A Principled Technologies report: Hands-on testing. Real-world results.

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

We verified VMware Carbon Black security features on VMs and in a containerized environment for private and hybrid cloud use cases

Security may be a complex issue for your enterprise to address, but bad actors won't sit idly by and wait while you deliberate. To safeguard your internet-facing systems, database servers, dev/test servers, mission-critical applications, and others, you need a security solution that integrates with your existing hardware and software while providing robust protection from a variety of threats.

At Principled Technologies, we tested a handful of major features of several VMware Carbon Black softwares on VMware vSphere® VMs and within a Tanzu Kubernetes® environment running on an on-premises Dell PowerEdge™ R750 server to demonstrate the security suite's real-world benefits. The features we tested include the prompt detection, alerting, and remediation of malware and suspicious threats; the ability to set security profiles for specific assets; and security report generation. We also tested these features in a public cloud setting, adding public cloud assets to Carbon Black to monitor both public and private cloud assets in one pane of glass.

This paper provides an overview of Carbon Black and what we found during testing. For a deeper look at our test methodology, see the science behind this report.

Detect vulnerabilities on servers, end-user devices, and the cloud

All from a single interface

Reduce human error in security monitoring

By automatically uncovering suspicious activity

Get security reports

Alert key staff to resolve issues quickly

Enjoy additional security features of Dell PowerEdge servers*

* See page 3 of the report for more information

About Carbon Black

In today's working environment, there is a great need for for advanced security measures that can deal with and get ahead of increasingly sophisticated threats against organizations. According to VMware analysis, global organizations saw a 148 percent increase in ransomware attacks in just a single month at the start of the COVID-19 pandemic, from February to March 2020.[1]

Carbon Black is a security solution for the cloud, cloud-based workloads and containers, and endpoints. The security solution comprises five products: Endpoint, Container, Cloud, Cloud Workload, and Endpoint sensors for Linux and Windows.

VMware claims that Carbon Black uses intelligent system hardening, behavioral prevention, and daily scans of more than 1 trillion security events to detect and deter emerging threats to businesses.[2]

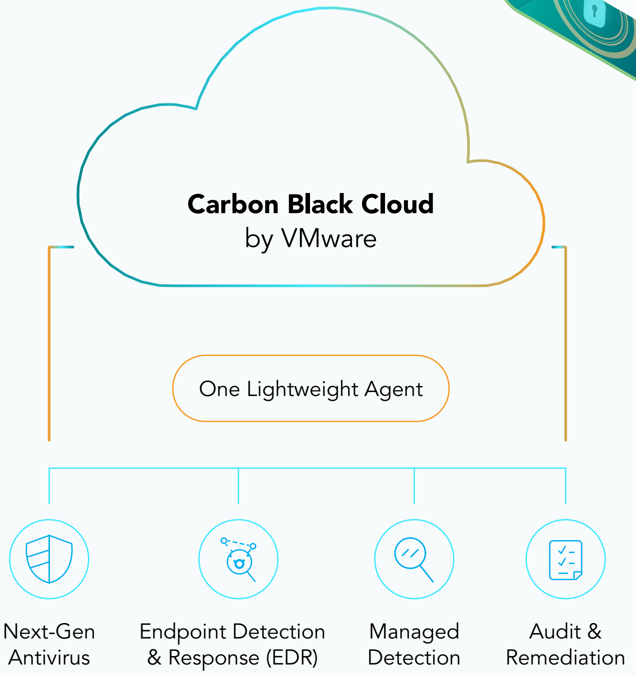
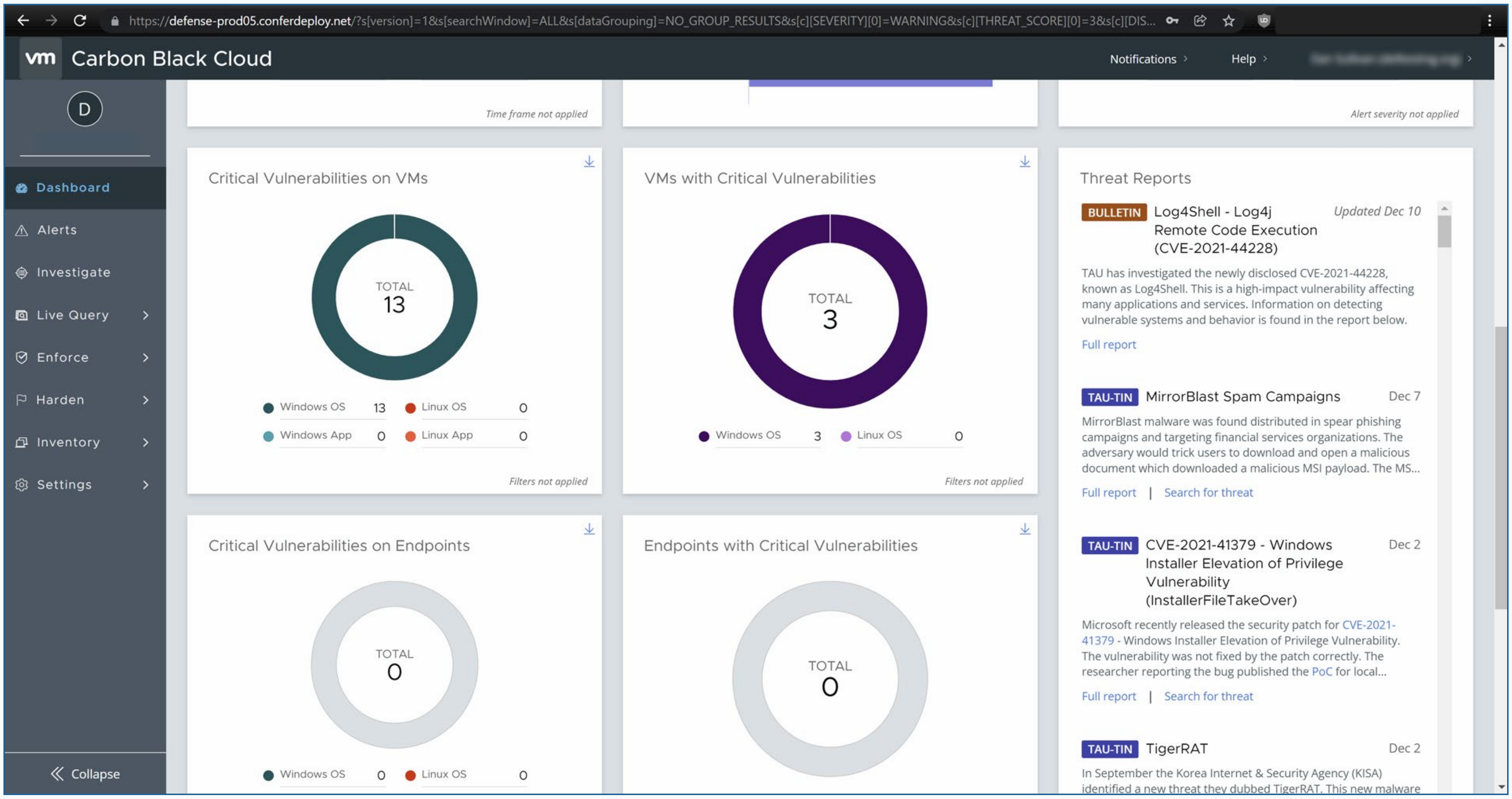


