IBM Cloud

Cost of a Data Breach

A view from the cloud 2021

IBM Security

IBM

Cloud-based data breaches

According to this year's X-Force Threat Intelligence Index from IBM Security®, the number of breached records – and the severity of these breaches – grew dramatically despite an overall decline in the number of breach incidents across public and private sectors[1]. In 2021, we saw these numbers rise again.

At times these breaches stem from the client, other times from the client's cloud provider, and sometimes the fault rests with both. Unfortunately, whether a company is at fault or not, the costs of a data breach, from lost revenue to brand damage, can be significant.

While the most common initial threat vector in the 2021 Cost of a Data Breach Report (CODBR) from the Ponemon Institute and IBM Security was compromised credentials, cloud misconfiguration was the third most-common threat, accounting for 15% of breaches. As more companies and clients rely on cloud solutions, it is increasingly important to look at the costs of cloud-based breaches and learn how to mitigate the risks.

When the COVID-19 pandemic pushed more companies and industries into remote working, the result was an uptick in cloud migrations; this was accompanied by more costly breaches. According to the CODBR, companies with higher levels of cloud migration had an average cost of breach of $5.12 million USD, compared to $3.46 million USD for those with low levels of cloud migration[2].

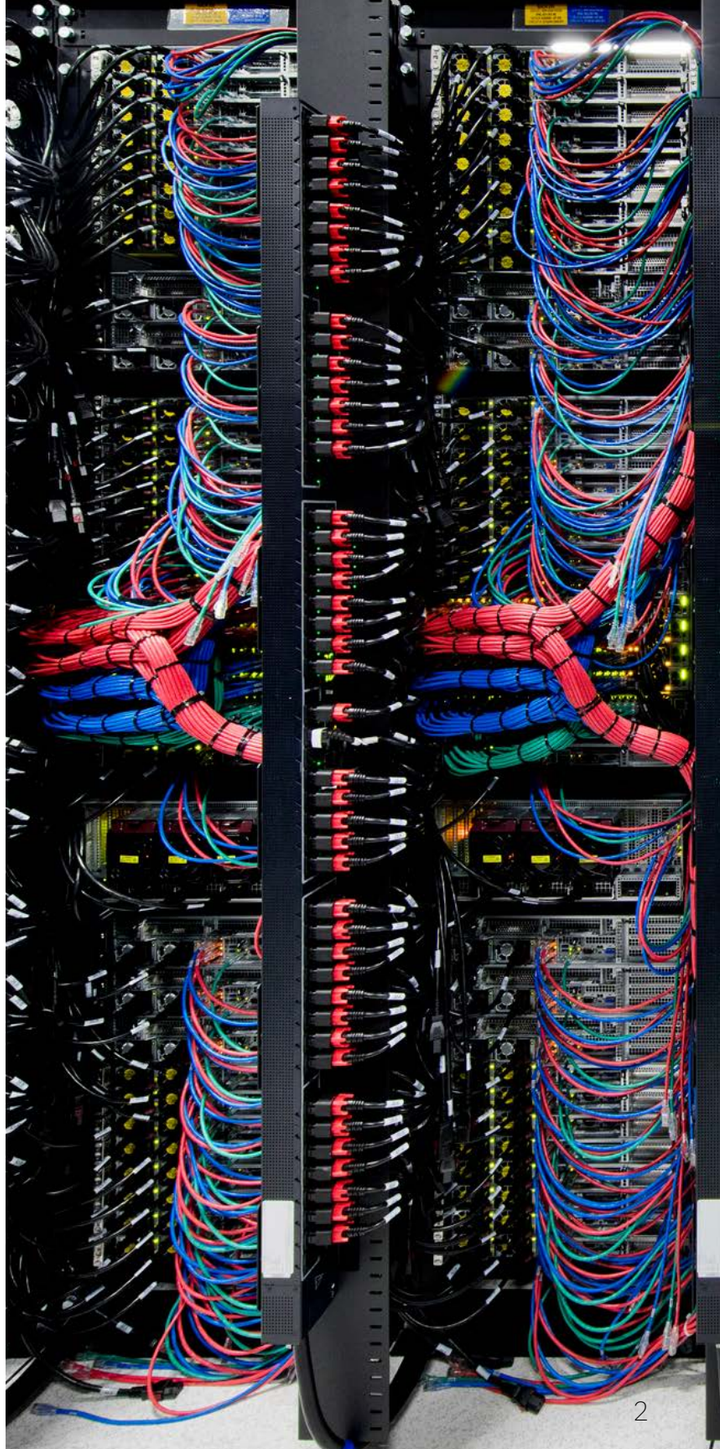
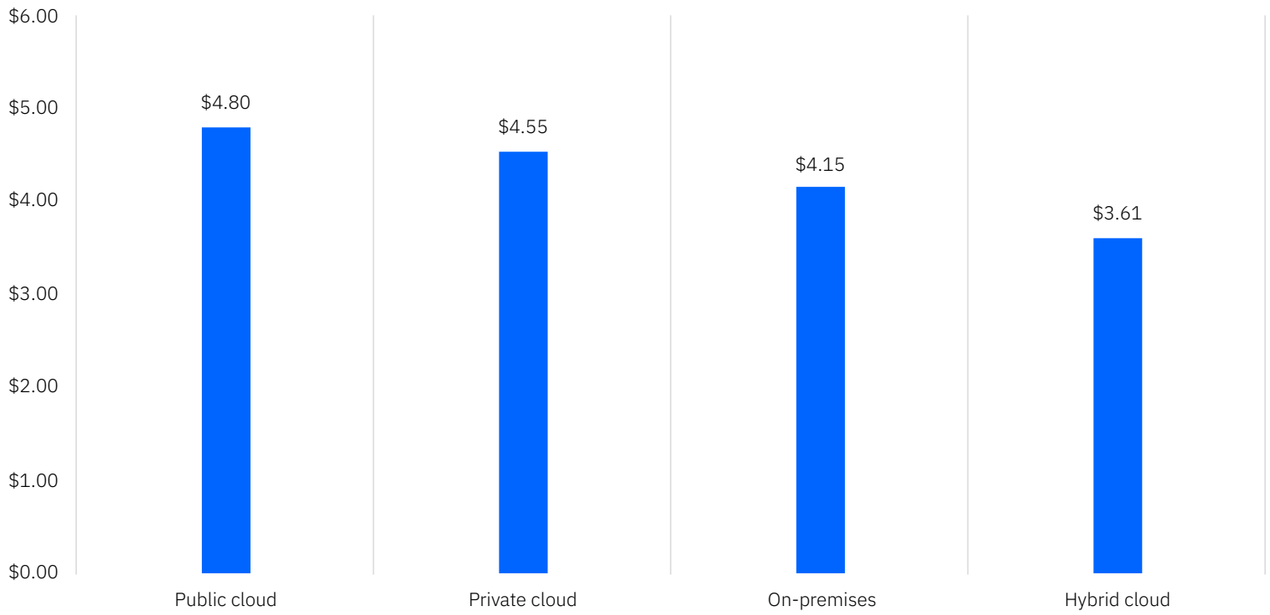


