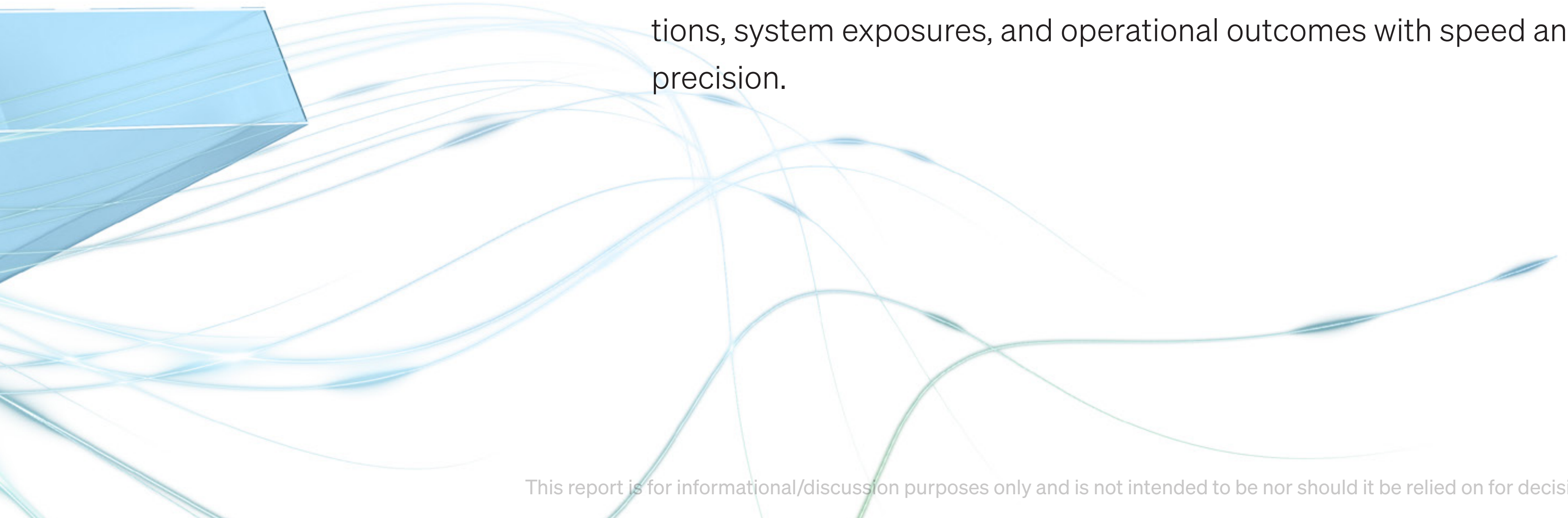
4

AI powered simulation enhances testing

Organizations will rely on advanced simulations to test, validate, and optimize products, processes, and scenarios before deploying them in the real world. These virtual environments will enable continuous, scalable experimentation, allowing teams to model user interactions, system exposures, and operational outcomes with speed and precision.



Synthetic users / user simulations

Creating synthetic representations of real people or populations to test ideas, gain insights and simulate behavior and action.

Synthetic users are virtual personas or agents powered by large language models (LLMs), designed to mimic the humanness of real people or populations – including beliefs, intent, preferences and choice actions.

Synthetic users can represent individuals, segments, or entire populations. These synthetic users can complete interviews, surveys and panels for user research and consumer feedback, test and optimize marketing materials such as text, images and video, and even interact with designs, applications, and experiences. In some instances, these users can be deployed into a synthetic environment to conduct simulations of interactions and information/idea dissemination – think a video game where synthetic users would be able to live, interact, learn and grow.

For example, User Research teams could generate synthetic users that represent hard to reach market segments (like traders). Likewise, UI/UX teams can create synthetic users to test new workflows, validate user interfaces or simulate employee interactions with enterprise software.

There are different model frameworks which can be leveraged to create synthetic users. Some vendors rely on singular models, such as ChatGPT, that serve as wrappers. Others use model switching, dynamically selecting the most suitable LLM for a given task. A third approach involves building and training proprietary foundational models tailored to specific needs.