Figure 1: Carbon Black Cloud feature diagram. Source: Principled Technologies, based on figure 1 of "VMware Carbon Black Cloud Enterprise EDR: Threat Hunting & Incident Response," VMware, 2020.[3]


https://defense-prod05.conferdeploy.net/?s[version]=1&s[searchWindow]=ALL&s[dataGrouping]=NO_GROUP_RESULTS&s[c][SEVERITY][0]=WARNING&s[c][THREAT_SCORE][0]=3&s[c][DIS...
vm Carbon Black Cloud
Notifications
Help
[redacted]
D
Dashboard
Alerts
Investigate
Live Query
Enforce
Harden
Inventory
Settings
Collapse
Time frame not applied
Alert severity not applied
Critical Vulnerabilities on VMs
TOTAL 13
Windows OS 13
Linux OS 0
Windows App 0
Linux App 0
Filters not applied
VMs with Critical Vulnerabilities
TOTAL 3
Windows OS 3
Linux OS 0
Filters not applied
Critical Vulnerabilities on Endpoints
TOTAL 0
Windows OS 0
Linux OS 0
Endpoints with Critical Vulnerabilities
TOTAL 0
Threat Reports

BULLETIN Log4Shell - Log4j Remote Code Execution (CVE-2021-44228) *Updated Dec 10*

TAU has investigated the newly disclosed CVE-2021-44228, known as Log4Shell. This is a high-impact vulnerability affecting many applications and services. Information on detecting vulnerable systems and behavior is found in the report below.

Full report

TAU-TIN MirrorBlast Spam Campaigns Dec 7

MirrorBlast malware was found distributed in spear phishing campaigns and targeting financial services organizations. The adversary would trick users to download and open a malicious document which downloaded a malicious MSI payload. The MS...

Full report | Search for threat

TAU-TIN CVE-2021-41379 - Windows Installer Elevation of Privilege Vulnerability (InstallerFileTakeOver) Dec 2

Microsoft recently released the security patch for CVE-2021-41379 - Windows Installer Elevation of Privilege Vulnerability. The vulnerability was not fixed by the patch correctly. The researcher reporting the bug published the PoC for local...

Full report | Search for threat

TAU-TIN TigerRAT Dec 2

In September the Korea Internet & Security Agency (KISA) identified a new threat they dubbed TigerRAT. This new malware

Figure 2: VMware Carbon Black Cloud dashboard provided visual summaries of our organization's IT assets that did not conform to our Carbon Black security policies and had non-zero risk assessments. Source: Principled Technologies.

Our environment

Our testing environment comprised two parts: an on-premises solution built on a Dell PowerEdge R750 server running VMware vSphere, and two Amazon Elastic Cloud Compute (EC2) t2.micro instances. One instance ran Amazon Linux 2, while the other ran Ubuntu 20.04.

Our findings

In our tests, we validated the following VMware Carbon Black features:

Endpoint detection:

- Cloud VMs*
- Kubernetes clusters*

Asset detection:

- Operating systems
- System applications
- Database applications
- Web applications

Vulnerability detection:

- Operating system (OS) / app vulnerabilities
- OS / apps out of date
- Misconfigured apps
- Malware
- Suspicious activity

Other features:

- Risk-level ratings
- Dashboard UI
- Reporting

*Detecting the Cloud VMs and Kubernetes clusters required the installation and use of Carbon Black sensors, which was a simple process requiring a single line of code.

