Illumio and IBM: Securing Quantum Computing with Illumio Segmentation

Containing breaches, eliminating lateral movement, and enabling post-quantum cyber resilience.

Quantum computing is coming. So are new security risks.

Quantum computing will transform industries from finance to healthcare, but it also threatens today's cryptographic protections. As quantum power grows, adversaries will be able to break traditional encryption, exposing sensitive data to "harvest now, decrypt later" attacks.

IBM, a leader in quantum technology, is preparing enterprises for this shift with IBM Quantum Safe, helping organizations assess and mitigate quantum risk. Illumio complements this with proven segmentation to stop lateral movement and contain breaches—even when encryption fails.

The post-quantum threat

Once current encryption is broken, attackers can exploit unsegmented environments to move laterally between systems. IBM drives post-quantum cryptography standards with NIST and delivers quantum readiness assessments, while Illumio ensures real-time visibility, enforcement, and breach containment.

Why segmentation matters

Whether in classical or quantum systems, attacks spread through human error and open ports. Human error can't be patched, but ports can be segmented. Illumio blocks unauthorized traffic instantly, preventing lateral spread. For example, if a quantum node suddenly pushes gigabytes of data over DNS, Illumio isolates it immediately, without waiting for deep inspection.

Illumio + IBM in action

Quantum risk	How Illumio + IBM respond
Broken post-quantum encryption	Illumio contains lateral movement; IBM replaces weak cryptography with quantum-safe alternatives.
Threats moving across clusters	Illumio enforces workload boundaries; IBM models and assesses quantum risk.
Unknown malware at quantum scale	Illumio isolates anomalies in real time; IBM provides integrated threat management.

Capabilities delivered

Together, Illumio and IBM deliver practical defenses that combine visibility, segmentation, and quantum-safe strategy. Key capabilities include:

- **Visualize communications**: Map connections across classical and quantum workloads, see open ports, and identify risky traffic.
- **Isolate and protect**: Segment workloads at the host level and enforce dynamic policies across nodes and apps.
- **Contain threats fast**: Instantly block abnormal flows (e.g., massive DNS transfers, RDP misuse).
- **Integrate quantum risk**: Use IBM's Quantum Safe assessments with Illumio enforcement to align segmentation with quantum-era threats.

Why Illumio + IBM

Illumio

Policy-first segmentation to stop lateral movement

Visibility and control across hybrid and edge systems

Anomaly detection without packet inspection

IBM

Leader in quantum computing and cryptography standards

Provider of IBM Quantum Safe, Threat Management, and Consulting

Expertise in quantum risk modeling and secure design

Preparing now: building a two-layer defense for the quantum era

The quantum threat is no longer distant; it is actively shaping today's security strategies. Organizations must not only plan for future-proof encryption but also strengthen defenses that can protect them immediately against lateral movement and breach propagation.

IBM Quantum Safe equips enterprises with a roadmap to navigate the cryptographic transition. This includes:

- Inventorying cryptographic assets to identify what is at risk
- Prioritizing upgrades for the most sensitive systems and data
- Implementing crypto-agility and key management best practices
- Engaging in NIST-led post-quantum cryptography efforts to align with emerging standards

At the same time, Illumio adds a critical second layer of protection: encryption-independent segmentation. By enforcing host-level policies and containing abnormal traffic flows, Illumio ensures workloads remain secure—even if cryptography is compromised by quantum attacks.

Together, IBM and Illumio help organizations move from theory to practice, combining strategic quantum readiness with real-time breach containment to stay resilient now and in the future.

Secure the future today

Quantum risks are imminent. Organizations must act now to strengthen defenses. IBM delivers quantum-safe cryptography; Illumio ensures breaches are contained. Together, they provide a clear path to post-quantum cyber resilience.

Start your quantum resilience journey

Contact Illumio today to take the next step.

illumio.com/support/contact

About Illumio

Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments – stopping the spread of attacks before they become disasters. Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.