SMART TECHNOLOGY INVESTMENTS

Tech Brief — AI Agents and Cybersecurity

Oct 22–Oct 29, 2025 | Sources: 3 | Confidence: 0.8

Executive Summary

Recent signals show a sharp bifurcation: AI-native, always-on agent platforms (autonomous cybersecurity, workflow and CX agents) are gaining pricing power, enterprise adoption and investor capital, while commodity sectors and expeditionary defense initiatives face headwinds from tariffs and weak troop commitments. Operators should treat action-capable, 24/7 agents as platform shifts: redesign workflow engines for durable state, enforce least-privilege, instrument immutable audit trails, and run staged pilots with tight rollback and human-in-the-loop gating to limit blast radius. Investors should prioritize firms with measurable ROI, recurring SLAs, compliance certifications (ISO 27001, SOC 2, HIPAA options), and scalable inference stacks; favor infrastructure plays (accelerators, hybrid cloud, observability) and reprice exposure to tariff-exposed commodities and troop-dependent contractors. Business development must sell outcomes, pursue regulated vertical pilots, partner with MSSPs/SIs, and bundle trade-compliance and logistics solutions for tariff-impacted customers. Immediate actions: deploy narrow autonomous workflows for low-risk, high-frequency use cases; obtain certifications and strong auditability to accelerate procurement; optimize models and hardware for 24/7 inference economics; and pivot defense sales toward non-combat cyber, ISR and training services. These moves capture upside from automation while mitigating geopolitical and supply-chain risk. Prioritize certified pilots, partner with cloud and hardware vendors, and monitor policy shifts closely for strategic positioning.

Topline

Most potential contributing countries likely to commit zero combat troops to a proposed force, signaling low chance of deployments; meanwhile Cogent's autonomous agents run 24/7 to continuously identify and remediate vulnerabilities, reducing exposure windows and strengthening cyber resilience.

Signals

2025-10-27 — H.A. Hellyer (senior associate fellow, Royal United Services Institute) said most potential contributing countries are likely to commit 0 combat troops to a proposed force (majority: >50%), signalling low likelihood of troop contributions. — strength: Medium | impact: Medium | trend: ↘ [1] [3]

MEDIUM

MEDIUM

↘

2025-10-28 — Cogent (AI-native cybersecurity platform) is reported to operate autonomous agents that continuously identify, prioritize, and remediate vulnerabilities — agents running 24/7 (168 hours/week) to reduce exposure windows. — strength: High | impact: High | trend: ↗ [2] [3]

HIGH

HIGH

↗

2025-10-29 — Paid announced AI agents that run whole operations workflows and take action (not just suggestions), meaning routine approvals and vendor onboarding processes can be executed autonomously — agents available to operate 24/7 (168 hours/week) for routine tasks. — strength: Medium | impact: High | trend: ↗ [2] [1]

MEDIUM

HIGH

↗

2025-10-30 — Maven (customer experience AI) is certified to ISO 27001 and SOC 2 Type II and offers HIPAA-compliant deployments, i.e., holds 2 named security certifications and 1 HIPAA-compliant deployment option. — strength: High | impact: Medium | trend: → [2] [1]

HIGH

MEDIUM

→

FORECAST

2025-10-31 — The government of British Columbia (Ravi Parmar, Minister of Forests) launched 1 digital ad campaign this week highlighting that US tariffs on Canadian lumber exceed those on Russian lumber, targeting U.S. audiences about rising forestry tariffs. — strength: Medium | impact: Medium | trend: ↗ [3] [2]

MEDIUM

MEDIUM

↗

FORECAST

2025-11-01 — Arab countries (collectively) stated they would withhold participation in a multinational force unless there is a single major diplomatic push to create a Palestinian state — conditioning participation on 1 major political/diplomatic initiative. — strength: Medium | impact: High | trend: ↘ [1] [2]

MEDIUM

HIGH

↘

FORECAST

Market Analysis

Summary: Recent signals point to pronounced bifurcation in pricing power and capital flows between fast-growing AI/automation cybersecurity vendors and legacy commodity sectors (notably forestry and traditional defense contracting) These shifts are reshaping investment, infrastructure funding, and supply-chain configuration across technology, natural resources, and security services.[^2][^3][^1] Pricing power dynamics: AI-native vendors that deliver autonomous, 24/7 agents (examples: Cogent, Paid, Maven) are accruing strong pricing leverage because they convert security and operations from fixed-headcount cost centers into productized, always-on services with measurable risk reduction and compliance credentials (ISO 27001, SOC 2, HIPAA) that justify premium pricing and recurring revenue models.[^2] By contrast, commodity sectors such as Canadian lumber face price compression and margin pressure due to tariff-driven market distortions — government-imposed U.S

