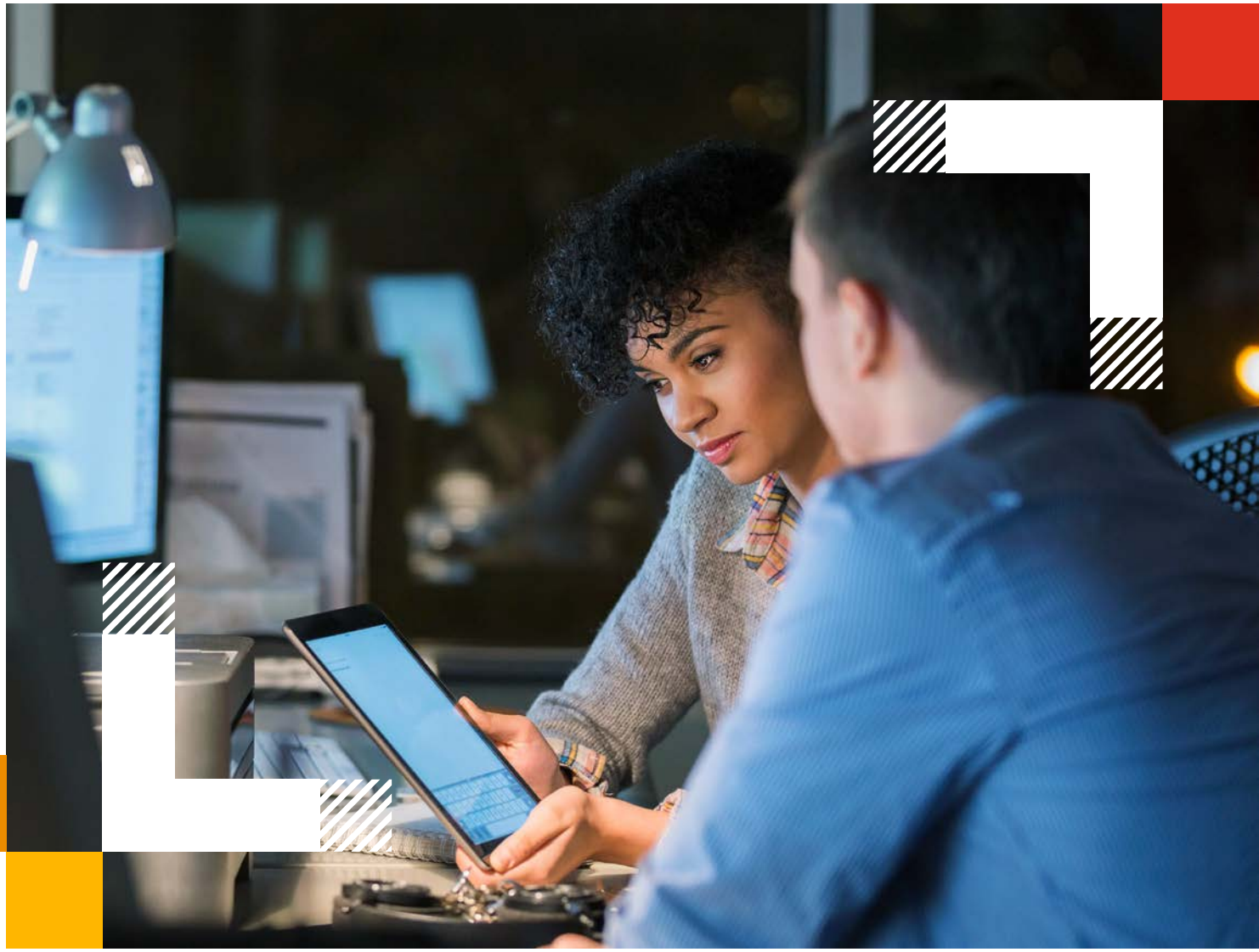
Transformation

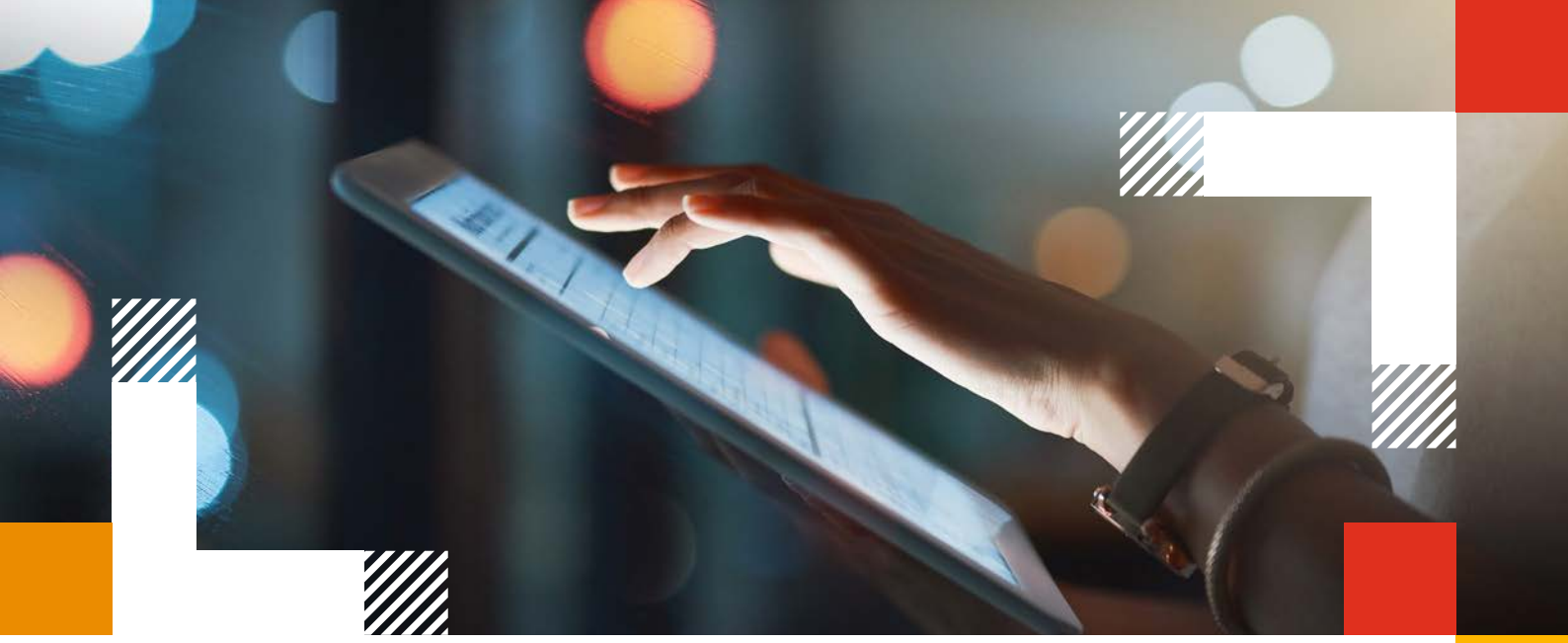
Leading with security

Cloud-powered businesses make security a priority

March 2024



pwc



Organisations that are furthest advanced on their cloud journeys are what PwC calls 'cloud-powered'. Findings from the PwC's EMEA Cloud Business Survey 2023 show that these businesses have moved data and applications more comprehensively to the cloud than their peers and are likely to outperform them across a range of key metrics, including higher growth. (1) Cloud-powered or 'all-in' cloud businesses also take a distinct approach to cloud security, adopting leading practices across cloud governance, risk and controls. 65% of cloud-powered organisations say they do this compared with just 25% of other businesses. (1)

They are also achieving measurable value: of the companies that havetaken an 'all in' approach to cloud, 53% have improved their cyber posture compared to 34% for non-cloud powered companies. (1)

Additionally, the survey showed that cloud powered organisations are particularly focused on building cybersecurity skills (48% of cloud-powered organisations vs 39% of others) to support their cloud transformation goals.

Major breaches on the rise

Building cybersecurity skills is more important than ever. PwC's Digital Trust insights Survey 2024 found that cloud-related attacks are part of the reason why major cyber breaches (those that cost targeted companies US$1m+) rose by one third in 2022 alone, cloud security has to be a C-suite priority.

Yet the survey shows that:

97%

of organisations still admit to gaps in their cloud risk management plans. Just 3% of respondents currently maintain up-to-date plans that address all cloud security areas.

