VMware Carbon Black Cloud

Endpoint protection that adapts to your business

A cloud native platform delivering best-in-class, next-generation antivirus and endpoint detection and response without compromising system performance.
Adaptive Prevention Delivers Better Protection

The majority of today’s cyberattacks feature advanced tactics such as lateral movement and island hopping that target legitimate tools to inflict damage. These sophisticated hacking methods pose a tremendous risk to targets with decentralized systems protecting high-value assets, including money, intellectual property and state secrets.

VMware Carbon Black Cloud™ thwarts attacks by making it easier to:

- Analyze billions of system events to understand what is normal in your environment
- Prevent attackers from abusing legitimate tools
- Automate your investigation workflow to respond efficiently

All of this is unified into one console and one agent, so that infrastructure and InfoSec teams have a single, shared source of truth to improve security together.

“VMware Carbon Black is essentially our Swiss army knife. We can do a lot of different things with a lot of information. The overall coverage and overall response times were greatly improved from what we had before. For us it was a no brainer.”

CARL ERICKSON, CISO, JOHNSON CONTROLS

---

**CYBERATTACKS MATURE**

6 Trillion
Estimated damages from cybersecurity attacks by 2021

70%
Of attacks featured lateral movement

57X
Predicted increase in ransomware damages from 2015-2021

56%
Of breaches took months or longer to discover

27%
Are confident that antivirus will protect them from ransomware
One Platform for Your Endpoint Security Needs

VMware Carbon Black Cloud consolidates multiple endpoint security capabilities using one agent and console, helping you operate faster and more effectively. As part of VMware’s intrinsic security approach, VMware Carbon Black Cloud spans the system hardening and threat prevention workflow to accelerate responses and defend against a variety of threats.

Endpoint standard – next-generation antivirus and behavioral EDR
Analyze attacker behavior patterns over time to detect and stop never-seen-before attacks, whether they are malware, fileless or living-off-the-land attacks.

Managed detection – managed alert monitoring and triage
Gain 24-hour visibility from our security operations center of expert analysts, who provide validation, context into root cause and automated monthly executive reporting.

Audit and remediation – real-time device assessment and remediation
Easily audit the current system state to track and harden the security posture of all your protected devices.

Enterprise EDR – threat hunting and containment
Proactively hunt for abnormal activity using threat intelligence and customizable detections.