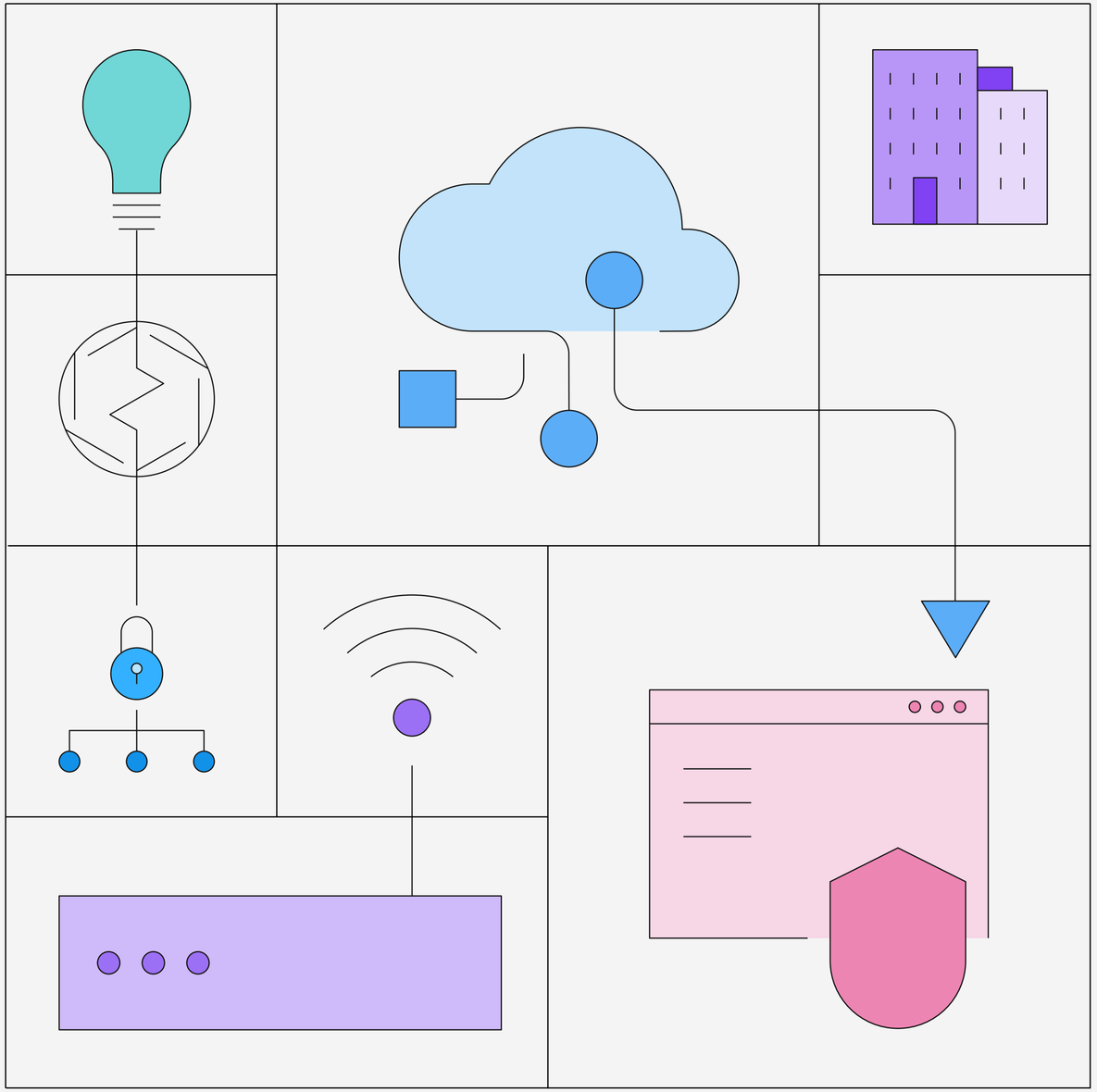
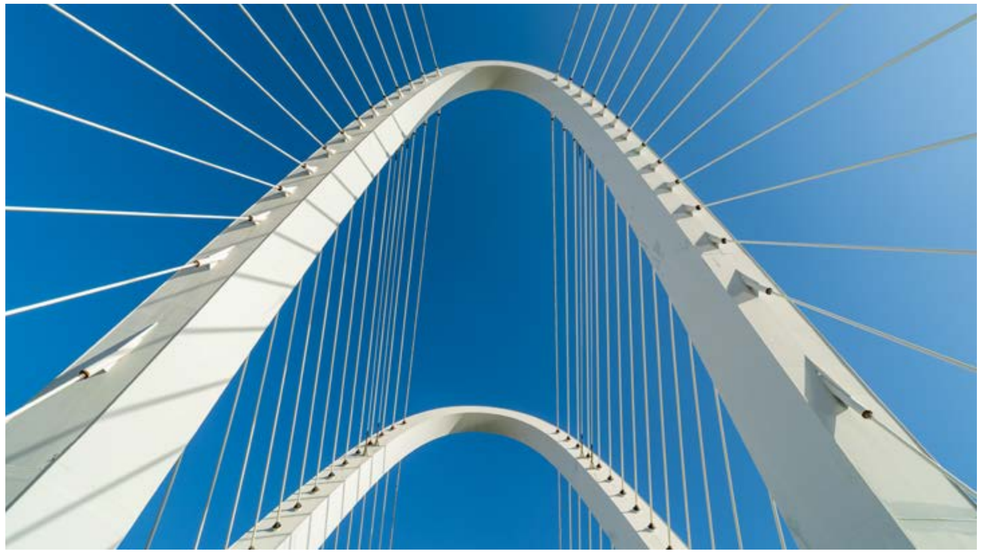
