accenture

Secure Cloud

How to accelerate resilience and make
your cloud-first journey safe from the start

Contents

Storm clouds on the horizon

Now more than ever, organizations need to prioritize a "cloud first" approach to enable their companies to transform with agility at scale. But, as its name suggests, every new instance of public cloud has the potential to brew up a security storm.

Cloud Service Providers (CSPs) have worked hard to secure their infrastructure and upgrade their native security features. They innovate to create and release new services and features at an increasingly rapid pace. But cloud service providers are not responsible for maintaining a strong security posture in a cloud-enabled environment.

The default settings when you create a new cloud instance are unlikely to satisfy even the basic security requirements of any business operation. It is still the responsibility of each organization to apply those tools to secure the environment they create—and the applications they build—for use in the cloud.

> **Security is often seen as the biggest inhibitor to a cloud-first journey—but in reality it can be its greatest accelerator.**

A deluge of disruption

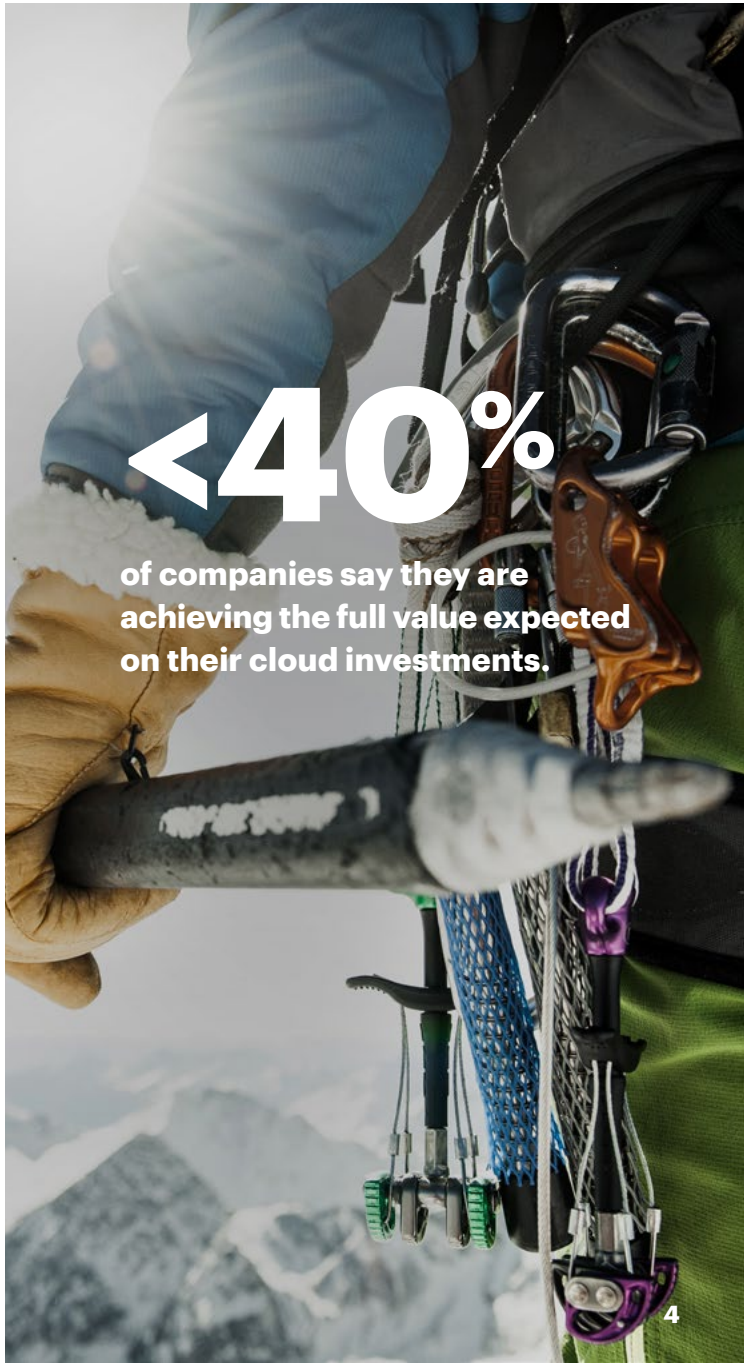
Many businesses have been drawn to the efficiency, elasticity and innovation of the cloud. But 2020 stands out as the year when organizations, across all industries, had a powerful and direct reminder of the importance of systems resilience, agility, adaptability and scalability.

Despite this unprecedented wake-up call, and the clear promise of cloud to deliver on the new demands, less than 40% of companies say they are achieving the full value expected on their cloud investments.[1]

While cloud offers new opportunities to modernize services and transform operations, security and compliance risk remains the greatest barrier to cloud adoption. Combined with the complexity of hybrid- and multi-cloud environments and a shortage of skills, these concerns can be major roadblocks to a cloud-first journey.