Cyber Resilient Architecture on the Dell PowerEdge R750 server

The Dell EMC PowerEdge R750, together with iDRAC9, delivers tools that aim to provide layers of security across hardware and firmware and integrate security "throughout the entire server lifecycle."[4] Dell calls this layered approach to IT security Cyber Resilient Architecture, and it applies to all 14G and 15G Dell PowerEdge servers. According to Dell, Cyber Resilient Architecture includes features such as:

- Silicon-based Root of Trust
- Cryptographically trusted booting
- Digitally signed firmware packages
- Hard drive encryption and enterprise key management
- Drift detection
- Dynamic System Lockdown
- Persistent event-logging
- Audit-logging and alerts
- Chassis Intrusion Detection
- Automated BIOS recovery
- Rapid OS recovery
- Firmware Rollback

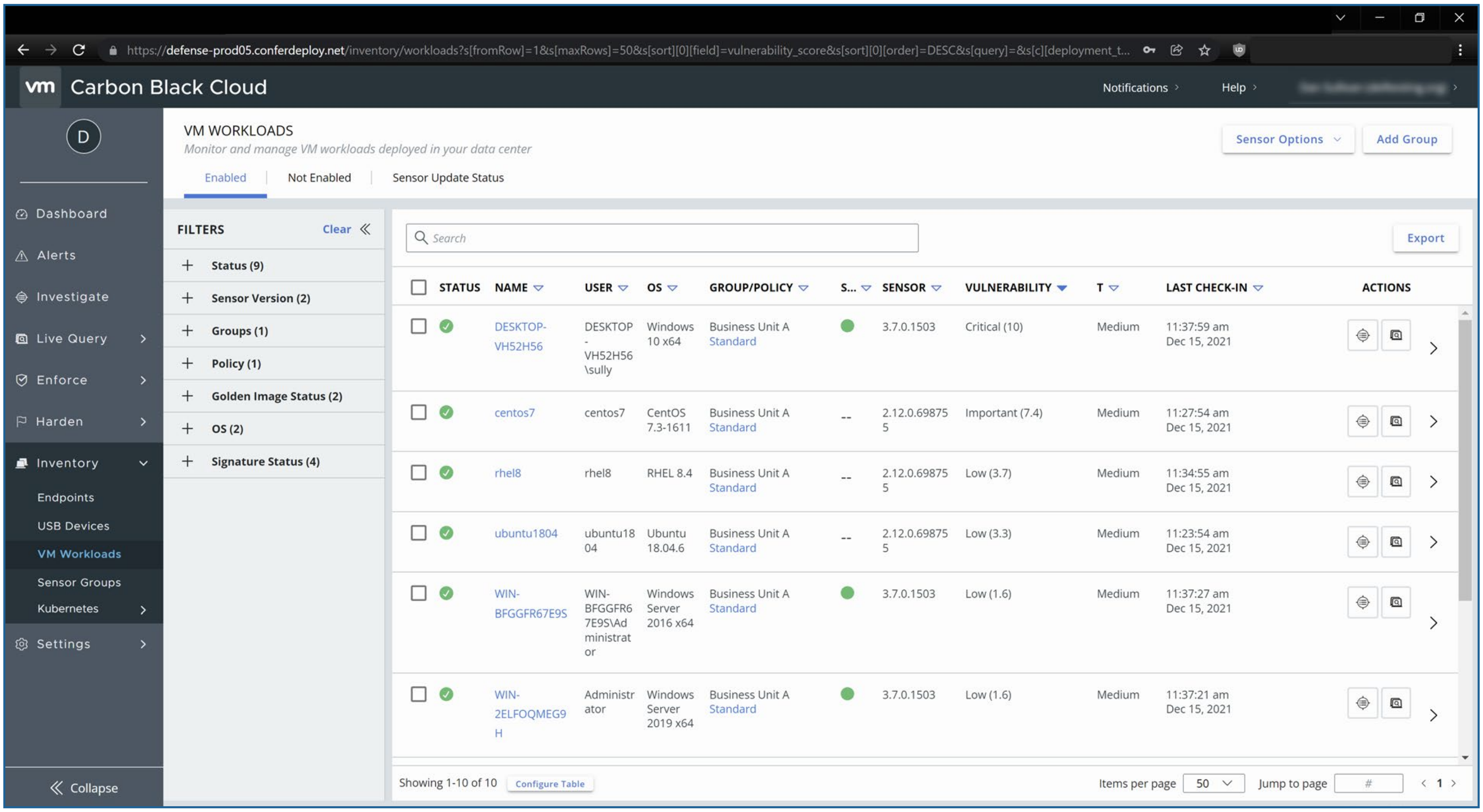
To learn more, visit https://www.delltechnologies.com/en-my/collaterals/unauth/white-papers/products/servers/cyber-resilient-security-with-poweredge-servers.pdf.

Installing Carbon Black and detecting our environment

For reliable and robust protection, it's paramount that a security solution is able to correctly identify all assets within your environment. This way, the security solution can detect unexpected changes or alert your team to potential security risks that require prompt action.

To test this capability, we deployed Carbon Black to a set of VMs in our VMware vSphere environment. Carbon Black successfully detected each of our assets and their patch statuses.

Figure 3 shows that Carbon Black detected a number of vulnerabilities within our environment, including 13 "Critical" vulnerabilities across three VMs. But what does critical mean to Carbon Black?



https://defense-prod05.conferdeploy.net/inventory/workloads?s[fromRow]=1&s[maxRows]=50&s[sort][0][field]=vulnerability_score&s[sort][0][order]=DESC&s[query]=&s[c][deployment_t...

