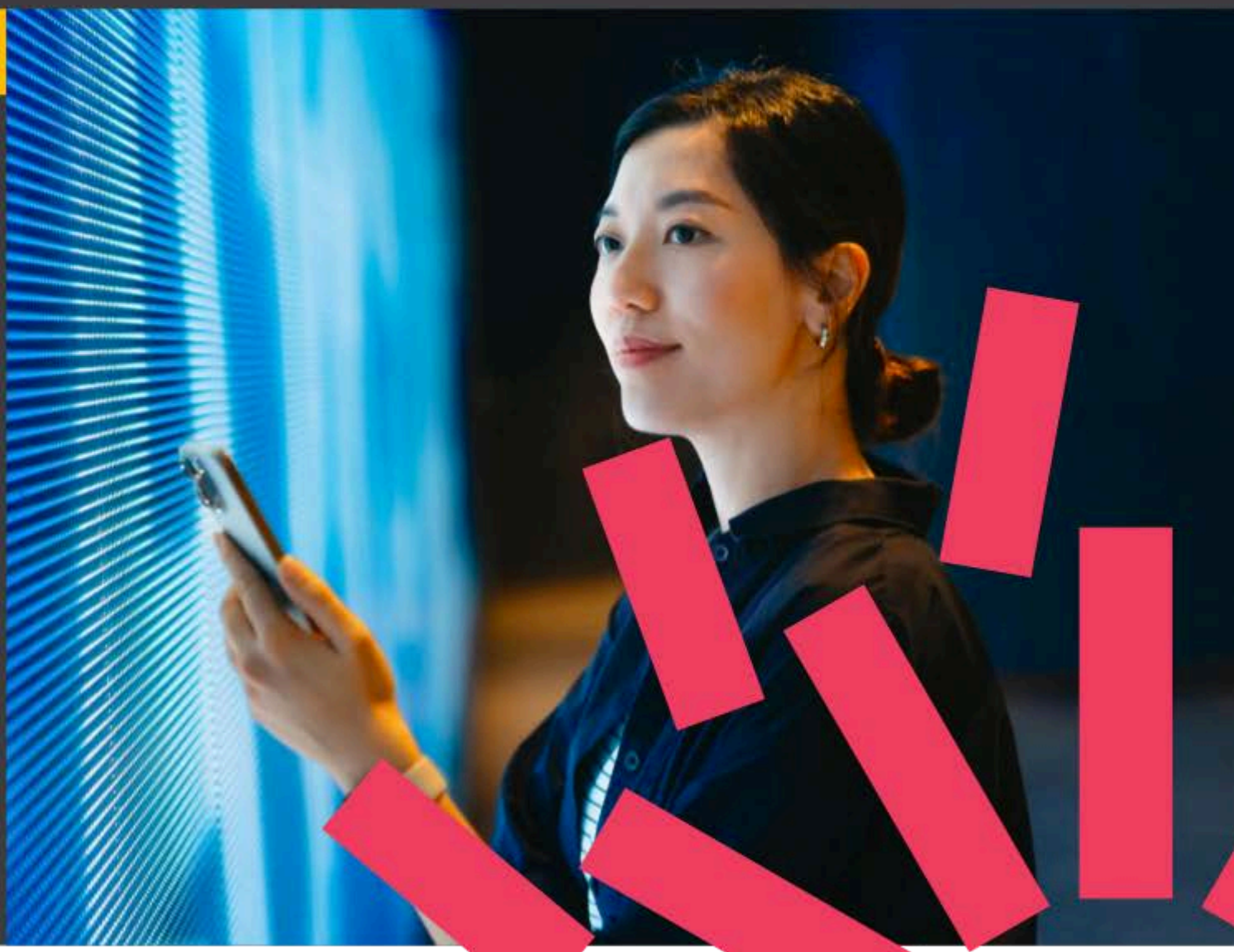
Harmonising cloud transformation and data security