tariffs are shifting effective demand and reducing exporters' bargaining power even as they pursue public diplomacy to mitigate the hit.[^3] Geopolitical clarity (or the lack of it) also affects defense suppliers' pricing leverage: widespread reluctance among prospective troop-contributing countries reduces predictable large-scale procurement for coalition operations, weakening demand-side leverage for certain defense contractors focused on expeditionary hardware and services.[^1] Capital flow patterns: Venture and growth capital is flowing heavily into automation and AI-native cybersecurity platforms that offer clear ROI through operational substitution (agents automating onboarding, approvals, continuous remediation), and into firms that can demonstrate enterprise-grade compliance — a magnet for corporate and strategic investors.[^2][^3] Simultaneously, capital is repricing exposure to natural-resource exporters facing tariff risk; some investment is likely to retrench from cross-border timber trade into domestic processing or alternative markets, while opportunistic capital may seek bargains if tariffs depress asset valuations.[^3] Reduced appetite for multinational kinetic deployments — signalled by limited troop

commitments — redirects public and private capital away from large coalition logistics programs toward remote ISR, cyber, and contractor-enabled security solutions.[^1][^2] Infrastructure investment trends: Funding is concentrating on cloud-native, secure AI infrastructure (agent platforms, integration middleware, compliance tooling) and on hardened cybersecurity operations that run continuously.[^2] In physical infrastructure, tariff-driven market shifts incentivize investments in alternative supply routes, storage, and domestic processing capacity for lumber markets to reduce exposure to cross-border duties.[^3] Planned on-the-ground multinational force infrastructure (bases, staging, logistic hubs) is less likely to receive broad international investment given low troop-commitment expectations, which will favor investment in deniable/low-footprint capabilities instead.[^1] Market structure changes: The AI-agent field is heating up with multiple specialized entrants (Cogent, Paid, Maven), setting the stage for rapid consolidation as incumbents buy capabilities to accelerate time-to-market, or as weaker startups are picked off.[^2][^3] In forestry and commodities, tariffs and political campaigning can accelerate consolidation among exporters and downstream processors as firms seek scale to absorb trade shocks.[^3] Defense and security markets may see strategic pivots and M&A as firms move from traditional force-support contracts toward cyber, ISR, and private security services.[^1] Supply chain and operational impacts: Autonomous agents reduce operational headcount and speed vendor onboarding/approval cycles, shifting supplier negotiation leverage toward platform providers and away from manual service providers.[^2] Tariff disruptions in lumber create immediate rerouting, inventory stocking, and price hedging behaviors in construction supply chains, raising near-term costs for builders and altering sourcing decisions.[^3] Finally, constrained multinational troop contributions increase reliance on remote force-multipliers (private contractors, cyber operators, and logistics firms), changing procurement and operational models for suppliers across the security ecosystem.[^1][^2]

Technology Deep-Dive

Model architectures and chip developments: Recent vendor announcements and product positioning point to a shift from suggestion-only LLM agents to closed-loop, action-capable agents that run continuous operational workflows Startups described in the reporting build agents that not only recommend steps but take actions across systems, implying heavier reliance on low-latency inference and persistent state management in production models [^2] That operational profile favors architectures optimized for fast, deterministic inference (e.g., trimmed transformer variants, quantized LLMs, and inference-optimized encoder–decoder hybrids) and suggests accelerating demand for inference-centric silicon (GPU/TPU-class accelerators and domain-specific ASICs) Market dynamics referenced in coverage of dominant chip vendors and macro sentiment further reinforce pressure on custom silicon and scale-out GPU farms to sustain 24/7 agent operation and real-time orchestration at enterprise scale [^3]

Geopolitical constraints on physical deployments — such as reluctance of national actors to contribute ground resources to multinational forces — also affect decisions about distributed edge

compute and ruggedized hardware placement in sensitive regions, adding a non-technical but material constraint to hardware rollouts and supply-chain choices [^1] Network infrastructure and automation stacks: The new generation of autonomous agents described are inherently integrative: they hook into multiple SaaS tools, identity systems, and orchestration layers to execute vendor onboarding, approvals, and compliance flows without human step-ins until required [^2] That pattern drives requirements for robust API gateways, event-driven message buses, service meshes for distributed microservices, and secure token exchange (OIDC, mTLS) across toolchains Cloud-native automation stacks will need to combine workflow engines (Durable Tasks, Temporal-like), observability pipelines, and policy-as-code (OPA/Rego) to balance autonomy with auditability

