Trellix | aws

SOLUTION BRIEF

AI-powered security to see the threats you missed

Detect more and investigate faster with Trellix and Amazon Security Lake

Top 5 security challenges

In a Trellix survey, respondents ranked their primary cybersecurity concerns.

44%
High cost of cybersecurity solutions and services

39%
Difficulty detecting and responding to advanced threats

36%
Limited threat intelligence and insights

36%
Shortage of skilled resources

34%
Inability to manage the overwhelming volume of threats

XDR: Redefining the future of cybersecurity, Survey Trellix, 2022

What if a seemingly generic, low-level alert actually indicated a much larger attack? Would your security team know the right questions to ask to follow up? Would they have the time to dig in?

Between the billions of security logs and thousands of alerts flowing through organizations every day, today's security teams are strapped. And corralling all those data points into a single solution is an added challenge. To free up time and uncover threats you missed, security teams need to automatically ask the right questions to triage alerts and target malicious behavior.

Trellix is a launch partner of Amazon Security Lake, a new AWS service that offers a centralized and efficient approach to security data management, enabling customers to gain valuable insights, and improve their overall security posture. It uses Open Cybersecurity Schema Framework (OCSF), an open standard that normalizes and combines security data from AWS and a broad range of enterprise security data sources.

In addition to creating a complete security picture, the solution includes the ability to apply AI-powered detection based on Trellix's years of building a repository of questions to ask data lakes using expert automated investigations.

Questions Trellix asks

- Was it a new user?
- Was it the first time they logged in?
- Did they log in from two locations simultaneously?
- What commands did they execute?

Answers that highlight alerts you missed

Answers that tell the full story:

The alert indicates that the Windows command "ping -n X" was executed, which can be indicative of nefarious activity performed by actors or malware trying to move stealthily through an environment or to map a network. Additionally, the alert mentions that the activity was conducted by a new user, which raises further suspicion.

Trellix XDR relies on AWS services:

Amazon SageMaker to power machine learning models that inform threat intelligence

Amazon Security Lake to centralize and normalize customer data so it is ready to be used in Trellix XDR advanced analytics

Trellix helps security teams focus on the human side of their work

Trellix—the result of McAfee and FireEye merging—is a security partner known for putting artificial intelligence (AI) to work for security teams. With a dynamic Extended Detection and Response (XDR) architecture, Trellix is fast enough to keep up with dynamic threats, intelligent enough to learn from them, and constantly evolving to keep the upper hand.

Trellix XDR uses AI with advanced machine learning to detect subtle attacks and has built-in investigations to ask the right questions about alerts and lower the mean-time-to-respond.

> "At Trellix, we leverage the simplicity that Amazon Security Lake provides to ensure that we collect and centralize our critical security events in one place using the standard OCSF schema, regardless of the account or region they originated from. This integration allows us to combine them with our Trellix XDR to detect and respond to threats within our AWS infrastructure effectively."

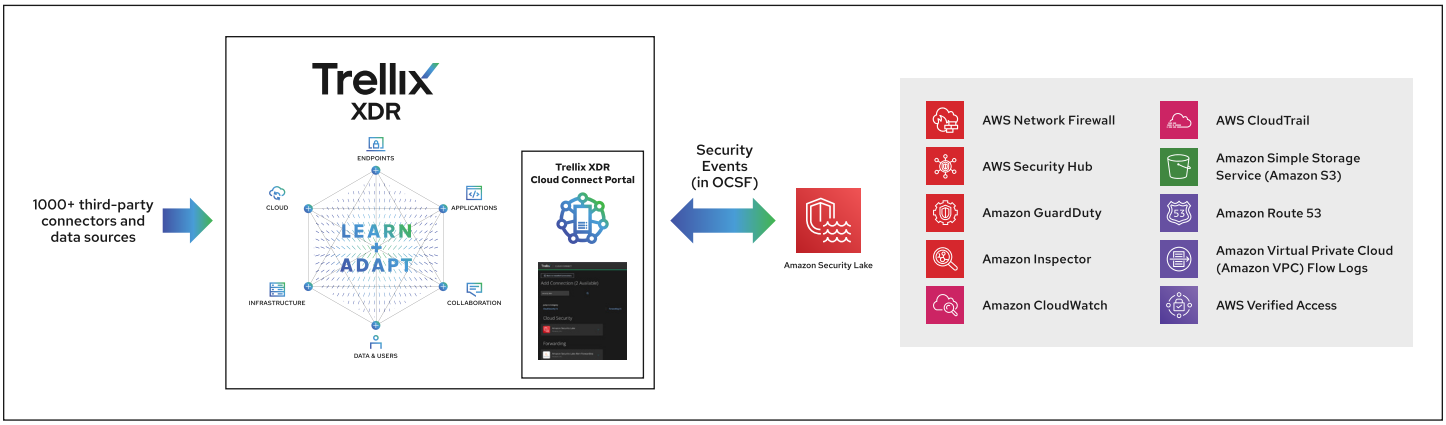
Bernadette Moloney, Trellix Manager Information Security

Trellix intelligence and telemetry combine in Amazon Security Lake

Trellix is one of a select few security independent software vendors (ISVs) offering both source and subscriber integration capabilities. It provides both holistic, AI-powered detection and the ability to centralize all security alerts in Amazon Security Lake.

Trellix is proud to be a contributing member of the open source OCSF community. Its solution combines the broad power of the Trellix security platform—which includes protection for endpoints, email, the network, and so on—with the best-in-class comprehension of third-party data in Amazon Security Lake, sourced by Trellix.

It combines endpoint security, endpoint detection and response (EDR), and platform events generated by telemetry to derive final answers.



Smarter, more empowered AI

By using the AWS platform, Trellix seamlessly integrates its own AI with advanced machine learning into its XDR environment. This means your valuable data remains secure within the network it originates from, ensuring privacy and that you maintain control over your information.

- **Smarter:** The Trellix AI benefits from years of knowledge from the same in-house experts who first identified major attacks like the SolarWinds hack in 2020.
- **Empowered:** Trellix mixes an incredible number of integrations with its Investigative Tips to fuel its proprietary machine learning algorithms to identify anomalous activity, such as impossible logins.

Trellix

See for yourself

Learn more about how Trellix and AWS have joined forces to bring you AI-powered cybersecurity that uncovers threats you missed and frees up your team. Living security starts here, visit trellix.com for more.

Reach out for a demo or to chat with our experts.