April 2024



pwc

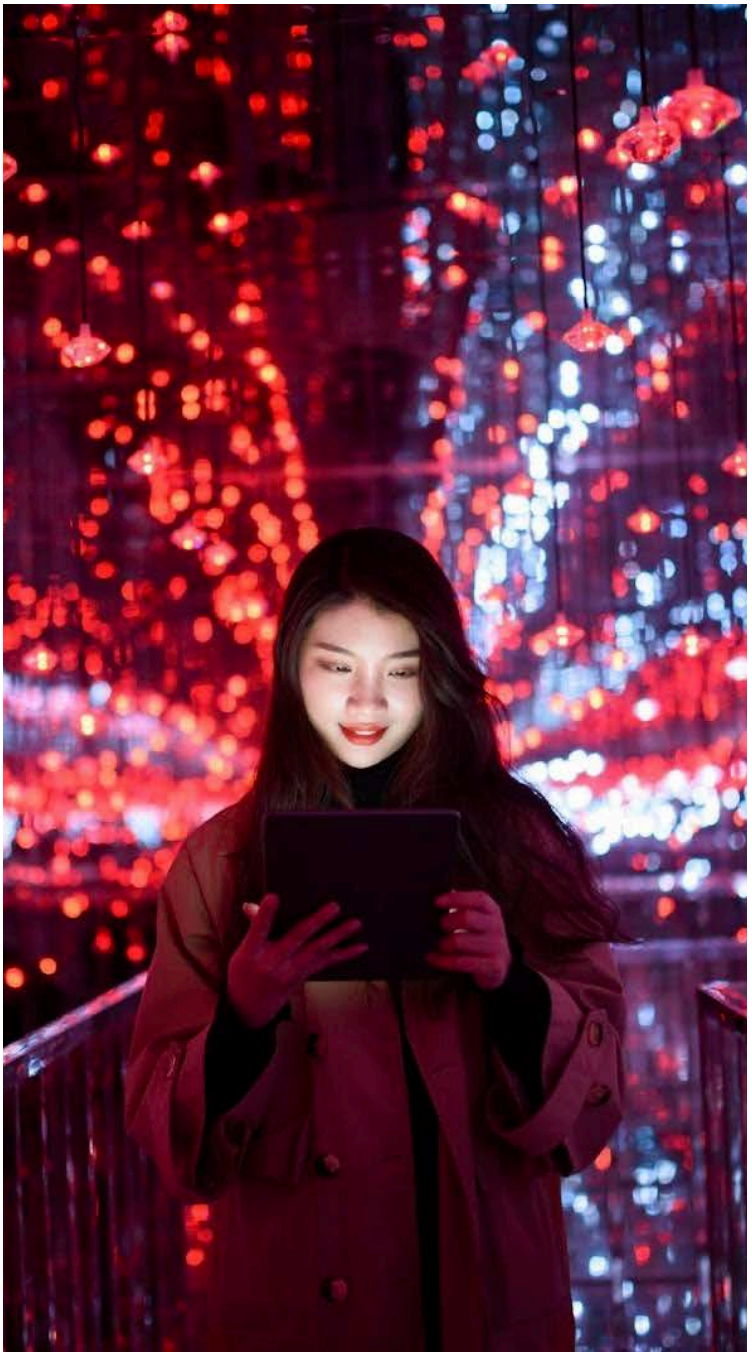
Table of content

How data security is a critical enabler for complex and agile cloud transformations

Background

Cloud transformation and data security are inextricably linked. However, potential conflicts between the cloud transformation leader, chief information security officer and data protection officer can not only impede implementation, but also impair cloud agility and performance. That is why it is so important to balance cloud security with usability by aligning the priorities of these key players. The results would turn data protection from an inhibitor to an accelerator of transformation.

As our latest CEO survey highlights, businesses are moving further and faster on transformation. Rapidly evolving industry cloud capabilities are powering this change. They can not only help your business to become more agile, efficient and innovative, but also improve customer experience and provide an entry point for emerging technologies such as **generative artificial intelligence** (GenAI).