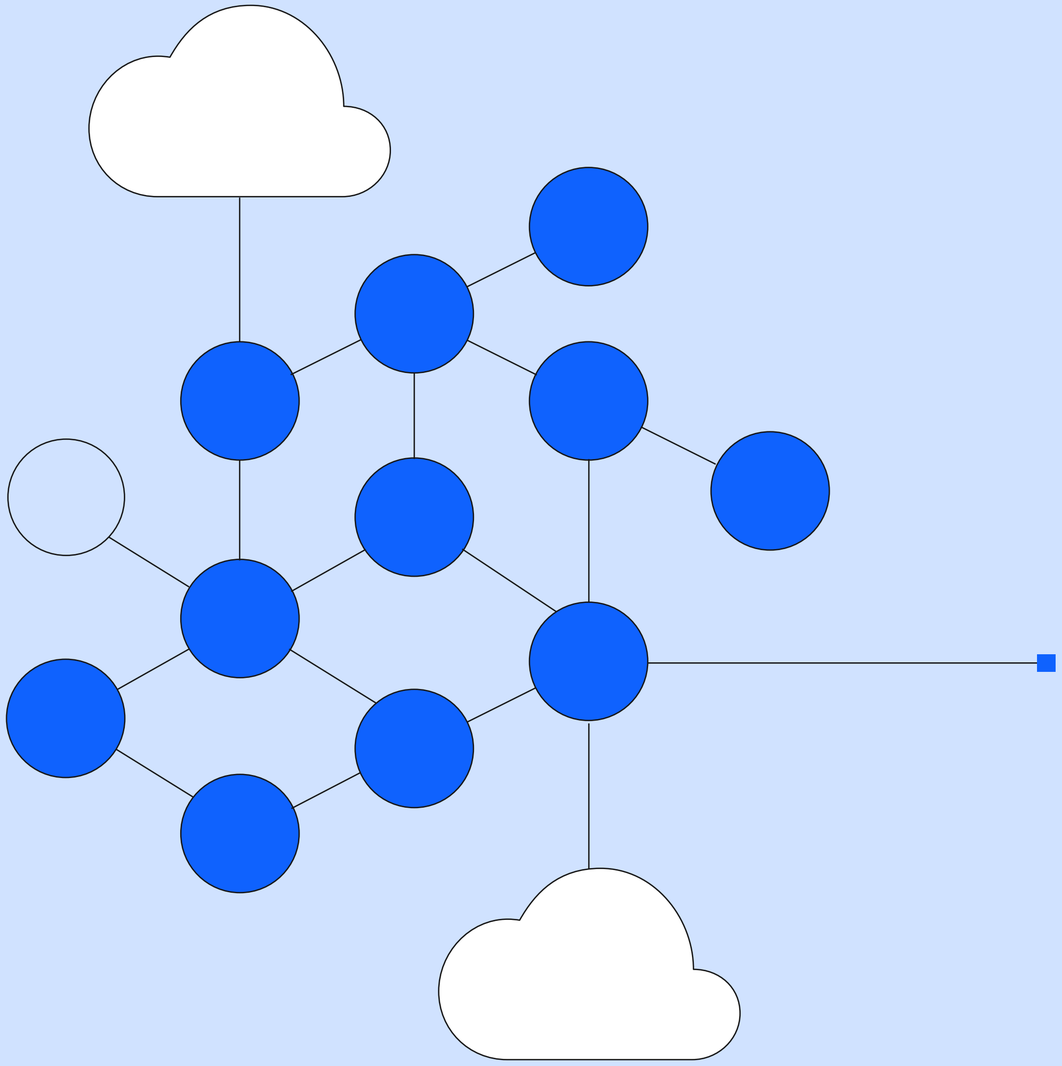
Strategies for building a resilient business with hybrid cloud