Carbon Black Cloud

VM WORKLOADS

Monitor and manage VM workloads deployed in your data center

FILTERS Clear

- Status (9)
- Sensor Version (2)
- Groups (1)
- Policy (1)
- Golden Image Status (2)
- OS (2)
- Signature Status (4)

STATUS	NAME	USER	OS	GROUP/POLICY	S...	SENSOR	VULNERABILITY	T	LAST CHECK-IN	ACTIONS
✓	DESKTOP-VH52H56	DESKTOP-VH52H56\sully	Windows 10 x64	Business Unit A Standard	●	3.7.0.1503	Critical (10)	Medium	11:37:59 am Dec 15, 2021	
✓	centos7	centos7	CentOS 7.3-1611	Business Unit A Standard	--	2.12.0.698755	Important (7.4)	Medium	11:27:54 am Dec 15, 2021	
✓	rhel8	rhel8	RHEL 8.4	Business Unit A Standard	--	2.12.0.698755	Low (3.7)	Medium	11:34:55 am Dec 15, 2021	
✓	ubuntu1804	ubuntu1804	Ubuntu 18.04.6	Business Unit A Standard	--	2.12.0.698755	Low (3.3)	Medium	11:23:54 am Dec 15, 2021	
✓	WIN-BFGGFR67E9S	WIN-BFGGFR67E9S\Administrator	Windows Server 2016 x64	Business Unit A Standard	●	3.7.0.1503	Low (1.6)	Medium	11:37:27 am Dec 15, 2021	
✓	WIN-2ELFOQMEG9H	Administrator	Windows Server 2019 x64	Business Unit A Standard	●	3.7.0.1503	Low (1.6)	Medium	11:37:21 am Dec 15, 2021	

Showing 1-10 of 10 Configure Table Items per page 50 Jump to page # 1

Figure 3: The VM assets in our environment that Carbon Black successfully detected. Source: Principled Technologies.

After detecting system vulnerabilities, Carbon Black assigns each a numerical score, and then uses the score to sort threats into categories to show how urgent each threat is to your organization. Figure 3 illustrates this process.

Carbon Black begins by giving each individual vulnerability a risk score from 0.0 to 10.0.[5] Based on the risk score, Carbon Black filters each vulnerability by severity to convey each threat's seriousness in a way that helps IT quickly assess threat levels. Carbon Black considers threats ranked 0.0 to 3.9 to be low-severity. 4.0 to 6.9 are Moderate; 7.0 to 8.9 are Important; and 9.0 to 10.0 are Critical.[6] By sorting threats in this manner, security staff can quickly triage and determine where to focus their efforts.

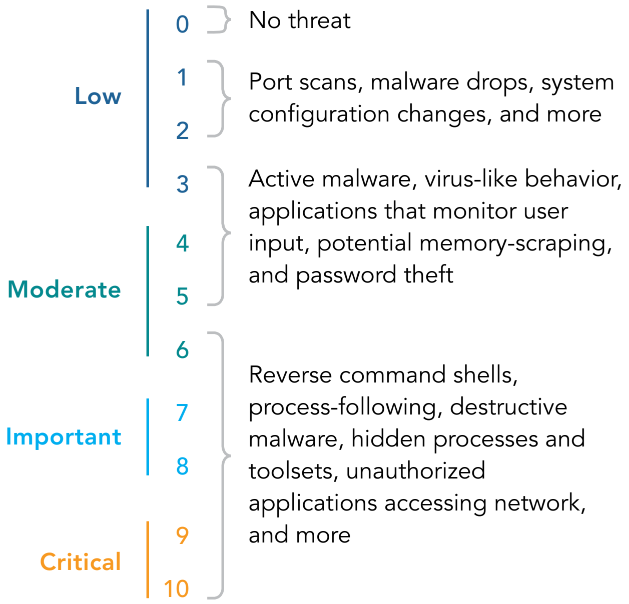

Low
Moderate
Important
Critical
0
1
2
3
4
5
6
7
8
9
10
No threat
Port scans, malware drops, system configuration changes, and more
Active malware, virus-like behavior, applications that monitor user input, potential memory-scraping, and password theft
Reverse command shells, process-following, destructive malware, hidden processes and toolsets, unauthorized applications accessing network, and more

Figure 4: Threat and vulnerability categorization in Carbon Black. Individual types of threats are given a score from 0.0 to 10.0, and thereafter sorted into four Severity categories from Low to Critical. Source: Principled Technologies.

Our testing

Malware and suspicious activity

Detecting harmful threats

VMware claims that Carbon Black can proactively empower companies to detect and stop emerging attacks.[7] To test this, we tampered with our system in the following ways:

- Removed OS patches
- Misconfigured applications
- Introduced malware

We wanted to see whether Carbon Black would detect these activities without an administrator needing to perform a manual scan, as automated detection can save time for security admins and cut down on potential human error. Carbon Black successfully detected all our removed OS patches and misconfigured applications in real-time.

To test Carbon Black malware detection, we first disabled Windows Security on a VM running Windows Server 2020 to ensure all malware alerts and warnings would come from Carbon Black alone. We then downloaded and began to install the security tool Metasploit 6.1.27, which contains a suite of exploits and vulnerability detection-testing tools. However, the Carbon Black sensor detected and prevented the installer from copying files containing exploits or malware to the VM's filesystem. Carbon Black logged each exploit on the OS system console, and pushed a single security event alert to the dashboard (as opposed to cluttering the dashboard view with individual alerts for each exploit detected during the event). We were able to view the event in full detail via the assets status page.

Dashboard view

Carbon Black provided an all-in-one view of our testbed's VMs, operating systems, and Kubernetes clusters. This can give management staff a quick overview of at-risk assets across the entire data center, enabling them to issue prompt warnings and recommendations for remediation. The dashboard also breaks down the status of individual applications across assets (such as MySQL, Adobe Web Server, etc.).

Alerting the right personnel

Of course, simply detecting malware or suspicious activity may not be enough to prevent a security emergency. Alerting the right personnel at the time of detection can help facilitate a swift and positive resolution to potential threats and wrongdoing.

Whenever Carbon Black detected suspicious activity or malware, it sent us alerts via email in addition to displaying them on the Carbon Black dashboard. This is important, as malicious activity doesn't always happen during regular business hours when security staff is more likely to be actively monitoring the dashboard. With email notifications, your security team can be more aware of their organization's security status and begin working toward solutions more quickly than if they relied on dashboard notifications alone.

