SMART TECHNOLOGY INVESTMENTS

Tech Brief — AI Agents and Robotics

Oct 22–Oct 29, 2025 | Sources: 4 | Confidence: 0.8

Executive Summary

AI agents and cloud to edge architectures are rapidly reshaping enterprise software, infrastructure and operations. Key signals, clustered multi agent robotics, predictions of 100 to 1000 times more agents per user, continuous autonomous cybersecurity, and demand for human in the loop correction, point to explosive agent proliferation, hybrid compute demand and consumption based pricing. Operators must reorganize around ML SRE: build agent lifecycle pipelines (training, canary deploys, monitoring, HITL correction, rollback), invest in low latency telemetry, edge accelerators, secure control planes and metering to control inference costs and blast radii. Investors should reprice software economics toward revenue per agent, favoring agent platforms, hybrid orchestration, edge chips, autonomous security and observability vendors while modeling compute sensitivity, regulatory and security risks. BD teams should pursue vertical, outcome focused pilots (continuous remediation, back office automation, robot learning), partner with cloud, chip and integrators, and offer SLA backed managed services and transparent consumption pricing. Immediate recommended actions: run narrow ROI pilots with HITL controls, instrument metering and audit trails, adopt canary and rollback policies, contract SLA aligned managed operations and prioritize partnerships with cloud and hardware vendors. Firms that combine scalable agent infrastructure, domain specialization, HITL controls and consumption billing will capture disproportionate value.

Topline

Hybrid cloud-to-edge robotics software uses cloud plus local compute and agent clusters to split natural-language prompts into subtasks, accelerating robot training; combined with Box's prediction of 100x–1000x more AI agents in enterprise SaaS, it signals rapid scaling of agent-driven automation.

Signals

2025-10-27 — Mbodi (Xavier Chi) announced a cloud-to-edge hybrid robotics software that uses two compute layers (cloud + local) and a cluster of AI agents to break user natural-language prompts into subtasks to train robots faster. — strength: Medium | impact: Medium | trend: ↗ [1]

MEDIUM

MEDIUM

↗

2025-10-29 — Box CEO Aaron Levie stated onstage at TechCrunch Disrupt that enterprise SaaS will run about 100× to 1,000× more AI agents than people, implying SaaS customers will see a 100x–1000x increase in agent users relative to human users. — strength: High | impact: High | trend: ↗ [2]

HIGH

HIGH

↗

2025-10-28 — Cogent is operating autonomous cybersecurity agents that continuously (24/7) identify, prioritize and remediate vulnerabilities for enterprise customers, enabling nonstop remediation. — strength: Medium | impact: High | trend: ↗ [3]

MEDIUM

HIGH

↗

2025-10-27 — Industry reporting in the Wall Street Journal this week highlighted the need for human-in-the-loop correction interfaces so 'anyone' can correct a robot and specify behaviors, enabling real-time corrective instructions in natural language per deployed robot. — strength: Low | impact: Medium | trend: → [6] [1]

LOW

MEDIUM

→

Market Analysis

The rapid rise of AI agents and hybrid cloud-to-edge systems is reshaping pricing power across enterprise software, infrastructure, and services Platform owners — cloud providers, large SaaS vendors and edge-compute suppliers — are positioned to capture disproportionate pricing leverage because agent-driven workflows increase consumption of compute, storage and orchestration layers (hybrid cloud + local compute) that vendors like Mbodi are building into robotics stacks [^1] Simultaneously, enterprise software business models are moving away from per-seat licensing toward volume- and consumption-based pricing for agent usage, a shift explicitly predicted by Box CEO Aaron Levie and likely to concentrate pricing power with firms that control metering, APIs and billing surfaces for agents [^2] Managed-service providers and outcome-focused vendors (autonomous cybersecurity, SLA-driven automation) also gain leverage because customers will pay premiums for guaranteed remediation, uptime and compliance [^3]

Capital flows are following the agent opportunity: investors are directing funding into agent-native startups that offer immediate ROI (e.g., continuous cybersecurity remediation, back-office automation and vertical accounting agents) as illustrated by recent company profiles in the market [^3] Venture and strategic capital is also flowing into cloud-edge orchestration and robotics

software that enable faster real-world learning and data capture — exactly what investor-backed companies such as Mbodi are commercializing [^1] TechCrunch coverage suggests heightened VC interest in agent platforms and tools, reflecting expectations of multiplicative agent counts per human user and corresponding revenue opportunities tied to consumption metrics [^5] At the same time, enterprises are redirecting internal CapEx and IT budgets toward agent deployment, telemetry, and human-in-the-loop tooling, driven by operational risk and ROI considerations noted in industry reporting [^6] Infrastructure investment trends show a clear bias toward hybrid architectures and continuous operational tooling