Training strategies also vary across the industry. Some companies train their models exclusively on public data, while others use proprietary data; or a combination of both. Additionally, there is debate over the necessity of injecting demographic, psychometric, and behavioral data to enhance the humanness of synthetic agents. Some believe that LLMs, already trained on vast internet data, inherently capture human characteristics, while others advocate for more targeted data enrichment.

Approaches for generating synthetic users can vary. Some providers create purely synthetic users, generated solely by AI models, while others augment these virtual personas with real human feedback. For example, a synthetic user might be regularly updated based on recurring interviews with actual people, as opposed to being generated once from a model like ChatGPT and left unchanged.

Market and industry perspectives

The synthetic user space is an emerging market, with most players still in the early stages of company formation and investment. Many began as research-focused initiatives and are now transitioning into commercial ventures, seeking to capture both revenue and market share.

Within the market, four main categories have emerged, each representing a different level of sophistication and capability:

Synthetic research – These solutions extend research efforts to fill gaps in representation but may lack detailed audience segmentation.

Comprehensive synthetic research – Platforms in this category create synthetic users for insights and feedback, offering detailed segmentation and analysis. Interaction is generally limited to text and images.

Multimodal synthetic research – This segment enables synthetic users to engage with live stimuli, including text, images, video, audio, applications and websites, providing a richer research experience.

Multimodal agentic simulations – Representing the next generation of synthetic user technology, these platforms allow multiple synthetic agents to interact within simulated environments, offering deeper insights into group dynamics and behaviors.

The market is rapidly converging toward solutions that feature interactive personas that can engage with live stimuli, combining both public and proprietary data. These platforms can leverage a customer’s private data and ground their insights in broader market data, creating highly representative and actionable research outputs.

This evolution is enabling newer synthetic user vendors to compete with, and in some cases augment, established traditional research and software tools. These include consumer research platforms, statistical modeling tools, survey platforms, and human-led research services and UX research.

Proactive defense through tailored, continuous attack simulation

Proactive testing and exposure management by continuously simulating attacker tactics on a dynamically adapted representation of the enterprise environment.

Cyberattacks are evolving at unprecedented speed, fueled by advances in AI, agentic systems, and increasingly automated adversary tradecraft. Attackers now can develop more dynamic, personalized, less traceable and continuous tactics and techniques, making it increasingly harder for defenders.

Digital twins help expose an enterprise's complete, real-world attack surface. The next frontier approach to defending against complex and scaled attacks is not limited explicitly to modeled twins but rather continuously learned real-time representations of the enterprise built by aggregating real-time telemetry from across the security and observability stack. By combining signals from the entirety of the digital environment, organizations can maintain a high-fidelity view of how their infrastructure is connected and exposed and use this model to continuously simulate attacks from an attacker's perspective.

Unlike traditional vulnerability scans or point-in-time penetration tests, this approach enables modeling of real-world, tailored and adaptive attack paths across the complete enterprise infrastructure including, network, cloud, data paths, endpoints, software supply chain, SaaS integrations and identity systems. Because they are derived from live telemetry, simulated attack tactics can dynamically adapt as configurations, permissions and dependencies change, enabling defenders to test exposure as it exists today, anticipate breach paths before they are exploited and harden configuration proactively.

This report is for informational/discussion purposes only and is not intended to be nor should it be relied on for decision making

Market and industry perspectives

Recent research of vulnerabilities exploited in a given year highlight a trend toward a negative time-to-exploit (TTE). The metric turning negative implies that attackers are now weaponizing vulnerabilities before patches are available, requiring a new expectation for vulnerability remediation and proactive resilience for effective defense. Beyond vulnerability exploitation, frontier AI labs have published research of advanced threat actors using their AI tools to create malware and execute AI-driven adversarial operation.

Leading security platforms are focusing on continuous exposure management, with incumbents expanding into continuous exposure testing. They envision a broader platform centric view of security, integrating multi-step attack path simulation from an external attacker perspective across the full estate. Amazon recently unveiled its internally developed Autonomous Threat Analysis (ATA) system where multiple AI agents compete against one another to investigate real attack techniques against a high-fidelity simulated testing environment and then propose security controls for human review.

Several emerging startups are innovating with AI and digital twin-like concepts to simulate adversary emulation and derive a complete picture of an organization’s exposure with an end goal objective of autonomous security built for the age of AI.

This report is for informational/discussion purposes only and is not intended to be nor should it be relied on for decision making

JPMorganChase