

Selling Agent Provenance to the CIO: Entire Changes Who Signs

Why Thomas Dohmke's Entire-Distributed Git Launch Reframes Control of Agent-Generated Code for Vendors, CIOs, and Enterprise Development Teams

Analyst(s): Mitch Ashley

Publication Date: July 14, 2026

Document #: AINMA202607

Key Points

- Entire's preview launch bundles two moves: agent-scale Git mirroring and repository-resident capture of agent reasoning. Only one determines who controls the agent-era software lifecycle.
- The market question is which categories a repository-resident provenance graph displaces, which incumbents it threatens, and where it opens new ground.
- Enterprise development teams inherit more than faster clones: a new governed asset, new platform ownership questions, and a new procurement calculus accompanying the checkpoints.
- The buying decision moves. Entire's provenance layer pulls the CIO, CISO, and legal into what presents as a developer tooling purchase, and enterprise teams inherit a new governed asset along with a new procurement path.

Recommendations for Vendors and Enterprise Buyers Evaluating Agent-Native Development Platforms

Vendors across the development toolchain and enterprises piloting coding agents should treat Entire's launch as a forcing function for provenance strategy, whether or not they adopt the platform.

1. **Classify Agent Session Data Before Capturing It:** Enterprise platform teams should define access control, retention, and residency policies for agent reasoning data before enabling any checkpoint tooling.
2. **Pressure-Test Incumbent Git Roadmaps:** Organizations committed to GitHub or GitLab should ask their provider directly for their agent-scale throughput and provenance product roadmap.

3. Reassess Category Assumptions: Code review, agent observability, and DevSecOps vendors should test the roadmap assumption that provenance data remains fragmented across tools.

What You Need to Know

Entire, founded by former GitHub CEO Thomas Dohmke and former GitHub deputy chief of staff Cole Driver, launched a preview of its distributed Git network with active regions in the US, Europe, and Australia. Developers mirror an existing GitHub repository in one step, and AI agents clone and pull from a faster, closer replica. The company emerged in February 2026 with a \$60 million seed round led by Felicis, with Microsoft's M12 participating, at a reported \$300 million valuation.

Entire records the reasoning behind AI-generated code changes, storing agent session context as checkpoints in the repository itself, with Entire Blame, Entire Review, and semantic search across change history and reasoning. It integrates with major coding agents, including Claude Code, Codex, Cursor, Factory AI, and GitHub Copilot; offers native repository hosting beyond mirroring with commercial and free tiers after the preview period; and has not disclosed pricing. Dohmke describes centralized Git hosting as a fundamental constraint in the agent era and argues that session logs should be stored in the repository alongside the code. Read the launch details in DevOps.com's [coverage of Entire's announcement](#).

Analysis

Entire's mirror network is the wedge, and the agent provenance graph is the control point that matters. Distributed Git mirroring solves a genuine throughput constraint, yet Git-compatible replication can be built by any competent infrastructure team. Checkpoints that pair every commit with the agent session that produced it create something no incumbent currently holds: a compounding corpus of how software decisions get made, and a purchase that ultimately lands on the CIO's desk.

The complementary posture toward GitHub reads as sequencing rather than an end state. Microsoft's M12 sits on the cap table while Madrona, another investor, states the goal is *"not only to supersede GitHub, but to superset it"* (Madrona, [The AI Era's Developer Platform: Why We Invested in Entire](#)). A company does not raise the largest developer tools seed round on record to run a caching layer for someone else's platform.

Agent Provenance Is the Control Point

In control plane terms, the reasoning graph is the audit and accountability substrate for agent-produced software, the layer that policy engines will query. Entire Blame and Entire Review are early expressions: review anchored to intent, blame that resolves to a session rather than a person.

This is [observability-native](#) architecture territory applied to the software lifecycle itself: telemetry emitted at creation, attached to the artifact, queryable in place. The vendor that owns this layer is the enforcement point for the questions enterprises must answer about agent-written code, including which agent wrote it, under what instructions, and with what review.

Figure 1: Observability-Native Agentic Cycle



Source: Futurum Research, 2026

Once review, audit, and incident forensics depend on the reasoning graph, switching costs compound at the pace of development itself. The mirror network accelerates that accumulation by placing Entire directly in the data path of agent traffic.

Futurum's [2H 2026 SLE Market Sizing & Five-Year Forecast](#) sizes the prize. The Agent Control Plane segment is the fastest-growing category in the software lifecycle market at a 48.7% CAGR, reaching \$12.9B by CY2030, and buyers increasingly favor open standards such as MCP and A2A. Entire's provenance graph is a control-plane play wearing infrastructure clothing,

entering the segment where growth is concentrated. Buyers evaluating coding tools today collect defect rates, usage frequency, and acceptance telemetry, and none of the commonly collected metrics touch provenance or audit (Futurum ETR AI Product Series, January 2026, N=181).

