Future-proof secure cloud

How security guides your path in the cloud

Flexing security on your cloud journey

The race to the cloud is underway. With business resilience under threat from the pandemic, a shift to remote working meant many organizations needed flexible, scalable networks made possible by the cloud.

At the same time, new cloud-based technologies offer opportunities to drive innovation, automate and pursue new growth—or simply save money and be more efficient. And fulfilling the bigger picture of digital transformation is creating a sense of urgency for organizations to be ready with cloud as a continuum of capabilities.

As these factors come together, historical uncertainties about cloud have drifted away. Yet, accelerated cloud adoption also exposes organizations to new business risks—especially when it comes to potential security vulnerabilities.

For instance, new cloud enabled digital experiences may clear the path to transformation, but they also create new threat vectors. In the health sector, more than half (53%) of connected medical devices and other Internet of Things devices were recently found to have critical vulnerabilities that could be detrimental to patient safety and privacy.[1]

Organizations should balance the security needs of today with those of tomorrow. They should be ready and agile enough to secure their existing technology footprint, while being prepared to manage what lies ahead—wherever they are on the cloud journey. And they must often do so without the luxury of additional resources.

On any cloud journey, if the Cloud Continuum is the map, security is the compass that guides organizations to navigate more effectively.

80%

of workloads could be in the cloud in the next few years.

Challenging times

Organizations should consider their security profiles against the backdrop of issues, such as:

Increasing attacks

Successful security threats are increasing—without industry or geographic boundaries. Our 2021 research reveals 270 attacks, a 31% increase over 2020 per company per year. These attacks are indiscriminate to cloud or on-premise environments.

Smart threat tactics

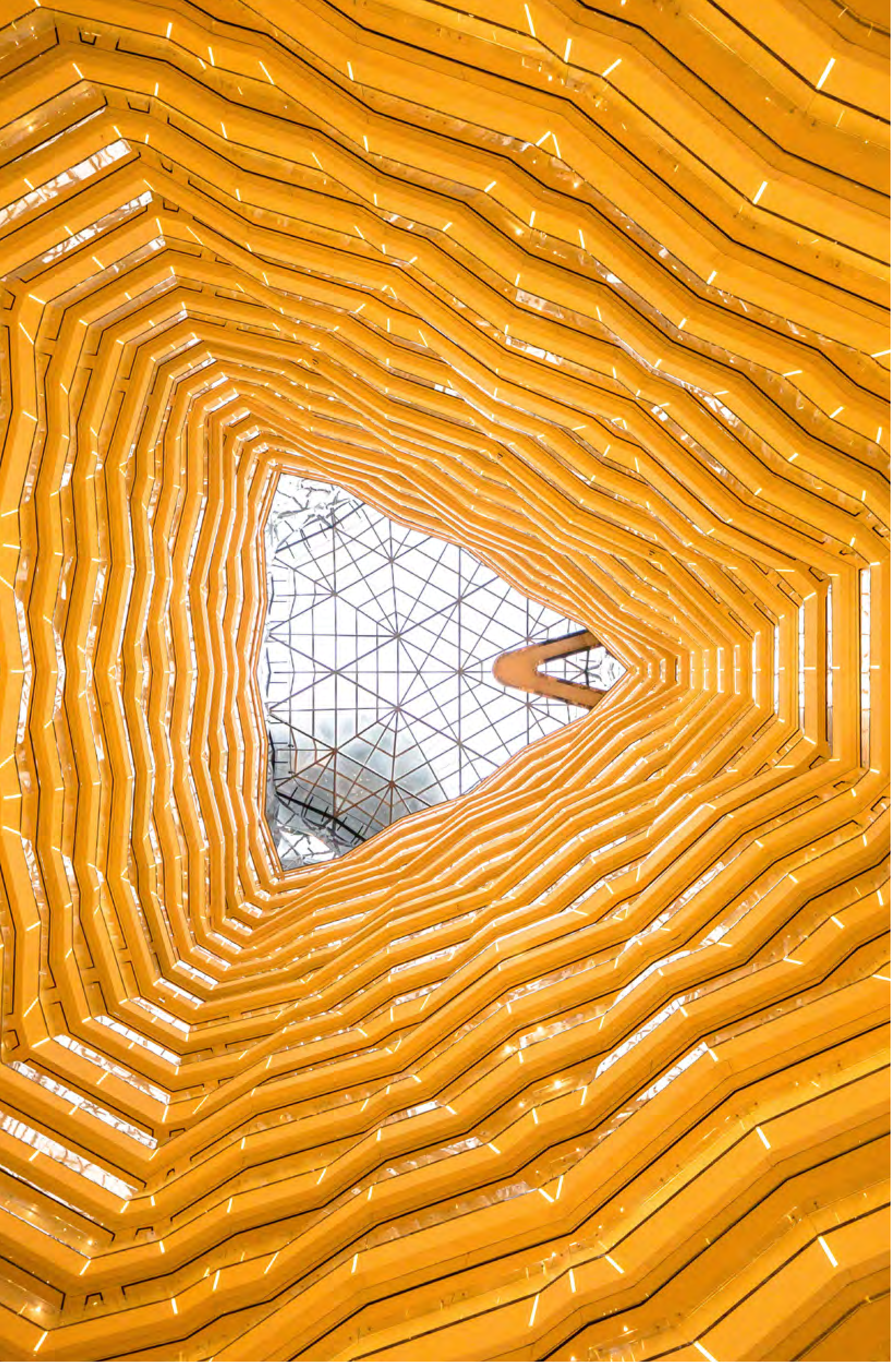
Cyberattacks are more sophisticated with threat actors nimbly shapeshifting to take advantage of emerging technologies faster than most organizations. For instance, ransomware operators are abusing cloud infrastructure and introducing new encryption techniques to better evade detection.

