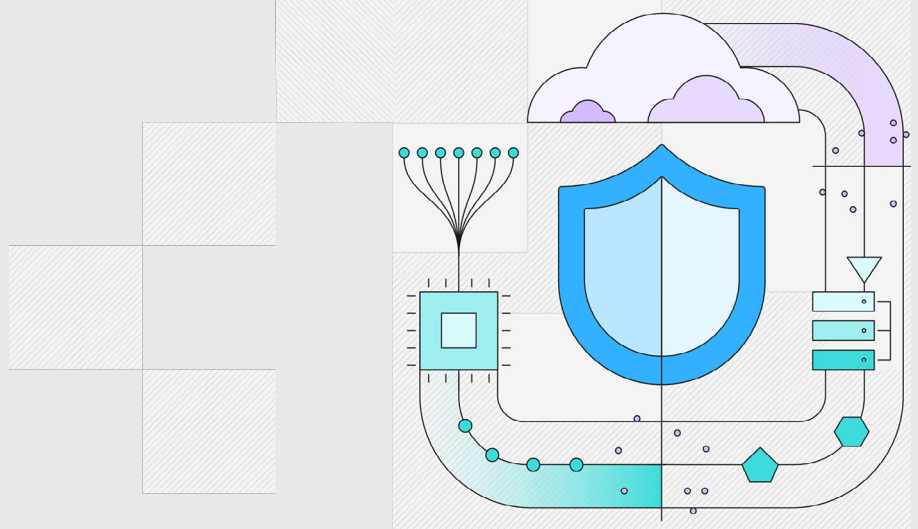


5 key steps to a modern infrastructure

Built with cyber resilience in mind

Cyber risks now outpace traditional security. For infrastructure leaders, thriving in this reality means having an end-to-end cyber resilience strategy that unifies organizational readiness, storage-layer protection and AI-driven defenses. See how you can build your own.



01

Establish foundational security and data ownership.

Without foundational security and data ownership, organizations struggle to identify critical assets, prioritize recovery, respond effectively to incidents, or drive downstream resilience activities.



02

Classify data and define minimum viable operations.

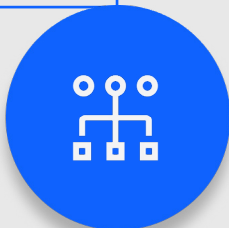
Not all data is created equal. To keep the business running, leaders must identify what is essential, then architect recovery workflows around those critical assets.



03

Implement resilient protection and isolation mechanisms.

Modern resilience requires protection mechanisms that arrest corruption and preserve clean recovery points—to ensure ransomware, breaches or system failures don't compromise the entire infrastructure.



04

Detect anomalies in real time using AI and behavioral indicators.

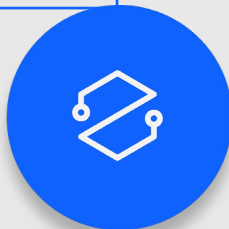
Today's threats evolve too rapidly for manual detection. With AI-driven anomaly detection, leaders can identify unusual behavior such as encrypted payloads, compression changes or abnormal I/O patterns—all within seconds.



05

Orchestrate automated, validated recovery workflows.

Fast recovery requires both clean data and automated, validated processes that bring systems back online quickly and consistently.



To access more proven strategies and checkpoints for building the resilience of your modern infrastructure, read [The Cyber Resilience Playbook for Modern Infrastructure](#).

[Download now](#) →

© Copyright IBM Corporation 2026

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on [ibm.com/trademark](https://www.ibm.com/trademark).

No IT system or product should be considered completely secure, and no single product, service, or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products, or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

