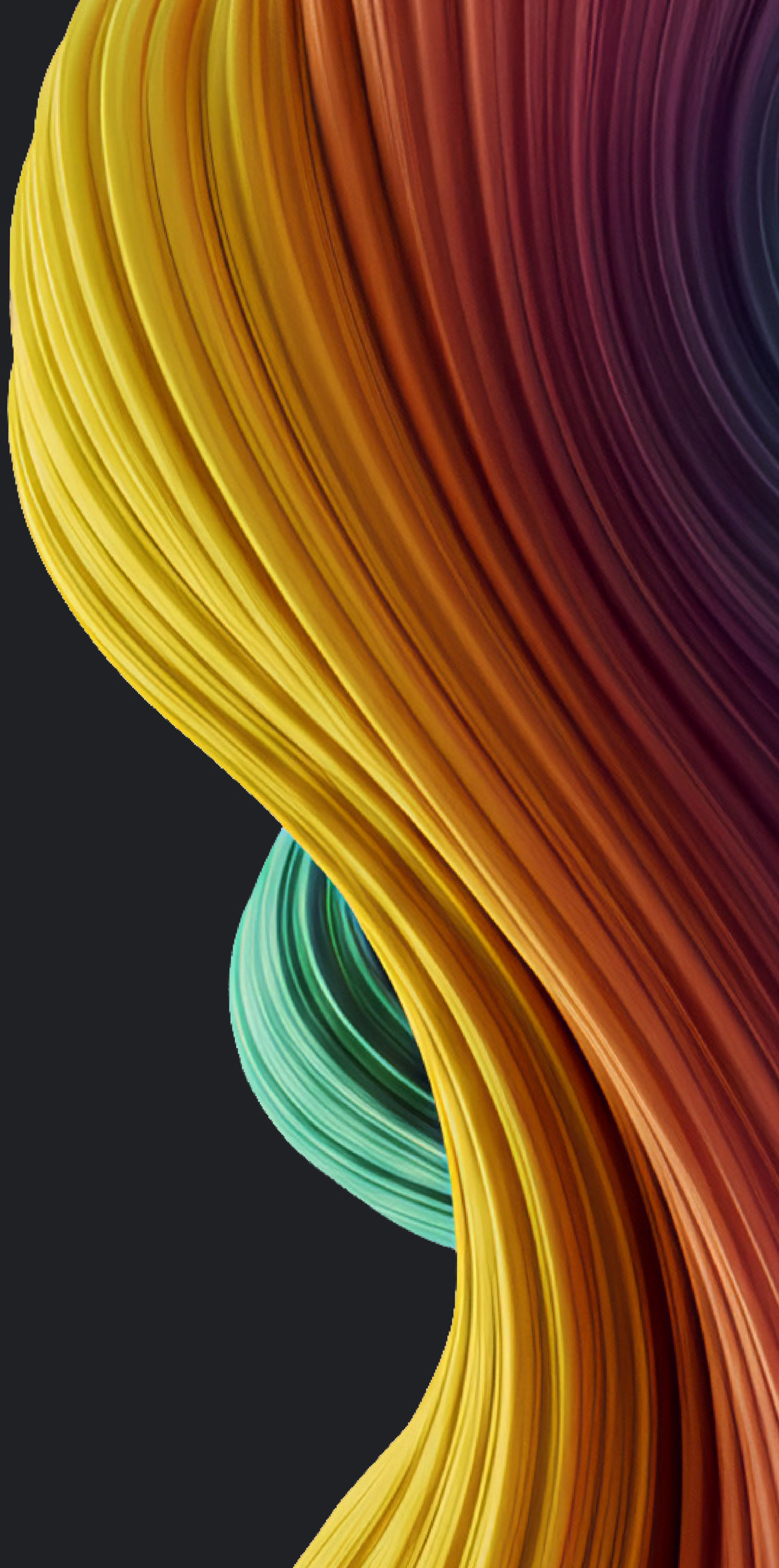
Google Cloud Deloitte.