Remedying vulnerabilities and threats

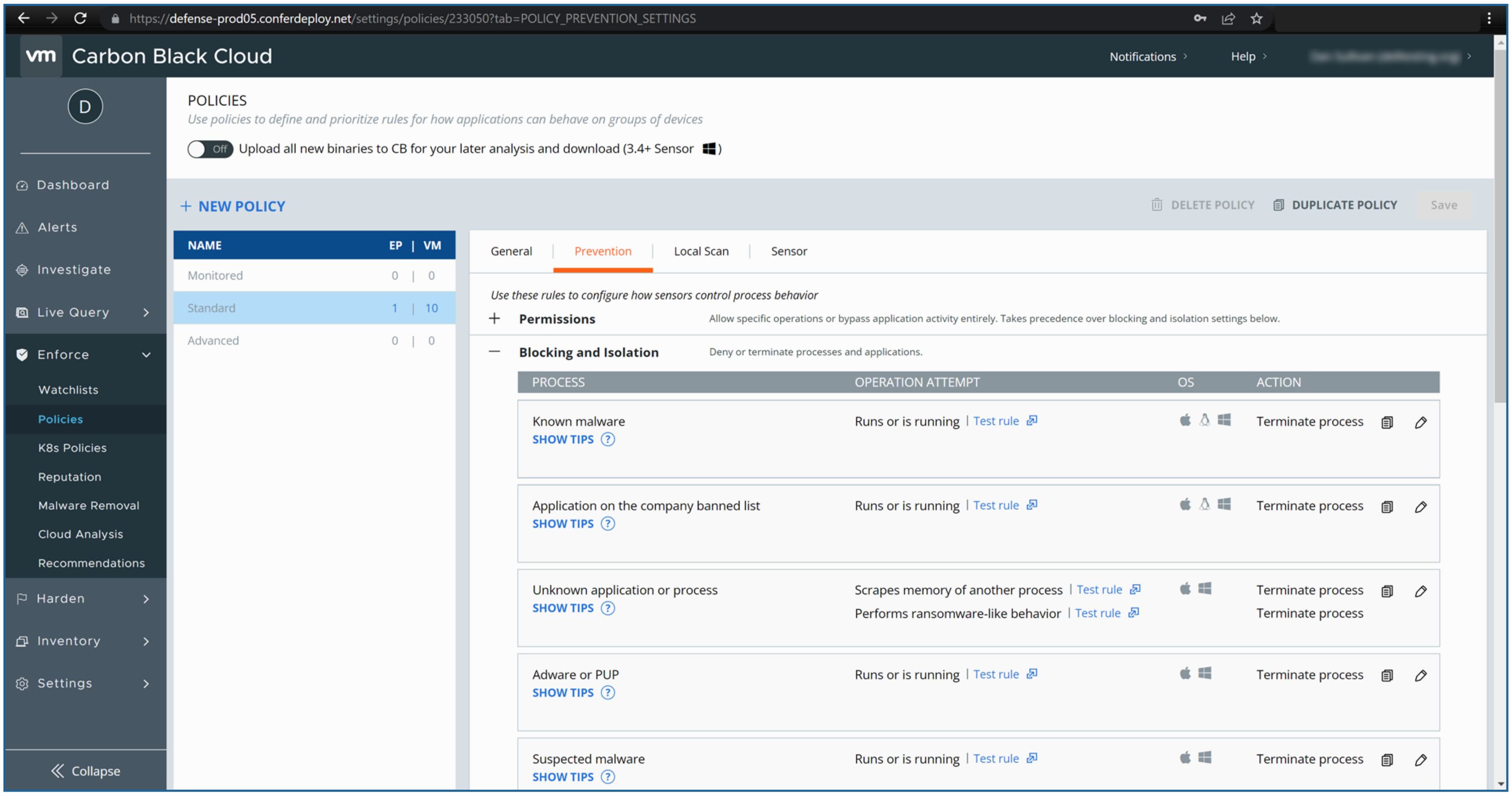
Once we became aware of the vulnerabilities on our systems, Carbon Black provided tools for quick remediation. Carbon Black contains internal tools specific to each OS that enabled us to apply patches to any out-of-date software. We also used the Carbon Black remote shell tool to update configuration files and prevent malware from fully extracting its payload.

User experience features

Carbon Black contains features that facilitate the user experience and make it easier for the humans running the solution to engage and take ownership of their system security.

Security profiles

We found that Carbon Black enables administrators to assign security profiles to specific assets.



https://defense-prod05.conferdeploy.net/settings/policies/233050?tab=POLICY_PREVENTION_SETTINGS

vm Carbon Black Cloud | Notifications › | Help › | [redacted] ›

D

Dashboard
Alerts
Investigate
Live Query ›
Enforce ⌄
- Watchlists
- Policies
- K8s Policies
- Reputation
- Malware Removal
- Cloud Analysis
- Recommendations

Harden ›
Inventory ›
Settings ›
Collapse

POLICIES

Use policies to define and prioritize rules for how applications can behave on groups of devices

Off Upload all new binaries to CB for your later analysis and download (3.4+ Sensor)