Displacement, Threats, and the Openings It Creates

Standalone AI code review faces displacement first: tools that see only diffs now compete against a review that sees the conversation that produced the diff. Agent observability point tools face the same squeeze because context attached to the commit beats context archived elsewhere.

Git hosting economics are next to come under threat. If agent traffic routes to mirrors while humans stay on GitHub for collaboration, GitHub maintains the engagement system, while Entire accumulates the system of record for agent work. Microsoft's strongest countermove, and the largest single risk to Entire's position, is native repository-resident session capture for Copilot at GitHub scale, a very likely move by Microsoft.

The counterargument that provenance is simply a feature GitHub can ship is right on infrastructure and wrong on the graph. If Entire's checkpoint format standardizes across agents, neutrality becomes the moat, because rival agent vendors may prefer a graph on which their competitors do not operate. If the format stays proprietary, enterprises trade GitHub concentration for lock-in to a startup's schema. That fork decides whether this thesis holds.

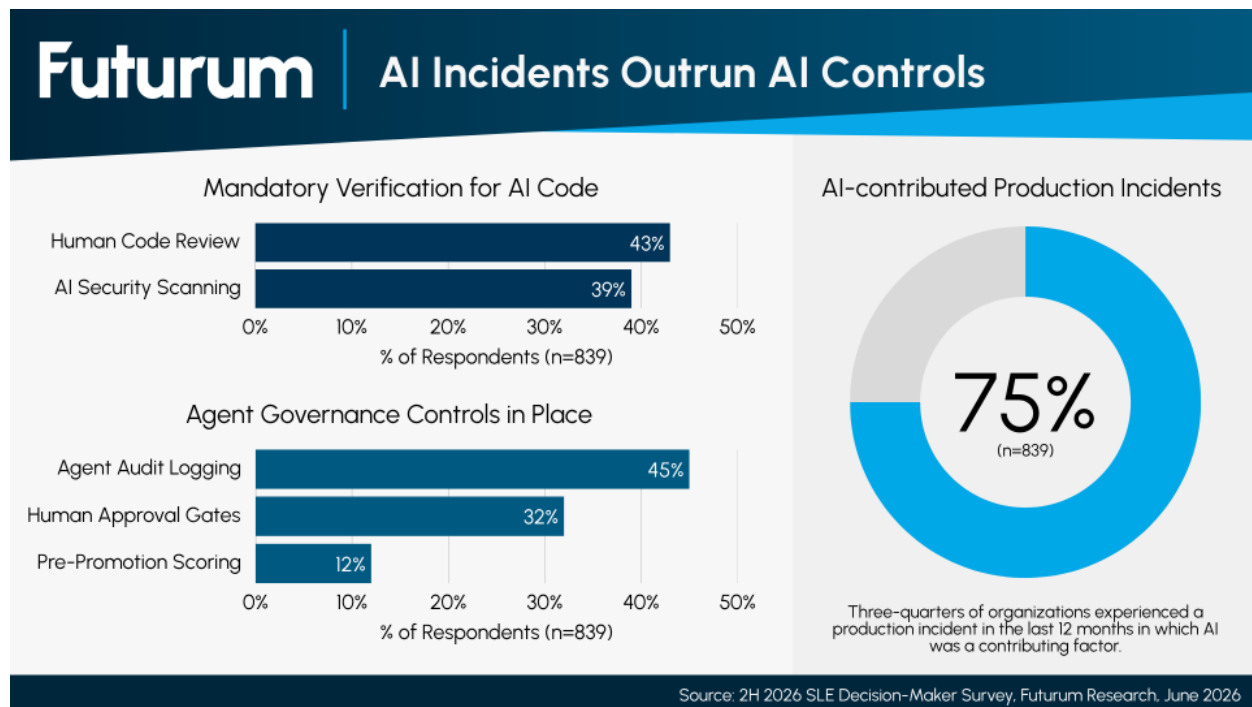
The openings favor security and platform vendors. A provenance graph provides supply chain security vendors with an attestation substrate for agent-authored code, extending SBOM-style evidence to include authorship, instructions, and approvals. Platform engineering teams gain a governable agent data plane. Regulated industries get an audit answer they currently lack.

What Enterprise Development Teams Inherit

The reasoning graph is a new governed asset class, and most organizations have no policy for it. Checkpoints consolidate prompts, internal constraints, architectural rationale, and potential secret exposure into a single queryable store. Entire's redaction claims and repository-resident design are the right instincts, and the control details that matter most, access control, data residency, and graph portability on exit, remain undisclosed.

The [2H 2026 SLE Decision-Maker Survey](#) (N=839) quantifies the gap. Three-quarters of organizations experienced a production incident in the last 12 months in which AI was a contributing factor. Set against that incident rate, only 43% mandate human review of AI-generated code in production, and 39% require AI-specific security scanning. Agent controls run thinner still: audit logging of agent actions stands at 45%, and evaluation before promotion at 12%. Provenance capture is arriving in organizations that have not yet governed far simpler controls (Figure 2).