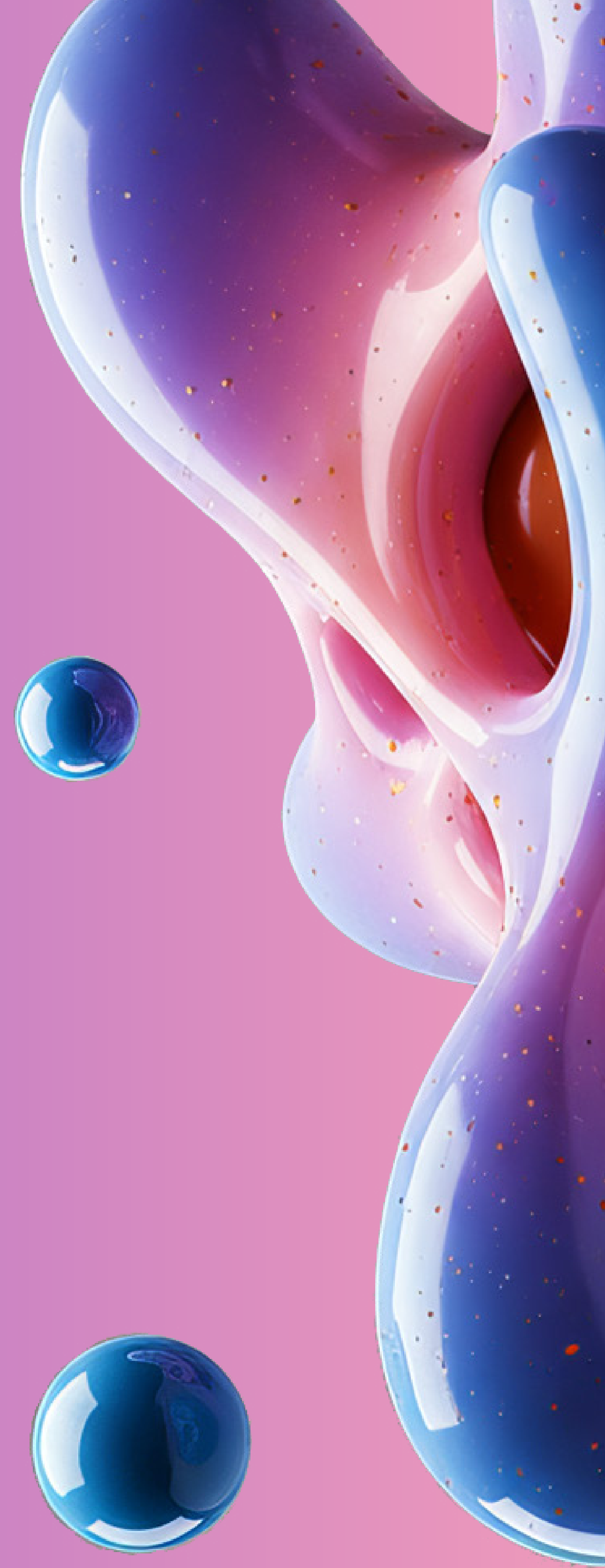
Scaling agentic AI

Opportunities, challenges, and cybersecurity considerations

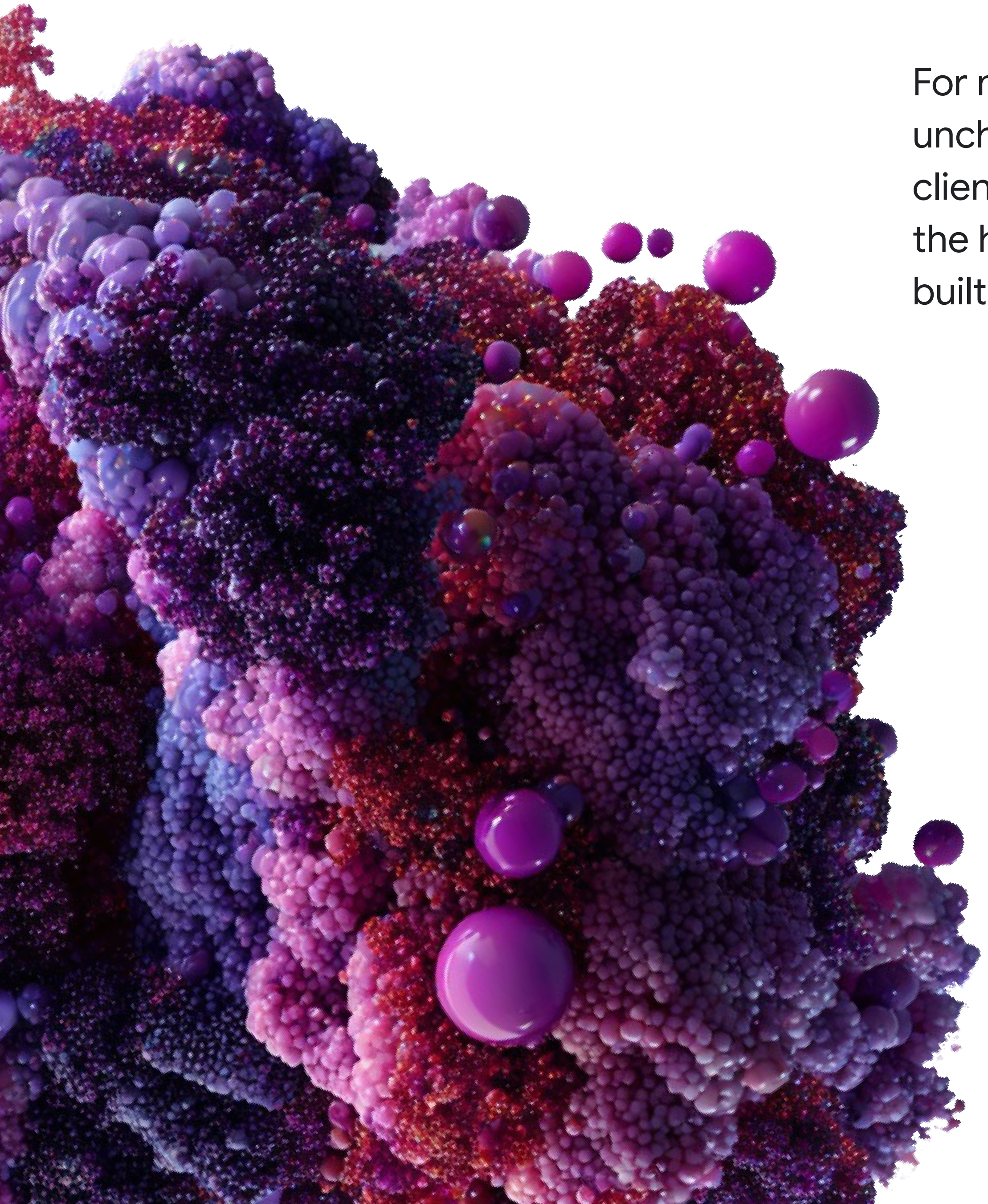


> “What if your next hire wasn’t a person? Imagine a digital workforce that never sleeps, executes complex strategies while you rest, and learns from every outcome. This is the world of agentic AI.”

Rayn Veerubhotla, Managing Director, Partner Engineering and Portfolio Strategy, Google Cloud