Additionally, continuous vulnerability remediation agents described imply real-time telemetry ingestion, threat scoring, and automated patch orchestration — elevating the role of telemetry pipelines and automated incident runbooks as part of the network fabric [^2] Bloomberg signals the commercial imperative to integrate market and operational data streams (including premium terminal feeds) into decisioning layers, which further pressures low-latency private links and hybrid cloud interconnects for regulated enterprises [^3] Technical risk assessment: Security and compliance risk is front-and-center Autonomous remediation agents reduce human latency but expand blast radius if misconfigured — a single agent with broad privileges can both remediate and inadvertently disrupt services; careful least-privilege architectures and strong approval gating are necessary [^2] Startups offering ISO 27001 and SOC 2 Type II certifications and HIPAA-capable deployments indicate enterprises are demanding formal controls, but certification does not eliminate zero-day or supply-chain risks from underlying model providers or hardware vendors [^2]

Scalability challenges include state management across long-running workflows, model drift from continuous learning, and cost blowouts from 24/7 inference unless models are aggressively optimized or offloaded to specialized accelerators [^2][^3] Finally, geopolitical and political constraints (e.g., conditional participation in multinational efforts) create operational and supply-chain risk vectors that can delay or constrain distributed infrastructure projects in certain regions [^1] Performance and efficiency improvements: Reported agent deployments running 168 hours/week highlight the potential for outsized efficiency gains (reduced headcount, faster mean-time-to-remediate) when automation is safe and well-instrumented [^2] Realizing those gains will depend on model optimizations: pruning, quantization (INT8/4-bit), distillation to smaller architectures for common sub-tasks, and hardware-aware compilation (TVM, XLA) to lower inference cost

On the hardware side, continued consolidation around GPU/accelerator vendors and the economics of scale (data-center utilization, spot-instance strategies) will drive cost per inference down — but market concentration and valuation dynamics flagged in industry coverage create a countervailing systemic risk for supply and pricing [^3] Integration and interoperability: The practical adoption path is through standardized APIs, certifiable security baselines, and cross-vendor connectors Firms advertising plug-and-play agent integrations and compliance certifica-

tions point toward an ecosystem where interoperability layers (well-documented REST/gRPC APIs, semantic event schemas, and connector ecosystems) are the primary route to enterprise adoption [^2] Financial and market data integration (including premium feeds) further requires contractual and technical gating for latency, provenance, and entitlements, emphasizing the need for unified identity and policy enforcement across disparate services [^3]

Finally, geopolitical constraints on multinational participation underscore the importance of flexible deployment topologies (cloud, hybrid, on-prem, edge) to meet both regulatory and operational requirements [^1].

Competitive Landscape

Winners and losers: AI-native automation vendors are emerging as clear winners while legacy, manual providers and geopolitically exposed initiatives face headwinds Startups such as Cogent (autonomous cybersecurity agents), Paid (action-taking operations agents), and Maven (customer-experience agents with ISO 27001, SOC 2 Type II and HIPAA options) are positioned to steal share from incumbent security, operations and CX vendors because they promise continuous, autonomous remediation and 24/7 execution that materially reduce exposure windows and operational headcount needs [^2] By contrast, traditional vulnerability-management and workflow vendors that only surface suggestions or depend on human-driven processes risk losing relevance unless they add active remediation and agent-driven automation [^2]

At a macro level, multilateral security initiatives seeking troop contributions are losing momentum as major potential contributors signal they will not commit combat troops, weakening demand for systems tied to expeditionary combat deployments and shifting near-term opportunities away from combat logistics to diplomatic, training and non-combat support services [^1] Political conditionality among Arab states further reduces the likelihood of broad participation, creating losers among prime contractors banking on a robust multinational force [^1] Whitespace opportunity mapping: There are multiple underserved niches First, enterprises in regulated industries need certified AI agents — a gap Maven explicitly targets with ISO/SOC/HIPAA compliance, creating an opening for more certified agent platforms for healthcare, finance and government customers [^2] Second, there is a whitespace for fully autonomous remediation in cybersecurity (beyond alerting), where Cogent's continuous 168-hours/week agents are a blueprint for reducing breach windows and creating a defensible technical moat [^2]

Third, geopolitical and trade friction (e.g., tariff-driven campaigns like British Columbia's digital ad push on lumber tariffs) opens demand for trade-compliance automation, rapid reputational-response platforms, and risk-advisory SaaS that fuse political signals with supply-chain execution — an underserved intersection between geopolitical intelligence and operations software [^3][^1] Strategic positioning analysis: Cogent frames itself as an AI-native defender that continuously identifies, prioritizes and remediates vulnerabilities — selling outcomes (reduced exposure)

rather than tools [^2] Paid differentiates by promising agents that take end-to-end operational actions (vendor onboarding, approvals) with human-in-the-loop governance, positioning itself for headcount-sensitive enterprises [^2] Maven leans into trust and regulation with certified deployments to win highly regulated clients [^2] Governments and defense-related vendors are being forced to reposition from combat-capable offerings toward coalition management, training, and non-combat support given the low likelihood of troop commitments [^1]

