aws marketplace

One-minute webinar

(Re)Defining XDR:
How to improve threat detection and response in AWS

Key Topics

#1

The how:
A brief look at how extended detection and response (XDR) emerged

#2

The what:
A closer look at XDR, piece by piece

X
understanding the extended capabilities

D
improving vulnerability detection

R
enhancing and automating responses

#3

The why:
Why modern organizations are adopting cohesive detection and response strategies with XDR

#1

How we got here

- Modern cloud footprints have grown to transcend corporate-managed endpoints or common firewalls
- Traditional endpoint and network detection products often have single or limited source telemetry that may not work together
- Security teams have been deploying more security controls in order to compensate, introducing complexity
- XDR has emerged to improve visibility and combine these security capabilities

#2

Breaking down XDR, piece by piece

X(-tended)
Extending your data sources

- Data sources are critical to an effective XDR strategy
- Begin by focusing on the technologies your enterprise uses, such as your endpoint and perimeter data sources
- Look to your cloud provider for additional network data, such as Amazon Virtual Private Cloud (VPC) Flow Logs

Detection
Utilize extended telemetry to detect activity

- Real-time telemetry in XDR can place security teams closer to the occurrence of a security event
- Cross-platform detection capabilities can provide deeper insight and context to issues
- When evaluating XDR products, consider their abilities to allow for customized detection and alerting capabilities to meet your environment's unique attributes

Response
Respond more rapidly to incidents

- Detection capabilities should correspond with strong response components
- Consider utilizing tools where security teams can detect and respond from the same platform
- Encourage security teams to write response playbooks and seek to improve processes
- Leverage automation to reduce response times and mitigate risks

#3

Why it's important

Single-source security tooling may not be enough to encompass the modern enterprise. In some circumstances, threats may be able to avoid these defenses with simple evasion tactics. The use of XDR helps bring detection and response capabilities to operational areas beyond endpoints and networks.

What security teams are doing today

Organizations are leveraging XDR solutions from AWS Marketplace sellers to enhance their security profile and consolidate capabilities for improved security team efficiency.

Next Steps

Watch Webinar
(Re)Defining XDR: How to improve threat detection and response in AWS.

View on-demand

Discover solutions
Build stronger detection capabilities and better response orchestration across device and traffic types.

Visit AWS Marketplace

Talk to an AWS expert
Get connected with a solution architect that can share best practices and help solve your business challenges.

Contact solution expert

AWS Marketplace is a curated digital catalog that simplifies software discovery, procurement, provisioning, and management. With AWS Marketplace, customers can also utilize features that speed up product evaluation, improve governance and cost transparency, and enhance control over software spend. AWS Marketplace offers third-party solutions across software, data, and machine learning tools that enable builders to find, test, and deploy solutions to expedite innovation.

Explore AWS Marketplace Solutions to assist with your XDR strategy

paloalto NETWORKS

TREND MICRO

humio

aws marketplace