Contents





Empower business with hybrid cloud

97% of organizations now operate on more than one cloud.[1]

01

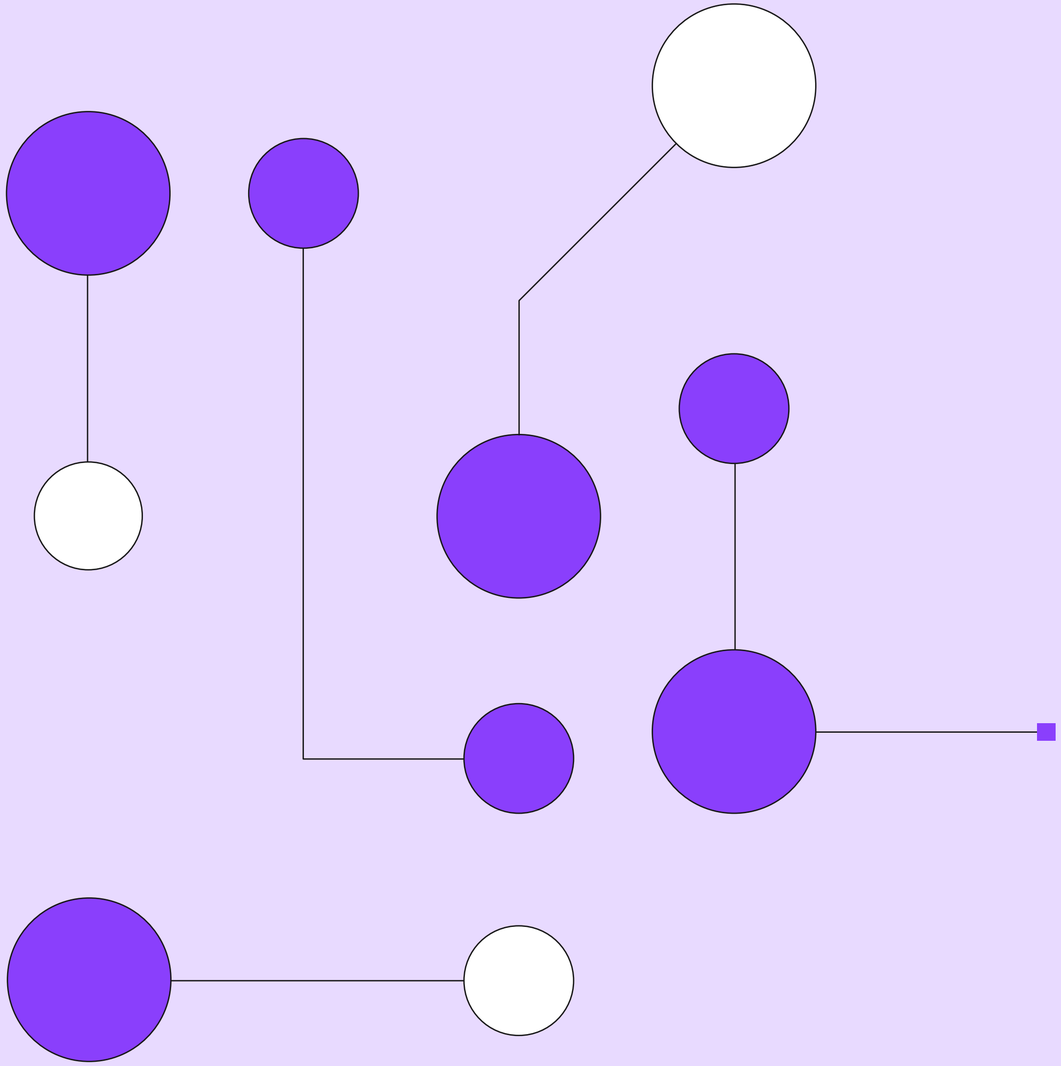
Minimizing risk and maximizing your organizational resilience

Every day, IT and security leaders contend with uncertainty and risk: not only do they navigate a constantly changing regulatory landscape, but they need to avert the nightmare scenario—a security breach that can halt essential business functions for weeks or months.

Faced with so many threats in the here and now, it can be challenging to strategize for the future. The need to maintain business resilience has fueled some businesses' reluctance to embrace a public cloud solution; they worry that if they're hit with a breach and their most critical and sensitive workloads are compromised, they could struggle to recover.

Fortunately, there's an approach that allows businesses to protect their operations, foster innovation and achieve unparalleled flexibility, and it involves exploiting a mix of cloud environments including public, private, multicloud and on-premises infrastructure. By building a plan for resiliency that entails moving workloads to the right destination, businesses can minimize risk, increase the security of their operations and drive innovation at speeds not possible with traditional infrastructure. And they can keep business up and running when the unexpected happens. Resilience becomes the new norm.

The following sections address the ways you can leverage a hybrid cloud platform deftly, so your organization can thrive.

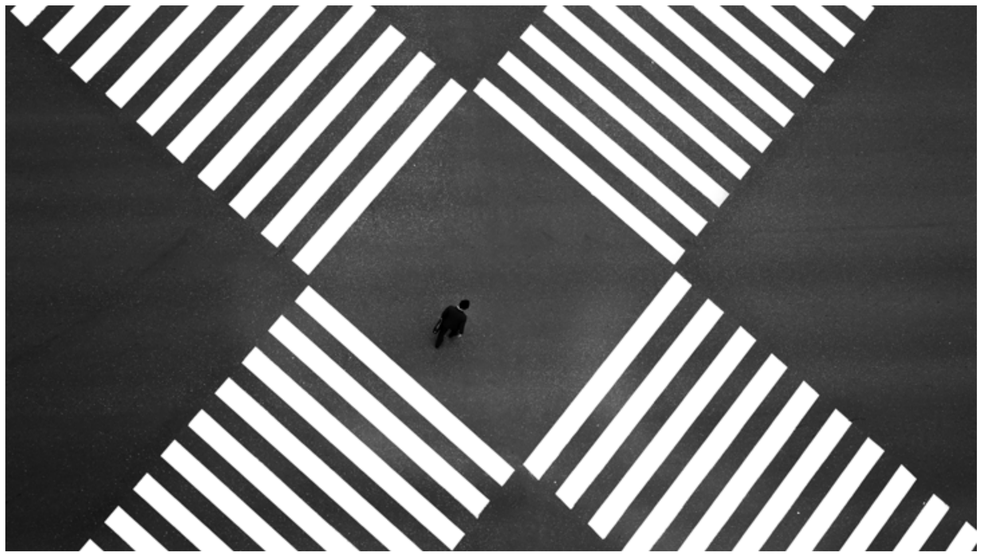


Understand the dynamic environment of security threats

Nearly 7 in 10 organizations have been compromised by shadow IT in the past year.[2]

02

Staying vigilant and protecting sensitive data



When the unthinkable happens, you want response mechanisms in place so your business can bounce back fast. This rapid recovery and response is a major component of cyber resiliency, and it's a challenge, given the ever-evolving risk landscape. Constant awareness and the proper security and cyber resiliency tools help IT and security leaders stay a step ahead of familiar and emerging risks.