Heightened vulnerability

Modernising systems and dealing with the proliferation of data comes with challenges, especially heightened cyber vulnerabilities. Today's far-reaching cloud transformations involve large amounts of confidential and sensitive data, with complex privacy and security requirements. The scale and complexity of the challenges are reflected in the fact that cloud security is the number one risk concern for business leaders taking part in our 2024 Global digital trust insights survey.

Pulling in different directions

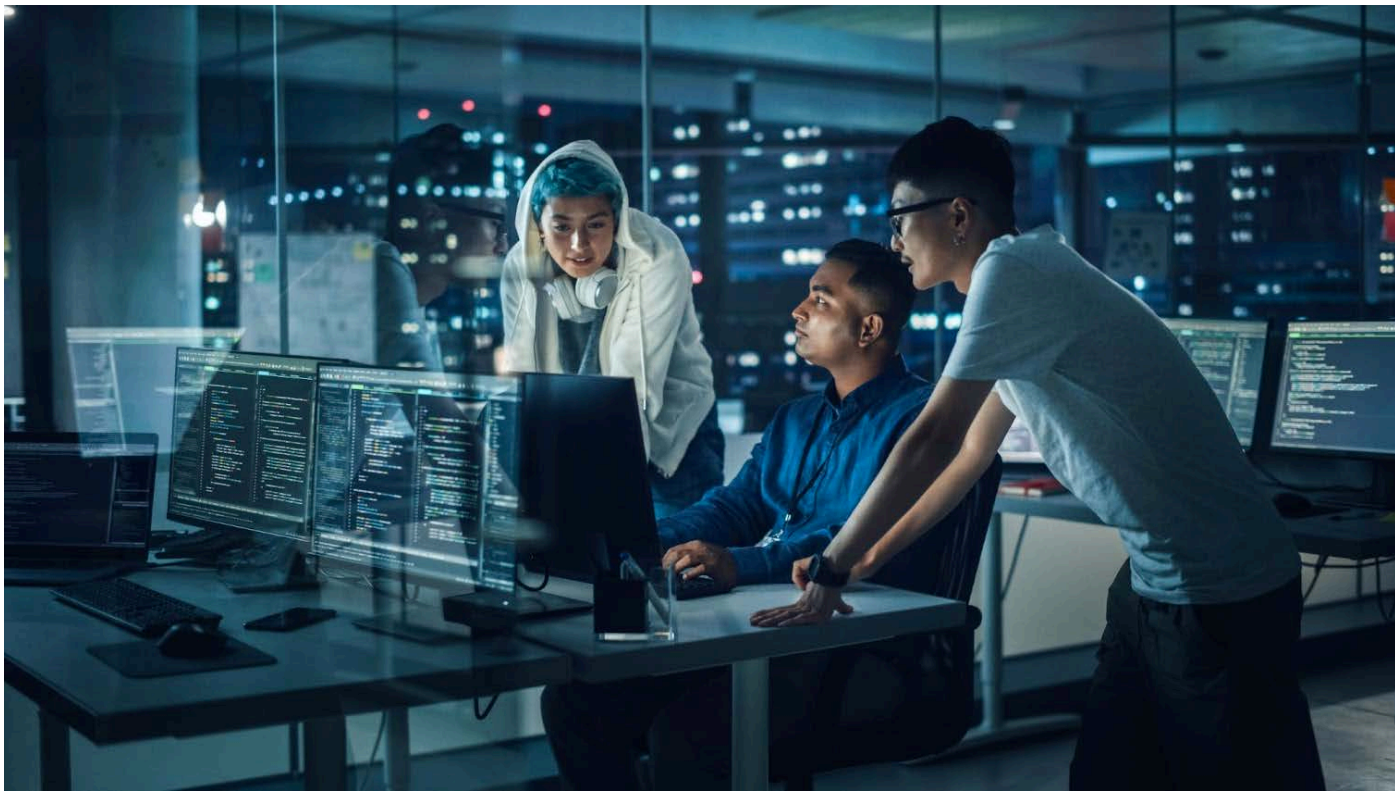
Putting data security at the centre of cloud transformation is therefore critical. This in turn demands organisation-wide understanding of the risks and collective responsibility and collaboration in their management.

