Trellix

SOLUTION BRIEF

Trellix® and AWS: GenAI for your biggest security operations challenges

We're living in the age defined by the integration of security tools and data. The vast array of tools and the high volume of events they generate are unsustainable for security teams. With the rise of AI and GenAI it's more necessary than ever to pick vendors who are built with integration in mind. The strategic choice empowers you to stay ahead in the security game. Trellix Helix Connect, Trellix EDR and Trellix Wise™ work seamlessly with Amazon Bedrock, Amazon Web Services (AWS) cloud infrastructure and the Trellix Advanced Research Center to provide a unified security platform that consolidates data from across your organization's IT environment for AI-driven Security Operations.

Built on over a decade of AI modeling, 25 years in analytics and machine learning, and powered by Amazon Bedrock, Trellix Wise uses GenAI capabilities to relieve alert fatigue and surface stealthy threats. It automatically escalates alerts with context, analyzes and correlates artifacts related to a threat to eliminate cognitive load on security teams. This allows you to identify what gaps need to be closed, and what systems need further inspection.

"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 the Trellix Security 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."

Never miss an alert again

Most security staff only look at about 10% of alerts due to the large volumes generated by their security tools and high volumes of false positives. With Trellix Wise, we finally have an answer to alert fatigue. Wise automatically investigates every alert, using the full context of your data to decide when teams need to take action. Instead of being overwhelmed by alert volumes, teams now have opportunities to dig deep and find advanced AI-enabled attacks. Wise is built on over a decade of AI modeling and 25 years in analytics and machine learning.

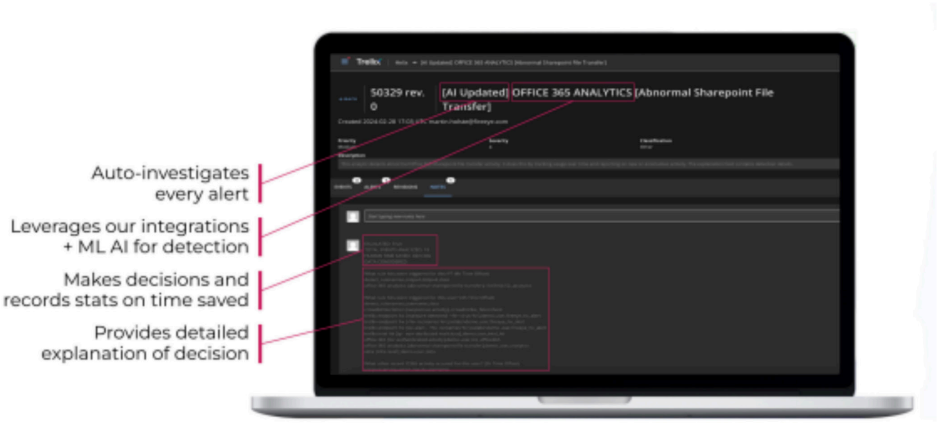

Figure 1: Trellix Wise uses built in Machine Learning, AI, and GenAI to make decisions in seconds.

Deep dive into data with AI-powered investigations

Once an incident is identified, Trellix Wise will automatically call upon our rich endpoint detection and response (EDR) data. After it analyzes all artifacts related to a threat, it auto-generates a summary with key findings, saving analysts the time of having to put it all together manually.

Wise also eliminates the tedious task of writing threat reports for executives. With the click of a button, Wise will generate a summary report that your leadership will appreciate and understand.

Trellix Wise eliminates guess work for analysts by providing auto-generated remediation recommendations based on the specifics of the incident, so you can reduce the time to remediation.

