Executive summary

**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

# 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.

## Asset detection in endpoints and cloud instances

For reliable and robust protection, it's paramount that a security solution is able to correctly identify all assets within your environment. In our tests, we were able to use Carbon Black and Carbon Black sensors to detect each of our endpoints (cloud VMs on Amazon Web Services and Kubernetes clusters) and assets running on these endpoints (operating systems, system applications, database applications, and web apps) and list them on the Carbon Black web interface.

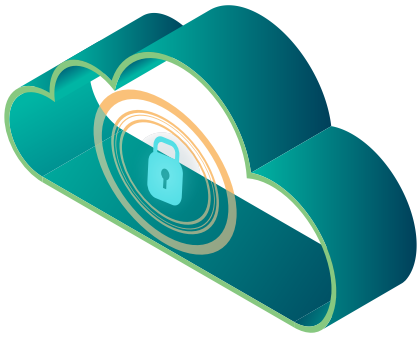
## Vulnerability detection

A good security solution can detect unexpected changes or alert your team to potential security risks that require prompt action. Carbon Black alerted us to vulnerabilities affecting our system, including OS and application vulnerabilities, out-of-date software, and suspicious activity such as misconfigured applications.

Carbon Black also detected malware in real time. We downloaded a suite of malware exploit tools called Metasploit 6.1.27. As soon as we began to install the tool, the Carbon Black sensor detected and prevented the installer from copying exploits and malware to our file systems.

## Other features

Carbon Black also contained features that facilitate user experience, such as a dashboard that provided an all-in-one view of our test VMs, operating systems, and Kubernetes clusters. When Carbon Black detects threats, it displays them on the dashboard as well as sends notifications via email. Carbon Black contained OS-specific tools for patching out-of-date software, and enabled us to generate high-level security reports that may be helpful for getting executives and other non-experts up to speed on important security events.



## Conclusion

Instead of relying on several disparate tools to safeguard your company's data, an all-in-one solution that tracks 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. For more on how Carbon Black can help you achieve security goals, visit https://www.vmware.com/products/carbon-black-cloud-endpoint.html.

**Cyber Resilient Architecture**

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

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

Principled Technologies®

Facts matter.®