Addressing this cyber security gap is a key challenge for all organisations making the move to cloud. Given the global shortage of cybersecurity professionals, upskilling existing employees in cloud solutions is crucial to improve every organisation's ability to protect its data and systems. These skills need to address cyber defence, data privacy, and security analysis.

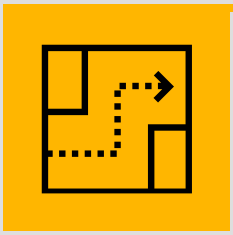
Securing the cloud journey

Not so long ago, organisations questioned the robustness of using infrastructure shared by hundreds, if not thousands, of a cloud provider's customers. The significant security investments made by the hyperscalers have turned that argument on its head. Cloud providers now make the provision of secure, trustworthy computing and identity management a fundamental element of their service offerings.

But while the security of public cloud is robust, the journey to these environments still poses challenges, from protecting systems and data to integrating security enterprise-wide and meeting compliance requirements. We see three distinct cybersecurity states in the cloud transformation journey to move from cybersecurity to cyber resilience:

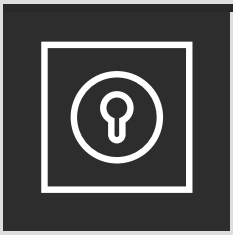
Present state:

Most organisations begin their cloud transformation journeys with a reactive approach to security geared to their on-premises assets and poor visibility of cloud assets.



Transition state:

As they progress on their journeys, they typically operate with hybrid security across on-premises and cloud, with a centralised cloud identity directory for users and assets.