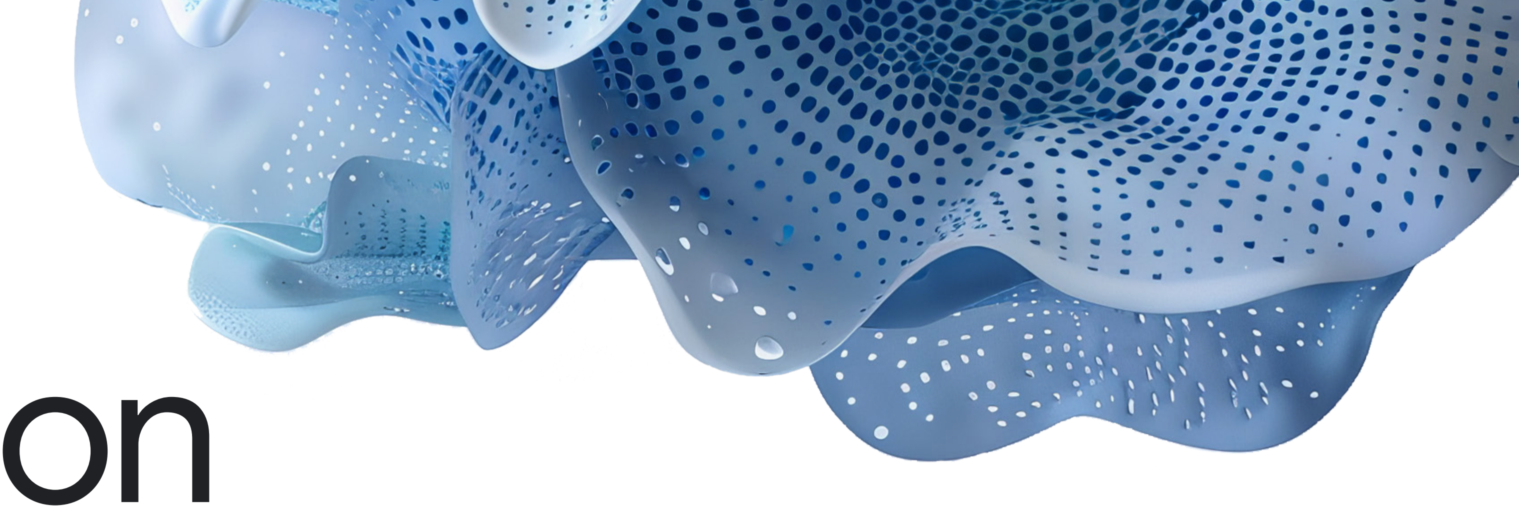


Introduction



For modern enterprises, the quest for a competitive edge feels like navigating a vast, uncharted sea. Every organization seeks its own treasures, such as operational efficiency, client loyalty, or market leadership, while contending with unpredictable tides of change. With the help of agentic AI though, they can now command an agile fleet of specialized agents built for speed and precision.