Firms are funding cloud-to-edge deployments for robotics and real-time systems so models can be trained and corrected in situ, and so agents can operate with low latency and resiliency [^1] There is parallel investment in always-on security stacks and autonomous remediation systems that monitor and act 24/7, reducing mean time to remediation and supporting business continuity [^3] Enterprises and consultancies are also investing in agent-building platforms, governance layers, and integration workstreams to embed agents into core workflows at scale [^4] Market structure is fragmenting and consolidating simultaneously New specialist entrants (agent vendors for cybersecurity, customer support, accounting, robotics) are proliferating, creating a long tail of verticalized players [^3]

At the same time, incumbent SaaS and cloud providers are poised to consolidate by acquiring agent tech or bundling agent capabilities into existing offerings to maintain control over billing and data ingestion points, a logical response to the shift away from per-seat models [^2] Professional services and systems integrators (e.g., Big Four players) are expanding their role as implementers and governors of agent programs, embedding consulting revenue into long-term service contracts [^4] Supply-chain and operational impacts are material Physical-world deployments require new hardware (edge compute, sensors, robotics components) and reliable supply chains for chips and edge devices, increasing demand for specialized suppliers and integration partners [^1] Continuous, autonomous agents change operational models — from episodic updates to ongoing human-in-the-loop correction interfaces and real-time supervision — shifting hiring toward ML ops, site reliability and governance roles [^6]

Finally, managed-agent operators (customer support, back-office, security) will alter support models and vendor SLAs, compressing incident-response timelines while introducing new dependencies on vendor-managed telemetry and remediation capabilities [^3].

Technology Deep-Dive

Model architectures and chip developments — The recent wave of multi-agent AI and cloud-to-edge robotics platforms highlights a shift from monolithic models to specialized, cooperating agent ensembles Mbodi's approach breaks natural-language prompts into subtasks that are handled by a cluster of communicating agents, accelerating task learning for robots by dividing and

conquering responsibilities and iterating from real-world data once deployed [^1] This multi-agent pattern favors smaller, task-specialized submodels and on-device inference for latency-sensitive control loops, rather than single huge models for all functions Aaron Levie's forecast that enterprise systems will host 100×–1,000× more agents than people implies explosive demand for inference capacity at scale, which will drive new chip and accelerator requirements — particularly efficient edge GPUs/TPUs or domain-specific ASICs to support many concurrent lightweight agents across hybrid cloud/local deployments [^2][^5]

While explicit chip designs are not detailed in the sources, the architectural signals (hybrid compute and massively parallel agents) point strongly to increased investment in edge accelerators and heterogeneous compute stacks to meet responsiveness and power constraints [^1][^2] Network infrastructure and automation stacks — Autonomous, always-on agent services such as Cogent's continuous vulnerability management and automated remediation demonstrate the need for robust orchestration, observability and secure connectivity between cloud control planes and edge endpoints [^3] Mbodi's cloud-to-edge robotics stack likewise requires low-latency telemetry, model update distribution, and data ingestion pipelines for on-device learning and feedback loops [^1] Enterprise deployments will layer agents on top of existing SaaS workflows, shifting traffic patterns from human-initiated interactions to high-volume machine-to-service calls; that will necessitate API rate management, fine-grained RBAC, and consumption-oriented metering in cloud infrastructure and networking stacks [^2][^4]

Automation platforms will increasingly include agent lifecycle management, rollback policies, and canary deployments to maintain reliability as agents proliferate [^3][^5] Technical risk assessment — Several technical risks arise from this architecture First, security and authorization risks increase when autonomous agents have remediation or action privileges: misconfigured or compromised agents can cause large blast radii, which platforms like Cogent explicitly aim to prevent via continuous prioritization and remediation workflows [^3] Second, scale-related complexity (100×–1,000× agent growth) creates operational and governance challenges: policy drift, inconsistent behavior across replicated agents, and orchestration bottlenecks are likely without strong standards and human-in-the-loop (HITL) interfaces for corrective control — a need emphasized by reporting that anyone may need to correct robots in real time via natural language interfaces [^6][^4]