Future state:

Automated security is embedded across agile product management. The application estate consists of connecting APIs that accept requests from authenticated users/systems, while simultaneously determining appropriate access to resources and data. A zero-trust strategy is adopted to enable digital transformation, deploying techniques such as strong authentication, network segmentation and least privilege.[3]

As enterprises continue on their cloud transformation journeys, they'll also need to pay attention to the potential for cybersecurity gaps to develop between their on-premises IT estate and their future cloud-first operations. This explains why in EMEA:

40% of organisations are using an integrated suite of cyber tech solutions (so-called security technology platforms), with a further 40% planning that move within the next two years.[2]

Protecting the cloud – a shared responsibility

Protecting the cloud means securing the services used and the data stored in the cloud.

One major difference with on-premises security is the shared responsibility model. In a cloud environment, the cloud service provider (CSP) is responsible for the security of the hosting infrastructure while the customer is responsible for the security of the services used, their data and applications (depending on the hosting model e.g. IaaS, PaaS and so on).

The areas to be secured remain the same (e.g. IAM, network, encryption), but the way in which they are secured differs. The security of items under the CSP's responsibility comes down to configuring the services used (e.g. whether to encrypt data buckets etc).

The security of elements under the customer's responsibility is similar to on-premises security and relies on other services offered by the CSP (such as HSM, SIEM and directories) or third-party tools.

In this case, the customer and CSP work together to secure the customer's data. However, another difference with on-premises security is that the data is provided to a third party (i.e. the CSP). They may be subject to extraterritorial regulation, such as the Clarifying Lawful Overseas Use of Data (CLOUD) Act or the Patriot Act in the US and an increasing number of digital sovereignty requirements emerging around the world, driven by geopolitics.

To protect themselves against these regulations, customers can use third-party tools, most of which rely on encryption such as confidential computing or bring your own encryption (BYOK) mechanisms. CSP's are also racing to build local data centers in high potential markets as data sovereignty becomes an increasing priority.

Cloud and generative AI

The emergence of Generative AI (GenAI) has provided added impetus to organisations' cloud journeys. Its requirements for massive computing power and huge data volumes make cloud
the only real option.

However, GenAI also creates additional cybersecurity risks. Malicious threat actors can use it to write malware, more believable phishing emails and more convincing fake identities, rapidly and for widespread dissemination. Managing these risks will be the key to successfully launching GenAI initiatives and for that you will need a risk management framework that also allows you to embrace opportunity.

Alongside the darker use cases, GenAI is set to play a growing role in strengthening cybersecurity.

64% of companies say they'll use GenAI for cyber defence in the next 12 months, with nearly half (47%) saying that they're already deploying AI for cyber risk detection and mitigation.[2]

Where are businesses investing today?

As they move forward, modernisation and optimisation top the cyber investment priorities for 2024. Nearly half (49%) of the business leaders selected technology modernisation, including cyber infrastructure. 45% chose optimisation of existing technologies and investments.[2] Hybrid cloud users are also the most likely to select cloud among their top three priorities for security investments over the next year. The trend towards modernisation and optimisation is also a key driver for the shift towards integrated cyber technology suites.

The priority from now? A 'security first' approach

With so many current and emerging risks, it's clearer than ever that security can't be bolted on to a cloud migration. It has to be an integral element of both the technology and migration approach from day one. As CISOs, CIOs and the entire C-suite work together to adopt a 'security-first' cloud transformation strategy their priorities should include:

1. Building an architecture based on zero trust principles as a foundation for cloud and digital transformation from the outset.
2. Implementing a framework to understand and tag data to facilitate the responsible AI principle of fairness, reliability and safety, privacy and security and inclusiveness.
3. Putting in place automated backup, mechanisms that enable recovery from a disruptive cyberattack and continuous monitoring.

"Organisations recognise the need to adopt cloud architectures in order to benefit from technology advances like GenAI. Understanding and managing the implications for security and resilience up front, rather than as an afterthought, will be key."

Richard Horne, Cyber Security Partner, PwC UK

Glossary

IaaS : Infrastructure as a Service

PaaS : Platform as a Service

IAM : Identity and Access Management

HSM: Hardware Security Module

SIEM: Security Information and Event Management

(1) PwC's EMEA Cloud business survey
(2) PwC's Digital Trust Insights Survey 2024

(3) Unlike solely perimeter-based security, Zero Trust promotes a micro-perimeter approach based on user access, data location and an application hosting model. Within this microsegmented network, sensitive data is protected, and any access is verified and requires authorisation. (PwC Zero Trust architecture: a paradigm shift in cybersecurity and privacy, 2021)

Contributors

Grant Waterfall

EMEA Cybersecurity & Privacy Leader, PwC Germany

Linkedin

Richard Horne

Cybersecurity Partner, PwC UK

Linkedin

Prafull Sharma

Advisory Partner, PwC Switzerland

Linkedin

Laurent Broto

Cloud Security Managing Director, PwC France

Linkedin

www.pwc.com

RITM15388010