Agentic AI has the potential to bring a level of speed and scale that leaders used to dream of. But even the most capable fleet can drift into dangerous waters without the right guidance. Leaders should keep a watchful eye for risks, whether it's hallucinations, an expanding attack surface, or cascading failures that could proliferate at machine speed. To claim their AI treasures and return safely to shore, AI leaders should chart a clear course grounded in strategy, governance, and security. AI-fueled success often depends on the right mix of specialist knowledge, human oversight, and robust risk frameworks. Read on to discover how leaders across industries can claim the AI treasures they seek while mitigating operational shipwreck.



Hoisting the sails of transformation

From automation to autonomy

Like a ship catching full wind in its sails, agentic AI takes the power of generative AI (gen AI) and propels organizations even further. While gen AI excels at understanding patterns in human knowledge and predicting what comes next—the next word, sentence, or idea—agentic AI takes this a step further. It doesn't just generate insights; it acts on them. It makes decisions, executes tasks, and initiates processes with limited or no human guidance.

Across sectors, incremental efficiency gains are not always enough to move the needle. To tackle persistent challenges that have long resisted solutions, leaders should move beyond task-level automation to deliver measurable outcomes. Agentic AI is where many leaders are placing their bets. In its 2025 Predictions Report, Deloitte US predicts that 25% of enterprises using gen AI are expected to deploy AI agents by 2025, growing to 50% by 2027.[1] This signals a massive transformation in enterprise data utilization.

For instance, agentic AI can rapidly triage cybersecurity threats and automate and optimize multi-channel marketing campaigns. It can also handle complex e-commerce return processes, manage inventory across systems, and help enhance the customer experience by assisting live agents and resolving common challenges. And these are just a few examples. Agentic AI has the potential to transform a number of other processes across functions and industries.

[1] Deloitte US, "Deloitte 2025 Predictions Report, Generative AI: Paving the Way for a Transformative Future in Technology, Media and Telecommunications," 2024.

> “Agentic AI can learn from outcomes, adapt, and improve over time. Simply give it a goal and it can perceive the environment, reason, plan, and act. The business and societal potential is immense.”

