIDR: 100.96.0.0/11
    SERVICE_CIDR: 100.64.0.0/13
    VSPHERE_SERVER: 10.220.1.100
    VSPHERE_USERNAME: administrator@vsphere.local
    VSPHERE_PASSWORD: XXXXXXXXX!
    VSPHERE_DATACENTER: /DC
    VSPHERE_RESOURCE_POOL: /DC/host/F1
    VSPHERE_DATASTORE: /DC/datastore/capacity
    VSPHERE_FOLDER: /DC/vm/F1
    VSPHERE_NETWORK: /DC/network/VM Network
    VSPHERE_CONTROL_PLANE_ENDPOINT: 10.220.40.41
    VSPHERE_SSH_AUTHORIZED_KEY: ssh-rsa AAAAB3NzaC1yc2EA … Qk72lAS/V62cMTqXw== ptuser@deploy
    VSPHERE_INSECURE: true
    DEPLOY_TKG_ON_VSPHERE7: false
    ENABLE_TKGS_ON_VSPHERE7: false
    SIZE: small
    ENABLE_MHC_CONTROL_PLANE: true
    ENABLE_MHC_WORKER_NODE: true
    MHC_UNKNOWN_STATUS_TIMEOUT: 5m
    MHC_FALSE_STATUS_TIMEOUT: 12m
    IDENTITY_MANAGEMENT_TYPE: "oidc"
    AVI_ENABLE: false
    AVI_CONTROL_PLANE_HA_PROVIDER: false
```

3. Using the worker-cluster.yaml template file, create the two worker clusters. Name these clusters `work1` and `work2` and set the cluster endpoint IP address as `10.220.40.41` and `10.220.40.43`.

```
tanzu cluster create -f worker-cluster.yaml -v 5
```

```
CLUSTER_NAME: work2
    VSPHERE_CONTROL_PLANE_ENDPOINT: 10.220.40.43
    CLUSTER_PLAN: prod
    INFRASTRUCTURE_PROVIDER: vsphere
    ENABLE_CEIP_PARTICIPATION: true
    ENABLE_AUDIT_LOGGING: true
    CLUSTER_CIDR: 100.96.0.0/11
    SERVICE_CIDR: 100.64.0.0/13
    VSPHERE_SERVER: 10.220.1.100
    VSPHERE_USERNAME: administrator@vsphere.local
    VSPHERE_PASSWORD: Password1!
    VSPHERE_DATACENTER: /DC
    VSPHERE_RESOURCE_POOL: /DC/host/F1
    VSPHERE_DATASTORE: /DC/datastore/capacity
    VSPHERE_FOLDER: /DC/vm/F1
    VSPHERE_NETWORK: /DC/network/VM Network
    VSPHERE_SSH_AUTHORIZED_KEY: ssh-rsa AAAAB3NzaC1yc2EA … Qk72lAS/V62cMTqXw== ptuser@deploy
    VSPHERE_INSECURE: true
    DEPLOY_TKG_ON_VSPHERE7: false
    ENABLE_TKGS_ON_VSPHERE7: false
    SIZE: small
    ENABLE_MHC_CONTROL_PLANE: true
    ENABLE_MHC_WORKER_NODE: true
    MHC_UNKNOWN_STATUS_TIMEOUT: 5m
    MHC_FALSE_STATUS_TIMEOUT: 12m
    IDENTITY_MANAGEMENT_TYPE: "oidc"
    AVI_ENABLE: false
    AVI_CONTROL_PLANE_HA_PROVIDER: false
```

Installing VMware Carbon Black Appliance on the local VMware environment

1. From the following URL, download the OVA for version 1.1 of VMware Carbon Black Workload: https://my.vmware.com/web/vmware/downloads.
2. Using the documentation at the following URL, deploy the appliance: https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.1/carbonblack_workload/GUID-DDE511BD-1D8D-41DB-B100-DA408863D2B5.html.
3. Using the documentation at the following URL, register the appliance with the local vCenter: https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.1/carbonblack_workload/GUID-01A26275-C9A1-4C1A-A446-5D9CF727C249.html
4. Using the documentation at the following URL, create an API access level from the Carbon Black Cloud console: https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.1/carbonblack_workload/GUID-9EA7512D-3841-45D4-9D12-E64C165373B3.html.
5. Using the documentation at the following URL, create API access credentials from the Carbon Black Cloud console: https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.1/carbonblack_workload/GUID-5EE3C9D2-5096-49EB-9C2D-2A6BFEE5A01B.html
6. Using the documentation at the following URL, connect the Carbon Black appliance with Carbon Black Cloud from the local vCenter: https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.1/carbonblack_workload/GUID-979BF9DD-875B-45F9-9640-0BD6BB52A865.html

Installing VMware Carbon Black sensors on the VMware VMs and Amazon Web Services instances

1. To install Carbon Black sensors on the VMware VMs, first download the sensors form the Carbon Black Cloud:
   - Inventory → VM Workloads → Sensor Options → Download Sensor Kits → Download Kit (Windows 64-bit, RHEL / CentOS / Oracle Linux, and Ubuntu & Debian).
2. To install Carbon Black sensors for Amazon Linux 2 and Ubuntu Linux from Carbon Black Cloud, select the following menu options, and download the kit:
   - Inventory → Endpoints → Sensor Options → Download Sensor Kits → Download Kit (Amazon Linux 2 and Ubuntu & Debian).
3. Copy the OS-specific sensor kit to each VM and AWS instance.
4. We obtained the "company code" from the Carbon Black Cloud console:
   - Inventory → Endpoints → Sensor Options → Company Codes

5. On each Linux system, perform the following steps:
    a. To install the Linux headers for the OS, run the first command on RHEL-like systems, and run the second on the Ubuntu systems:

