TAG CYBER

ANALYST REPORT: EDR AND CDR ARE DIFFERENT. HERE'S HOW.

TAG CYBER ANALYST TEAM
SUPERVISED BY
DR. EDWARD AMOROSO

sysdig

TAGCYBER

ANALYST REPORT: EDR AND CDR ARE DIFFERENT. HERE'S HOW.

TAG CYBER ANALYST TEAM
SUPERVISED BY DR. EDWARD AMOROSO

This report proposes that endpoint detection and response (EDR) is a fundamentally different discipline than the various protection methods being increasingly referred to as cloud detection and response (CDR). The goal here is to help buyers differentiate between the marketing messages coming from commercial cybersecurity vendors.

INTRODUCTION

The cybersecurity industry uses many different acronyms, such as SIEM, SOAR, CWPP, CDR, SOC, CIEM, CSPM, DSPM, SSPM, CNAPP, IAM, IDP and IGA, most of which were created to help differentiate between the various commercial products available for enterprise buyers.

The acronym EDR, which stands for endpoint detection and response, is used to designate modern endpoint security solutions which evolved from early antivirus and endpoint protection software. EDR generally references commercial products that provide continuous monitoring and malware protection for endpoints, often using behavior analysis and machine learning.

A new term is emerging, CDR, which stands for cloud detection and response. The term helps characterize products that are designed to modernize security operations and threat detection and response capabilities for cloud environments. Such environments include identities, service interactions, containerized workloads and virtualized workloads. This new category is prompted by the obvious shift of enterprises to cloud services and infrastructure.

In this article, we explain the differences between EDR and CDR. Our goal is to support the enterprise buyer who might be led by vendors to believe the two capabilities are the same. While it is fine for a commercial vendor to include both in their roster, EDR and CDR represent different technologies.

WHAT IS ENDPOINT DETECTION AND RESPONSE?

Because the cybersecurity industry has not standardized any category of solution, acronyms will reference whatever a given vendor chooses to include. That said, an EDR solution typically includes the following set of capabilities to protect endpoints such as Windows PCs:

- *Activity Monitoring* – This involves collecting data from an endpoint to highlight relevant activity that might indicate a cyberthreat.
- *Continuous Analysis* – This references the ongoing and real-time nature of EDR solutions to analyze activity and data for threat evidence.
- *Automated Response* – This designates the goal to quickly respond to any detected issues with an automated task, usually in the form of an alert.

While EDR references activities—namely, detection and response—that are reactive in nature, most EDR solutions are installed specifically to prevent malware and other attacks that target endpoints. (It is worth mentioning that the types of protections that work for laptops, desktops and servers don't always work in cloud and cloud-native environments.)

It is beyond the scope to list all EDR vendors, but TAG Cyber analysts can help buyers in this regard. That said, CrowdStrike, SentinelOne and Microsoft are three of the larger EDR vendors, and we mention them to establish context. Buyers should select the EDR vendor that best matches their needs.

WHAT IS CLOUD DETECTION AND RESPONSE?

As suggested earlier, no accepted standards exist to define acronyms in the cybersecurity industry, so buyers should pay close attention to the features included in a commercial offering. That said, we view references to CDR as typically including the following set of capabilities to protect cloud assets:

- *Containers and Kubernetes* – These include integrated protections for scanning images, fixing configurations, addressing threats to containers, benchmarking compliance, enforcing policy and avoiding risky activity related to Kubernetes.
- *Cloud Workloads* – These detect and remove threats and vulnerabilities from physical and virtual machines, containers, serverless workloads, and other cloud-hosted resources and assets.
- *Cloud Infrastructure* – This includes protection of cloud computing support and infrastructure to ensure best practice design and deployment, and to ensure that user access, entitlements and other cloud attributes are properly secured.
- *Cloud Identities* – These analyze user and machine identities and associated permissions for all assets in cloud and cloud-native environments.
- *Service Interactions* – These analyze how identities, workloads and functions interact with other resources across environments to inform event correlation and detect potential indicators of compromise.
- *Cloud Remediations* – This involves remediation of threats to the cloud, with a focus on the vulnerabilities involved and support for managing fixes, and planning root cause analysis.

As can be seen from the above descriptions, the various activities included in CDR range from detection and response activities inherent in most cloud protection suites, to security monitoring and reporting of metrics for operational, management and board-level teams.

HOW DOES THIS IMPACT CISOs?

The key observation for CISO-led teams is that EDR and CDR solutions might be marketed and presented as being closely linked, at least as far as vendors claims about protecting your assets. As analysts, we see them as largely separate tasks. Endpoint systems and cloud assets require different handling, support and attention due to abstraction, virtualization and containerization. Therefore, when a vendor claims that workloads are "just a different type of endpoint," we find the reference misleading.