Data breaches
Cloud computing environments are targets for cybercriminals looking to steal sensitive information. With data stored in multiple locations and consumers demanding rapid, uninterrupted access, vigilance is essential. Implementing a multilayered strategy for data and cyber resilience—which includes strict access controls and encryption mechanisms—becomes imperative to protect sensitive data, such as Social Security numbers or financial information.

Shadow IT
Unauthorized applications or cloud services used without the knowledge or consent of the IT department fall under the category of shadow IT and can pose a significant threat to the company by creating virtual "doors" that let in bad actors. For example, a department might independently set up its own unsecured cloud account, leaving the company vulnerable to hacks or data exposure.

Misconfiguration
Configuration errors in cloud infrastructure, such as faulty encryption or open ports, can expose data to attacks and breaches. A study of 553 organizations conducted independently by Ponemon Institute and sponsored, analyzed and published by IBM Security® indicated that cloud misconfiguration is the third most common initial attack vector, accounting for 15% of breaches.[3] Proactively baking in security controls

By focusing on the right location for different workloads, businesses can confidently minimize risk. Resilience becomes the new norm.

as part of application development, deployment and operations will reduce the risk of creating a vulnerable posture.

IBM Cloud® with built-in controls can reduce or eliminate misconfiguration issues that businesses face, especially when they use validated services. Hundreds of NIST standards and business controls have been built into the fabric of our public cloud that businesses can take advantage of and manage by way of the IBM Cloud Security and Compliance Center.

Access management
Managing data across multiple users, devices and locations in a cloud environment can be daunting. These complex entries and exits make monitoring and controlling access to sensitive data difficult and increase the risk of data breaches and cyberattacks. Therefore, it's important to have effective privileged access management (PAM) controls alongside mitigating the risk from compromised credentials, which are the most common cause of data breaches.

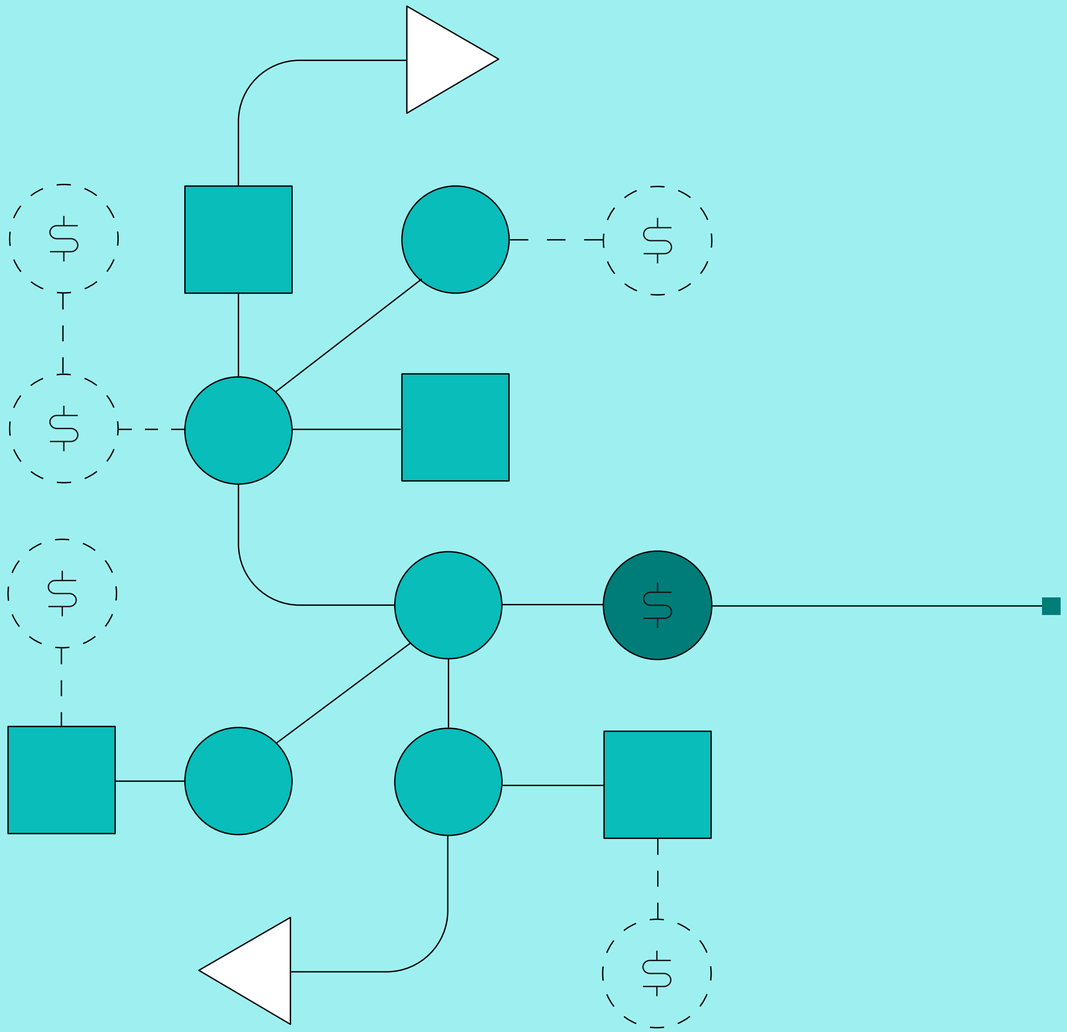
Edge security
There are billions of edge devices in the field today, and these small, inexpensive computational resources bring both convenience and risk. Network-enabled sensors, cameras and other edge devices outside the data center or cloud become easy targets for bad actors.

