SOLUTION BRIEF

VMware Carbon Black XDR™

Strengthen lateral security and unify security tools to see more and stop more

USE CASES

- Triage cyberattacks across multiple components
- Investigate and respond faster
- Threat hunt proactively
- Spot ransomware faster

BENEFITS

- Visibility across endpoints, networks, workloads, and users
- Effective threat hunting
- Reduced mean time to detect (MTTD) and mean time to respond (MTTR)
- Open scalable ecosystem

RESOURCES

- VMware Carbon Black XDR
- TechZone Product Path
- Forrester Whitepaper: The XDR Paradigm Shift
- XDR Industry Guide
- VMware Contexa

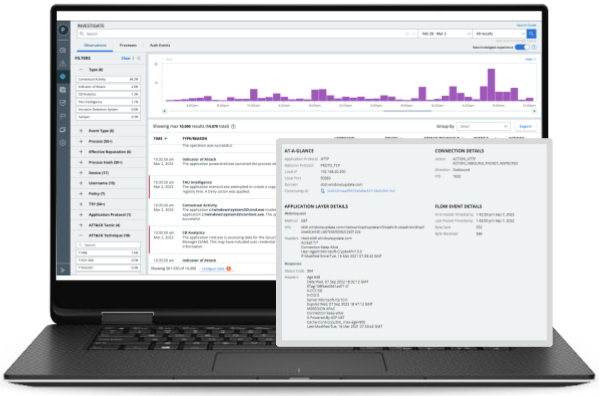
Cyberattacks are proliferating rapidly and growing in scope as adversaries move laterally across the network and traverse diverse environments. As the Security Operations Center (SOC) works to deal with the increasing threat, they can find themselves overwhelmed by an unacceptably high level of false positives, overworked, and let down by legacy detection and prevention controls. Improving the SOC analyst experience comes down to modernizing tools and processes closing visibility gaps, and removing friction from the detection, incident investigation, and response workflow.

VMware Carbon Black XDR shifts the balance of power away from adversaries and back to security teams. As the evolution of Carbon Black Enterprise EDR, Carbon Black XDR delivers on modernizing the SOC by enabling rapid and accurate detection, visualization and analysis of endpoint, network, workload, and user data in context.

Powered by VMware Contexa™, Carbon Black XDR surfaces new results by preserving and extending the endpoint and network contexts during analysis and display. Carbon Black XDR telemetry is analyzed in the VMware Contexa™ threat intelligence cloud, combining billions of security events. This gives you authoritative context across endpoints, workloads, users, and networks.

Carbon Black XDR requires no hardware-based network taps and deploys with no changes to infrastructure. You can now:

- Transform a fleet of endpoints and workload systems into a distributed network sensor
- Deliver pervasive visibility across endpoints, networks, workloads, and users in an open scalable ecosystem
- Make it harder for attackers to hide



Key Capabilities

Carbon Black XDR optimizes threat detection and response and reduces alert fatigue by leveraging rich telemetry and deeper integration across unified security tools.

Network connection visibility with Intrusion Detection System (IDS) Observations

Visualize and analyze network data in context using the Carbon Black Cloud. The XDR network telemetry includes continuous capture and analysis of network fingerprints, flow, and TLS data, and applications-protocol data.

User-centric event visibility

Identity intelligence provides additional context for user-centric event visibility with network telemetry that is indicative of malicious activity, such as various forms of account misuse, anomalous authentication behavior, and insider threats.

Effective threat hunting

With extended detection and response capabilities, Carbon Black XDR surfaces new results by preserving and extending the endpoint and network contexts during analysis and display. Proactively threat hunt for abnormal network and identity activity using threat intelligence and customizable queries.

Reduce dwell time with MITRE ATT&CK automatic tagging

Automatic tagging of endpoint and network related events to the MITRE ATT&CK Tactics, Techniques, and Procedures (TTP) framework exposes the root cause and reduces dwell time. Visibility into network connections and IDS observations spanning your entire organization - including hybrid work environments - alongside automated TTP tagging gives analysts the advantage when responding to the latest attacks.

Detect and respond faster

Detect and respond faster to modern attacks by leveraging XDR capabilities with endpoint prevention, EDR, network, vulnerability assessment, and CIS Benchmarking all delivered from the same lightweight agent and managed from the same console.

Open scalable ecosystem

Easy integration with your preferred tools. The typical SOC relies on proven tools such as SIEM and SOAR and leverages other key prevention controls. Carbon Black XDR delivers out-of-the-box integrations with the industry leading vendors across domains. Gain value from our XDR Alliance partnership, which shares our commitment to an inclusive and collaborative XDR framework and architecture.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com