+ NEW POLICY | DELETE POLICY | DUPLICATE POLICY | Save

NAME	EP | VM
Monitored	0 | 0
Standard	1 | 10
Advanced	0 | 0

General | Prevention | Local Scan | Sensor

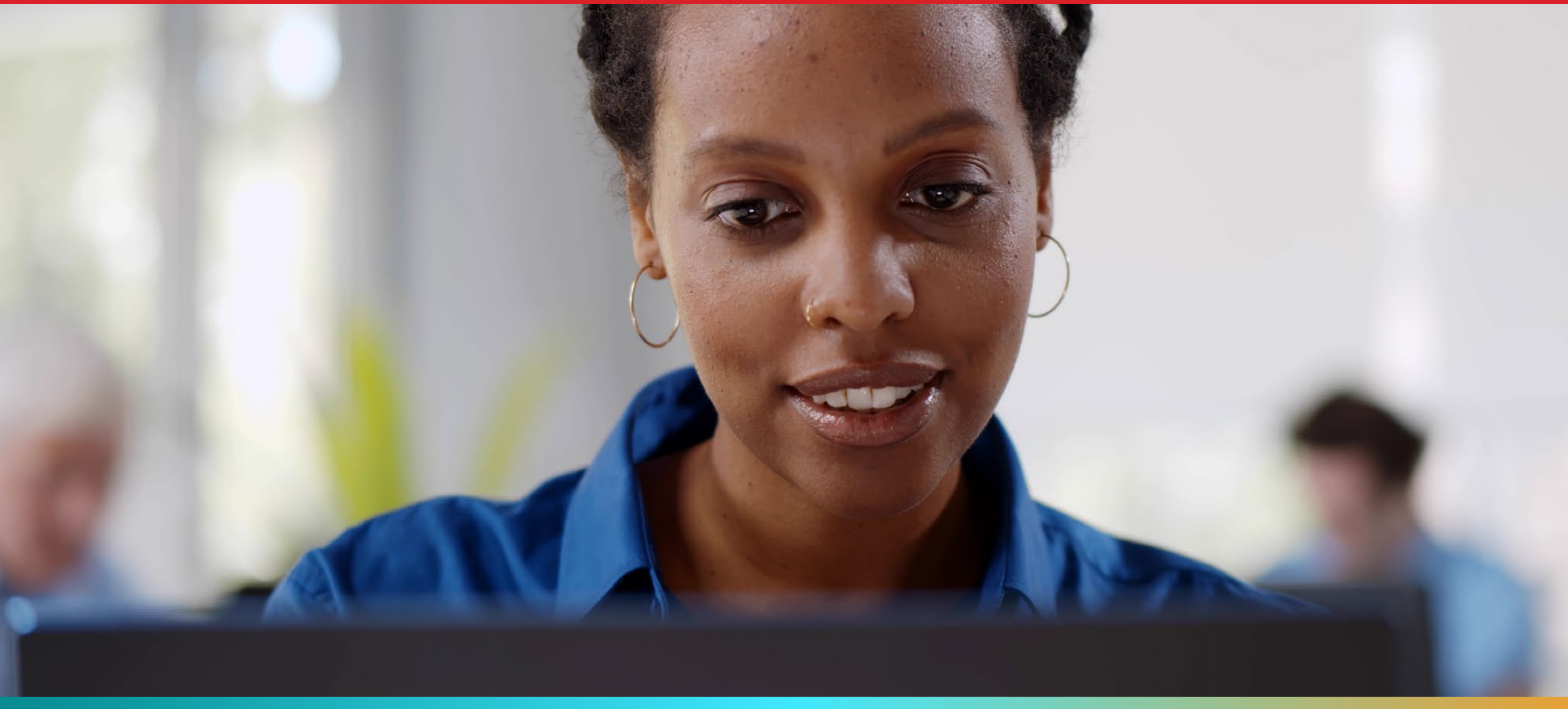
Use these rules to configure how sensors control process behavior

+ **Permissions** Allow specific operations or bypass application activity entirely. Takes precedence over blocking and isolation settings below.

— **Blocking and Isolation** Deny or terminate processes and applications.

