Carbon Black.
by Broadcom

PRODUCT BRIEF

KEY FEATURES

- Prebuilt recommended queries
- SQL query (open text field)
- Query scheduler
- Copy and re-run queries
- Save and favorite queries
- Email notifications
- Filter and group results
- Data export
- Secure shell for remote remediation
- Two-way API

BENEFITS

- Leverage 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
- 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 impromptu scripts and manual tasks with a structured security platform
- Automate operational reporting with scheduled queries

Carbon Black® Live Query

Real-Time Device Assessment and Remediation

Overview

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.

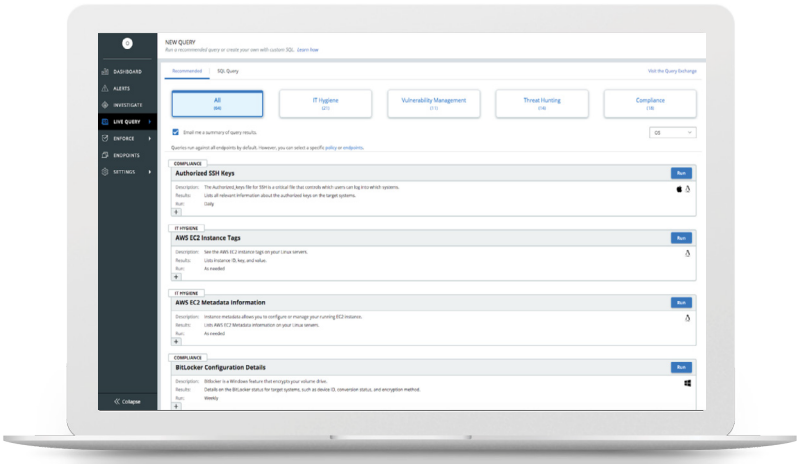
Any delays during the investigation prolong downtime and leave the organization open to increased risk. Once the scope of an attack is understood, dispersed processes and toolsets can cause bottlenecks that delay the remediation of problematic endpoints.

Carbon Black® Live Query is a real-time assessment 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, Live Query enables teams to make quick, confident decisions to harden systems and improve security posture. Live Query 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.

A Network Support Services Manager's experience with Live Query is noted in the Metropolitan Educational System 2024 Carbon Black TEI Report, "In the past, the handling of security events was reaching out to the help desk, requisitioning a technician to get the device, investigating the device, finding out what's wrong with it, and then remediation. So there were a lot of hands in that process. Now, we've been able to confidently remediate remotely without even touching the device."

Figure 1: Create Custom Queries and Return Results from across All Endpoints a Single Cloud-Based Console



APPLICATIONS

- Maintain IT hygiene and track drift
- Assess vulnerabilities in real time
- Prove and maintain compliance
- Confidently respond to incidents
- Audit and protect production workloads

PLATFORMS

- Windows 7 and above
- Windows Server 2008 R2 and above
- MacOS 10.10 and above
- RedHat 6 and above
- CentOS 6 and above
- Ubuntu 16.04 and above
- SUSE 12 and above
- OpenS USE 15 and 42
- Amazon Linux 2

Key Capabilities

Single Agent, Cloud Platform

Live Query is built on the Carbon Black Cloud, 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

Live Query gives Security and IT Operations teams visibility into even the most precise details about the current system state of all endpoints, enabling you to make quick, confident decisions to reduce risk.

Immediate Remote Remediation

Live Query 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

Live Query allows you to schedule daily, weekly, or monthly queries to automate operational reporting on patch levels, user privileges, disk encryption status and more to track and maintain the desired state of your ever-changing environment.

For additional information, visit:
broadcom.com/products/carbon-black/threat-prevention/endpoint-protection.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

CB-LiveQuery-PB100 March 14, 2025