



Dell SafeGuard and Response

VMware Carbon Black Cloud Endpoint Enterprise
An Endpoint Protection Platform featuring

VMware Carbon Black Cloud Endpoint Standard, Audit &
Remediation and Enterprise EDR

	Next Generation AntiVirus (NGAV)	Behavioral Endpoint Detection and Response (EDR)	IT Hygiene	Realtime Endpoint Query (System Audit)	Endpoint Remediation	Enterprise Endpoint Detection and Response (EDR)	Advanced Event Analysis (Threat Hunting)
CB Cloud Endpoint Standard	x	x					
CB Cloud Audit & Remediation			x	x	x		
CB Cloud Enterprise EDR						x	x

CB Cloud Endpoint Standard is an industry-leading next-generation antivirus (NGAV) and behavioral endpoint detection and response (EDR) solution. Delivered through the VMware Carbon Black Cloud, an endpoint protection platform that consolidates endpoint security in the cloud using a single agent and console.

It is certified* to replace standard AV and designed to deliver leading endpoint security with minimal administrative effort. It protects against the full spectrum of modern cyberattacks, including the ability to detect, prevent, and respond to both known malware and unknown non-malware attacks.

CB Cloud Audit & Remediation is a real-time audit and remediation solution that gives security teams faster, easier access to audit, and change the system state of endpoints and containers — Leveraging the same VMware Carbon Black Cloud agent and console to enable IT, administrators, and security teams, to maintain IT hygiene, respond to incidents, and assess vulnerabilities to make quick, confident decisions to improve their security posture. VMware Carbon Black Audit & Remediation closes the gap between security and operations. By allowing administrators and security teams to perform full investigations and take action to remotely remediate endpoints.

CB Cloud Enterprise EDR endpoint detection and response solution delivering continuous visibility for top security operations centers (SOCs) and incident response (IR) teams. Enterprise EDR reduces lengthy investigations from days to minutes, empowers teams to proactively hunt for threats, and gives them the power to respond and remediate in real-time.

Endpoint Protection Platform

The VMware Carbon Black Cloud goes beyond disrupting attacker behavior by giving you the power to analyze endpoint activity, adapt your prevention for emerging threats, and automate manual efforts across your security stack. All from one console and a single lightweight agent to secure your endpoints online and offline.

*<https://www.carbonblack.com/products/solutions/use-case/risk-and-compliance/pcidss/>

Learn more at DellEMC.com/endpointsecurity

Learn and Prevent

The advanced machine learning models analyze complete endpoint data to uncover malicious behavior to stop all types of attacks, online and offline.

Capture and Analyze

Continuously captures activity from every endpoint, analyzing each event stream in context to uncover emerging attacks other solutions miss.

Respond Quickly

Industry-leading detection and response capabilities that reveal threat activity in real-time, so you can respond to any type of attack as soon as it's identified. Visualizes every stage of the attack with easy-to-follow attack chain details to uncover root cause in minutes.

On-Demand Queries

Provides your Security & IT Operations team visibility into the most precise current system state of all endpoints, enabling you to make quick, confident decisions to reduce risk. Query endpoints for the latest threat vectors, indicators of compromise, and indicators of attack.

Immediate Remote Remediation

Closes the gap between security and operations, giving administrators a remote shell directly into endpoints to perform full investigations and remote remediations all from a single cloud-based platform.

Simplified Operational Reporting

Allows admins and security teams to save and re-run queries to automate operational reporting on patch levels, user privileges, disk encryption status, and more to stay on top of your ever-changing environment. The ability to easily create custom queries and return results from across all endpoints in their environment to a single cloud-based console.

Consolidate Your SecOps Stack

Consolidate your security stack by leveraging the only real-time audit and remediation tool built on a cloud-based endpoint security platform.

IT Hygiene

Know what you have, how it is connected, how it is configured across your cloud, endpoints, APIs, device, and user accounts. Vulnerability Management and Patching: Firmware, OS, and Application Level, including auditing of the above.

Continuous Event Capture

Investigations that typically take days or weeks can be completed in just minutes. CB Cloud Enterprise EDR correlates and visualizes comprehensive information about endpoint events, giving security professionals greater visibility into their environments.

USB Device Control

Gain visibility with detection and monitoring of external USB storage devices connected to any Windows endpoint with VMware Carbon Black Endpoint Standard with sensor v3.6.0.1897 or greater. Reduce common threats associated with USB storage devices by blocking read, write, and execute operations. Inform and educate internal users and administrators with automated alerts whenever a block occurs. Allow approved USB devices by the manufacturer or serial number.

Use Cases

Next Generation AntiVirus | Behavior Endpoint Detection and Response | Respond to Incidents | Maintain IT Hygiene
Track Drift | Assess Vulnerabilities in Real-Time | Prove & Maintain Compliance

Contact your dedicated Dell Endpoint Security Specialist today at, endpointsecurity@dell.com,
about the SafeGuard and Response products that can help improve your security posture.