Trend Micro to Introduce Most Comprehensive Offering for Enterprise AI Risk Management

AI Application Security will accompany a package of new solution capabilities at AWS re:Invent

DALLAS, Nov. 24, 2025 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, is set to launch Trend Vision One™ AI Security Package—the first solution package delivering proactive, centralized exposure management with unparalleled analytics for AI-driven environments—at AWS re:Invent in December. This new package protects the full AI application stack from model development to runtime, extending proactive security across every stage of AI deployment, and will launch alongside a suite of other leading AI security capabilities to be introduced at the event.

To learn more about the AI security package and additional Trend Vision One innovations at AWS re:Invent 2025, please visit: https://resources.trendmicro.com/AWSreInvent.html

Rachel Jin, Chief Platform and Business Officer at Trend: "Innovation without oversight is a risk businesses cannot afford. Our goal is to provide the foundation for AI safety and guardrails to align AI transformation with security and trust. By building with these principles from the start, organizations can move forward with confidence as AI becomes central to their growth."

Organizations are building AI systems at speed, but most lack visibility into how those systems process data, make decisions, or could be exploited by threat actors. Traditional security tools serving endpoints, network, and cloud were not built to understand model behaviors or AI-specific risks like prompt injection, data poisoning, or output manipulation. This leaves organizations exposed to errors and blind spots that existing tools were never designed to address.

This is where Trend Vision One™ changes the game—offering a comprehensive way to detect risks in AI models and automatically protect them through intelligent AI guardrails. With AI Application Security, the AI Scanner continuously monitors models to uncover vulnerabilities and applies AI guardrails to defend against threats—creating a seamless, proactive, closed-loop system for AI risk management.

Despite growing awareness of AI risks, most organizations still deploy systems without adequate security checks. According to the World Economic Forum (2025), only 37% of organizations assess AI security before rollout, even as theaverage cost for a data breach surpasses $4.4 million.

To address emerging threats and simplify security management, Trend has several integrated security tools designed to deliver proactive, AI-powered protection across cloud-native environments, including:

- **AI Security Blueprint and Risk Insights:** Establishes auditable AI governance with a unified risk posture visualization, delivering actionable insights to enforce compliance and protect proprietary models across the development pipeline and enterprise.
- **Cloud Risk Management (CRM) – Project View:** Breaks dev-security silos with real-time monitoring, instant threat alerts, and full-stack risk visibility across supply chain pipelines. Agentless vulnerability detection across multi-cloud environments, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), provides zero-impact deployment with 24-hour updated asset visibility.
- **Container & Code Security**: Delivers shift-left security by moving vulnerability evaluation earlier in development, reducing manual overhead through automation, and ensuring consistent policy application. New File Integrity Monitoring (FIM) for critical system files with Kubernetes and eBPF support enhances runtime protection.
- **File Security with NetApp Storage Support (FSx)**: Provides real-time malware and ransomware protection for cloud storage with a security-first design—files never leave the environment, and scanning happens locally with only metadata sent to Trend. Kubernetes-based architecture enables automatic scaling with unified Trend Vision One visibility.
- **Agentic SIEM with AWS Native Logs Integration**: AI-native cloud detection and response combining real-time observability, IOC sweeping with threat intelligence, and automated security playbooks. Supports rapid ingestion of new cloud application logs within hours for correlation with Trend threat intelligence.
- **Zero Trust Secure Access – AI Secure Access:** Extends zero trust to generative AI tools, enabling granular policy enforcement to control employee interaction, prevent sensitive data exposure, and mitigate critical shadow IT risks.

"As organizations race to gain advantage through the use of AI throughout their operating environment, most face significant risks across the many facets of AI security and governance," **said Dave Gruber, Principal Analyst at Omdia**. "Mitigating these risks requires comprehensive visibility and governance throughout model and application development, deployment, and utilization."

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information between people, governments, and enterprises. Trend leverages security expertise and AI to protect more than 500,000 enterprises and millions of individuals across clouds, networks, endpoints, and devices worldwide. At the core is Trend Vision One™, the only AI-

of individuals across clouds, networks, endpoints, and devices worldwide. At the core is Trend Vision One™, the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management and security operations, delivering layered protection across on-premises, hybrid, and multi-cloud environments. The unmatched threat intelligence delivered by Trend empowers organizations to proactively defend against hundreds of millions of threats every day. Proactive security starts here. TrendMicro.com

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---