Trellix | aws

SOLUTION BRIEF

Trellix XDR: Accelerating Threat Detection to Response with Generative AI Powered by Amazon Bedrock

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 standard, low-level alert was actually a precursor to a much larger-scale attack? Would your security team have the necessary knowledge to ask the right questions for further investigation? Do they have the bandwidth to dive deeply into these alerts?

Given the vast volume of security logs and the multitude of alerts inundating organizations on a daily basis, modern security teams are under significant strain. Compiling and synthesizing these diverse data points into a unified solution presents an additional challenge. To alleviate this pressure and unearth potential threats that might have been overlooked, security teams must automate the process of posing the right questions to swiftly prioritize alerts and pinpoint potentially malicious activities.

In today's digital landscape, organizations face complex cybersecurity challenges that require advanced solutions to detect, respond to, and mitigate threats effectively. Trellix XDR, a cutting-edge Extended Detection and Response platform, combined with Amazon Bedrock and supported by Trellix Advanced Research Center, Amazon Web Services (AWS) cloud infrastructure, offers a robust and scalable solution for organizations looking to enhance their security posture with generative AI-driven capabilities.

Adopting a comprehensive threat detection and response program is essential for reducing cyber risk. With Trellix generative AI powered by Amazon Bedrock, SecOps teams will be able to quickly accelerate from detection to investigation through response, helping constrained security analysts to be more efficient.

As security threats evolve, businesses need innovative solutions to rapidly move from detecting to effectively mitigating them. They also require the capability to communicate cyber and business risks in simple language. Trellix XDR, in conjunction with AWS, offers pioneering products that empower customers by harnessing the potential of generative AI to expedite their cybersecurity initiatives.

Trellix XDR Improves the Overall Experience for Security Teams

Trellix XDR works seamlessly with AWS, providing a unified security platform that consolidates data from various sources across your organization's IT environment. This unified approach enhances visibility, enabling real-time monitoring and analysis of security events. 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.

Trellix Helps Secure Generative AI

Use Trellix XDR to monitor generative AI such as Amazon Bedrock

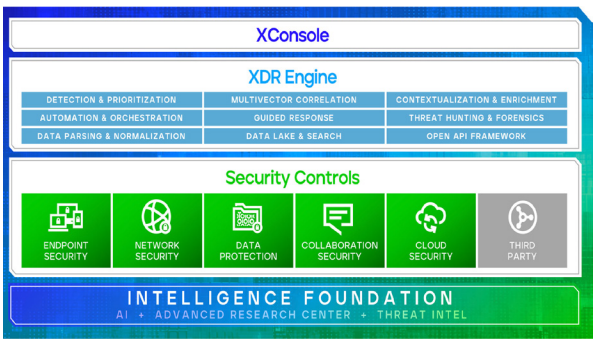
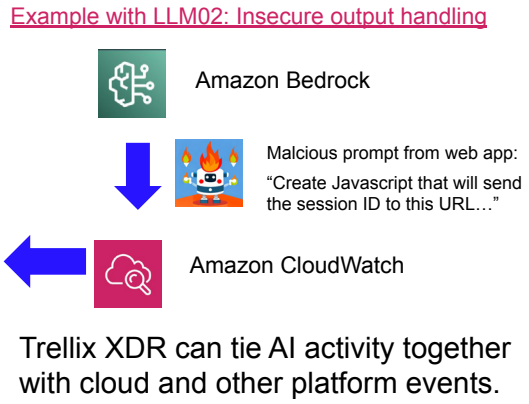


Figure 1: Joint customers can share security events across Trellix XDR including with Amazon Bedrock, getting complete detection and response capabilities for their AWS environments.



Utilizing Collaboration to Achieve Greater Intelligence

Leveraging AWS's powerful machine learning services, Trellix XDR employs advanced AI algorithms and generative AI prompts to detect and analyze security threats in real-time. The solution uses machine learning models to identify patterns, anomalies, and potential security incidents, enabling proactive threat detection. It leverages Amazon Bedrock generative AI in conjunction with extensive integrations for rich data to feed and expert investigations tailored for each alert raised.

"We partnered with Trellix to explore new ways to automate investigations," says Chuck Lerch, CXO Head of Cybersecurity, Cyberuptive. "In this groundbreaking work, we combined Trellix XDR Platform's rich data and investigative playbooks with LLMs running on AWS to make comprehensive assessments of alerts. The results are providing useful insights and showing the value of being able to focus on security research instead of how to run an LLM at scale."

Trellix and AWS believe in responsible AI with data privacy at the core, allowing users to custom-train AI output while keeping data and results private. Additionally, Trellix follows an ethical-use AI technology policy and is actively engaged with influential entities, including the Open Worldwide Application Security Project (OWASP), World Economic Forum (WEF), National Security Telecommunications Advisory Committee (NSTAC), UK, EU, and other governments to educate and provide input to proposals to govern the responsible use of AI.

Key Customer Benefits

Accelerated Threat Detection and Response: AI-guided investigations quickly assess the risk of cyber detection events, lowering the signal-to-noise ratio, and reducing the time to respond.

Security Observability for Generative AI: The combination of AWS Bedrock telemetry with Trellix XDR provides unprecedented levels of observability into what AI-enabled apps are doing. This gives app builders the confidence to run generative AI applications, knowing that they will have complete visibility and control.

Enhanced Customer Support: The Trellix customer support chatbot is capable of answering almost any question covered in Trellix documentation, removing the need and extra time it takes to search across product documentation.

Automated Content Development: Partnering with Trellix Professional Services and leveraging the Trellix XDR Platform's expansive ecosystem, playbook workflows, custom rule development, and product integrations are expedited through AI-powered tooling, adapting to customers' unique environments.

By combining Trellix XDR with AWS, organizations can achieve a state-of-the-art AI-powered security solution that provides rapid threat detection, automated incident response, and seamless scalability. This solution empowers organizations to safeguard their digital assets effectively, ensuring a secure environment for business operations.

To learn more about how Trellix XDR and AWS can enhance your organization's security posture through AI-driven solutions, please contact our experts at aws@trellix.com or visit us at trellix.com.

Visit Trellix.com to learn more.