
VCONIC and CORTEGA Partner to Secure AI Voice Agents

FOR IMMEDIATE RELEASE

VCONIC and Cortega Partner to Stop AI-on-AI Voice Fraud, With Every Attack Recorded as an Auditable vCon

Joint live demo at VON Evolution in Atlanta shows an AI "hacker bot" attacking a customer service voice agent, with and without Cortega's guardrails, and a full audit trail recorded through the VCONIC Conserver.

ATLANTA, October 13, 2026 — VCONIC, the company commercializing the open IETF vCon standard for structured conversation records, and Cortega, an AI security and governance company, today announced a technology partnership to secure AI voice agents. The integration pairs Cortega's real-time guardrails with VCONIC's Conserver platform, so every agent-to-agent exchange, every attempted attack and every enforcement decision is captured in a standards-based vCon record. The companies will demonstrate the joint solution live at VON Evolution in Atlanta on October 13 and October 15.

When bots talk to bots, trust has to be engineered

Enterprises are moving customer service onto AI voice agents that can issue refunds, change account details, and access personal data. The next wave of fraud will not come only from human callers. It will come from AI agents built to manipulate other AI agents, using pressure, false authority and fabricated context to talk them into breaking policy.

That shift creates two problems at once. Companies need to stop the attack in the moment, and they need a trustworthy record of what happened afterward, for compliance teams, regulators, and dispute resolution. Cortega addresses the first. VCONIC's vCon and Conserver platform addresses the second.

The demo: a hacker bot versus a customer service agent

The joint demonstration stages a live contest between two AI agents. A customer service voice agent, built on real-world automotive dealership conversations supplied by VCONIC, operates under a defined policy. An adversarial "hacker bot" tries to break it. Scenarios include:

- **SIM swap fraud:** pushing the agent to approve an account recovery it should refuse.
- **PII extraction:** pressuring the agent to reveal a customer's personal information.
- **Impersonation:** posing as a supervisor or law enforcement officer, or claiming identity was "already verified" minutes earlier.
- **Legitimate customer:** a real customer provides personal information as part of an allowed transaction, showing that Cortega protects the agent without blocking normal service.

- **vCon record retrieval:** a caller posing as a detective pressures the agent over several escalating rounds and tries to pull records directly from the vCon MCP server with no valid credentials. A genuine investigator is then checked for consent or lawful basis in real-time before any record is released.

Each scenario runs side by side, with standard guardrails as the baseline and with Cortega Policy Guardrails. Every call is a live LLM, so no two runs play out identically. In the baseline, the hacker bot can often talk the agent into leaking data or approving the swap. With Cortega in the loop, the agent holds its ground and declines the request.

Every run is captured as a vCon through the VCONIC Conserver. The resulting log ties the vCon UUID to the total LLM calls, MCP tool calls, Conserver enrichment, processing cost and the exact point where the attack was detected, then posts the record to the Conserver API. The result is a portable, standards-based audit trail of an AI-to-AI interaction: what was said, what was attempted, and how it was stopped.

What the partners are saying

"The next wave of fraud won't come only from human callers. It will come from AI agents built to defraud other AI agents," said Sri Ramachandran, CEO of Cortega. "Cortega Policy Guardrails use patent-pending technology to stop those attacks in fewer turns and at much lower cost. As a VCONIC partner, we've made the evidence as strong as the defense: every attempt and every block is captured as a vCon that compliance and legal teams can verify."

"This is something you simply couldn't do before," said Thomas Howe, CTO of VCONIC and co-author of the vCon standard. "vCons don't just let you analyze a conversation. They let you save that analysis and share it. Cortega shows exactly why that matters when the participants are AI."

"Enterprises adopting AI voice need security and accountability together," said Perry Evans, CEO of VCONIC. "Cortega brings the real-time protection, and VCONIC brings the open-standard record that compliance and legal teams can trust."

See it live at VON Evolution, Atlanta

VCONIC and Cortega will present the demo in two sessions, alongside fellow vCon ecosystem partners INLayer and JLINC:

Date	Time (ET)	Session
Tuesday, October 13	3:45–4:05 pm	20-minute panel introducing the joint solution and how it works with vCon
Thursday, October 15	9:55–10:40 am	40-minute extended session with a deeper walkthrough of the live demo

Attendees interested in a private walkthrough can contact VCONIC to arrange time during the event. Cortega has also published a white paper detailing how its guardrails work with vCon,



available on request. The live arena is also open to try at vcon-arena.cortega.ai, where each run can be downloaded as a vCon.

About VCONIC

VCONIC builds commercial infrastructure for vCon, the open IETF standard for structured conversation records. Its Conserver platform captures, enriches, secures, and shares conversation data across voice, messaging, and AI channels, giving enterprises a portable, auditable record of every interaction. Launched as a venture from Strolid Inc., VCONIC is led by a team that includes vCon standard co-author Thomas Howe. Learn more at vconic.com.

About Cortega

Cortega is an AI security and governance company using patent-pending technology to protect enterprise AI agents, such as customer service chatbots that use voice and text, from manipulation, fraud and policy violations. Its guardrails detect and stop adversarial behavior in real time, in fewer turns and at lower cost than standard approaches, while supporting compliance requirements. Learn more at cortega.ai.

Media contact

Chris Celiberti, VCONIC chris@vconic.com

Sri Ramachandran, Cortega, sri@cortega.ai