Competitive dynamics and responses: Expect partnerships and M&A as incumbents seek to buy AI-native capabilities rather than build them; managed security providers will partner with or acquire agent platforms to offer autonomous remediation at scale [^2] Defense primes and contractors will pivot to advisory, logistics, and platform-enabled non-combat services in response to coalition reluctance, while regional actors and NGOs could fill niche support roles [^1] Trade-policy shocks will drive public campaigns and a need for tech-enabled advocacy and compliance — creating alliances between policy shops and digital platforms [^3] Market-share shifts and advantages: Firms that deliver demonstrable 24/7 autonomous execution and that hold security/regulatory certifications will gain disproportionate share, given measurable ROI (reduced breaches, faster vendor onboarding, consistent CX) and lower procurement friction in regulated sectors [^2] Incumbents that delay integrating autonomous agents or obtaining certifications will cede share

Meanwhile, geopolitical uncertainty redistributes addressable markets away from large-scale troop-dependent contracts toward software-enabled, non-combat services and trade-risk solutions [^1][^3].

Operator Lens

Operators must treat the arrival of action-capable, always-on AI agents as a platform-level transformation rather than a point tool Systems and processes will shift from human-mediated, batch workflows to continuous automated pipelines that run 24/7 and hold persistent state Practically this means: redesigning change-control and approval flows for machine actors; building durable workflow engines that support long-running state, checkpoints, and rollback; and instrumenting every action with immutable audit trails and fine-grained policy enforcement Automation opportunities and challenges - Opportunities: automate vendor onboarding, routine approvals, continuous vulnerability identification and remediation, and customer-experience tasks that are highly repetitive

This reduces MTTR, staffing needs for repetitive tasks, and latency in compliance workflows Agents that can act (not only suggest) create clear ROI levers for headcount substitution and faster time-to-value - Challenges: expanding blast radius if agents are over-privileged or misconfigured; model drift producing incorrect actions over time; state explosion for long-running flows; and balancing autonomy with human oversight when failures are rare but high impact Infrastructure and tooling implications - Core platform needs: workflow orchestration (temporal-like), event buses, service meshes, API gateways, secure token and identity integration (OIDC, mTLS), and policy-as-code for real-time governance (OPA/Rego)

- Observability and telemetry: high-cardinality logging, distributed tracing, policy audit logs, and model action provenance pipelines to support forensic and compliance needs - Compute and hardware: sustained 24/7 inference accelerates demand for inference-optimized silicon, efficient model runtimes (quantization, pruning), and cost control patterns like spot-instance scheduling and model-offload tiers - Deployment topologies: hybrid and on-prem options will be required for regulated workloads (HIPAA, government) and to respect geopolitical constraints on edge placement Operational risk and efficiency considerations - Security posture: enforce least-privilege and just-in-time credentialing; adopt strong approval gating and human-in-the-loop thresholds for high-risk actions

- Compliance: certifications (ISO 27001, SOC 2 Type II, HIPAA-capable deployments) reduce procurement friction but do not eliminate zero-day/model supply-chain risk; continuous control testing is required - Cost/efficiency: mitigate runaway inference costs via model distillation, quantization, caching, and tiered action policies (auto-remediate low-risk, human-oversight for high-risk) - Change management: reskill ops teams toward supervision, policy management, and incident playbook development Run staged pilots with narrow scopes and tight rollbacks to validate safe autonomy before scaling.

Investor Lens

Macro signal: capital is rotating toward AI-native automation and continuous cybersecurity providers while repricing exposure to commodity exporters and combat-centric defense plays Public and private markets are likely to reward vendors that demonstrate measurable operational outcomes, enterprise-grade compliance, and the ability to run persistent agents at scale Market impact and investment opportunities - Winners: AI-native cyber and ops automation companies that deliver active remediation, end-to-end agent workflows, and certified deployments Infrastructure plays that enable 24/7 agent operation (inference accelerators, workflow platforms, observability and identity stacks) also benefit