Figure 1

Impact of cloud on the average cost of a cloud-based breach based on model

Measured in US$ millions

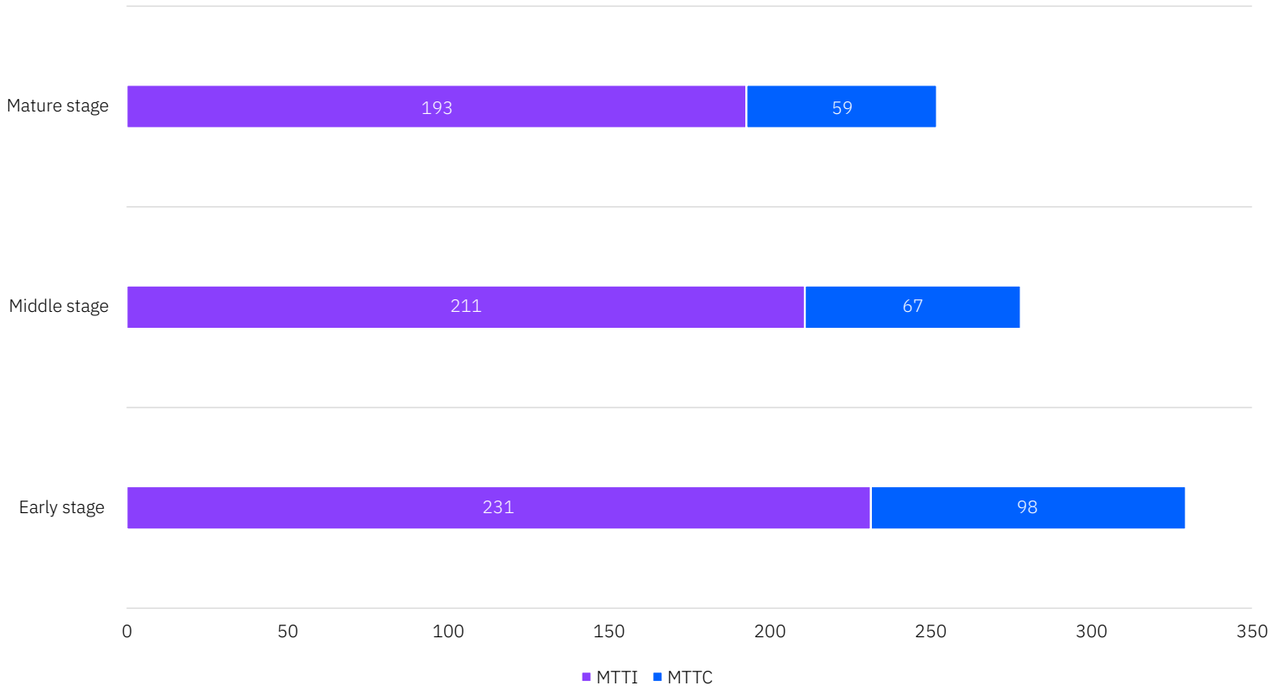


Different cloud solutions leave companies exposed to varying degrees of risk. The CODBR 2021 shows public cloud-based breaches cost the most – an average of $4.80 million USD – while breaches in hybrid cloud-based models cost the least at $3.61 million USD.

Source: Cost of a Data Breach Report 2021

Figure 2

Days to identify and contain cloud-based data breach incidents by cloud migration stage



If one were to stop there, the conclusion might be to minimize cloud migration altogether. However, a cloud presence is not the single greatest risk factor. The 2021 CODBR tells us the stage of migration is a significant factor in the likelihood of a breach, the median time to identify a breach (MTTI), and the median time to contain a breach (MTTC). These factors, in turn, affected the total cost of a data breach for surveyed organizations.