Third, technical debt from ad hoc integrations of agents into legacy SaaS could accumulate quickly if consumption billing models and API contracts are not carefully designed to support versioning and backward compatibility [^2][^5] Performance and efficiency improvements — Multi-agent decomposition yields measurable efficiency gains by parallelizing subtasks and allowing specialized models to run at lower compute cost than a single large model performing all roles; Mbodi's fast robot training from clustered agents exemplifies this optimization path [^1] Domain-specific agent deployments (accounting, support, cybersecurity) benefit from transfer learning and policy distillation, where high-performing agent behaviors are replicated and tuned for cost-efficiency, as described by companies offering turnkey agent replication and agent-as-a-service models [^3] Economically, the move to consumption-based pricing tied to agent volume

incentivizes optimizations that reduce inference cost per agent and improve throughput per accelerator, lowering total cost of ownership for enterprises [^2][^3]

Integration and interoperability — The dominant integration pattern will be agents layered atop existing SaaS APIs and business workflows; agents must interoperate with established authentication, audit logging, and data schemas to be trusted in enterprises [^2][^4] Commercial offerings that replicate top-performing agents to align with company policies illustrate an ecosystem trend toward packaged, policy-compliant agent components that integrate end-to-end rather than as isolated toolkits [^3][^5] Finally, the industry will need standards for agent behaviors, telemetry, and human override APIs to ensure safe cross-vendor composition and to enable governance at scale — a requirement underscored by press coverage stressing HITL correction mechanisms for deployed robots and automated systems [^6]

Overall, the technical trajectory is toward heterogeneous, agent-oriented architectures running across cloud and specialized edge hardware, backed by new networking and orchestration primitives; realizing that vision will require focused work on security, governance, and efficient accelerator utilization as agent counts balloon in enterprise environments [^1][^2][^3][^4][^5][^6].

Competitive Landscape

Winners and losers Winners in the near term are startups and platforms that can (a) scale large numbers of AI agents, (b) embed human-in-the-loop correction, and (c) integrate across cloud and edge compute Startups such as Mbodi (cloud-to-edge robotics orchestration) and autonomous-agent cybersecurity firms like Cogent demonstrate those capabilities — Mbodi's cluster-of-agents approach and hybrid cloud/local architecture position it to capture robotics deployments that require fast real-world learning, while Cogent's continuous, autonomous vulnerability remediation addresses 24/7 enterprise security needs and drives clear operational ROI [^1][^3] Managed-agent specialists that provide end-to-end implementation (Notch, Basis) are also advantaged because enterprises prefer turnkey deployments that reflect corporate policies and tone of voice [^3] Losers will be incumbents that cling to per-seat SaaS pricing and architectures that can't economically support 100x–1,000x growth in agent users

Box's CEO forecasts a future with orders-of-magnitude more agents than people, which undermines per-seat economics and favors consumption or volume-based models — vendors that don't adapt pricing and agent-scale architectures risk losing share to consumption-first challengers [^2] Similarly, vendors that ignore human-in-the-loop correction interfaces will struggle with real-world robotic and agent failure modes called out in industry reporting [^6] White-space opportunity mapping 1) Cloud-to-edge orchestration for physical-world AI: Mbodi's model highlights a gap for hybrid compute stacks that let robots learn in situ while leveraging cloud models — a white space for toolchains, observability, and data pipelines optimized for physical deployments [^1] 2) Turnkey, policy-aligned managed agents: Demand exists for fully managed agent

services that replicate best-in-class human behaviors and compliance (Notch, Basis), especially in regulated industries and accounting firms [^3]

3) Human-in-the-loop tooling and interfaces: WSJ reporting and vendor demos show a need for easy corrective UIs so non-engineers can instruct agents and robots in natural language — an underserved UX/controls layer [^6] 4) Pricing & metering platforms for agent economies: With agent counts expected to balloon, marketplaces and billing infrastructures that meter agent usage will be needed [^2] Strategic positioning analysis Startups are positioning as verticalized, outcome-oriented providers (security, accounting, robotics) that either (a) replace discrete manual workflows or (b) attach to existing SaaS as agent layers Cogent and Basis emphasize domain specialization and continuous actionability [^3] Mbodi differentiates through hybrid architecture and real-world learning, positioning as robotics-native infrastructure rather than a pure cloud AI stack [^1] Large consultancies and professional services (EY) position themselves as enterprise integrators, democratizing agents across org levels and focusing on adoption and governance rather than raw model capability [^4]