Security analysis paralysis

Visibility and controls assurance is necessary but security teams can get lost in analysis paralysis or overengineer solutions to close a vulnerability gap. For instance, when a regulator wants evidence of how an organization has secured its cloud foundation, the security team may struggle to deliver because the older, data center-focused controls frameworks do not align and properly address modern digital capabilities.

Security teams should be agile and aligned with the business to be ready to protect their organizations and enable cloud opportunities.

Our annual State of Cybersecurity Resilience research found that those organizations that closely align their security practices with the business strategy achieve better business outcomes. They are better at stopping attacks, finding and fixing breaches faster and reducing their impact.



Security blind spots

Security teams should recognize where their organization is on the cloud journey. Yet, they are hampered by:

A security culture shift

The traditional security mindset is one of control, for example, control of the perimeter to limit who has access to technology. But as network security adopts a zero-trust approach—where, by definition, no one is trusted—a pivot from direct control to shared responsibility is needed. Learning how to relinquish control demands a culture shift. In addition, security teams today are often focused on process rather than outcomes; they need to be aware that security actions should keep pace with the ever-changing context of an evolving cloud journey to avoid new risks.

A scarcity of skills

Traditional security resources include two core skill sets: security administrators (infrastructure, vulnerability management, network security skills) and cyber defense teams (threat intelligence, investigation, incident response). Current resources are being asked to do their jobs in new ways, which introduces new skill requirements. What's missing are resources with security domain expertise and cloud technology skills, such as software engineers who have skills in identity and access management. Upskilling existing resources and adding new skills will be required to make full use of a Cloud Continuum approach.

Software automation advances outpace security

As cloud initiatives progress and trigger advances in software automation, traditional Software Development Lifecycle (SDLC) management has become more agile. Security must keep up with capacity demands and the only way to achieve that is through automation. Increasing software automation requires the same from security capabilities to effectively secure emerging services on cloud platforms. Unfortunately, skills and capacity in the security domain lag these software automation advances.

An inability to balance resources

Cloud can enable security technologies, such as endpoint detection and response, security information and event management (SIEM), trust-based architectures and cyber threat intelligence. But as organizations open the door to those technologies, the stress on existing security resources and capabilities can reach a breaking point, introducing new vulnerabilities. CISOs should adjust multiple levers to manage their cloud journey—including technology, resourcing and strategic partners. Given we are over a decade into securing cloud, there is much to be learned from those who have already gone down this path. Where skills are lacking in-house, there are lessons, there is capacity and there is ample open source security automation content available to jump-start organizations on the journey.

42%

of respondents said security and compliance risk was a top pain point of cloud adoption.