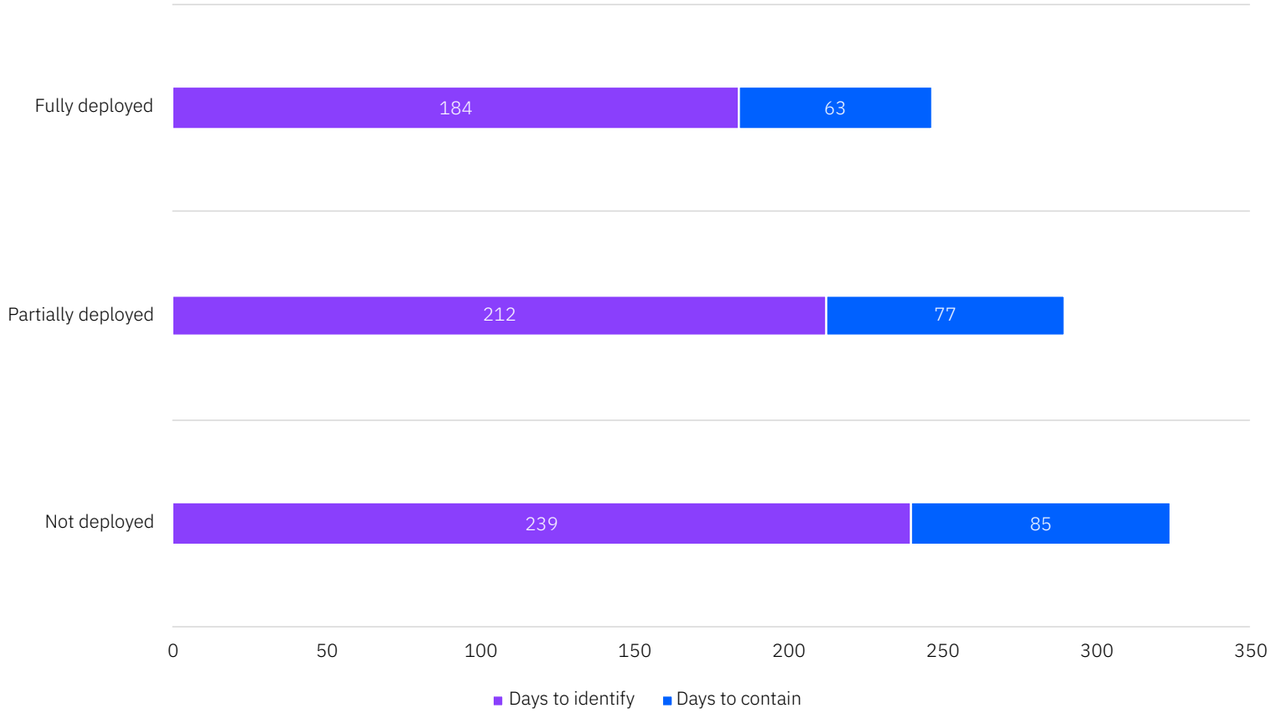
For responding organizations early in their cloud migration, public cloud and hybrid cloud environments seem to have been challenging to secure and manage. These challenges can result in higher front-end costs, as users employ more tools and software for the sake of securing cloud environments they don't understand. This early lack of understanding and lower level of clear management across tools and processes might explain why MTTI and MTTC are longer for responding organizations in an early stage of cloud migration.

Source: Cost of a Data Breach Report 2021

Figure 3

Average time to identify and contain a data breach by level of security automation