Competitive dynamics Expect intensifying partnerships (agent vendors plugging into incumbent SaaS), talent-driven consolidation, and M&A as startups with domain traction are folded into larger security, enterprise software, or robotics portfolios Founders' pedigrees from Abnormal, Coinbase and others signal talent flows and ecosystem consolidation in cybersecurity and enterprise agents [^3] Box's public framing pressures incumbents to change pricing and partner models or acquire agent capabilities [^2] Market-share shifts and advantages Competitive advantage will accrue to firms that combine scalable agent infrastructure, domain specialization, human-in-the-loop controls, and viable consumption pricing Those capabilities map directly to market-share gains in robotics, security, and enterprise automation; firms slow to deliver them will cede share to agile, managed-agent players and cloud-to-edge specialists [^1][^2][^3][^6] Enterprise adopters and consultancies (EY) will moderate disruption by embedding agents responsibly, creating a two-speed market of fast-moving startups and integrator-led enterprise deployments [^4] [^5].

Operator Lens

The operator view centers on turning a surge of autonomous agents and cloud-to-edge robotics into reliable, safe, and cost-effective operations Systems and processes will shift from episodic project deliveries to continuous operation, where agents run 24/7, telemetry streams are constant, and model updates are frequent Expect teams to reorganize around agent lifecycle management: model build/train, canary deploy, monitoring, HITL correction, rollback, and automated remediation Traditional DevOps will converge with MLOps and Site Reliability Engineering to form ML-SRE teams responsible for observability, latency SLAs, and inference capacity planning Automation opportunities are significant

Routine incident remediation, vulnerability patch orchestration, and back-office tasks can be automated end-to-end, reducing MTTR and headcount for repetitive work Robots and physical agents can learn faster via in-situ training pipelines that shorten iterations However, automation challenges include runaway actions from misbehaving agents, policy drift across thousands of agent instances, and maintaining consistent behavior across replicated agents Human-in-the-loop tooling becomes a first-class control surface to correct behavior in real time, especially for physical-world systems Infrastructure and tooling implications are concrete: hybrid cloud-to-edge stacks, efficient edge accelerators, secure control planes, low-latency telemetry pipelines, and metering surfaces for consumption billing

Operators must deploy robust orchestration that supports frequent model rollouts, canarying, and fast rollbacks Observability needs to capture agent decisions, state, and provenance; audit trails and RBAC must be baked into agent APIs Cost-control tooling is essential to manage exploding inference and storage consumption as agent counts grow by orders of magnitude Operational risk and efficiency considerations are elevated Security posture must be rethought because agents with remediation privileges increase blast radius; privilege management, signed artifacts, and runtime attestation are mandatory Governance is required to prevent policy drift and to ensure regulatory compliance in regulated verticals

Staffing priorities will shift to ML ops, SRE, and governance engineers Efficiency gains depend on decomposing functionality into small, specialized agents that minimize per-agent compute, and on leveraging transfer learning and distillation to reduce inference cost Finally, operators must adopt SLA-driven contracts with vendors to ensure predictable outcomes and embed fallback human workflows for edge-case recovery.

Investor Lens

The investor view sees this wave as a structural re-pricing of software economics and infrastructure demand Agent proliferation converts per-seat SaaS into consumption markets; revenue growth will decouple from headcount growth and instead track agent volume, API calls, and inference hours High-level investment opportunities include agent platforms and orchestration for cloud-to-edge deployments, autonomous security and remediation providers, managed-agent service vendors, edge accelerator and chipmakers, and observability/metering firms

Capital is already rotating: venture dollars will flow into agent-native startups that show immediate operational ROI, while strategic and public-market capital will push into cloud providers and infrastructure vendors that capture metering and billing surfaces Expect M&A as incumbents acquire agent capabilities to protect gross margins and reassert control over data ingestion and billing Valuation models will emphasize revenue per active agent, gross margin sensitivity to compute costs, and stickiness from embedded governance and HITL workflows Valuation implications and risk factors are nuanced

