BLUVECTOR® | Carbon Black.

BluVector and Carbon Black

Solution Guide

BluVector® Cortex™ is an AI-driven sense and response network security platform designed to accurately and efficiently detect, analyze and contain sophisticated threats including fileless malware, zero-day malware, and ransomware in real time. When deployed with Carbon Black, the solution comes together to provide end-to-end and immediate protection from advanced malware, while driving significant efficiency improvements throughout the security organization.

Comprehensive Breach Prevention from Network to Endpoint

Challenge

The number of threats that can impact an organization is far greater than the number to which most analysts can manually respond. This problem is made worse by the sheer volume of alerts generated by existing tools and the difficulty inherent in prioritizing these alerts. By the time a threat is detected, investigated, and manually remediated, the dwell time has already been significant, increasing the risk of damage.

For example, ransomware can begin to harm a compromised endpoint almost immediately. Even if detected within seconds of the initial installation, the malware is likely to have already encrypted hundreds or even thousands of critical business files. Seeing and responding to the attack before the compromise is crucial to preventing impact.

Solution

BluVector Cortex's AI-driven detection engines identify malicious files entering or traversing the network in real time, sending alerts identifying the files to all Carbon Black-protected endpoints. Carbon Black can then block high-priority threats at the endpoint, before damage is done. For potential zero-day threats, BluVector can prompt Carbon Black to send the alert to an analyst for immediate response. BluVector can also send lower-priority alerts to Carbon Black's event log for later investigation.

In the case of ransomware, if a campaign were to target an environment protected by this combined solution, the threat would be detected on the network and prevented from ever running on the endpoint. This ensures comprehensive breach prevention, automating protection from advanced threats from detection to response.

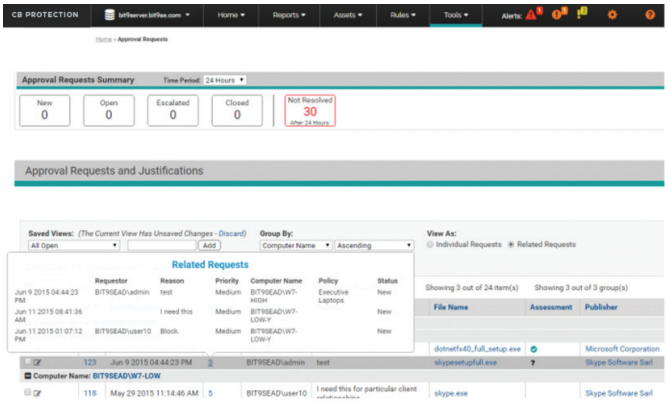
Benefits

- **Integrated Detection and Defense**
  When BluVector detects file-based threats, the details of these files are communicated to Cb Protection and distributed out to all protected endpoints. This allows for the endpoints to block or contain the identified malicious files.
- **Accelerated Investigation and Response**
  Upon detecting suspicious file-based events, BluVector communicates these events to Cb Response. This enables an automated or analyst-led hunt for the identified files on all protected endpoints, whether within the corporate network or on remote systems.
- **Comprehensive Network and Endpoint Threat View**
  By providing a full view of an event from the network to the endpoint, BluVector and Carbon Black help analysts to quickly understand, respond to and remediate all types of security alerts.

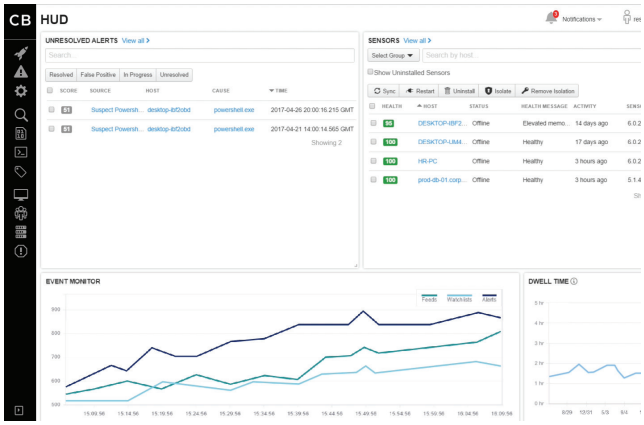
How It Works

BluVector and Carbon Black have worked together to integrate their solutions to enable a unified security fabric. Malicious files detected by BluVector Cortex are sent to Carbon Black Protection and/or Response to enable blocking, investigation and remediation:

- Provides a simple integration setup between BluVector Cortex and Cb Protection, Cb Response, or both.
- The BluVector Cortex administrator creates policies regarding which events from BluVector Cortex should be sent to Carbon Black for further action.
- Based on the policies set, BluVector Cortex sends all relevant adjudicated files directly to the integrated Carbon Black product(s).
- Users can create Carbon Black protection profiles for all events generated by BluVector Cortex.
- Profiles include all standard enforcement levels:
  - High – Block
  - Medium – Prompt
  - Low – Monitor
- Enables Carbon Black to initiate alerting, investigation and blocking of the detected file, based on the protection profiles.



Carbon Black Protection Dashboard



Carbon Black Response Dashboard

Learn More

About Carbon Black

Carbon Black (NASDAQ:CBLK) 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 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.

About BluVector

BluVector is revolutionizing network security with state-of-the-art AI, sensing and responding to the world's most sophisticated threats in real time. With the unmatched advantage of 8 years of work with the US Intel Community and their threat data, only BluVector has the proven ability to protect against emerging threats on average 13 months in advance. Stop waiting for breaches to happen. Get ahead of the threat.