- Sectors to watch: autonomous cybersecurity, workflow automation, observability/GRC, inference hardware, hybrid cloud interconnects, and compliance-first SaaS for regulated industries Sector rotation and capital allocation - Growth capital will favor startups with product-market fit in regulated verticals (healthcare, finance, gov) and enterprises demonstrating contractable SLAs around continuous remediation - Capital will retrench from commodity exporters facing tariff risks (timber) and from contractors heavily exposed to large expeditionary deployments, reallocating into software, cloud infra, and private security/cyber services Valuation implications and risk factors - Valuations: premium multiples for recurring revenue and demonstrable ROI (reduced breach costs, faster onboarding)

Certification (ISO/SOC/HIPAA) materially lowers buyer friction and can justify higher multiples - Risks: model failure or major security incident causing reputational damage; acceleration in inference costs if hardware supply is constrained; regulatory backlash (automated actions in sensitive domains); and geopolitical shifts that change addressable markets for defense and commodity plays Specific tickers and investment themes (research-oriented, not advice) - Cyber and security software: CrowdStrike, Palo Alto Networks, SentinelOne, Zscaler for enterprise-grade detection/response and partner ecosystems - Infrastructure and cloud: Nvidia, AMD, Intel for accelerators; Microsoft, Google, AWS for managed inference and hybrid cloud services

- Observability and identity: Datadog, Okta, Splunk for telemetry and identity plumbing - Defense/cyber services: Leidos, Booz Allen for non-combat ISR and cyber services; traditional primes (Lockheed Martin, Raytheon) may see near-term headwinds on expeditionary buys but remain long-term strategic plays - Commodities/forestry exposure: re-evaluate timber-linked equities and consider downstream processors and domestic substitutes as hedges Private markets: favorable environment for growth investments and M&A where incumbents buy agent capabilities Look for capital-efficient startups with compliance certifications, revenue-based pricing, and managed-service GTM via MSSP channels.

BD Lens

The commercial playbook should center on outcome selling, integration depth, and compliance assurances 24/7 autonomous agents open a clear wedge for vendors that can demonstrate reduced MTTR, automated onboarding throughput, and certified operations Business development opportunities - Offer outcome-based contracts (SLA for mean-time-to-remediate, vendor onboarding throughput) and usage-based pricing for active remediation minutes or workflows executed - Target regulated verticals first (healthcare, finance, government) where certifications accelerate procurement and where HIPAA-capable deployments are a competitive differentiator Partnership and collaboration prospects - MSSPs and managed service partners: bundle agent platforms with SOC services to accelerate adoption and provide human oversight tiers

- SI and workflow vendors: deepen integrations with ServiceNow, Jira, identity providers (Okta), SIEMs, and EHR systems to become the default action layer - Cloud and hardware partners: partner with cloud providers for validated reference architectures and with accelerator vendors for cost-optimized inference footprints - Policy and public affairs: for customers in tariff-impacted industries (lumber), partner with trade-advisory firms and logistics providers to bundle compliance and supply-chain mitigation services Market entry strategies and competitive positioning - Penetrate via pilots addressing high-frequency, low-risk workflows (routine approvals, vendor onboarding, low-impact patching) and then expand to higher-risk automations once controls are proven

- Differentiate on certifications and on human-in-the-loop governance: market the combination of always-on automation plus strict approval gates and auditability - Leverage case studies that quantify headcount savings, remediation speedups, and regulatory audit time reduction Customer acquisition and retention strategies - Channel-first: recruit MSSPs and value-added resellers to provide white-glove initial integration and managed governance - Land-and-expand: start with a single use case and instrument ROI to upsell adjacent workflows; use outcome-based pilots to shorten procurement cycles

- Retention levers: continuous compliance attestations, automated control reports for auditors, SLA-backed uptime/action guarantees, transparent explainability and rollback capabilities, and a vibrant connector ecosystem For defense and commodity-exposed customers - Defense suppliers should pivot BD messaging toward non-combat services: cyber, ISR, logistics, training, and contractor-enabled support Build consortiums with regional partners to mitigate coalition shortfalls - Forestry and exporters should offer trade-compliance tooling, warehousing/hedging services, and domestic-processing partnerships to reduce tariff exposure and win business from risk-averse buyers.

Sources

[1]

From cargo hub, US plots complex goal of forming international force for Gaza - Reuters

Reuters, 2025-10-24. (cred: 0.85)

https://www.reuters.com/world/middle-east/cargo-hub-us-plots-complex-goal-forming-international-force-gaza-2025-10-24/

[2]

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/

[3]

Carney Pushes Back on Provinces Spoiling for a Fight With Trump - Bloomberg.com

Bloomberg, 2025-10-26. (cred: 0.90)

https://www.bloomberg.com/news/articles/2025-10-26/carney-pushes-back-on-provinces-spoiling-for-a-fight-with-trump