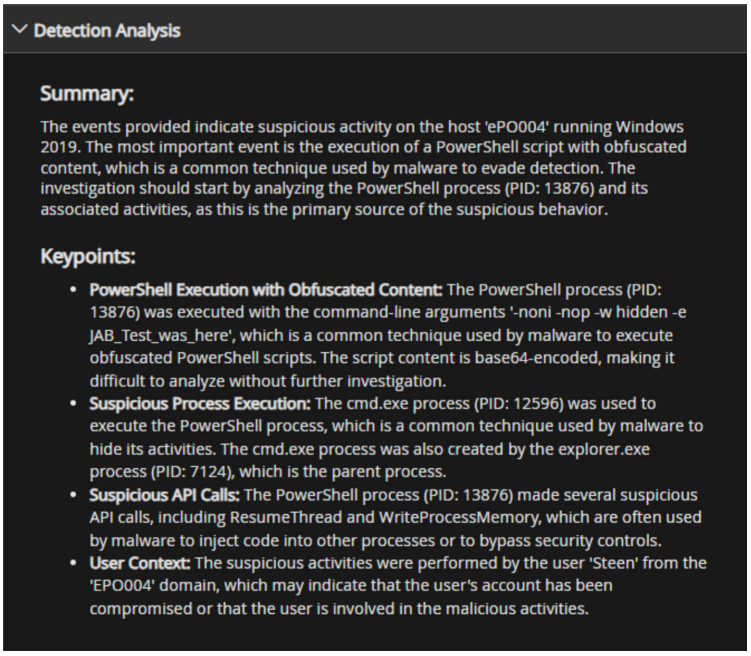

Figure 2: Trellix Wise analyzes all artifacts related to a threat and auto-generates a summary with key findings

Improving the overall experience for security teams

Trellix Helix Connect 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.

Helix Connect 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

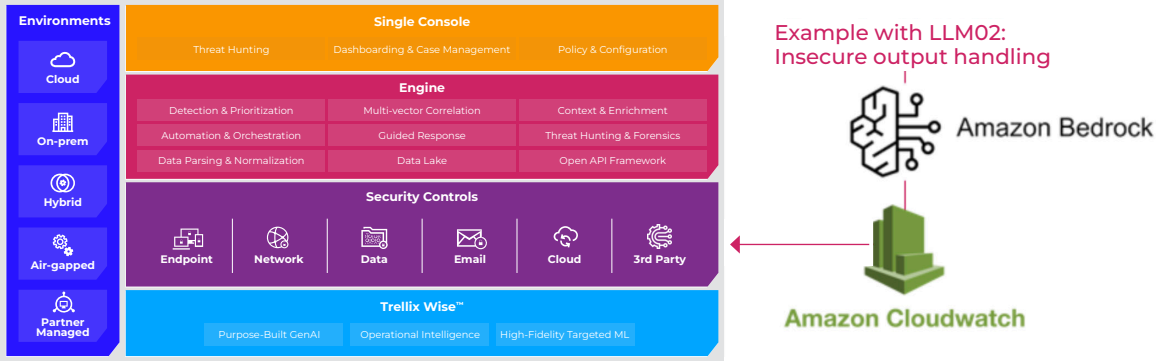

Figure 3: Monitoring Generative AI like Amazon Bedrock with Trellix

Leveraging AWS's powerful machine learning services, Trellix 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.

Solve today's biggest security challenges with Trellix

Don't put off changes that can make a real impact to your efficacy, efficiency and make better use of your current resources. Trellix Wise connects hundreds of security tools and can be implemented in on premises, air-gapped and cloud environments. With Trellix Wise, your organization can finally solve some of your most common challenges:

- **Automatic alert investigation in <3mins:** Ensure all alerts are triaged, scoped and assessed in <3mins.

- **Decrease MTTD:** Triage, scope and **investigate 90% more alerts, saving the work of 5 analysts/day**.
- **Improve MTTI:** Automated incident containment and streamlining investigations, summarizing events with risk scores and recommendations.
- **Improve MTTR by up to 300%:** Using AI-powered responses that reduce risk to your organization with faster, accurate responses.
- **Leverage current resources better:** With automated and accelerated workflows, security content creation, and natural language AI interactions.
- **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:** 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 Helix Connect, Trellix EDR and the Trellix Security Platform 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.

Discover how ai-driven security transforms your defense strategy – contact our experts today!

To learn more about how Trellix 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.