```
sudo yum install -y kernel-devel-$(uname -r)
sudo apt install linux-headers-$(uname -r)
```

    b. Unpack the contents of the sensor archive:

```
tar xf cb-psc-sensor*.tgz
```

    c. Run the installer with the "company code" as the sole argument:

```
sudo ./install.sh "company code"
```

6. On the Windows systems, run the following command with the "company code" as the final argument.

```
msiexec /q /i .\installer_vista_win7_win8-64-3.3.0.953.msi /L* log.txt COMPANY_CODE="company code"
```

Installing the VMware Carbon Black sensors for the Kuberbetes clusters

For each Kubernetes cluster, perform the following steps.

1. On the Carbon Black Cloud console, navigate to the cluster setup page:
    - Inventory → Kubernetes → Clusters → Add Cluster
2. On the CLUSTER DETAIL page, type the name of the cluster, and click Next.
3. On the AUTHENTICATION page, select Generate a new API key. Enter a name for the key, and click Next.
4. On the SENSOR page, click Next
5. On the FINISH SETUP page, copy the three commands that will be used to install the Carbon Black operator, add Kubernetes secrets, and apply the cluster configuration.
6. Click DONE.
7. From the auxiliary VM, run the three commands. For example:

```
curl -s https://setup.containers.carbonblack.io/operator-v5.1.0-apply.sh | bash
kubectl create secret generic cbcontainers-access-token --namespace cbcontainers-dataplane \ --from
    literal=accessToken=XXXXXXXXX4JAW3ZWS3FVB7D/LEMVFZDKEL
kubectl apply -f https://setup.containers.carbonblack.io/cr-a30d93d9-eae0-42ae-b5e8-519d55026a28
```

Running malware on a monitored VM

1. On the Windows 2022 VM, disable the real-time detection of threats for Windows Defender.
2. On the Windows 2022 VM, download version 6.1.25 of Metasploit Framework.
3. On the Carbon Black dashboard, run the Metasploit installer and observe the alerts on the VM's console.
4. Carbon Black should prevent the installer from copying the required files and folders that contain malware, leading the installer to stall. On the VM, kill the stalled installer process.

Read the report at https://facts.pt/WTG9n01 ▶

This project was commissioned by Dell Technologies.