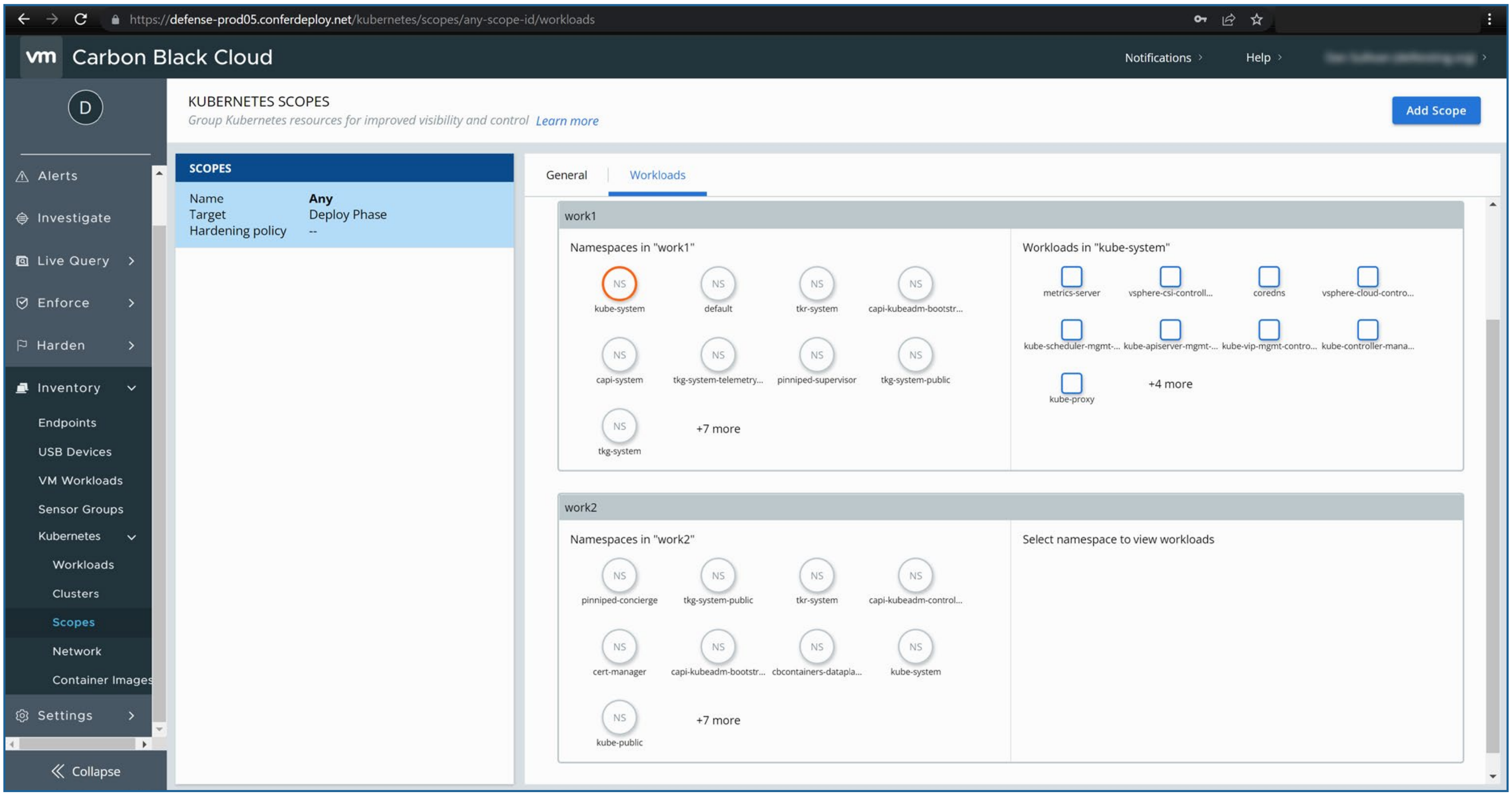
PROCESS	OPERATION ATTEMPT	OS	ACTION
Known malware SHOW TIPS ?	Runs or is running | Test rule		Terminate process
Application on the company banned list SHOW TIPS ?	Runs or is running | Test rule		Terminate process
Unknown application or process SHOW TIPS ?	Scrapes memory of another process | Test rule Performs ransomware-like behavior | Test rule		Terminate process Terminate process
Adware or PUP SHOW TIPS ?	Runs or is running | Test rule		Terminate process
Suspected malware SHOW TIPS ?	Runs or is running | Test rule		Terminate process

Figure 5: Carbon Black security profile UI. Source: Principled Technologies.



Dashboard interface

A clean, well-designed user interface can help your staff to quickly understand the state of your system security at a glance. In our hands-on work with Carbon Black, we found that the dashboard provided a clean view of assets conducive to good user experience.



https://defense-prod05.conferdeploy.net/kubernetes/scopes/any-scope-id/workloads

KUBERNETES SCOPES

Group Kubernetes resources for improved visibility and control *Learn more*

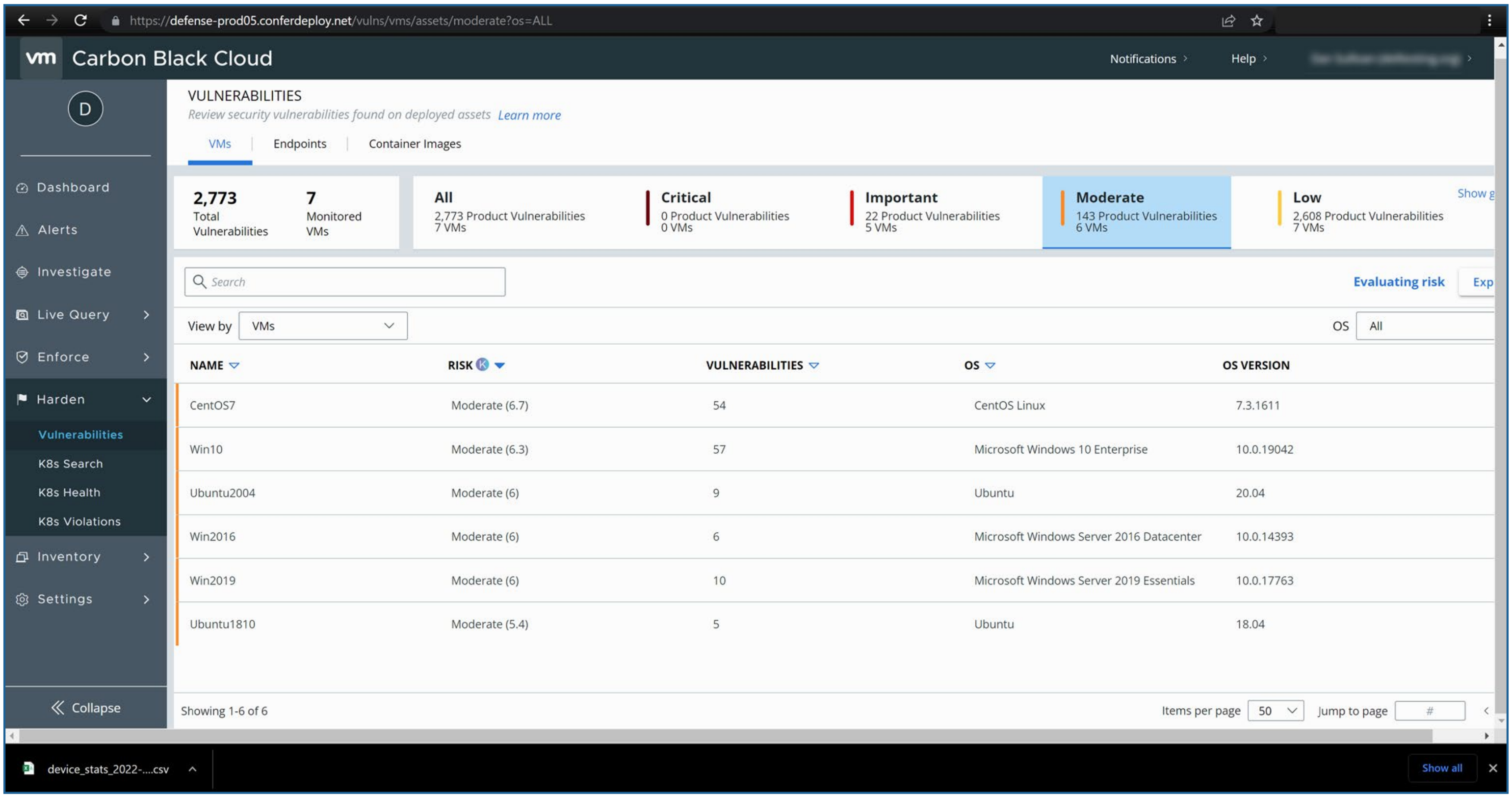
SCOPES	
Name	Any
Target	Deploy Phase
Hardening policy	--