30%

of CISOs said they don't have the skills needed to move into the cloud.

A secure cloud journey is not a one-and-done event

Security organizations will be challenged to stay in front of threats and adapt continuously to avoid delays on their organizations' cloud journeys.

As we shift toward a more human-centric internet and embrace advances like the metaverse, security teams should improve their cloud security competency and agility to clearly identify and respond to the evolving risks.

Leaders should be confident they have identified the highest risk threat vectors and are effectively managing new risk exposures as fast as software developers create new services.

Where are you going?

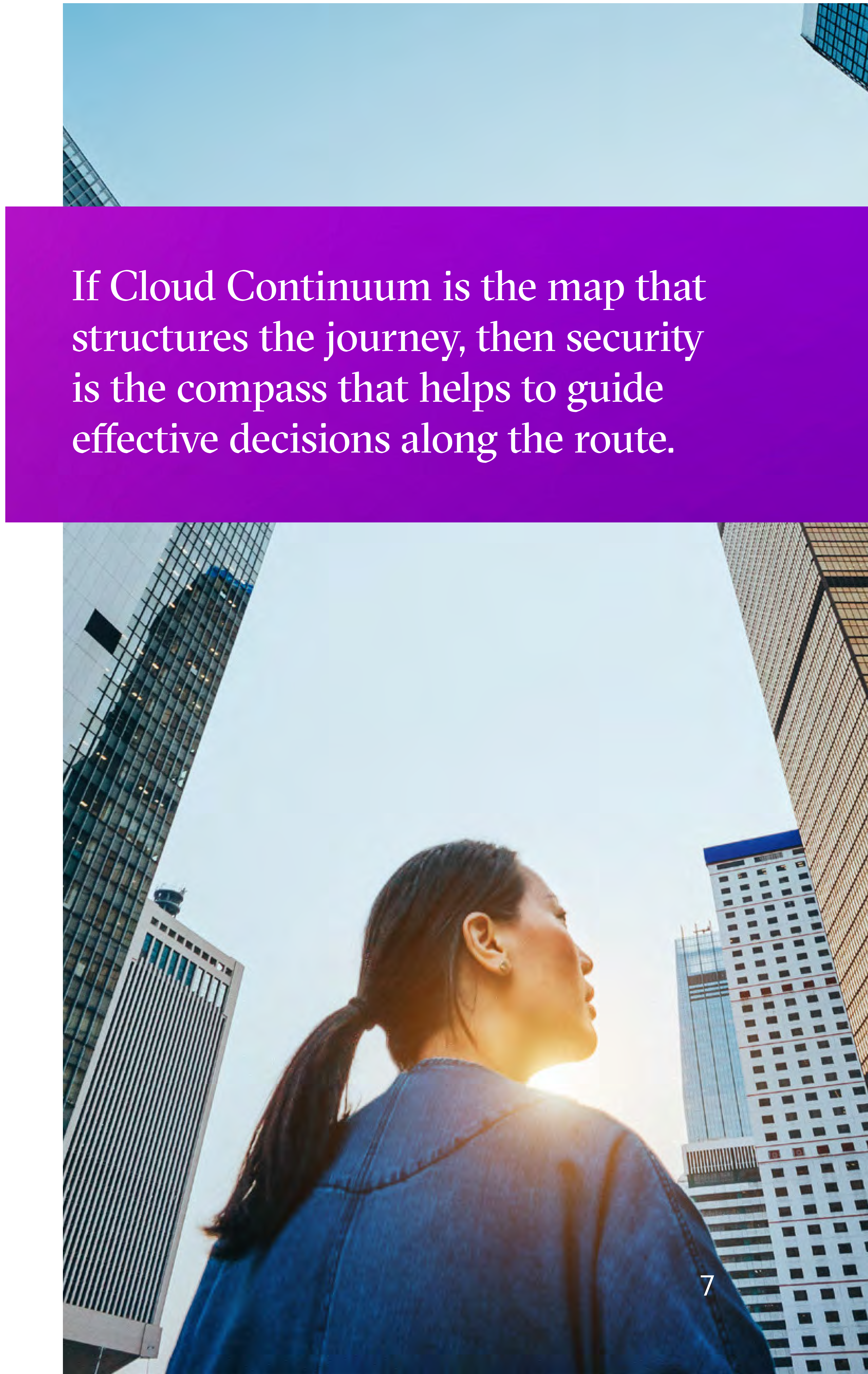
Whether just starting out or already well along the cloud journey, organizations need clear visibility into business outcomes and residual or emerging risks and the ways to address them. They should understand the status of current progress and have an overarching view of the planned direction.