Cyberattacks, human error, sabotage: whatever the cause, your response and recovery should focus on cyber resiliency and data resiliency—an enterprise-wide strategy to be proactive about risks, threats, vulnerabilities and the effects on critical information. Not only does that approach give you a prevention plan, it also provides a strategy to recover quickly if systems go down or bad actors tamper with your technology.

02

USD 4.45M

Global average cost of a data breach in 2023[3]



Enable innovation by way of regulations

Data breaches at organizations with high levels of noncompliance cost USD 5.05 million on average, **exceeding the average cost by 12.6%.**[3]

Guidelines for avoiding noncompliance risk

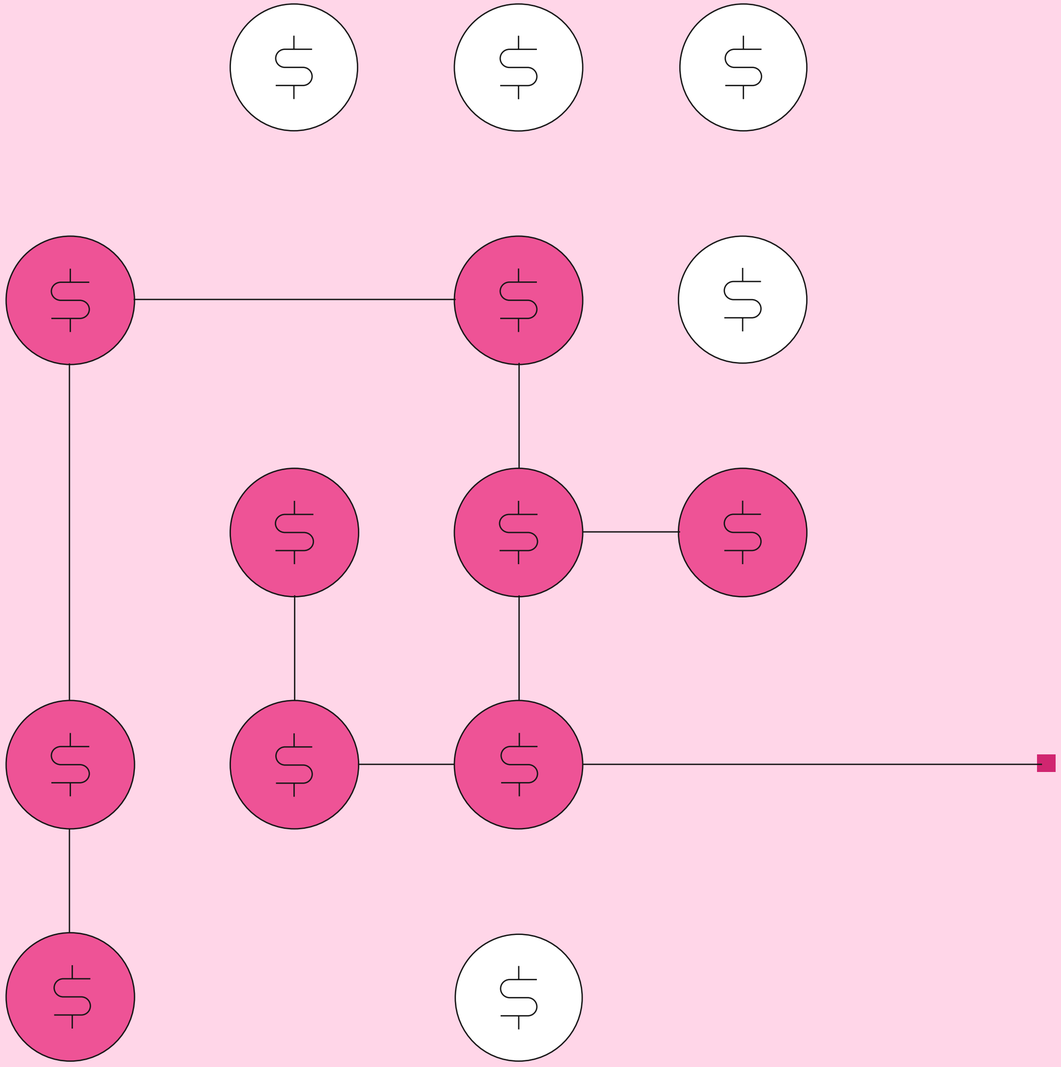
Many industries have cloud-specific requirements around compliance, such as the European Banking Authority guidelines on information and communication technology and security risk management for financial services. It's critical that leaders know how at risk they are—with both vertical (sector-specific) and horizontal (cross-sector) requirements—and set up the right guardrails to protect them from threats. Leaders can define prescriptive controls that can be codified, implemented consistently and automated at scale. Following these rules of the road, compliance and innovation can happen together to help ensure business resilience.

