Carbon Black.

Cb LiveOps on the PSC

Real-Time Endpoint Query & Remediation

Any delays during an 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.

Even the most effective security teams are often forced to play catch-up during emergency situations because there is limited time to perform regular analysis and evaluate potential risks.

Cb LiveOps is a real-time security operations solution that enables organizations to ask questions of all endpoints and take action to instantly remediate issues.

By allowing administrators to dive a level deeper into the current state of all endpoints, Cb LiveOps empowers Security and IT Operations teams to act confidently in the moment to prevent breaches. Cb LiveOps saves Security & IT teams hours of manual work, allowing administrators to perform full investigations and take action to remotely remediate endpoints all from a single solution.

Cb LiveOps is delivered through the Cb Predictive Security Cloud, a next-generation endpoint protection platform that consolidates security in the cloud using a single agent, console and dataset.

"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

- On-demand vulnerability assessment
- Real-time investigation of any data
- Simplified compliance auditing
- Remote remediation via the cloud
- Easy asset management and IT hygiene

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 Cb Defense's 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 next-generation protection platform that offers consolidated prevention, detection and response in the cloud using a single agent, console, and dataset.

On-Demand Queries

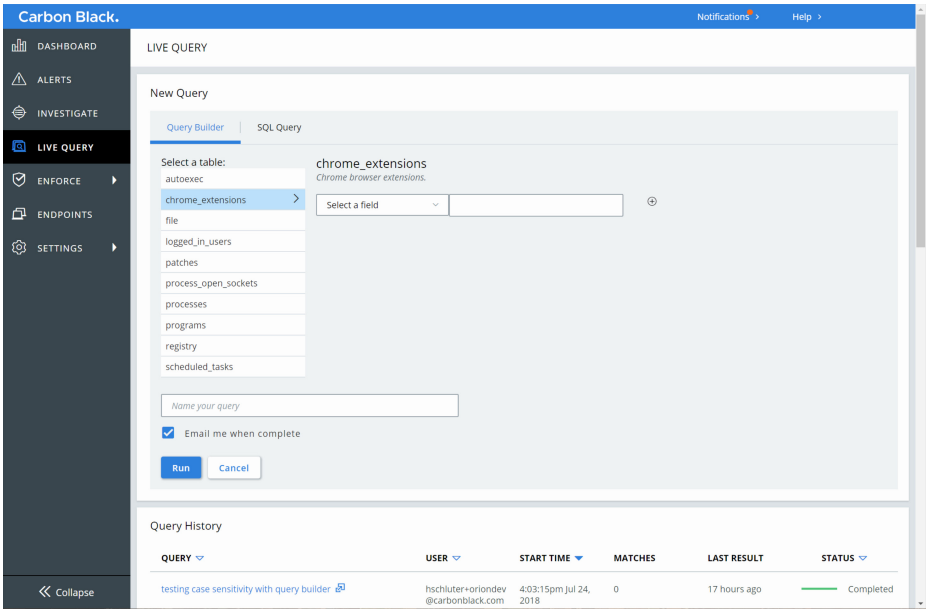
Cb LiveOps gives your Security & IT Operations team visibility into even the most precise details about the current state of all endpoints, enabling you to make quick, confident decisions to reduce risk..

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 leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,300 global customers, including 35 of the Fortune 100, trust Carbon Black to keep their organizations safe.

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

Features

- Easy query builder
- SQL query (open text field)
- Save and favorite queries
- Email notifications
- Filter and group results
- Data export
- Secure shell for remote remediation

Platforms

Cb LiveOps is an add-on to Cb Defense, which supports:

- Windows 7
- Windows 8.1
- Windows 10
- Windows Server 2012

REQUEST A DEMO

Contact us today to schedule a demonstration.

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