Leaders across the business need a line of sight into how security is performing across the organization. They should recognize when their security team's actions are enabling business objectives and when they're not. They should be able to discern the difference between security teams blocking progress and protecting the business from unseen threats.

They should understand the nuance between thinking the business is secure and knowing it is secure. They should consider whether cloud security is slowing them down or helping them to accelerate the journey.

And for their part, security leaders should understand the desired speed of progress on any cloud journey, so that they can apply the appropriate guardrails to protect the business.

To take advantage of the cloud in the most secure way, organizations need to ask themselves: is our security capability helping us to navigate and progress our cloud journey?



If Cloud Continuum is the map that structures the journey, then security is the compass that helps to guide effective decisions along the route.

Understand the route

Whenever we take any journey, there's a mental checklist we normally follow: Do I know where I'm headed? Have I planned my route? Did I pack my travel essentials?

Let's assume the fundamentals are covered for an organization's cloud journey—the general direction is set, a cloud service provider is on board, the security team is engaged. Now, there's the matter of which route to take and no one size fits all.

While we recognize that there are a range of approaches that can be taken, the following routes represent the two ends of the spectrum commonly considered when moving to the cloud:

The direct route takes organizations through some challenging terrain—but uses the freeway to help fast-track innovation. Taking this 'drive and learn' approach enables executives to see the cloud journey through an incremental, tactical lens—less up-front investment, more cloud native approach. Here, security capabilities may be predominantly extensions of an existing ecosystem.

The scenic route takes organizations on a more meandering road through culture shifts and cloud complexity but picks up the benefits of business transformation along the way. Taking this 'intense and intentional' road enables executives to see the cloud journey through a transformative lens—less turnkey and more North Star strategy and governance. Here, security capabilities may be more transformational in terms of moving security networks to a zero-trust approach.

Essential pit stops should offer visibility into cyber defense and controls assurance. And periodic check-ins can help to reassure that the route that is chosen maps to an organization's business strategy.

Both routes will see organizations reach their end goal but create different experiences. From a security perspective, each route is effective but has different risks and requires a different approach.

31%

of CISOs said security was not part of the discussion around moving to cloud from the beginning and they were trying to catch up.

Choose the route

Each route has different implications for how security teams steer progress on the cloud journey.
These routes highlight how an organization's current security tactics may need to be adjusted to proceed effectively:

	THE DIRECT ROUTE Drive and learn	THE SCENIC ROUTE Intense and intentional
Cloud journey	Move to a primary cloud provider in a SaaS, IaaS and PaaS environment to expand footprint.	Move to a hybrid/multi-cloud environment; more complex but provides longer-term resilience.
Security focus	Security initiatives are focused on optimizing integration and incremental change, with security that adds to your existing tool suite; working in native environments and infusing that into tools your teams already know; involves software engineering policy as code (DevSecOps).	Security initiatives are focused on disrupting and modernizing complex systems and involve taking on more North Star-type activities, such as adopting zero trust to transform the network security approach; initiate talent and culture shifts and changes to underlying security architecture.

For both routes, employ identity management and data security.
The degree of complexity depends on which route is selected.

Manage risk

Factors that influence risk and progress on the cloud journey are:

Industry-specific: Some industries are more likely to be successful on one route rather than another. For example, regulatory and compliance issues have been known to affect the Banking industry's move to secure cloud.

Location-specific: Geographic footprints can influence progress. For example, global or multi-national vs regional organizations have different security demands. Also, sovereign cloud, enabling organizations to control the location, access to and processing of data in a cloud environment, has implications for emerging industry standards in certain countries or sectors.

Customer engagement-specific: Consider the risks associated with different types of customer engagement. For example, engaging directly with customers through a digital platform such as Uber or Airbnb carries different risks than managing the numerous suppliers and payment processes in a business-to-business (B2B) context.

