IBM Technology Atlas

Security roadmap

Generative AI, secure agentic frameworks, crypto-agility, and semiconductor innovations secure decentralized, multi-cloud environments.

Updated April 2025

✓ Realized
↻ In progress

	2024	2025	2026	2027	2029	2030+
Security journey	✓ ***Drive multi-cloud security, compliance, and cyber resiliency with generative AI.***	↻ ***Secure the lifecycle of data for generative AI.***	***Enable enterprise migration to quantum safety while delivering security foundations of human-agent collaborations.***	***Secure decentralized IT deployments and build the governance foundations of generative AI.***	***Protect the full data lifecycle using cryptographic schemes with hardware acceleration and confidential computing.***	***Provide ubiquitous workload protection with fully integrated hardware and software security controls.***
Strategy overview	✓ In 2024, we will leverage automation and generative AI to strengthen defenses and optimize risk posture with continuous compliance. ↻ This will lead to fewer failures and faster response and will make organizations more resilient.	We will protect the lifecycle of data with enterprise key and certificate lifecycle management, lineage tracking, classification, and leakage protection, transforming data security for the age of AI.	We will implement quantum-safe cryptography and crypto agility, enhance human-agent collaboration through robust identity and entitlement management, and utilize secure agentic middleware for secure reasoning.	Establish security and trust management across decentralized computing and digital environments using digital assets to enhance protection and trust in IT deployments.	Privacy-preserving technologies, such as fully homomorphic encryption (FHE) and confidential AI computing, will protect enterprise workloads against data breaches and adversarial attacks.	By 2030, we will implement security controls throughout the entire computing stack, from the lowest level to multi-cloud applications and systems.
Why this matters to our clients and the world	✓ Business transformations are expanding the attack surface, making protection increasingly difficult. Generative AI and automation are crucial to enhancing hybrid cloud security, compliance, and cyber resiliency.	Organizations will be empowered to address the security challenges associated with the growing complexity of data environments, ensuring robust protection against threats in generative AI and enhanced trust in digital interactions.	Organizations will be empowered to address emerging security threats in an increasingly complex digital landscape, ensuring robust protection against cryptographic vulnerabilities in the quantum era and enhancing trust in human-agent collaborations.	These innovations will help enterprises tackle the security challenges posed by the expanded attack surface of decentralized IT deployments, such as consumer identity and sovereign clouds.	Technologies such as fully homomorphic encryption and confidential computing will secure the full data lifecycle, enabling AI on always-encrypted data, even while it is being used.	Security controls at the lower levels of the stack and across multi-cloud environments will help counter adversaries attempting to exploit technologies driving the transition to multi-cloud.
The technology or innovations that will make this possible	✓ Generative AI–based security and compliance controls will automate security hygiene, demonstrate compliance, and protect hybrid cloud deployments. ↻ We will enable continuous monitoring and adaptive policy management with distributed enforcement (e.g., identity-driven data security and policy management).	Accountability enhancements, extensive monitoring, unified data security frameworks, advanced data loss prevention solutions, and automated key and certificate lifecycle management will strengthen data protection in generative AI applications and foster trust in digital ecosystems.	Quantum-safe algorithms, advanced IAM solutions, and secure agentic middleware will enable robust data protection and facilitate secure human-machine collaboration in digital environments.	Open standards and privacy-preserving techniques will enhance decentralized environments such as sovereign clouds, digital assets, and decentralized identities.	Fully homomorphic encryption and confidential computing will enable privacy-focused AI.	A multi-cloud hybrid security control plane will be developed, focusing on hardware security mechanisms like chiplet security. This system will monitor and counter adversarial threats, protecting attack surfaces across applications and data.
How these advancements will be delivered to IBM clients and partners	↻ Security and compliance capabilities infused with generative AI will be included in IBM Z, Guardium, Concert, IBM Cloud, and RH/OS to protect IBM's hybrid cloud.	These advances will be delivered on AI middleware, data security, and identity access management (IAM) products that support scalability, interoperability, and compliance with industry standards, ensuring robust security for generative AI applications.	These advances will be delivered on AI middleware, data security, and IAM products that support scalability, interoperability, and compliance with industry standards.	Sovereign hybrid cloud and other distributed deployments will feature decentralized identity and compliance, ensuring and managing trust across all platforms.	Tools for developing secure AI applications on encrypted data will include frameworks and crypto libraries for trusted execution environments and hardware acceleration.	The multi-cloud platform will utilize trusted hardware designed through secure, cloud-native processes embedded in chips produced in trusted foundries.