Partner Data Sheet

CARBON BLACK
ARM YOUR ENDPOINTS

Industry

Endpoint Security and Response

Website

www.carbonblack.com

Company Overview

Carbon Black leads a new era of endpoint security by enabling organizations to disrupt advanced attacks, deploy the best prevention strategies for their business

Product Overview

The Carbon Black Security Platform is the first next-generation endpoint security solution to disrupt attacks, protect every endpoint and automate regulatory compliance controls.

Solution Highlights

With Carbon Black, you can align your cyber-security initiatives with the latest guidance and frameworks from the FFIEC, PCI and NIST, helping you ensure a secure and compliant operating environment.

ANOMALI

Next Generation Security Solutions

The threat landscape is continually expanding and organizations are under continuous attack and overwhelmed with alerts. Thousands of incidents occur each day and security professionals only have time to deal with dozens. This creates operational chaos. Security teams need next-generation security solutions to help them respond faster, defend proactively and invest smarter.

Just-in-Time Intelligence

Anomali's Carbon Black content adds real-time threat intelligence to event data in your Carbon Black deployment. Threat intelligence is continuously gathered, categorized, risk ranked (for severity and confidence) in Anomali's ThreatStream platform and then delivered in real-time to your Carbon Black instance for monitoring and detection of security threats in your enterprise infrastructure for the security and threat intelligence teams to quickly see high priority threats to your business. The intelligence is based on common industry-accepted Indicators of Compromise (IOC) such as source and destination IP addresses and domains, but is enriched with factors such as risk score to add context and relevance to the delivered information.

Benefits of the Joint Offering

The Anomali Carbon Black integration is quick and easy. A small piece of software, Anomali Link, automatically delivers threat intelligence with the relevant context on a regularly scheduled basis to be picked up by the Carbon Black either in the cloud or at the appliance.

IP's, Domains, and MD5 Hashes

Carbon Black then pushes these indicators to the endpoints and looks for matches to the IPs, domains, or MD5 hashes provided by the ThreatStream platform. Bit 9 is then able to take action on these detections by automating next steps, such as blocking the connection.

Extend Functionality with the ThreatStream Platform

Our integrated External Lookup also enables your analysts to have access to more information about the Alert than ever before by taking them to the ThreatStream details page showing every related aspect and impact of the Indicator of Compromise in question.

Benefits of Anomali

- Easy-to-use interface to view threat information received through STIX/TAXII feeds.
- Analyze and correlate data into actionable information: SIEM rules, reports, and dashboards.
- Pinpoint IOCs - quickly search for a specific indicator, search for an indicator type over a time range, and drill-down into details.
- Eliminate unnecessary, duplicative and irrelevant indicators - before they enter your infrastructure.
- Identify and prioritize the events that matter now - without DIY scripting.
- Machine-to-Machine learning algorithms scale to accommodate thousands of IOCs per minute across your environment.

Benefits of Carbon Black

- Continuous, always on, never sleeps, because you can't know what's bad ahead of time.
- Collect the right data, based on our offensive security expertise.
- Stream all data to an aggregated "system-of-record" for a single source of truth. Manage as a key IT asset.
- Retain a persistent history of attackers' every action, the root cause of their attacks, and patterns of behavior.
- Non-intrusive. Never impact endpoint or user.
- Visibility. Know what's happening on every endpoint.
- Scope an incident in minutes.
- Historical traceability for investigations.
- Apply new detection rules retrospectively.

Seamless and Automated

Anomali Carbon Black integration via the cloud or appliance provide seamless, automated integration of indicator data to deliver real-time threat intelligence to your Carbon Black instance so you can start using the threat feeds in meaningful ways more efficiently and more effectively than ever before.

About Anomali

Anomali delivers earlier detection and identification of adversaries in your organizations network by making it possible to correlate tens of millions of threat indicators against your real time network activity logs and up to a year or more of forensic log data. Anomali's approach enables detection at every point along the kill chain, making it possible to mitigate threats before material damage to your organization has occurred.

About Carbon Black

Carbon Black leads a new era of endpoint security by enabling organizations to disrupt advanced attacks, deploy the best prevention strategies for their business, and leverage the expertise of 10,000 professionals to shift the balance of power back to security teams. Only Carbon Black continuously records and centrally retains all endpoint activity, making it easy to track an attacker's every action, instantly scope every incident, unravel entire attacks and determine root causes. Carbon Black also offers a range of prevention options so organizations can match their endpoint defense to their business needs. Carbon Black has been named #1 in endpoint protection, incident response, and market share. Forward-thinking companies choose Carbon Black to arm their endpoints, enabling security teams to:

Disrupt. Defend. Unite

For more information contact Anomali sales at info@anomali.com

ANOMALI

808 Winslow Street, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com