

# Carbon Black.

## CB LIVEOPS ON THE PSC

### Real-Time Endpoint Query & Remediation

Even the most effective security teams are often forced to play catch up during emergency situations due to limited time and resources to perform regular, proactive analysis and evaluate potential risks.

Any delays during the investigation prolongs downtime and leaves the organization open to increased risk. Once the scope of an attack is understood, dispersed processes and tool sets can cause bottlenecks that delay the remediation of problematic endpoints.

CB LiveOps is a real-time query and remediation solution that gives teams faster, easier access to audit and change the system state of endpoints across their organization.

By providing administrators with real-time query capabilities from a cloud-native endpoint protection platform, CB LiveOps enables teams to make quick, confident decisions to improve their security posture. CB LiveOps closes the gap between security and operations, allowing administrators to perform full investigations and take action to remotely remediate endpoints all from a single solution.

**“CB LiveOps enables our incident response team to acquire key forensic artifacts that normally would require additional collection and offline parsing. It allows our teams to scale out our response from one to hundreds of systems.”**

**— TIM STILLER, SENIOR INCIDENT RESPONSE CONSULTANT, RAPID7**

### USE CASES

- Maintain IT Hygiene & Track Drift
- Assess Vulnerabilities in Real Time
- Prove & Maintain Compliance
- Confidently Respond to Incidents

### BENEFITS

- Execute a broad range of operational activities quickly and confidently
- Establish proactive IT hygiene to prevent attacks
- Build consistency into operational reporting and auditing processes
- Remove barriers between security analysis and IT operations
- Extend existing investigation and remediation capabilities
- Replace ad hoc scripts and manual tasks with a structured security platform

### CB LIVEOPS AND THE PSC

- Leverages the same agent and console as NGAV, EDR and threat hunting platform
- Cloud-based storage of all query results
- Easy access to unified data across Security and IT teams.



# Carbon Black.

## Key Capabilities

### Single Agent, Cloud Platform

CB LiveOps is built on the PSC, a cloud-native endpoint protection platform that offers converged prevention, detection, and response with additional services that can be activated as you need them, using the same converged agent, without any additional deployment or infrastructure.

### On-Demand Queries

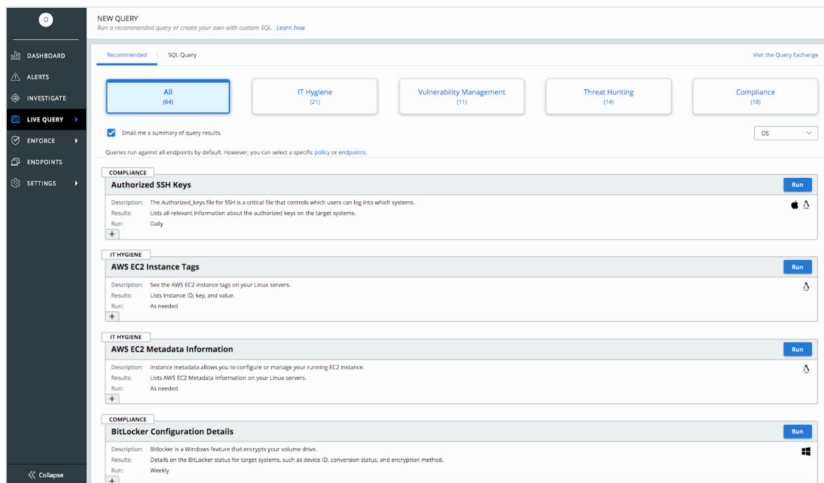
CB LiveOps gives your Security & IT Operations team visibility into even the most precise about the current system state of all endpoints, enabling you to make quick, confident decisions to reduce risk.

### Immediate Remote Remediation

CB LiveOps 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

CB LiveOps allows you 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.



CB LiveOps gives administrators across the SecOps team the ability to easily create custom queries and return results from across all endpoints in their environment to a single cloud-based console.

## ABOUT CARBON BLACK

Carbon Black (NASDAQ: CBLK) is a leader in cloud endpoint protection dedicated to keeping the world safe from cyberattacks. The CB Predictive Security Cloud® (PSC) consolidates endpoint protection and IT operations into an extensible cloud platform that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks. More than 5,300 global customers, including 35 of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use Carbon Black's technology in more than 500 breach investigations per year.

Carbon Black and CB Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and/or other jurisdictions.

## FEATURES

- Pre-Built Recommended Queries
- Easy query builder
- SQL query (open text field)
- Copy & Re-run Queries
- Save and favorite queries
- Email notifications
- Filter and group results
- Data export
- Secure shell for remote remediation
- Two-way API

## PLATFORMS

- Windows 7 and above
- Windows Server 2008 R2 and above
- MacOS 10.10 and above
- Red Hat 6 and above
- CentOS 6 and above
- Ubuntu 16.04 and above
- SUSE 12 and above
- OpenSUSE 15 & 42
- Amazon Linux 2

## REQUEST A DEMO

**Contact us today  
to schedule a  
demonstration.**

[CONTACT@CARBONBLACK.COM](mailto:CONTACT@CARBONBLACK.COM)

617.393.7400

**Carbon Black.**

1100 Winter Street  
Waltham, MA 02451 USA  
P 617.393.7400 F 617.393.7499  
[www.CarbonBlack.com](http://www.CarbonBlack.com)