VMware Carbon Black XDR™

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

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

INVESTIGATE				
Q, 26937			0 × 40	29-Mr2 v Alixouto v
Generation Process	Autom			Ant pointer from a
PATIRS Crow i	¢ _ ()			
- Tate #	1			
DemolulAters H2				
Indexes of Array 240	1.1		_	
GANNO UR				
Myrneligene U.S.		Aller Aller Aller	the the title the title	Tollan Aldan Balan D.S
Intruston Delevitor Springer. Call		Adam Biller Utilan	Aller Aller Dilyr Aller	solar solar solar U.S.
Tanpar 6.0				
+ Event Type IX	Showing	(mai Note multi (Note tata) 🛞		firstp by Inst V
+ Process DR-C	TIME -			
+ Affective Reputation (C)		The operation and inclusion.	AT A GLANCE	CONNECTION DETAILS
	1010.00	Indicator of Attack	Application Protocol 18778	tation affide affid
+ Process Roah (2010)	Mar 3, 3	13 The application power shell one (auxiliar) drap resonant		ACTORUMBOLAGUARMETURAPECTED
+ Denice (TT)			Lood (* 110,108,40,300	PD 101
-1 Unersame 210	1015.50	un THU Intelligence	Lood Port S089 Bonam dbdrwedowsgatata.com	
	Mar 3, 3	121 The application maniful area attempted to create a copy registry from A Dany action and applied.	Conversity 0 Conversity Conversit	
+ Putky (5		offend over a conduction and dilater.		
+ TIP-58+1	19.95.58	Conserval Activity The application characteristic application as involve applications characteristic approximation and as a track the application second of the second sec	APPLICATION LAYER DETAILS	FLOW EVENT DETAILS
+ Application Produced CD	Mar 3, 3			Internation Treasure 14239-04-3401-8281
			MARING GET	Like Packet Trimetorip 1.4880 ph 34p T.8083
+ ATTACKTarde (4)	12,25,26	un chambrin	17. etid advisora, pilata concinatioari landi potaral (Intel/chromehrlmithall ove00432, 00755572832207238	Apertant 202
 AFTBER Sochnique (19) 	1938-50 Mar (,)			systematic IN
0, Search		Manager (SAM), This may have included user-oridential information		
1148 1.4			User-Apert Microsoft Crystalin (1-3) Printed Party Trans 1-1 Microsoft (1-3)	
THEN 444 444	10.555	un indicator of Amach	P Madifed Smartun, 16 Mar 2021 07 33-02 GHT Response	
T100001 0.0	Stealing 5	ELSSofTRam output tata	Todate and a set	
12.20			Institute Markiel Institute Ins	

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

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

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 Copyright © 2023 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMware Carbon Black XDR Solution Birls 3/23