Visium Technologies Launches TruContext™ AI Governance Layer to Contain 'OpenClaw' Style Autonomous Agent Risks

Graph-based cyber intelligence gives enterprises visibility and control over Shadow AI, prompt injection, and high risk autonomous actions

Visium Technologies, Inc.

FAIRFAX, VA, UNITED STATES, March 19, 2026 /EINPresswire.com/ -- Visium Technologies, Inc. (OTCID: VISM), an AI-driven cyber intelligence company, today announced new TruContext™ AI governance capabilities designed to secure autonomous agents and eliminate unmanaged “Shadow AI” across the enterprise. These enhancements help organizations discover, monitor, and control powerful agentic AI frameworks such as “OpenClaw” (also referred to as Clawdbot or Moltbot) before they expose sensitive data, make unauthorized changes, or execute harmful actions.

> Every organization racing to deploy AI agents is unknowingly expanding its attack surface - TruContext™ gives leaders the visibility to govern AI the same way they govern people”
>
> *Mark Lucky, CEO of Visium Technologies*

OpenClaw, an open-source framework, represents a new frontier in agentic AI: powerful, highly autonomous, and easy to use. When deployed without appropriate controls, these capabilities can create significant new security risks. OpenClaw enables autonomous agents to operate with broad permissions, persistent memory, and limited oversight. Without proper safeguards, these agents may be manipulated into exposing sensitive data, making unauthorized changes, or carrying out harmful actions that go undetected until meaningful damage has occurred.

“Every organization racing to deploy AI agents is unknowingly expanding its attack surface,” said Mark Lucky, CEO of Visium Technologies. “The question is no longer whether your network has autonomous AI operating inside it — it’s whether you can see it, understand it, and control it. TruContext™ does all three, giving leaders the visibility to govern AI the same way they govern people: with context, accountability, and a human hand on the wheel.”

OpenClaw is not just another tool; it can become an amplifier of risk when deployed without human oversight. By operating autonomously and at machine speed, these systems can quickly exceed intended boundaries, leading to configuration errors, privilege escalation, or data exposure that traditional security tools may miss until long after the fact.

The TruContext™ Difference: Field Proven Intelligence for the Modern Enterprise

Visium's TruContext™ platform was built for high stakes environments where autonomous decisions carry real world consequences. TruContext™ does not simply execute rules; it reasons over a living map of an organization's digital ecosystem using advanced graph structured intelligence.

Key Ways TruContext™ Secures the AI Driven Enterprise

• Prompt injection defense – Evaluates instructions against safe behavior maps to prevent attackers from steering agents like OpenClaw toward harmful actions.

• Digital lighthouse – Provides continuous visibility and instantly flags Shadow AI or unapproved agents the moment they appear on a network.

• Human assurance – Explains why an AI reached a conclusion and can require human approval for high risk actions before execution.

• Anomaly detection – Detects suspicious data movement and interactions between AI agents that traditional tools often overlook.

By aligning with Zero Trust principles — never trust, always verify — TruContext™ helps ensure that as AI becomes more ubiquitous and autonomous, it also becomes more accountable. Security and risk leaders gain the visibility and control they need to map hidden nodes and relationships, enforce policy, and keep increasingly powerful AI systems securely under human command.

Designed for CISOs, CIOs, and AI governance leaders, TruContext™ sits above existing AI frameworks and security tools as a unified control layer. It discovers autonomous agents, maps their permissions and behaviors, and enforces policy so organizations can adopt powerful AI safely and in line with Zero Trust and emerging AI governance requirements.

About Visium Technologies
Visium Technologies, Inc. (OTCID: VISM) leads in agentic AI-powered data analytics and surveillance solutions for governments and enterprises in emerging markets. The TruContext™ platform offers advanced threat detection, behavioral analytics, and intelligent surveillance with ethical safeguards and data sovereignty. With partnerships in Latin America, Africa, and the Middle East, Visium supports smart cities, critical assets, and national security.

For more information, visit www.visiumtechnologies.com.

Forward-Looking Statements
This press release contains forward-looking statements within the meaning of Section 27A of the Securities Act of 1933 and Section 21E of the Securities Exchange Act of 1934. These statements involve risks and uncertainties that could cause actual results to differ materially, including deployment timelines, infrastructure dependencies, government contract performance, security conditions, and international expansion opportunities.

Mark Lucky
Visium Technologies, Inc.
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X
