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.

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

"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
- Remote remediation via the cloud
- Easy asset management and IT hygiene

Benefits

- Execute a broad range of operational activities quickly & 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

- Next-gen endpoint security delivered from the cloud
- Single consolidated agent, single unified console
- The only platform to combine on-demand query with advanced prevention, detection and response

Carbon Black.

Key Capabilities

Single Agent, Cloud Platform

Cb LiveOps is built on the PSC, a powerful security 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

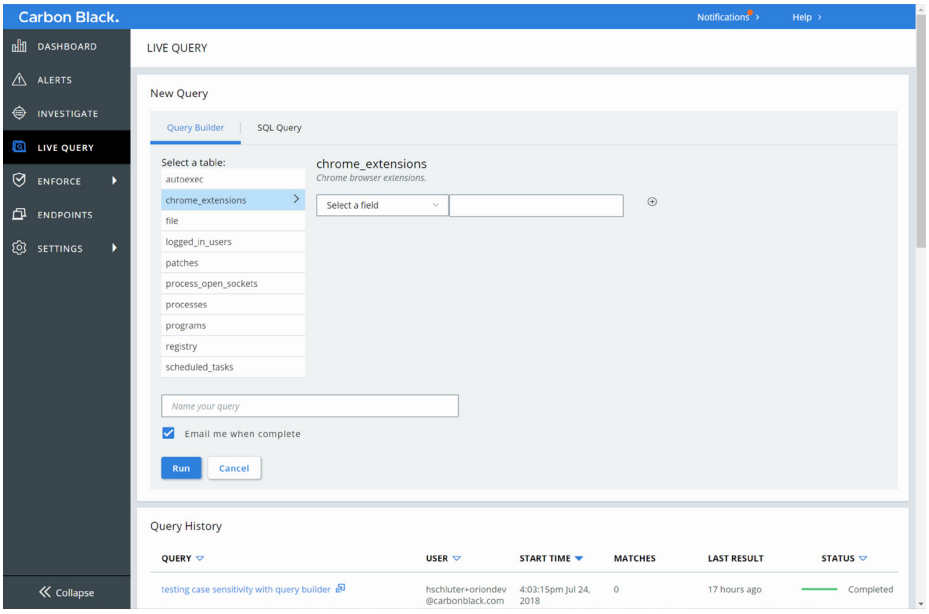
Cb LiveOps gives the entire SecOps team visibility into even the most precise details about the current state of all endpoints, enabling you to make quick, confident decisions to reduce risk.

Immediate Remote Remediation

Cb LiveOps closes the gap between security and operations, allowing administrators to 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 schedule queries to automate operational reporting on patch levels, user privileges, disk encryption status and more to stay on top of their 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.

Features

- Easy Query Builder
- SQL Query (open field)
- Save & Favorite Queries
- Email Notifications
- Filter & Group Results
- Data Export
- Secure Shell for Remote Remediation

Platforms

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

- Windows 8.1
- Windows 10
- Windows Server 2012

About Carbon Black

Carbon Black is a leading provider of next-generation endpoint security. Carbon Black serves more than 3,700 customers globally, including 33 of the Fortune 100. 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). Leveraging its newly introduced big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus. For more information, please visit www.carbonblack.com or follow us on Twitter at @CarbonBlack_Inc.

Carbon Black.

2018 © Carbon Black and Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and other jurisdictions. All other trademarks and registered trademarks are the property of their respective owners.