This is easier said than done. One of the most difficult challenges is aligning the security, privacy and business priorities of stakeholders within a leadership team. In particular, there are often subtle but important differences between the interests of the three key players at the heart of cloud transformation and data security. Let's consider how their concerns differ:

Key player one: Transformation lead (CIO, COO or CTO)	Key player two: Chief Information Security Officer (CISO)	Key player three: Data Privacy Officer (DPO)
The CIO, COO or CTO is responsible for implementing the digital transformation strategy. They're focused on delivering business objectives such as efficiency, innovation and growth and are keen to foster a cloud-native mindset and culture.	The CISO oversees the security of data and information systems. Their main concern is protecting data from unauthorised access, misuse or loss, while complying with relevant legislation and regulations.	The DPO directs the enterprise-wide privacy strategy and ensures compliance with data protection legislation and regulations. Their primary priority is protecting personal or sensitive data that is stored or used within the cloud infrastructure.

Delays and costs

It is difficult to move forward unless data privacy and protection concerns are addressed, so the differing priorities of these three key players can hold up cloud transformation and lead to cost overruns. A case in point is not being able to complete functional and user acceptance testing for enterprise business applications. Other common problems include delays in realising value from data platforms due to the risks of data aggregation.



Five priorities for successful transformation

How can your business balance cloud security and usability and embrace transformation with confidence? Drawing on our collaborative approach to cloud transformation, five priorities stand out:

01 Embed data security up front

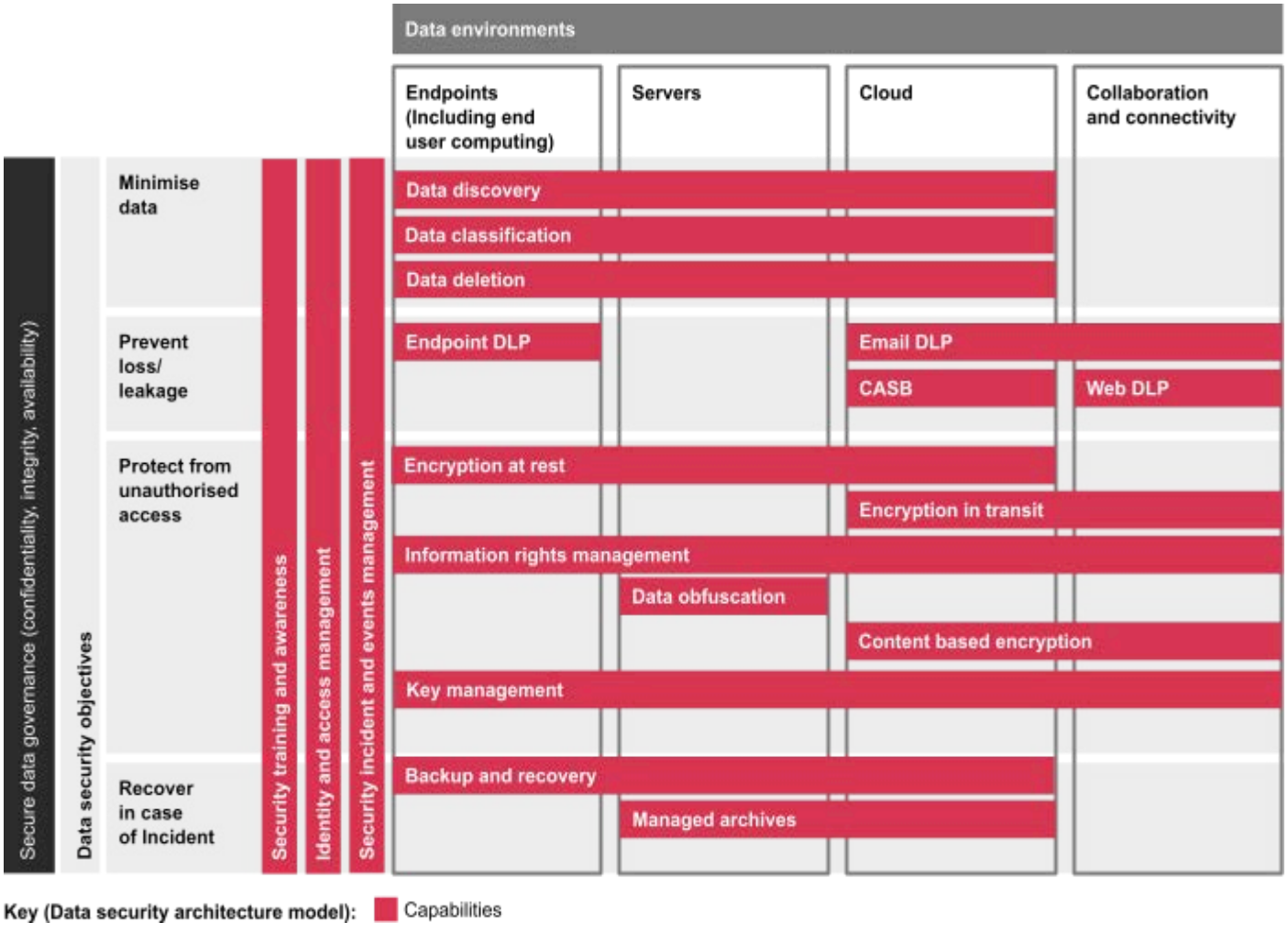
Bring the key players together to align their priorities and iron out any differences and concerns before you begin your cloud transformation. Key questions include how to handle special category data, align safeguards within a multi-cloud environment and comply with GDPR and other data regulations, all without stifling performance and innovation. Identifying and addressing the potential stumbling blocks up front will help you to avoid delays and deliver transformation at pace.