IT and security leaders must comply with all applicable regulations and standards, from CCPA (the California Consumer Privacy Act) to DORA (the EU's Digital Operational Resilience Act), to avoid legal and financial repercussions.

When putting together a secure cloud strategy, adopt strong risk-based, data-centric security policies and governance to mitigate risk and achieve compliance.

To innovate rapidly, understand the risks and establish consistent, prescriptive policies and controls to protect the business across hybrid cloud deployments—whether on premises or in the cloud.

Automated preconfigured controls can help organizations get back to innovating by helping to ease compliance concerns and streamline reporting.



Manage security and boost inovation

66% of executives view cybersecurity primarily as a revenue enabler.[4]

04

Reaping benefits while keeping a lock on data

Embracing a hybrid cloud approach to building cyber resiliency into your infrastructure brings the benefits of public and private clouds while minimizing the constraints associated with each. Some key examples follow.

Secure data management

Adopting a hybrid cloud approach can help IT and security leaders keep sensitive data and workloads safe across multiple environments—private cloud, public cloud, on premises, multicloud and edge. 82% of breaches occurring between March 2022 and March 2023 involved data stored in and across multiple cloud environments.[3] Thus, it's self-evident that a hybrid cloud approach to data security holds the greatest promise to stave off bad actors and potentially avoid costs from data breaches. Leaders can feel confidence in putting sensitive data in a secure IBM Cloud environment, because they're provided technical assurance that private workloads, data and access keys remain in their control.

Products like IBM Cloud Hyper Protect Crypto Services provide dedicated key management with Keep Your Own Key capabilities, offering exclusive control of your encryption keys. With Unified Key Orchestrator, a component of IBM Cloud Hyper Protect Crypto Services, businesses can manage keys not only for their internal keystores but across multiple cloud providers, including Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform. With IBM Cloud Data Security Broker, enterprises can achieve granular control with field-level encryption to gain technical assurance that sensitive data stored in the cloud, such as personal identifiable information (PII), is safeguarded.

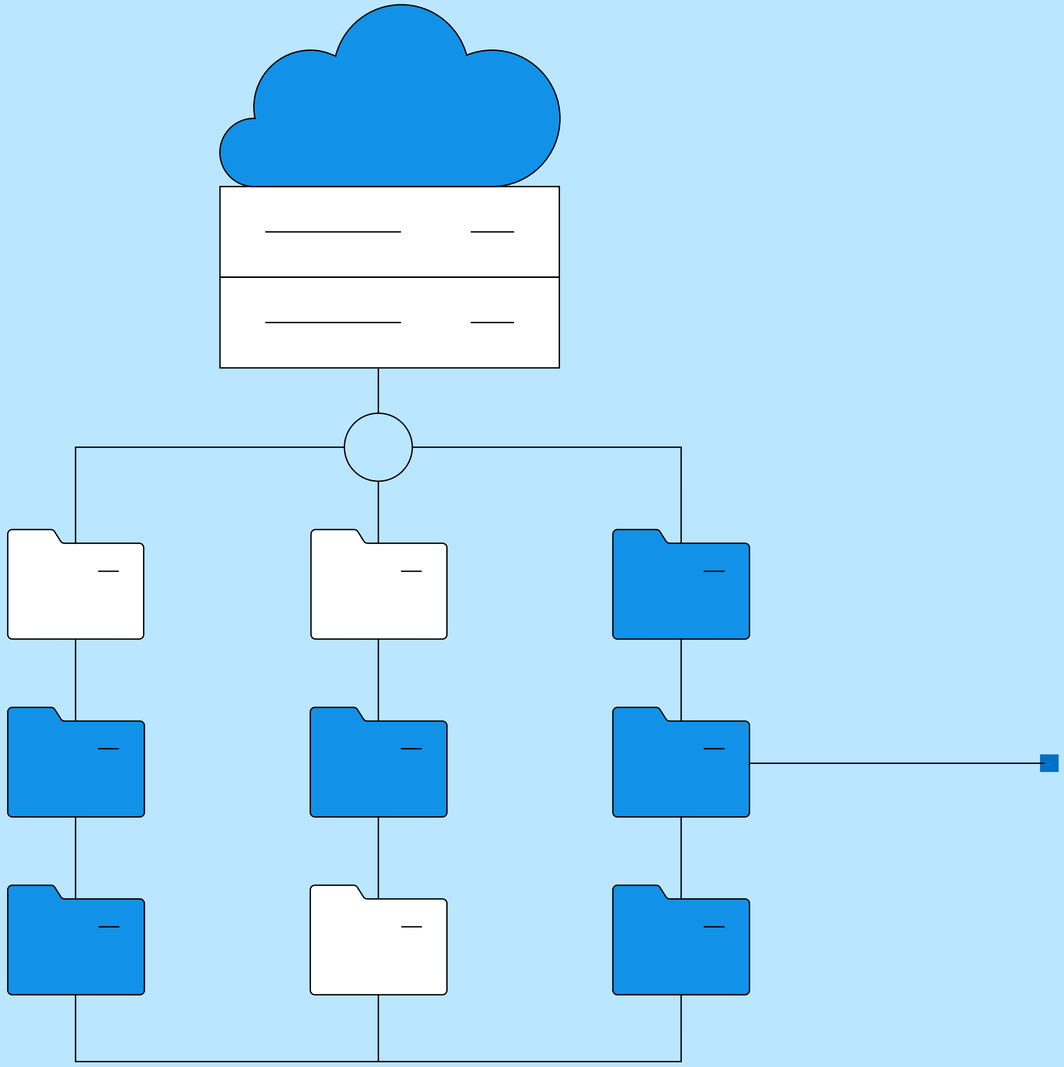
In short, a hybrid cloud approach provides a higher level of security for critical data while enabling innovation to occur outside the private cloud.