Figure 6: The Kubernetes cluster view of the Carbon Black dashboard. The dashboard also contains views for VMware workloads and cloud instances (not pictured). Source: Principled Technologies.

Reporting the state of your security to executives and managers

Your company's security experts may be deeply familiar with the day-to-day status of your business assets, but executives and other decision makers need to understand where your company security stands at a high level and where it can improve.

We used Carbon Black to generate reports that overviewed the security states of all our assets, a type of reporting that real-world companies might use for busy management personnel who need quick information for daily decision making. Figure 6 shows one example of such a report.



VULNERABILITIES

Review security vulnerabilities found on deployed assets *Learn more*

2,773 Total Vulnerabilities

7 Monitored VMs

All: 2,773 Product Vulnerabilities, 7 VMs

Critical: 0 Product Vulnerabilities, 0 VMs

Important: 22 Product Vulnerabilities, 5 VMs

Moderate: 143 Product Vulnerabilities, 6 VMs

Low: 2,608 Product Vulnerabilities, 7 VMs

View by: VMs

OS: All

NAME	RISK	VULNERABILITIES	OS	OS VERSION
CentOS7	Moderate (6.7)	54	CentOS Linux	7.3.1611
Win10	Moderate (6.3)	57	Microsoft Windows 10 Enterprise	10.0.19042
Ubuntu2004	Moderate (6)	9	Ubuntu	20.04
Win2016	Moderate (6)	6	Microsoft Windows Server 2016 Datacenter	10.0.14393
Win2019	Moderate (6)	10	Microsoft Windows Server 2019 Essentials	10.0.17763
Ubuntu1810	Moderate (5.4)	5	Ubuntu	18.04

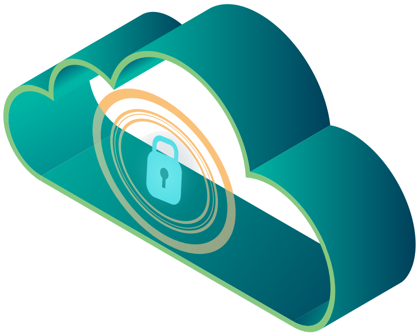
Showing 1-6 of 6

Items per page: 50

Figure 7: Report of assets that Carbon Black labeled moderately at risk. Source: Principled Technologies.

Extending Carbon Black features to hybrid cloud use cases

VMware Carbon Black doesn't just work with private cloud infrastructure—businesses that use a hybrid cloud model can also take advantage of Carbon Black security features. We installed the Carbon Black sensors on our public-cloud-based assets (two Amazon Web Services instances, with one running Amazon Linux 2 and the other running Ubuntu 20.04), and Carbon Black was able to easily scan, detect, and alert us to their vulnerabilities.



Conclusion

From employee devices and laptops to on-premises servers and cloud instances, your enterprise organization may have many assets to keep secure. Instead of relying on several disparate tools to safeguard your company's data, an all-in-one solution that keeps track of all major assets can help IT security staff achieve a better picture of your entire company's IT security health while enabling them to quickly mobilize to neutralize threats, vulnerabilities, and attacks.

In our tests, VMware Carbon Black collated the security status of employee devices, on-premises servers, and cloud instances; scanned these systems for vulnerabilities and malware; and proactively alerted us to the issues it found.

For more information, visit https://www.vmware.com/products/carbon-black-cloud-endpoint.html.

[1] "Amid COVID-19, Global Orgs See 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted," accessed December 20, 2021, https://blogs.vmware.com/security/2020/04/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted.html.

[2] VMware Carbon Black Cloud," accessed October 7, 2021, https://www.vmware.com/products/carbon-black-cloud.html.

[3] VMware, "VMware Carbon Black Cloud Enterprise EDR: Threat Hunting & Incident Response," accessed March 1, 2022, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-enterprise-edr-datasheet.pdf.

[4] Dell Technologies, "Cyber Resilient Security in Dell EMC PowerEdge Servers," accessed February 10, 2022, https://www.delltechnologies.com/en-my/collaterals/unauth/white-papers/products/servers/cyber-resilient-security-with-poweredge-servers.pdf.

[5] "Alert and Report Severity," accessed December 21, 2021, https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-95388BA8-00FA-432C-ABC0-7C3353D19D35.html.

[6] "Risk Evaluation," accessed December 20, 2021, https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-F99243BC-3CD5-4EEE-B9D5-CE31A112BD66.html.

[7] VMware Carbon Black Endpoint," accessed December 20, 2021, https://www.vmware.com/products/carbon-black-cloud-endpoint.html.

Read the science behind this report at https://facts.pt/kptXe2l ▶

Principled Technologies®

Facts matter.®

This project was commissioned by Dell Technologies.