10 Sep 2026 15:38:19 ET | 9 pages

Artificial Intelligence and Systems Software

Enterprise AI: Island - Day 3 Takeaways from Citi's Global TMT Conference

Heath Terry[AC]
Fatima Boolani[AC]
Shelby Spencer
Ashley Kim
Janna Withrow

CITI'S TAKE

We hosted Mike Fey, the CEO of Island, for a fireside chat on September 10, 2026, at our Global TMT Conference in NYC, moderated by Fatima Boolani. The discussion covered Island's evolution from enterprise browser to full agentic control plane, the state of AI-driven data security, and the cybersecurity budget outlook in an agentic world. Key takeaways below.

Agentic wave requiring step-change in control plane investment. Fey pushed back on the narrative that cybersecurity budgets are not responding to AI risk, arguing that the constraint is organizational readiness rather than dollars, with security teams playing catch-up to technology rollouts rather than governing them. He noted that 1/3 of Island's deals now originate from the CISO, 1/3 from the CIO, and 1/3 from the line of business, reflecting a convergence of AI and security budgets rather than two separate funding pools. On the agentic frontier, Fey prescribed four control planes as prerequisites for safe agent deployment: endpoint, data, identity, and network, noting Island has scaled from 4 agentic workers internally six months ago to several thousand today, with an expectation of approximately 30,000 by year-end. He framed validating every agent's behavior and credentials as an eventual requirement for Fortune 1000 companies, describing the cost of doing so at current technology capabilities as significant.

Enterprise browser to full agentic control plane. Fey described Island 1.0 as purpose-built for the knowledge worker, addressing limitations of legacy browser and network infrastructure. Traditional backhaul architectures can now inspect less than 30% of enterprise traffic, creating security gaps across tools such as Office, Slack, and Salesforce. Island 2.0 extends that control plane to agents, governing endpoint, data, identity, and network across both human and agentic workers. The go-to-market motion is use-case led, typically displacing 10-20 vendors on entry and funded through displacement ROI, with browser seats priced at approximately $100 per user per year and network modules at double to triple that. Fey noted that they are beginning to see big expansions show up with over 50% of customers running multiple modules. Fey sees Island's cost structure as fundamentally differentiated as they don't have to carry the customer's bandwidth, compute, or token spend, which supports 85-90% gross margins.

Telemetry points to AI data exfiltration, model fluidity. Fey described the data picture across Island's install base as disorganized, with even the most security-conscious enterprises experiencing data leaving to external AI models, often through

See Appendix A-1 for Analyst Certification, Important Disclosures and Research Analyst Affiliations

ways that appear benign to network infrastructure (e.g., Gemini traffic appearing as Google). He noted there are effectively no switching costs in AI, making model governance across the enterprise particularly difficult, and flagged that approximately 80% of observed prompts reflect non-productive use, pointing to early-stage enterprise adoption dynamics. Fey characterized AI as the largest security challenge enterprises have faced, exceeding the complexity of the cloud transition, and argued that incumbent security vendors are architecturally misaligned to the problem that meaningful responses will require either large-scale acquisitions or fundamental platform reinvention.