Innovation-specific: New cloud services need a risk evaluation prior to their introduction; security must keep pace with sanctioning and evaluating those services that open the door to incremental risk. For example, threat modelling, a risk or business impact assessment and residual risk determination can ease new service introduction.

As the metaverse unfolds, security leaders should adapt to meet the needs of the business.

Your security compass

Organizations that want to take advantage of the opportunities presented by the Cloud Continuum should understand what decisions must be taken and what security is needed to support the outcome.

On the journey, organizations have a number of areas to consider around their security engagement—related to their people, their technologies and their ecosystem of partners.

How these elements are handled depends on your own specific cloud journey maturity—whether just starting out, accelerating or 'all the way there', organizations need to shift security efforts on the move.

What's more, risks and factors change, so it's important to pause at the pit stops and continue to ask questions about the journey—is our security approach still in step with business strategy? Do we have the relevant skills? Have we planned for capacity?

By taking an optimal break, executives can check in with—and even adjust—their direction to make sure that they're on a suitable route.

Three considerations when using security as a compass to ease the cloud journey

Where are you?

Align security with the business
Make sure that CISOs and their security teams are deeply aligned and instigate business outcomes using security as the enabler to drive the cloud journey.

Take action: Accelerate application and data migration; evaluate/rebalance the appropriate skillsets; make sure data is appropriately permissioned; demonstrate that what has been built meets regulatory demands.

What should you do?

Be secure by design
Use technology as a lever to integrate and automate security solutions and steer toward a cloud native architecture.

Take action: Test the technology being used for its current security posture; take advantage of a cloud-native security architecture and services to free up staff for higher priority cybersecurity activities.

Who should you partner with?

Lean in to your ecosystem
Pause along the journey to engage with strategic vendors and security peers and benefit from insights and industry expertise.

Take action: Reach out to your ecosystem, including other CISOs and vendors, to hear how they're dealing with common challenges; anticipate skills demands by building new communities of technical or managed service experience.

Organizations should not feel fixed to their chosen path; they can change direction from direct to scenic route and back again to correct any wrong turns. What will clarify the route is a consistent guide from a security compass as it introduces the agility to navigate any cloud journey.

What is the Cloud Continuum?

The Cloud Continuum includes a spectrum of capabilities and services from public through edge and everything in between, seamlessly connected by cloud-first networks and supported by advanced, Cloud Continuum practices. The array of technologies that makes up the Cloud Continuum varies by ownership and location, from close to the enterprise to completely off-premise. Cloud-first 5G and software-defined networks unify the Continuum, allowing access to the cloud from virtually anywhere and ensuring that there are no silos among private, public, hybrid, edge or multi-clouds.

For more visit:
www.accenture.com/us-en/insights/cloud/cloud-continuum

What is the metaverse?

Accenture sees the metaverse as an evolution of the internet that enables a user to move beyond browsing to inhabiting and/or participating in a persistent shared experience that spans the spectrum of our real world to the fully virtual and in between. Accenture looks at the metaverse as an evolving and expanding continuum on multiple dimensions; we call this the Metaverse Continuum.

For more visit:
www.accenture.com/us-en/services/metaverse-index

Contacts

Dan Mellen
Managing Director,
Accenture Security
daniel.w.mellen@accenture.com

Gretchen Myers
Cloud Security Principal,
Accenture Security
gretchen.myers@accenture.com

References

1 Health IT Security, January, 2022

Data sources

80% of workloads could be in the cloud in the next few years. Accenture Technology Vision 2022

42% of respondents said security and compliance risk was a top pain point of cloud adoption. Accenture Cloud Continuum

30% of CISOs said they don't have the skills needed to move into the cloud. Accenture State of Cybersecurity Resilience 2021

31% of CISOs said security was not part of the discussion around moving to cloud from the beginning and they trying to catch up. Ibid.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Technology and Operations services and Accenture Song—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 699,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly-skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter or visit us at accenture.com/security.

This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.

This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. The information in this report is general in nature and does not take into account the specific needs of your IT ecosystem and network, which may vary and require unique action. As such, Accenture provides the information and content on an "as-is" basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report. The reader is responsible for determining whether or not to follow any of the suggestions, recommendations or potential mitigations set out in this report, entirely at their own discretion.

220184