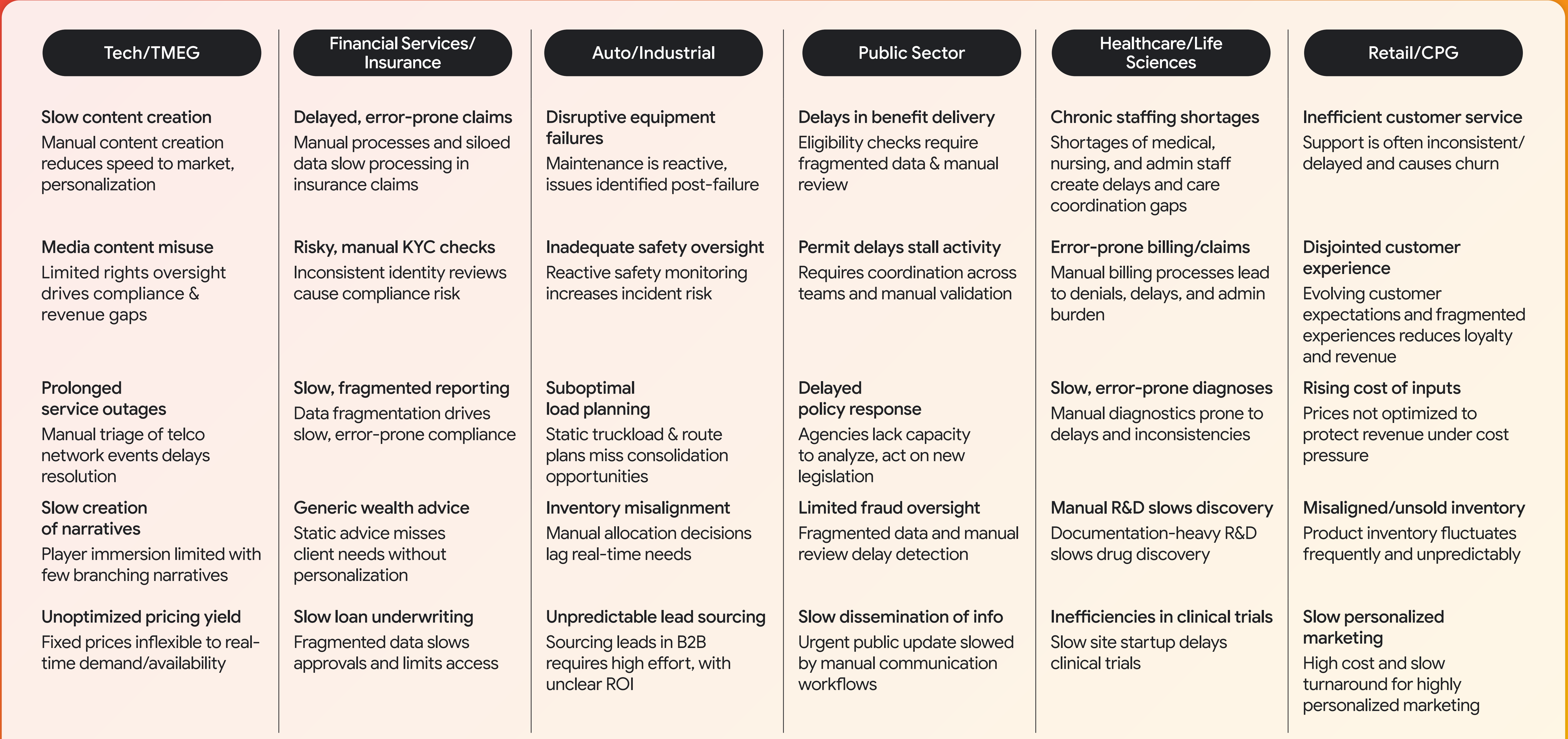
Aman Azad, AI Evangelist and Global Alliance Lead for AI, Google Cloud

Agentic AI

Solving "trillion dollar problems" across industries

Across sectors, modern organizations face pressure to do more with less, be more efficient and profitable, and deliver personalized experiences at scale. For instance, banks and insurers grapple with slow, error-prone processes and rising compliance demands. Retailers struggle with fragmented customer journeys, volatile supply chains, and margin pressure. Healthcare providers and life sciences companies contend with staff shortages, admin burdens, and lengthy development cycles. Tech, telecom, media, and gaming (TMEG) companies face bottlenecks that slow innovation and limit their ability to deliver personalized experiences.[2]

[2] Google Cloud, "Shaping the future: The transformative potential of agentic AI and the strategic imerative for Google Cloud partners," 2025.



Tech/TMEG	Financial Services/ Insurance	Auto/Industrial	Public Sector	Healthcare/Life Sciences	Retail/CPG
Slow content creation Manual content creation reduces speed to market, personalization	**Delayed, error-prone claims** Manual processes and siloed data slow processing in insurance claims	**Disruptive equipment failures** Maintenance is reactive, issues identified post-failure	**Delays in benefit delivery** Eligibility checks require fragmented data & manual review	**Chronic staffing shortages** Shortages of medical, nursing, and admin staff create delays and care coordination gaps	**Inefficient customer service** Support is often inconsistent/ delayed and causes churn
Media content misuse Limited rights oversight drives compliance & revenue gaps	**Risky, manual KYC checks** Inconsistent identity reviews cause compliance risk	**Inadequate safety oversight** Reactive safety monitoring increases incident risk	**Permit delays stall activity** Requires coordination across teams and manual validation	**Error-prone billing/claims** Manual billing processes lead to denials, delays, and admin burden	**Disjointed customer experience** Evolving customer expectations and fragmented experiences reduces loyalty and revenue
Prolonged service outages Manual triage of telco network events delays resolution	**Slow, fragmented reporting** Data fragmentation drives slow, error-prone compliance	**Suboptimal load planning** Static truckload & route plans miss consolidation opportunities	**Delayed policy response** Agencies lack capacity to analyze, act on new legislation	**Slow, error-prone diagnoses** Manual diagnostics prone to delays and inconsistencies	**Rising cost of inputs** Prices not optimized to protect revenue under cost pressure
Slow creation of narratives Player immersion limited with few branching narratives	**Generic wealth advice** Static advice misses client needs without personalization	**Inventory misalignment** Manual allocation decisions lag real-time needs	**Limited fraud oversight** Fragmented data and manual review delay detection	**Manual R&D slows discovery** Documentation-heavy R&D slows drug discovery	**Misaligned/unsold inventory** Product inventory fluctuates frequently and unpredictably
Unoptimized pricing yield Fixed prices inflexible to real-time demand/availability	**Slow loan underwriting** Fragmented data slows approvals and limits access	**Unpredictable lead sourcing** Sourcing leads in B2B requires high effort, with unclear ROI	**Slow dissemination of info** Urgent public update slowed by manual communication workflows	**Inefficiencies in clinical trials** Slow site startup delays clinical trials	**Slow personalized marketing** High cost and slow turnaround for highly personalized marketing

