REPLY

Compliance and security challenges in the era of Agentic AI

Learn how the adoption of Agentic AI expands compliance and cybersecurity challenges

Agentic AI: a new dimension of risk

The transition **from LLMs to AI agents** marks a turning point in security and risk management. These agents, equipped with autonomous execution capabilities and able to interact with other agents and tools in increasingly complex orchestration chains, radically transform the attack surface. Their autonomy introduces new vulnerabilities, going beyond the limits of traditional **data governance and cybersecurity** controls.

This scenario requires advanced protection strategies, capable of dealing with dynamic threats and of quickly adapting to changing environments. It is therefore essential to integrate the principles of **fairness, accountability, transparency and explainability** into the design of AI agents, to ensure safe, reliable and regulatory compliant systems to realize a Responsible AI.

Trust and governance in AI agents: from control to collaboration

After the first phase of security, a more subtle but equally crucial challenge emerges: **how to maintain trust and control** in an ecosystem of autonomous AI agents?

The distribution of decisions among multiple agents makes the **cause-effect chain less transparent** and more difficult to reconstruct, increasing governance complexity and testing traditional auditing and risk management models. It is therefore necessary to rethink **security as an integral part of the agency architecture**, developing dynamic governance mechanisms that allow us to monitor, track and intervene in real time on the behavior of agents. In this way, it will be possible to build a reliable ecosystem, able to evolve in harmony with the required ethical and compliance principles.

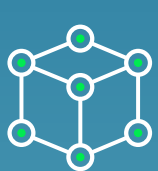
The AI Security Governance and Compliance Framework

Agentic AI requires a significant revision of traditional security and governance models. **Reply's AI Security Governance and Compliance framework** responds to the new challenges introduced by decision-making autonomy and complex interactions between intelligent agents, and is aligned with the most recent cybersecurity standards such as the OWASP Agentic AI Threat Model (2025). Key elements of the AI security framework are:

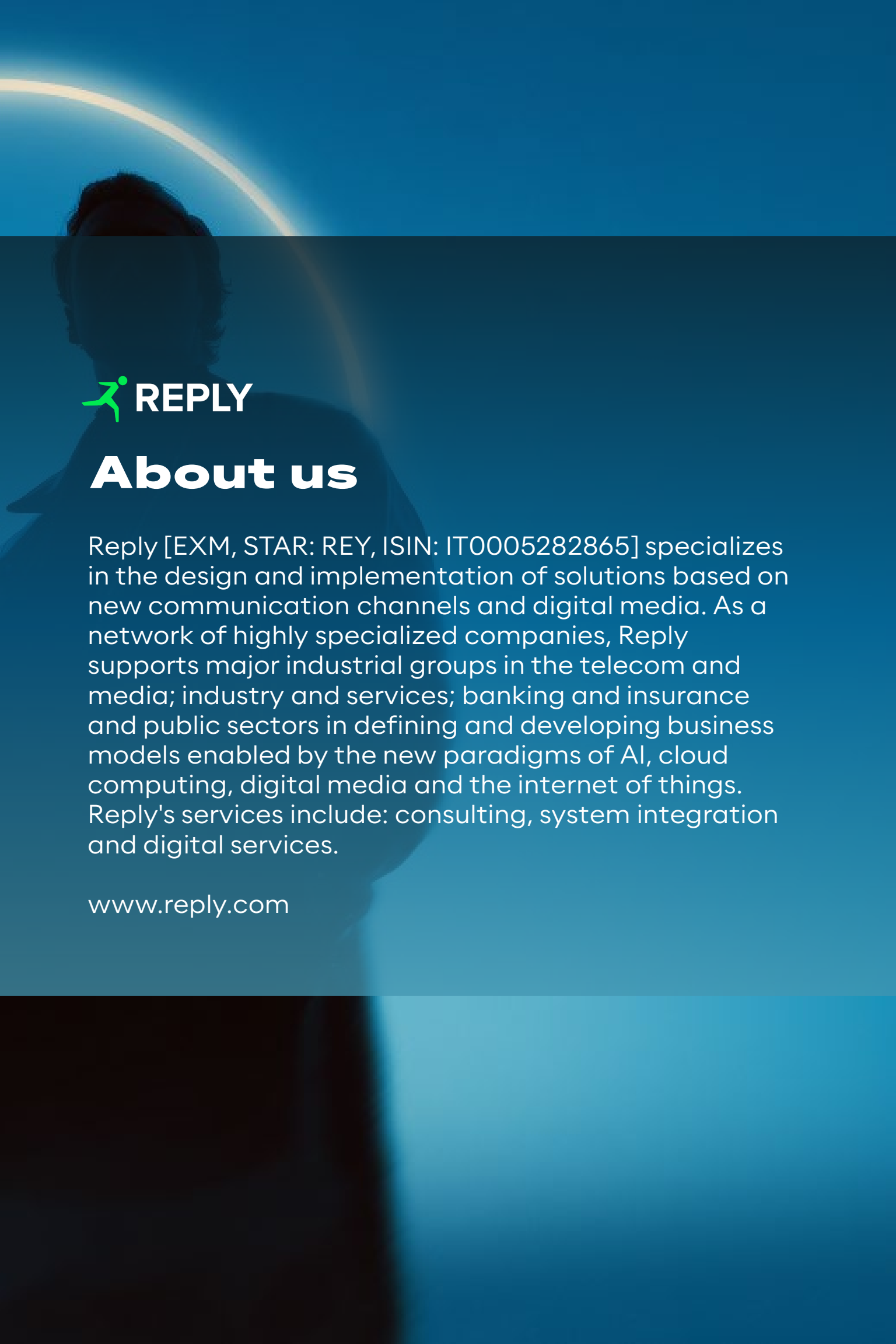
Monitoring of agentic goals and behavioral deviations to identify any anomalies.

Advanced digital identity management, including non-human agents and sub-agents, with strong authentication and authorization.

Validation of external interactions through auditable records to ensure transparency and accountability.



Implementation of dynamic governance interventions, with risk thresholds, temporary limits and automated escalations.



REPLY

About us

Reply [EXM, STAR: REY, ISIN: IT0005282865] specializes in the design and implementation of solutions based on new communication channels and digital media. As a network of highly specialized companies, Reply supports major industrial groups in the telecom and media; industry and services; banking and insurance and public sectors in defining and developing business models enabled by the new paradigms of AI, cloud computing, digital media and the internet of things. Reply's services include: consulting, system integration and digital services.

www.reply.com