

# Dell SafeGuard and Response

## VMware Carbon Black Cloud Endpoint Advanced

An Endpoint Protection Platform featuring VMware Carbon Black Cloud Endpoint Standard and VMware Carbon Black Cloud Audit & Remediation™

	Next Generation AntiVirus (NGAV)	Behavioral Endpoint Detection and Response (EDR)	IT Hygiene	Realtime Endpoint Query (System Audit)	Endpoint Remediation
CB Cloud Endpoint Standard	X	X			
CB Cloud Audit & Remediation			X	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 VMware Carbon Black Cloud 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.

### 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.

### 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.

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

## **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 reveal threat activity in real-time, so you can respond to just about any type of attack as soon as it's identified. Every stage of the attack is visualized with easy-to-follow attack chain details to uncover the root cause in minutes.

## **On-Demand Queries**

Provide 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 and the ability to query endpoints for the latest threat vectors, indicators of compromise, and indicators of attack.

## **Dell SafeBIOS Integration**

The combined power of VMware Carbon Black Audit and Remediation and Dell SafeBIOS provides state of the art security both above and below the OS and enables telemetry from the off-host BIOS verification status on the Dell Commercial PC offering. The integrated solution allows security and IT teams to automate reporting of the verification status so they can take action to remediate compromises resulting from BIOS tampering. This partnership reinforces Dell as the industry's most secure commercial PC provider.

## **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, 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 across all endpoints in their environment to a single cloud-based console.

## **Consolidate SecOps Stack**

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

## **IT Hygiene**

Helps IT Admins and SecOps understand what they have, how it is connected and configured across cloud, endpoints, APIs, devices, and user accounts. This feature also provides vulnerability management, patching at the firmware, OS, and application levels, including auditing features.

## **Vulnerability Management**

Leverages a proven data science approach to vulnerability risk scoring to empower security teams to focus on patching or remediating the most critical vulnerabilities in their environment. Provides teams with direct access to vulnerability intelligence and context so they can ensure vulnerabilities that pose the highest security risk are prioritized for remediation over less critical vulnerabilities.

## **Use Cases**

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

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