Figure 2: AI Incidents Outrun AI Controls



Source: 2H 2026 SLE Decision Maker Survey, Futurum Research, June 2026

Ownership shifts toward platform engineering: mirror topology, residency placement, and checkpoint policy become platform-managed resources. Review practice moves from line-level diff inspection toward intent and rationale review. Procurement calculus changes last and matters most: exit rights over the accumulated reasoning graph will be worth more than favorable per-seat pricing, because the corpus grows with every commit.

The CIO and Tech Buyer Lens

The purchase decision lands here, and it lands awkwardly: for CIOs, Entire straddles three budget categories at once: developer tooling, infrastructure, and governance risk. That straddle slows procurement: the buyer who funds faster clones is rarely the buyer accountable for a new corpus of decision data, and the reasoning graph pulls the CISO, legal, and data governance into what looks at first like a developer productivity purchase.

CIO consolidation posture works against a preview-stage startup company in the most sensitive layer of the toolchain. Entire is asking enterprises to add a pre-pricing vendor to the record of how their software is made. The counterweights are Dohmke's and Driver's track record and the delay penalty: unrecorded history can never be rebuilt.

Selling into this layer requires a governance-first motion, and a few developer-tools vendors do so. Entire and its competitors must arrive with the security review packet, residency options, and portability terms already drafted. Developer-led adoption creates pull; it does not clear procurement when the product records how the company builds software.

The pitch splits by audience: throughput for engineering leaders, audit evidence for the CISO, and compliant delivery speed for the business units that increasingly fund agent initiatives. Incumbents hold the opposite hand: GitHub and GitLab can sell no new vendor and no new data store, so challengers must make neutrality and portability concrete enough to outweigh consolidation. Free tiers create the land; enterprise controls decide whether anything expands.

What to Watch

- Native session capture and agent-scale infrastructure commitments from GitHub over the next two to three quarters would narrow Entire's wedge to neutrality alone.
- Open confirms the control point sits in graph services; closed converts provenance into lock-in.
- Continued silence on exit rights should harden buyer caution.
- Entire plans to eventually host new repositories natively. That move ends the complementary framing and tests whether M12's cooperative posture survives.

Read the launch details in DevOps.com's [coverage of Entire's announcement](#).

Other Insights from Futurum

[Microsoft Build 2026 – The Platform, Integration Plane, and Developer Surface](#)

[IBM and Red Hat Bet \\$5B on Curating the Open Source Supply Chain](#)

[Google I/O: Did Google Just Ship the Full AI Stack?](#)

[MuleSoft Omni Gateway: As Close to an Agent Control Plane as It Gets](#)

[Bedrock Advanced Prompt Optimization Cuts the Cost of Model Switching](#)

About Us

About the Author

Mitch Ashley is VP and Practice Lead for the CIO & Technology Buyers and Software Lifecycle Engineering practices at The Futurum Group. A multi-time CIO and CTO with 30+ years leading technical organizations, Mitch built and operated production systems spanning cybersecurity for the U.S. Department of Defense, PKI services for the broadband, 5G, and IoT industries, SaaS platforms, large-scale telecom and banking systems, and a nationwide broadband network. His work with AI began early, developing expert systems that diagnosed and repaired complex mainframe environments. That operator foundation grounds his analysis in operational consequence, covering the technology buyer's world of software engineering, cybersecurity, DevOps, cloud, and AI. Mitch can be reached at mashley@futurumgroup.com.

About The Futurum Group

Every day, The Futurum Group's analysts, researchers, and advisors help business leaders worldwide anticipate tectonic shifts in their industries and leverage disruptive innovation. Unlike traditional analysts, The Futurum Group works not only in analysis and research but also takes that insight and knowledge even further, engaging all the way through the go-to-market process.

Futurum Research provides in-depth research and insights on global technology markets using advisory services, custom research reports, strategic consulting engagements, digital events, go-to-market planning, and message testing. It also creates, distributes, and amplifies rich media content that all stakeholders read, watch, and listen to.

See more details on The Futurum Group at futurumgroup.com.

Copyright & Use License

Copyright Notice

Copyright ©2026 by The Futurum Group, LLC. All rights, including that of translation into other languages, are specifically reserved. No part of this publication may be reproduced in any form, stored in a retrieval system, or transmitted by any method or means, electrical, mechanical, photographic, or otherwise, without the express written permission of The Futurum Group futurumgroup.com. United States copyright laws and international treaties protect this publication. Unauthorized distribution or reproduction of this publication, or any portion of it, may result in severe civil and criminal penalties and will be prosecuted to the maximum extent necessary to protect the publisher's rights.

License Notice

This document may be distributed within the licensed organization only.

The following acts are prohibited:

Transmittal to others outside your immediate organization including partners, resellers, external consultants, etc. in any media format

Posting on a website which is accessible to others outside your immediate organization

The possession or use within an unlicensed organization

Limitation of Liability Notice

The information contained herein has been obtained from sources believed to be reliable. The Futurum Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve their intended results. The opinions expressed herein are subject to change without notice.