Visibility and risk management
Keeping pace with the rapid changes in cloud environments requires constant vigilance. Integrating security and compliance across a hybrid multicloud environment can provide continuous visibility into your security, compliance and risk posture. This helps reduce risks associated with the public cloud while allowing organizations to reap the benefits of cloud usage. Organizations can also apply the same approach to their software and SaaS vendors to mitigate third-party risk. Features like the IBM Cloud Security and Compliance Center and the IBM Cloud Framework for Financial Services offer built-in controls and continuous compliance to keep security and compliance concerns in check.

Flexibility and scalability
By taking advantage of the flexibility of hybrid cloud, organizations can quickly scale up or down in response to changing business needs while maintaining control over critical data. Capitalizing on the cloud ecosystem enables businesses to modernize applications and migrate mission-critical workloads to the cloud, ensuring they can keep up with increased demand. This promotes innovation without compromising the enterprise's risk posture.

Automation
Adopting an agile DevOps workflow, such as the continuous integration and continuous delivery (CI/CD) pipeline, simplifies application development and operations. By combining work from different contributors into a single cohesive product, the CI/CD pipeline accelerates the development process and improves accuracy. And by infusing security and compliance controls using prebuilt, repeatable and secure architecture blueprints, enterprises can achieve a mature DevSecOps process that yields consistent and continuous security. Automation tools can help development teams seamlessly integrate and test their code, which results in faster and more reliable application deployment.

Continue →

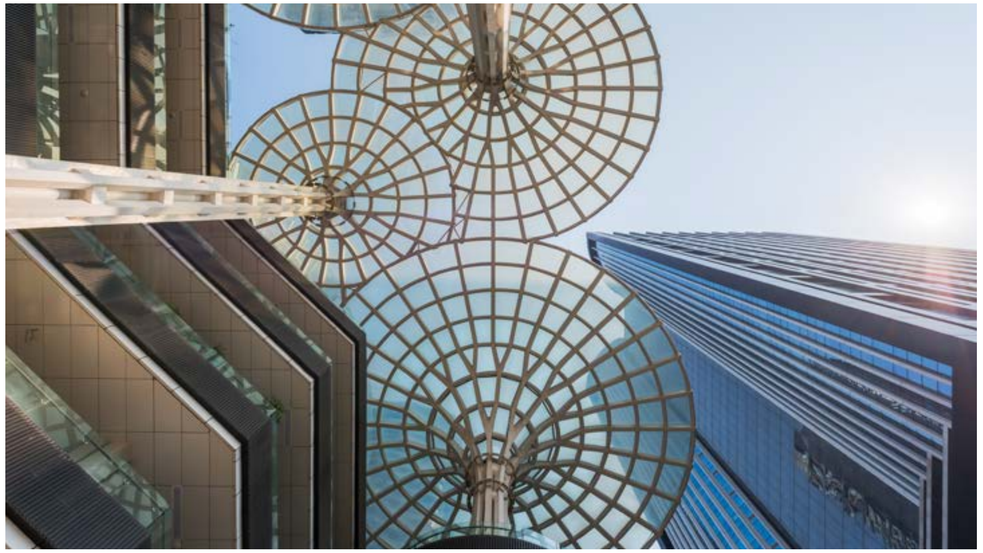


Harness hybrid cloud for security, agility and growth

71% of executives think it’s difficult to realize the full potential of a digital transformation without having a solid hybrid cloud strategy in place.[5]

05

Understanding the holistic benefits of a secure hybrid cloud environment



Having confidence in your cloud strategy frees up your organization to think beyond the cloud and unleashes holistic benefits for your business. Here are a few ways a hybrid cloud can fuel growth and innovation.

Lay the groundwork
Combining hybrid cloud with other levers of business transformation can generate up to 13 times greater benefits than cloud alone.[6]

Empower the edge
Hybrid cloud simplifies edge computing and vice versa. Furthermore, 61% of IT leaders plan to run Internet of Things (IoT), edge computing or both in the next 12 months.[7]