02 Seeing the big picture

An effective security reference architecture would allow you to take a holistic and data-centric approach to data privacy and protection, without compromising agility and performance.

In a hybrid environment, critical considerations include identifying the nature and location of data. It is also important to appropriately encrypt data; either at-rest, in-transit or in use, ensuring you are developing data loss prevention strategies across different types of environments.

Data security reference architecture model



By considering the shared responsibility of the cloud providers in a typical multi-cloud environment, our approach would help you to develop a better understanding of your risk landscape and associated controls. You can then plan and apply appropriate security measures for each data type or use case.

From a risk management perspective, this kind of reference architecture can help you to determine what works for you in practice as your business becomes more data-centric and data-led. This includes how to address the inherent complexities of protecting different data sets that are typically brought together in data lakes, but may have varying sensitivities and data security requirements.

The other key advantage of this approach is allowing you to identify and overhaul outdated policies or standards that may no longer be relevant following cloud transformation. For example, the use of production data in a cloud-based test environment may actually be acceptable as the cloud has the same enterprise grade security whether it's used in production or testing.

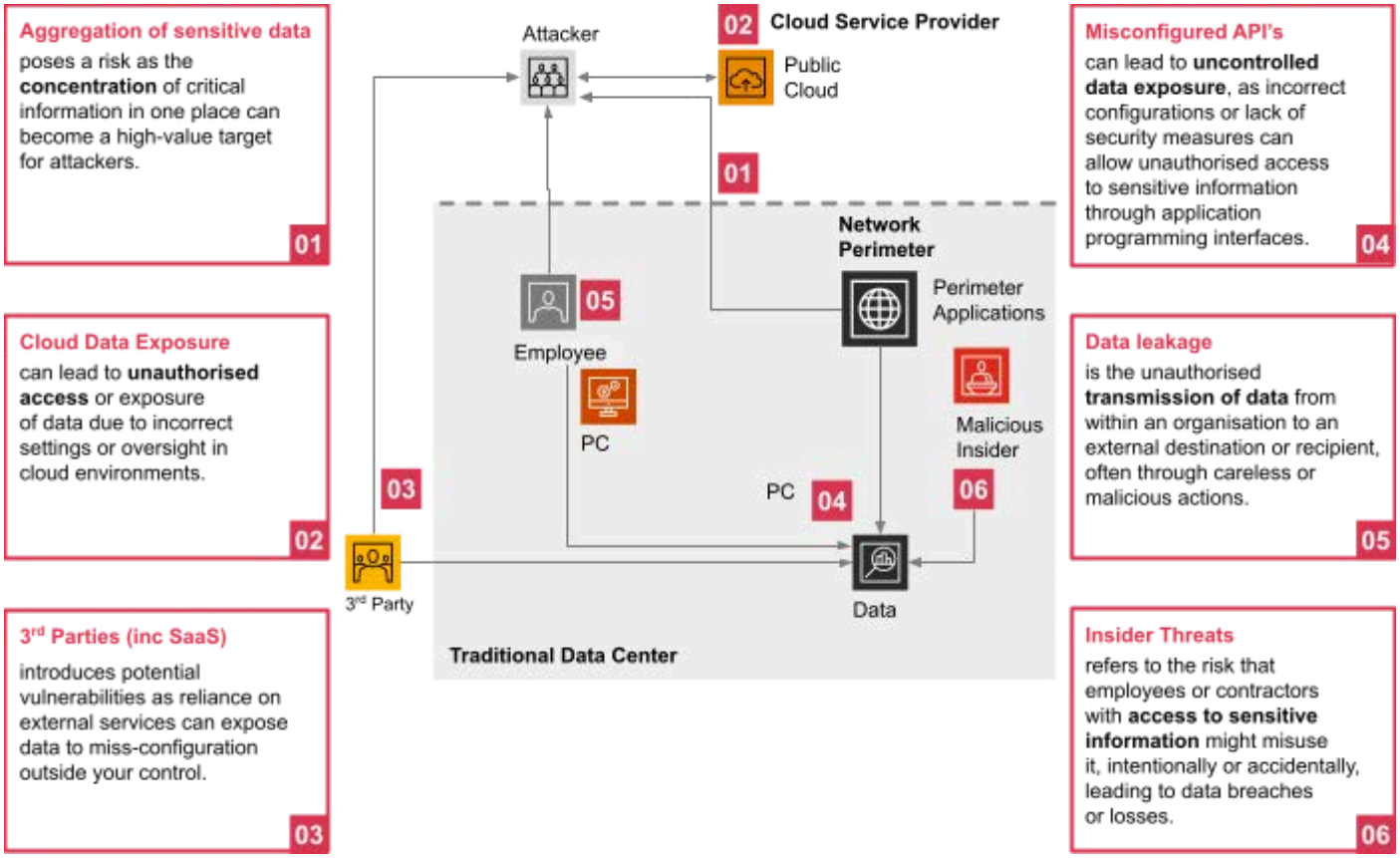
03 Recognise the threats

Identifying and understanding your key data risks would improve your ability to prepare for and mitigate threats. Potential vulnerabilities include the aggregation of sensitive data, which creates a single, high-value target for cyber attacks. Also on the threat radar are external software-as-a-service (SaaS) providers, which if breached allow attackers to maximise the number of victims and profits. Threats close to home include the misuse or deliberate sharing of information by people within your organisation.

It is also important to keep pace with evolving vulnerabilities. These include misconfigured application programming interfaces (APIs) at a time when operational and commercial ecosystems are becoming more complex and extended. Your security is only as effective as the weakest link in the chain.

Our threat modelling framework can help you to identify potential targets and vulnerabilities that could be exploited by attackers – internally as well as externally. The results would enable you to determine the most appropriate monitoring, control and mitigation.