Measured in days

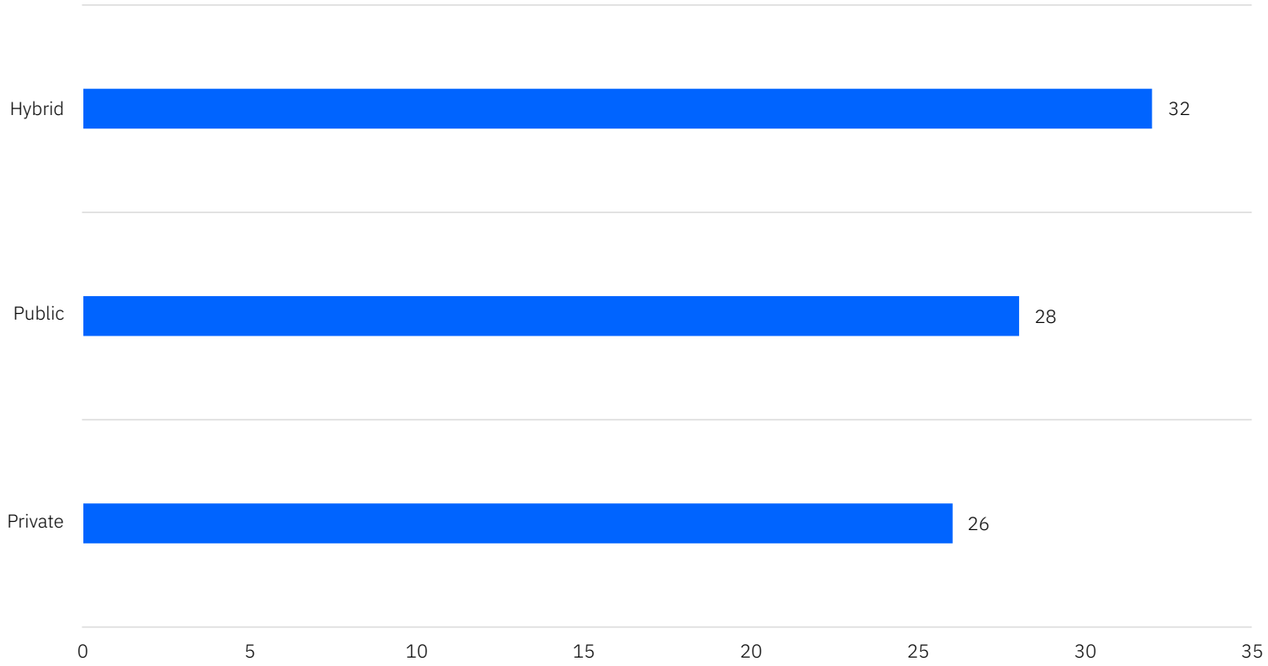


The increase in cloud migration and remote working led more companies to increase their use of security automation and artificial intelligence (AI). Employing these tools was associated with a lower average cost of data breach and shorter breach lifecycle. Responding companies with no security AI and automation averaged a hefty cost of $6.71 million USD per breach, whereas an organization with a fully deployed system saw costs averaging $2.90 million USD. The 2021 CODBR indicates that using an AI platform was a leading factor in mitigating costs, with an average cost difference of $1.49 million USD.

Source: Cost of a Data Breach Report 2021

Figure 4

Average number of cloud-based security tools by cloud model



Unfortunately, having more tools does not inherently equal better security; the array of products and services across several dashboards can mean that vulnerabilities can be missed. The 2021 CODBR shows that it took responding organizations less time to identify and contain breaches from a mature stage of cloud migration, indicating that correct configuration and greater platform management can play significant roles in minimizing risk and cost. Therefore, companies with higher rates of cloud migration and higher average costs of data breaches may be at risk due to being in an early stage of cloud migration and not having a clear view of all tools and systems in place.