Consumption models can boost upside because they scale with usage, but they introduce revenue variability and sensitivity to unit economics of inference Firms that control metering, APIs, and billing have pricing power; pure-play vendors without differentiation may face margin compression from rising compute bills Key risks include large-scale security incidents, regulatory scrutiny about autonomous decisioning, integration complexity with legacy systems, and talent scarcity for ML ops and edge engineering Tickers and themes to watch: cloud and platform providers that own control planes — MSFT, AMZN, GOOGL — will benefit from agent-hosting and marketplace capture

Semiconductor leaders supplying inference accelerators — NVDA, AMD, INTC — are direct beneficiaries of increased inference demand, with NVDA particularly exposed to datacenter and edge GPU demand Security and autonomous remediation plays include CRWD, PANW, FTNT and ZS, which can layer agents into existing offerings Observability and metering plays include DDOG and SPLK SaaS vendors that embrace consumption monetization and partner models — BOX and NOW — are interesting to track for business-model transitions Professional services and integrators such as ACN stand to gain from implementation spend

Allocate capital across infrastructure, security, and managed-agent services while building scenario-based models that stress-test compute cost, regulatory drag, and customer adoption curves.

BD Lens

From a business development perspective, agents and hybrid cloud-to-edge stacks open many GTM wedges and partnership plays The primary BD strategy is to identify high-ROI vertical workflows — continuous vulnerability remediation, back-office accounting automation, and physical-robot learning loops — and build outcome-focused offerings that replace manual toil Positioning should emphasize guaranteed outcomes (MTTR reduction, cost savings) and consumption-aligned pricing to ease procurement friction Partnership opportunities are rich Cloud providers offer co-sell and marketplace channels for agent runtimes and metering Chip and hardware vendors can be OEM partners for edge-accelerated appliances

Security vendors and MSSPs are natural collaborators for autonomous remediation bundles Systems integrators and consultancies are distribution partners for large enterprise rollouts; co-delivered managed services reduce internal implementation friction and increase stickiness Market entry strategies should favor verticalization and pilot-first motions Start with a narrowly scoped pilot that demonstrates concrete ROI and embeds HITL controls to reassure stakeholders Use pilot outcomes to create templated agent packs for rapid replication in adjacent accounts and industries Differentiate by offering turnkey integrations to popular SaaS platforms and by providing out-of-the-box governance, audit trails, and policy-compliant agent templates

Competitive positioning must stress hybrid-cloud-to-edge capability, human-in-the-loop tooling, and billing transparency Offer value props that incumbents struggle to copy quickly, such as fast real-world robot learning, continuous autonomous remediation workflows, and pre-built compliance modules For customer acquisition, target CIOs for infrastructure concerns, CISOs for security automation, and business ops leaders for productivity use cases Leverage case studies showing measurable reductions in MTTR, headcount reallocation, and improved throughput to accelerate procurement Retention strategies include embedding agents into core workflows, offering agent replication and policy-tuning services, and providing SLA-backed managed operations

Channel plays with MSPs and consultancies will broaden distribution while co-selling with cloud providers accelerates enterprise trust Be mindful of pricing conflicts with incumbent vendors; design partnership agreements that clarify resale, data ownership, and metering to avoid channel friction Focus BD on delivering fast, measurable outcomes and on institutionalizing agents through governance and ongoing managed services.

Sources

[1]

Mbodi will show how it can train a robot using AI agents at TechCrunch Disrupt 2025 - TechCrunch

TechCrunch, 2025-10-27. (cred: 0.90)

https://techcrunch.com/2025/10/27/mbodi-will-show-how-it-can-train-a-robot-using-ai-agents-at-techcrunch-disrupt-2025/

[2]

Box CEO Aaron Levie on how AI is changing the enterprise SaaS landscape - TechCrunch

TechCrunch, 2025-10-29. (cred: 0.90)

https://techcrunch.com/2025/10/29/box-ceo-aaron-levie-on-how-ai-is-changing-the-enterprise-saas-landscape/

[3]

Meet the AI Disruptors 60: The Startups Defining AI's Future - TechCrunch

TechCrunch, 2025-10-28. (cred: 0.90)

https://techcrunch.com/sponsor/greenfield-partners/meet-the-ai-disruptors-60-the-startups-defining-ais-future/

[6]

Afraid to Try AI? These Tech-Savvy Seniors Will Change Your Mind - The Wall Street Journal

Wall Street Journal, 2025-10-25. (cred: 0.80)

https://www.wsj.com/tech/ai/afraid-to-try-ai-these-tech-savvy-seniors-will-change-your-mind-2e3c5441