Potential data security threats in a cloud environment



04 Guard your data

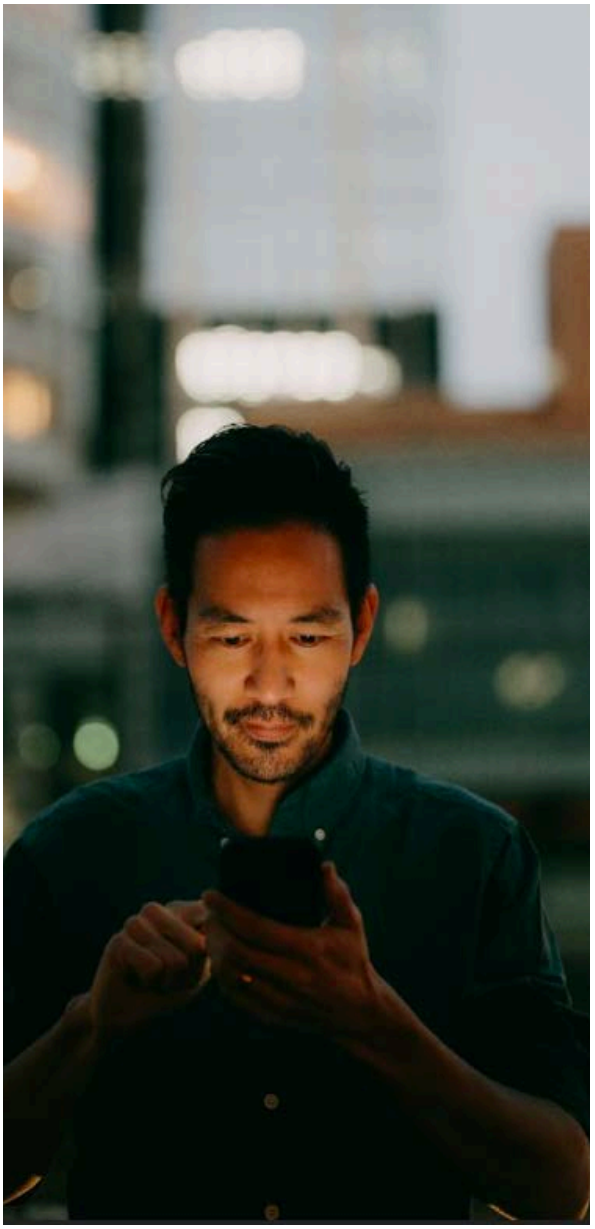
Data privacy and protection is everybody's business, so it's important to embed data-centric principles within your organisation.
Key priorities include purpose limitation. In practice, this means that data should only be accessible to those who need to see it. It's also important to consider how you'll protect data during cloud migration and implementation. This includes data-centric security measures such as anonymisation, encryption, discovery, classification and key management.
Other areas to determine include the right balance between data encryption (transforming the data into an unreadable format with key based decryption), data masking (hiding or replacing sensitive data with realistic but fake data and pseudo tokenisation) and data anonymisation (replacing sensitive data with random tokens that have no correlation to the original data).
Data security requirements for industry clouds may differ. In particular, certain industries often deal with sensitive and confidential data that require higher levels of protection and compliance than are available within generic cloud solutions. That is why we've developed industry specific solutions built around our deep understanding of the sector and its risks, a range of cloud service providers and the ability to apply the most appropriate technologies.

05 Look beyond migration

Your cloud transformation is an opportunity to rethink how you manage data and wider cyber security and embed them into your organisation. In recognition of the increasing complexities of today's cloud environments, many businesses are now looking for advice and support that goes beyond one-time transformation. This includes using managed cloud security services to bolster threat intelligence, create a single view of cloud exposures and support the people and processes required to drive ongoing change. More than two thirds of companies are using managed services for strategic advantage or to close capability gaps.

Your trusted partner

PwC is a recognised leader in industry cloud solutions. Using our deep technical cyber security expertise, breadth of business knowledge and our powerful technology alliances, we help organisations embrace cloud transformation with confidence.
From strategy and delivery to incident response and recovery, we can help you stay ahead of cyber security threats to protect your organisation and unlock new opportunities to accelerate growth.



Thank you

pwc.co.uk