Image source: Google Cloud: The transformative potential of agentic AI and the strategic imperative for Google Cloud partners

3. Google Cloud, "Shaping the future: The transformative potential of agentic AI and the strategic imerative for Google Cloud partners," 2025.

By putting agentic AI in the captain's seat, leaders across all industries are sailing through choppy water towards greater growth and innovation.

By integrating agentic AI at the heart of operations, organizations can help eliminate friction, enhance the customer experience, and ride the winds of growth. But before they can haul in the treasure, leaders should navigate an expanding and evolving threat: cybersecurity.

Financial Services

AI agents can handle claims, optimize processes, and monitor risk in real-time for a better customer experience and greater efficiency.

Retail and consumer packaged goods

AI agents can resolve customer service challenges, forecast demand, personalize offers, and optimize campaigns—for more revenue, less waste, and a better shopping experience.

Healthcare and life sciences

From claims processing to fraud detection, patient care coordination, and drug discovery, AI agents can help reduce errors, accelerate treatments, and enable faster breakthroughs.

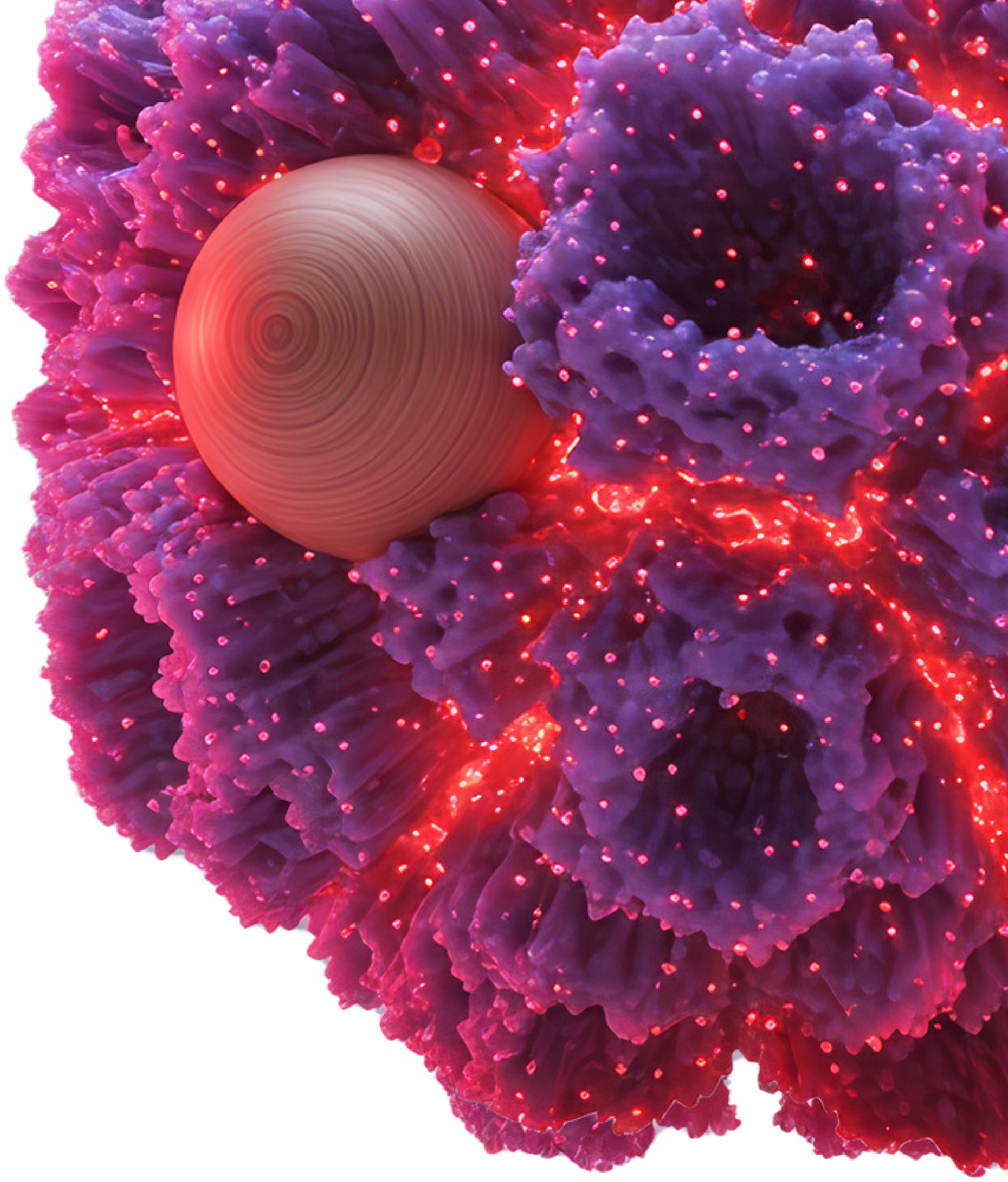
Tech, telecom, media, entertainment, and gaming