Source: Cost of a Data Breach Report 2021

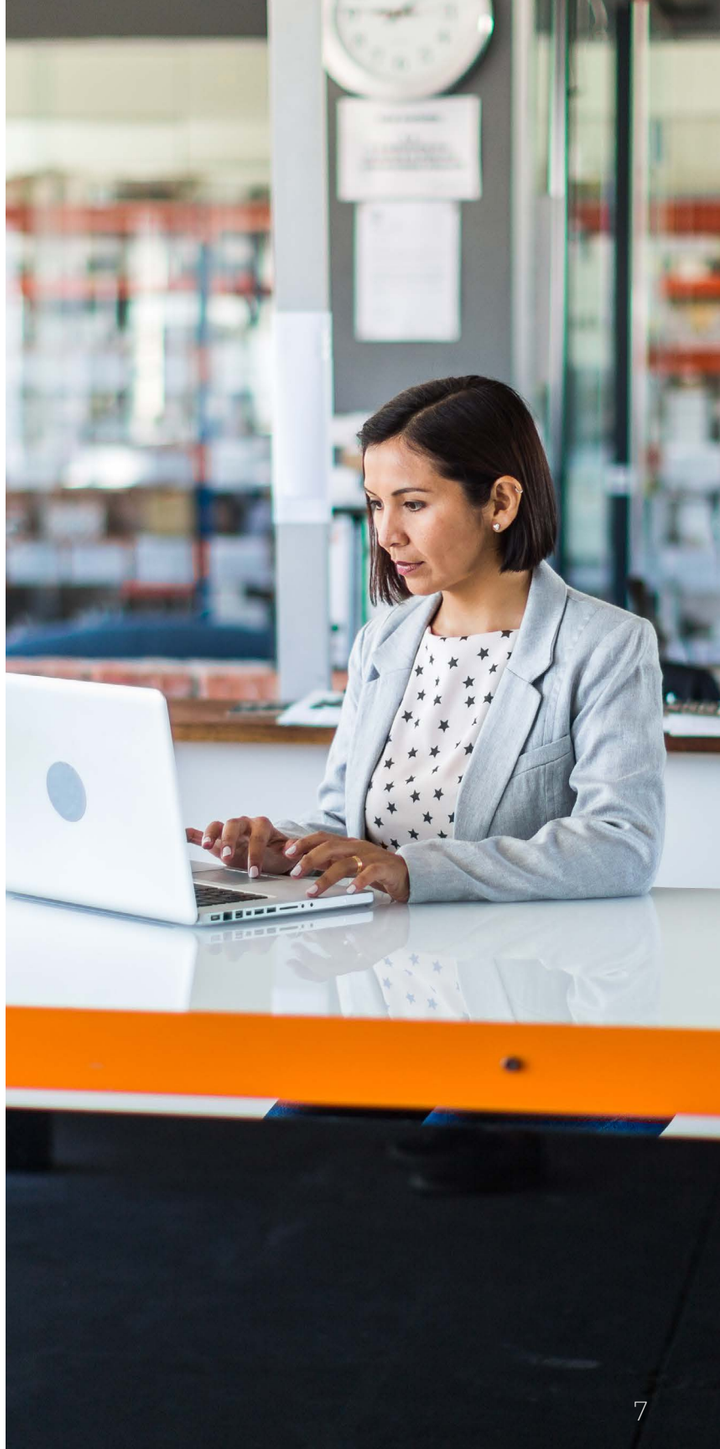
Mitigating incident impact with confidential computing

The findings highlighted above point to two key areas of improvement when it comes to mitigating risk and cost: 1) having a more mature, hybrid cloud infrastructure, and 2) having your hybrid cloud environment configured correctly and managed effectively for your end-to-end security needs.

These two areas of improvement apply across client use cases, including:

- A large financial services institution with strict regulatory requirements for technical assurance that only they have access to their encryption keys.
- A major health insurance provider with strict data protection and user privacy regulations that needs their cloud platform to provide a trusted execution environment (TEE) for processing data.
- A digital assets custody (DAC) case in which the owner of the asset needs to maintain control of the associated private key, even when that key is in use.

For these clients and many more, their needs can be addressed with confidential computing, a cloud computing technology that helps protect data in use by isolating sensitive data in a protected CPU and performing computation in a hardware-based TEE. The data and data processing techniques are accessible only to authorized programming code and invisible or unknowable to anything or anyone else. The goal is to provide companies with technical assurance that their cloud-based data is confidential and secured, and not even their cloud service provider can access it.



Managing risk with IBM Cloud®

For more than a decade, IBM has invested in technologies to help clients manage and secure their workloads across ecosystems. IBM Cloud and IBM Security bring unified dashboards for manageability and visibility.

Data security and confidential computing
Confidential computing with IBM Cloud gives clients authority over their data by protecting it across the compute lifecycle – at rest in storage containers and databases, in use during processing, and in transit across the network.

IBM Cloud offers a range of confidential computing services, including IBM Cloud Hyper Protect Crypto Services and IBM Cloud Data Shield. IBM Cloud Hyper Protect Crypto Services leverages FIPS 140-2 Level 4 certified commercial cloud hardware security module (HSM), while providing Keep Your Own Key (KYOK) and technical assurance which means not even IBM can access client data. IBM Cloud Data Shield, built on Intel® SGX and Fortanix Runtime Encryption Platform, enables clients to protect containerized applications in a secured enclave on a Kubernetes service and Red Hat® OpenShift® clusters without requiring a code change.