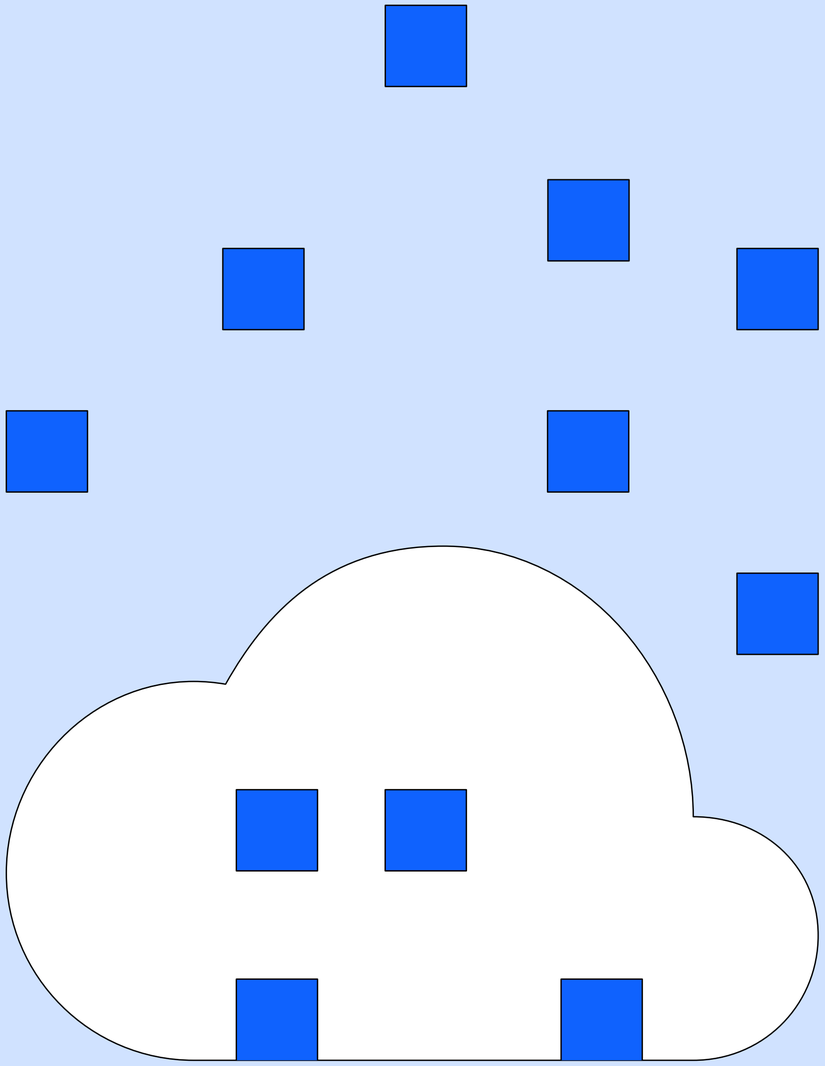
Accelerate business
A hybrid cloud environment enables shorter product development cycles and accelerated innovation and time to market. In addition, businesses could achieve faster response to customer feedback, swift delivery of applications closer to the client (for example, edge, e-commerce) and seamless integration with partners or third parties to deliver new products and services.

Learn more about how hybrid cloud can accelerate innovation →

05

USD 5.9M

Average cost of a data breach in the financial sector[3]



Embrace the power of a hybrid cloud platform

- Done right, a hybrid cloud platform can help your business stay resilient.

06

Ensuring seamless business operations with hybrid cloud

Here are a few key ways to ensure seamless business operations with hybrid cloud.

Connect and streamline IT environments
Hybrid cloud builds trust around security and compliance, safeguards your data and speeds innovation, regardless of where your data sits or where your workloads are. With IBM Cloud for Financial Services®, financial institutions can automate their compliance needs with preconfigured controls that operate with agility everywhere. That means banks can confidently deploy essential workloads while protecting sensitive data and staying up to date with compliance standards.

Simplify data management
With cyber-resilient data storage operating across disparate environments, your hybrid cloud platform streamlines administration and reduces complexity. Organizations that consolidate and manage all storage as if it were one pool reduce administrative effort. IBM FlashSystem® makes that possible. With IBM FlashSystem, businesses are also prepared to recover more quickly from cyberattacks. This was the case with Micro Strategies Inc.—an IBM Business Partner and IBM IT solutions provider. The company installed IBM Cyber Vault on IBM FlashSystem 7200 to secure data for America's fastest-growing mortgage lender. Now, the lender doesn't risk losing millions in a ransomware attack.

Resilient storage at enterprise scale
By scaling up to manage billions of objects per backup server with a hybrid cloud platform, organizations can drive efficiency, reduce backup infrastructure costs and protect the storage environment for physical file servers, virtual environments and a wide range of applications. IBM® Storage Defender, a SaaS suite for data resiliency, provides visibility for end-to-end data resilience across your primary and secondary workloads. Detect threats such as ransomware, exfiltration and insider attacks, leveraging intelligent software from IBM and its ecosystem partners.

IBM Cloud Cyber Recovery, a solution for approaching cyber-risk mitigation, provides an isolated and secure recovery environment with resources to verify and recover data. Recover from ransomware attacks while maintaining compliance, regulatory requirements and protection through an isolated data-recovery infrastructure.

By leveraging a hybrid cloud platform along with these essential components, you can keep your business running smoothly and navigate the unexpected—and free up your teams so they spend less of their day-to-day work worrying about risks and more time building for the future. With IBM, you can build a resilient foundation that supports your long-term success in an always-changing landscape.

To learn more about accelerating your digital transformation with IBM Cloud, set up a no-cost consultation with an IBM Garage™ expert.

Book a consultation →

1. Cloud's next leap, IBM Institute for Business Value, October 2021.

2. The State of Attack Surface Management 2022, Randori, February 2022.

3. Cost of a Data Breach Report 2023, IBM Security, July 2023.

4. Prosper in the cyber economy, IBM Institute for Business Value, November 2022.

5. The new era of cloud security, IBM Institute for Business Value, June 2021.

6. IBM Transformation Index: State of Cloud, IBM Institute for Business Value, September 2022.

7. Innovating at the Edge? How Hybrid Cloud Overcomes the Complexity, IBM, November 2022.

IBM Cloud
IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
October 2023