AI agents can generate content, help ensure rights compliance, resolve outages, create better game narratives, and accelerate software development—so teams can be more creative and strategic.

From leaky lifeboat to sturdy ship

Agentic AI and cybersecurity

The modern security operations center (SOC) faces a constant flood of security alerts, most of which are just noise.[4] Given this, it's no wonder 71% of data analysts report burnout and 64% consider abandoning their posts within just a year.[5] Agentic AI can offer some reprieve. By autonomously sensing and responding to threats with unprecedented speed, AI can rebuild the metaphorical boat versus simply patching the leaks. AI agents can prioritize alerts and detect unusual activity. They can also automate routine tasks and free up analysts to focus on the most critical threats.



[4] Dave Brown, CPO Magazine, "Beyond Burnout: Three Ways to Reduce Frustration in the SOC," 2025.
[5] Dave Brown, CPO Magazine, "Beyond Burnout: Three Ways to Reduce Frustration in the SOC," 2025.

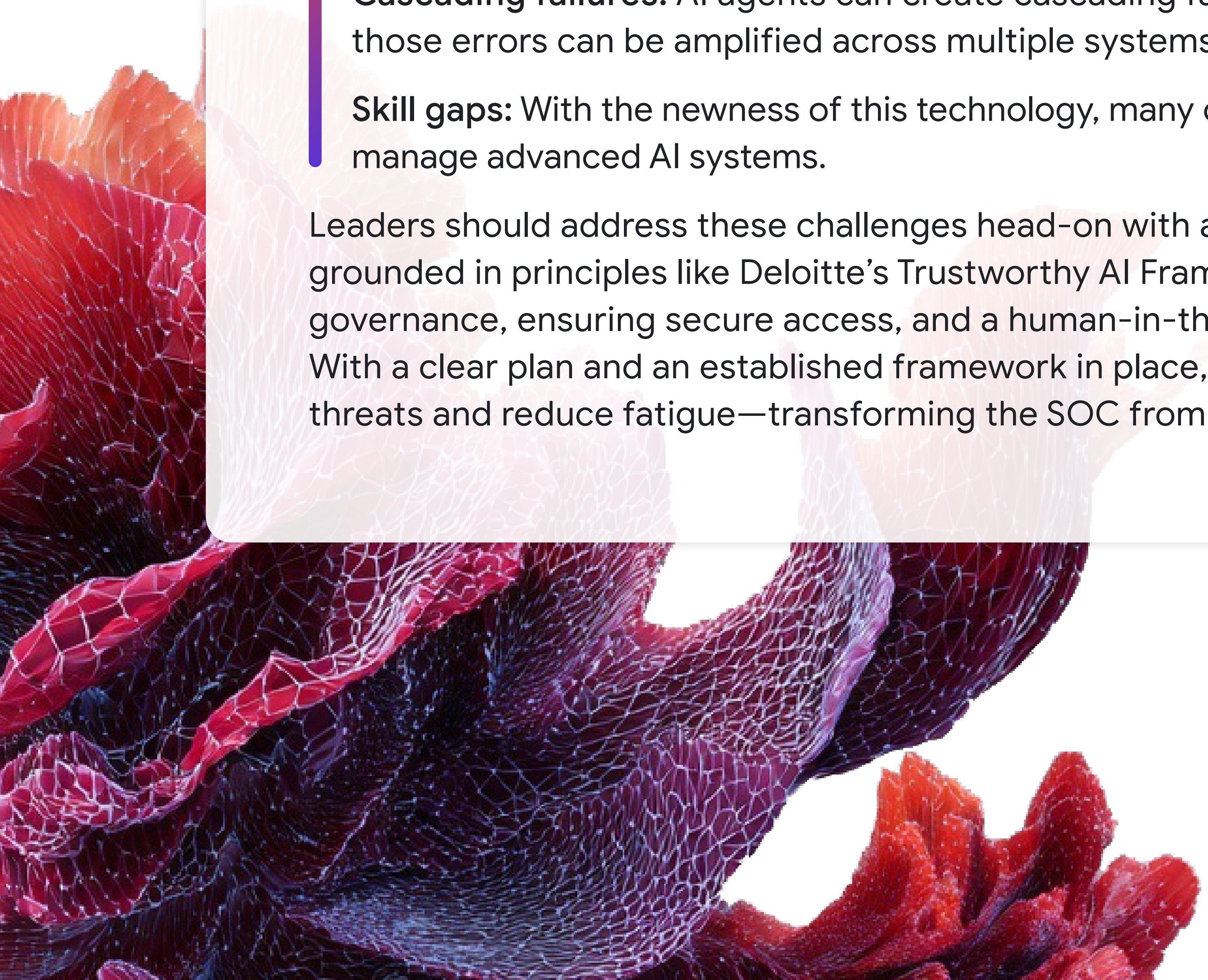
But for every risk AI mitigates, there’s a risk or challenge to be considered, including:

A growing attack surface: Agentic AI can operate across multiple systems, creating new potential security vulnerabilities that traditional access controls might not handle.

Cascading failures: AI agents can create cascading failures if they make a mistake or hallucinate, and those errors can be amplified across multiple systems.

Skill gaps: With the newness of this technology, many organizations lack the knowledge to build, scale, and manage advanced AI systems.

Leaders should address these challenges head-on with a clear strategy and a “navigation plan” for adoption, grounded in principles like Deloitte’s Trustworthy AI Framework.™ This involves implementing robust governance, ensuring secure access, and a human-in-the-loop review process at important checkpoints. With a clear plan and an established framework in place, agentic AI can help SecOps teams effectively handle threats and reduce fatigue—transforming the SOC from a leaky lifeboat into a sturdy ship.



"Agentic AI is like a self-sailing ship. But beneath the surface lie hidden icebergs, risks that can sink operations. AI brings unprecedented speed and capability, but without guardrails, even a small misstep can have outsized consequences."

Gopal Srinivasan, Principal, Alphabet Google Alliance Generative AI Leader, Deloitte Consulting LLP

The treasure map

Unearthing the value of agentic AI

In industries long anchored by arduous manual processes, agentic AI smooths the sails of operations, guiding leaders toward the treasure buried beneath the sand. AI can improve efficiency and decision-making and lead to stronger outcomes for customers and shareholders alike. But without the right people, processes, and knowledge—including a strong focus on cybersecurity—leaders may find themselves hunting for treasure without a map. Teams should be ready to work alongside agentic AI, gain new skills, and reshape roles and processes while safeguarding systems and data.

Organizations should consult with collaborators who have deep industry and cybersecurity experience to help ensure every decision is well-informed and every risk is considered. Without this alignment, even the most capable AI agents can drift off course or remain moored and motionless. However, with the right strategy, crew, and security measures at the helm, organizations can set sail for unprecedented levels of efficiency, personalization, and innovation—claiming the treasures that lie beyond the breakers.

Don't let complexity capsize your operations. Book your complimentary AI readiness assessment to learn how agentic AI can help you navigate risks and accelerate growth.

Contact us

Learn more about Deloitte and Google Cloud. For more information, contact your Deloitte or Google Cloud representative.

Google Cloud Deloitte.

About

Google Cloud

Google Cloud is the new way to the cloud, providing AI, infrastructure, developer, data, security, and collaboration tools built for today and tomorrow. Google Cloud offers a powerful, fully integrated and optimized AI stack with its own planet-scale infrastructure, custom-built chips, generative AI models and development platform, as well as AI-powered applications, to help organizations transform. Customers in more than 200 countries and territories turn to Google Cloud as their trusted technology partner.

Deloitte

Forge the future. Unite Deloitte's deep industry insights with the transformative power of Google Cloud. Together, we'll craft tailored strategies to address your unique challenges and aspirations to spark progress for your enterprise. Unlock the Google Cloud ecosystem and create bold new possibilities, transform operations, and capitalize on measurable results. With Deloitte and Google Cloud, you won't adapt to change. You'll shape it. Forging a future that's sustainable, impactful, and uniquely yours. www.deloitte.com/googlecloud

Disclaimer

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.