With IBM Cloud data protection, the client is the only party that governs and has access to their private data, so that the client is in control. These capabilities can be game-changing for industries including financial services, government, and healthcare, which need to adhere to strict regulatory requirements for data protection.

Security and compliance management
Within the IBM Cloud platform, the IBM Cloud Security and Compliance Center provides each client with a single, unified dashboard from which they can view and control all their security and compliance postures. With the recent integration of Tanium Comply, clients can view their compliance data associated with IBM Cloud and Tanium in the same format in one location. The Tanium integration also positions IBM Cloud clients to potentially extend their organization's endpoint management capabilities to include scanning for vulnerabilities and misconfigurations against industry security standards and vulnerability definitions.

Additional IBM Cloud Security and Compliance Center features include:

- Automation for security and compliance postures
- Configuration governance
- Vulnerability and threat detection protocols
- Predefined and custom profiles to address client needs
- Network and user behavior monitoring
- Audit reports and evidence
- Endpoint management and visibilty with Tanium Comply

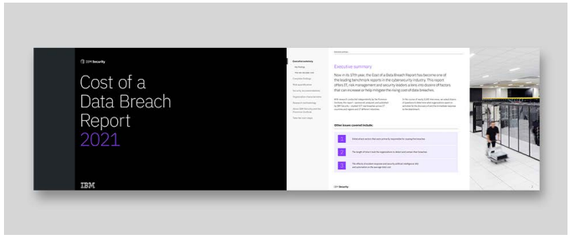
In short, the IBM Cloud platform is designed to lower the levels of common data breach risk and cost amplifiers: cloud migration, system complexity and misconfiguration, and compliance or visibility failures.

Visibility and end-to-end security

IBM Cloud clients can help mitigate their risk of a data breach with built-in capabilities that provide visibility, proactive monitoring, and security intelligence across their hybrid cloud deployments. In short, clients can mitigate risk with a more comprehensive end-to-end approach to cloud security.

The unified solution means clients can avoid unnecessary expenditures on extra tools to help reduce the cost or risk of data breaches. More is not necessarily better. When it comes to compliance, security, and risk management of vital data, the right cloud solution is the best defense. Whether a client needs different tools to make early migration a smoother process, solutions to consolidate their migration to the cloud, or a better way to visualize secure data end-to-end, IBM Cloud can help.

Take the next steps



Cost of a Data Breach Report 2021

Download the full report.

Download now →

Confidential Computing on IBM Cloud

Gain a higher level of privacy assurance with complete authority over your data in use, at rest, and in transit.

Learn more →

IBM Cloud Security and Compliance Center

Manage security and compliance controls from a unified dashboard.

Learn more →

Confidential Computing for Total Privacy Assurance

Learn why confidential computing is essential to protecting your sensitive data.

Read the smartpaper →

About IBM Cloud

IBM Cloud is a full stack cloud platform with over 170 products and services covering data, containers, AI, IoT, and blockchain. Built on the design principles of hybrid, multicloud, open, secure, and consistent management, IBM Cloud offers industry expertise in mission-critical processes.

IBM Cloud clients can confidently build and run anywhere with Red Hat® OpenShift® while leveraging the latest innovations from the open-source community.

Trusted by 47 of the Fortune 50 companies, all 10 of the top 10 largest banks, and 8 of the 10 largest airlines, IBM Cloud is considered the most open and secure public cloud for business. To learn more, visit ibm.com/cloud.

Citations

1. IBM Security, “X-Force Threat Intelligence Index 2021.” https://www.ibm.com/downloads/cas/AWJ3PE1M

2. IBM Security, “Cost of a Data Breach Report 2021,” July 2021. https://www.ibm.com/account/reg/us-en/signup?formid=urx-50915

IBM Cloud

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
August 2021

IBM