Perhaps the best way to view EDR and CDR is via a Venn diagram where the respective security and functional concerns are represented separately, and where common sharing and support functions intersect. The result is a view of how EDR and CDR work together in a typical enterprise, and while this appeals to our observation as analysts, we say that buyers should handle source selection carefully for these important areas.

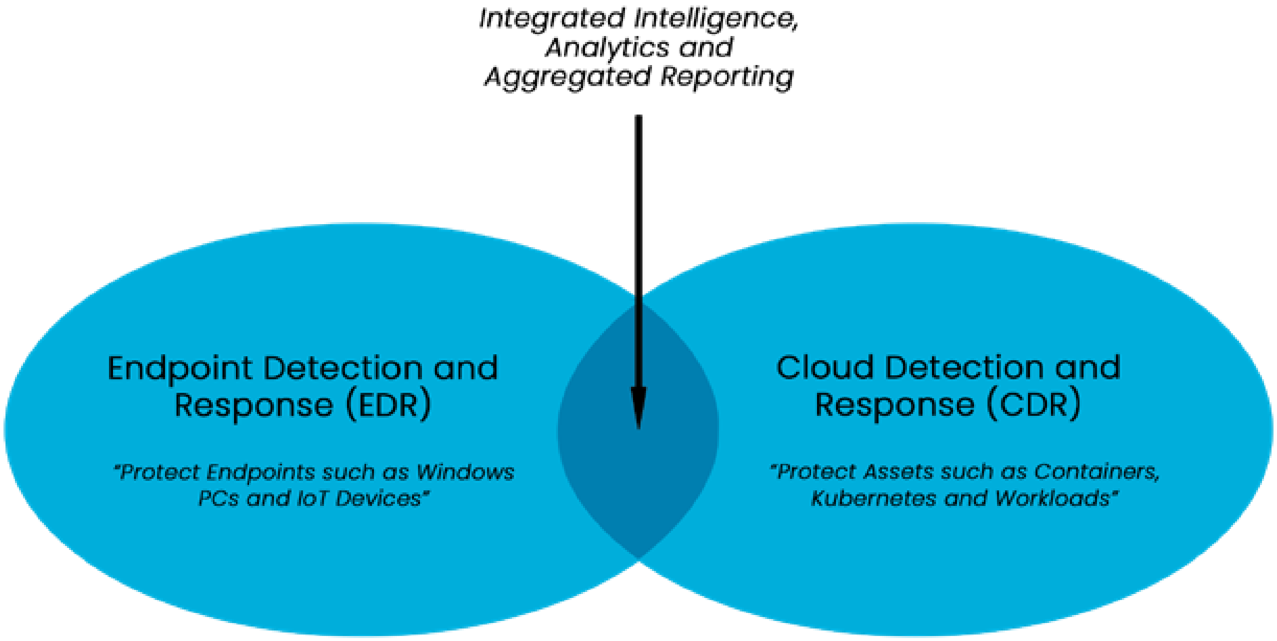
Integrated Intelligence, Analytics and Aggregated Reporting
Endpoint Detection and Response (EDR)
"Protect Endpoints such as Windows PCs and IoT Devices"
Cloud Detection and Response (CDR)
"Protect Assets such as Containers, Kubernetes and Workloads"

Figure 1. Understanding the Roles of EDR and CDR

Our advice to security professionals is to focus on the following three issues when selecting both EDR and CDR commercial offerings:

- *Details of Security Requirements* – The primary goal is to ensure that the EDR provider meets the desired security requirements of your diversified cloud assets and that the CDR provider meets the desired security requirements. This does not demand that the same vendor offers EDR and CDR. In fact, it will be common that EDR and CDR vendors will be different.
- *Select the Best Vendor* – The goal should be to select the best set of vendors with the optimal technology and support for both EDR and CDR. Endpoints and cloud are such important assets that enterprise teams should not compromise on quality or effectiveness. Good vendor selection will have a significant impact on cloud security operations.
- *Integration is Desirable* – The primary goal for EDR and CDR should be comfortable integration with available cyberanalytic support, common sharing with the SIEM or other security tools, and the ability to benefit from common resources such as threat intelligence.

If the selected vendor for EDR and CDR should happen to be the same provider, that's fine, so long as the granular security requirements are met, integration is supported, and sufficient effectiveness and coverage are offered. However, we see only marginal benefit from the claim that EDR and CDR are essentially the same type of activity. Our observation is that this is misleading, and vendors specialize in different domains.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner's perspective.

IMPORTANT INFORMATION ABOUT THIS PAPER

Contributor: TAG Cyber Analyst Team Supervised by Dr. Edward Amoroso

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Citations: This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "TAG Cyber". Non-press and non-analysts must receive prior written permission from TAG Cyber for any citations.

Disclosures: This paper was commissioned by Sysdig. TAG Cyber provides research, analysis, and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Disclaimer: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. TAG Cyber disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of TAG Cyber's analysts and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

TAG Cyber may provide forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment and opinion on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements considering new information or future events.