IBM Technology Atlas

Security roadmap

Unified threat management, quantum-safe cryptography, and semiconductor innovations secure multicloud, decentralized environments.

Updated May 2024

✓ completed
→ pushed to next year
⟳ on target

	2023	2024	2025	2027	2029	2030+
Security journey	✓ ***Use secure foundation models in unified threat management to protect high-value assets.***	⟳ ***Drive multicloud cyber resiliency with automated and intelligent security and compliance.***	***Quantum-safe cryptography and a secure supply chain are the norm.***	***Secure insights and data while in use with robust AI and fully homomorphic encryption.***	***Use security to bring trust to a decentralized digital world.***	***Secure semiconductor chips and power ubiquitous controls.***
Strategy overview	✓ In 2023, the protection of high-value assets in the hybrid cloud will tighten with unified threat management and compliance. ✓ AI will raise the mean time to failure and lower the mean time to recovery to within an hour.	⟳ 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.	In 2025, we will protect multicloud deployments with quantum-safe cryptography and a secure supply chain of software and services to address security threats of quantum computing and open-source software vulnerabilities.	By 2027, technologies like fully homomorphic encryption (FHE) and robust AI will be widely used to protect enterprises against data breaches and adversarial AI.	By 2029, we will bring security and management of trust across decentralized computing/ digital environments with self-sovereign identity and digital assets. This will bring protection and trust to IT deployments and sovereign clouds.	By 2030, security controls will be incorporated along the full computing stack, from the lowest level up, and across multicloud applications and systems.
Why this matters to our clients and the world	✓ With an evolving security threat landscape, unified threat management and compliance will protect businesses from growing threats and allow faster response across hybrid cloud environments.	⟳ Generative AI will empower attackers, increase attack sophistication, and grow the attack surface. Organizations will be required to adopt automated and generative AI-based security and compliance to ensure resiliency across multicloud environments.	Quantum-safe cryptography will protect classical cryptography from quantum attacks, while a secure software supply chain protects enterprises with provenance and security checks to filter vulnerabilities.	Fully homomorphic encryption will enable analytics and privacy on always encrypted data, including when it is in use. Robust AI will protect against adversarial attacks on AI services.	The innovations we will deliver in 2029 will enable organizations to solve the security challenges posed by the expanded attack surface of decentralized IT deployments like sovereign clouds and virtual worlds.	Security controls for the lower levels of the stack and across multicloud deployments will counter adversaries trying to attack the very technologies driving the shift to the multi-cloud.
The technology or innovations that will make this possible	✓ Standardized industry controls, development of an industry-leading open assessment platform, and compliance management tools will protect the attack surface. ✓ An IBM-driven, cloud-native, and enterprise-grade log management solution with open-standards, behavior analytics, and AI will monitor the attack surface. ✓ Automation with AI will enhance the response time.	⟳ IBM-curated, robust security and prescriptive hybrid cloud compliance controls based on generative AI will protect and enable continuous monitoring and adaptive policy management with distributed enforcement (e.g., risk-based threat management, data security policy management, and confidential containers).	IBM-led innovation for quantum-safe crypto standards, quantum-safe posture management, and crypto agility will enable the migration to a quantum-safe future. IBM technology for software composition analysis will enable a crypto and software bill of materials (CBOM, SBOM) and industry certifications like the supply chain levels for software artifacts (SLSA).	IBM technology for robust AI will discover and remediate vulnerabilities in AI. IBM's approach will protect the training data (DataSecOps) and models (ModelSecOps) throughout the lifecycle of machine learning security operations (MLSecOps). IBM toolkits for fully homomorphic encryption and open standards for protecting data in use will produce privacy-enabled AI on encrypted data.	IBM-driven open standards and privacy-preserving techniques will secure decentralized environments like sovereign clouds, digital assets, and decentralized identity. With a risk-driven approach, IBM's early breach notification driven by generative AI will help address threats proactively and prevent breaches. A mature risk operation center will improve monitoring.	The integrated hardware root of trust will provide a vertically-integrated IBM security stack that will protect and monitor the attack surfaces across applications and data. A hybrid cloud security control plane anchored in hardware security mechanisms such as chiplet security and secure, cloud-native electronic design automation (EDA) will track and counter adversaries.
How these advancements will be delivered to IBM clients and partners	✓ We will deliver an AI differentiated, cloud-native, open unified threat management platform (e.g. QRadar). It will be simple to use and integrated with infrastructure, the multicloud platform, applications, and data.	⟳ Automated security and compliance capabilities infused with generative AI will be delivered as cloud-native offerings to protect hybrid cloud environments, e.g., QRadar, Guardium, and Verify.	Guardium will be extended to provide quantum safe posture management to ease the migration to quantum-safe cryptography. We will deliver innovations in software supply chain security in a cloud-native manner to meet SLSA level 4 for containers.	Frameworks for developing robust and secure AI applications on encrypted data, crypto libraries with hardware acceleration, and AI robustness toolkits will become embedded in AI developer tooling.	Sovereign hybrid cloud and other distributed deployments will have decentralized identity and compliance, ensuring and managing trust everywhere.	The hybrid cloud platform will be available with trusted hardware designed by secure, cloud-native processes and embedded in chips in trusted foundries.