Delivering security in the cloud is not a "lift and shift" exercise. It takes clear strategic intent, a nimble governance model, alignment —across the IT organization and the rest of the business—and implementation in line with enterprise risk tolerance.

> **Security leaders can help to deliver better business outcomes and make a cloud-first journey be secure by design.**



CHALLENGE 1:

Weaknesses in security governance and compliance

Security and compliance risk is the greatest barrier to realizing the benefits of cloud according to 65% of senior IT executives.[2] CISOs need to be able to communicate a transparent governance risk framework, along with close monitoring and remediation of anomalies, to maintain compliance.

CHALLENGE 2:

Proactively addressing the complexity of secure configuration

Cloud strategies are evolving with a hybrid, multi-cloud approach in many organizations. But as the National Security Agency has stated: "Misconfiguration of cloud resources remains the most prevalent cloud vulnerability."[3] Asset and configuration controls must be defined early and automated configuration used to enable successful cloud migration that has security baked in from the start.

CHALLENGE 3:

Finding and retaining the right skills

Automation helps with talent shortages, but organizations need to be more creative to ensure the right skills are in place. Cloud security people are in short supply. In our research, 30% of better performing leaders provided training for more than three-quarters of users when it was needed, versus just 9% of non-leaders.[4] Security teams need to develop the right mindset, along with the right security policies, processes and procedures, to effectively manage a secure cloud environment.

Security governance and compliance

In a time of accelerated cloud adoption, governance and policy compliance can be easily overshadowed by the need to move fast and enable the business. But consistent security and privacy oversight for security is possible, even during periods of rapid transformation.

Transparent governance

As companies embrace multiple cloud environments and cloud providers create and release new services at an increasing pace, security is just as important as it has always been. But whether it is tools, processes or even skill requirements, securing cloud environments is substantially different from securing on-premise environments.

Organizations still need to build or acquire the ability to scan and monitor all its cloud environments to identify anomalies and then remediate them to maintain compliance.

Proactive compliance

By defining new policies and procedures, configuring to the appropriate framework, identifying the relevant controls and creating a cloud-specific reference architecture, a company can securely, and more quickly, take advantage of cloud providers' ongoing stream of new services to build new capabilities and improve business decisions.

It is not enough to send alerts to flag vulnerabilities. Putting in place security guardrails with pre-built accelerators for cloud native services can mitigate risk before incidents happen. Blocking or self-healing functionality enables continuous and automatic enforcement of policies in support of industry regulations and enterprise standards.

Proactive cloud security

A security reference architecture has six key pillars that define the minimum requirements for organizations to securely place workloads in the cloud.

What you should do:

Secure the platform

Design and deploy base security controls to create secure landing zone on the cloud solution provider platform.

Secure the services

Design reusable cloud solution provider secure PaaS templates with integrated security controls.

Integrate tools and operations

Combine the platform and services to bring together existing client enterprise security tools with operational processes and procedures.

How you should do it:

Identity access management

Spell out the roles that are authorized to operate in the environment and what they are allowed to do.

Network security

Secure connectivity to on-premise data centers and use a “hub and spoke” network security model.

Secure cloud configuration

Secure landing zone configuration policies and apply cloud service provider platform security controls.

Tackling talent

There is a shortage of both security and cloud talent, which is amplified when looking for professionals with cloud-specific security capabilities. The high demand and limited supply forces CISOs to be creative in attracting and retaining the skills needed for the journey to secure cloud.

Shift mindsets

With ready-made skills hard to acquire, some CISOs are looking for traditional infrastructure SecOps professionals with native premise security skills to succeed in the cloud. The most important thing that can determine the success or failure of that transition is a desire to change. Making a mindset shift is sometimes the biggest obstacle traditional security professionals face.

Extend security skills

The developer community is emerging as a promising pool of security talent. Developers are starting to recognize that security skills are a valuable addition to their own skill sets. As the distribution of security controls reach developers who are working with automated infrastructure and application pipelines, there is a natural extension of security capabilities into other areas of the business.

Cloud-first strategy

Cloud migration strategies are evolving to become more complex. An original focus on lift and shift point-in-time virtual machines has given way to hybrid, multi-cloud computing environments and heavy Platform-as-a-Service use.

Getting transparency into this complex environment is not straightforward but is an imperative in monitoring a rapidly evolving computing environment.

Without a formal strategy and strong governance, individual lines of business can develop competing cloud initiatives which result in redundant work, duplicative control solutions, poor communication, higher costs, longer time to value and, most importantly, a reactive approach to security.

> **Security leaders need to consider the four dimensions of complexity that influence their strategy outcomes.**

The four dimensions of complexity

#1 **Buy versus build:** How much native? How do third parties keep up with ever-evolving cloud service provider services?

#2 **Fit for purpose:** How do you select a cloud model/ provider based on application functionality and the intersection of security?

#3 **Multi-cloud:** When should you replicate security controls versus abstracting?

#4 **Scale and maintainability:** How do you drive consistency in security operations?

Shift security to the left

While mitigating risk and protecting data in the cloud is a priority, security should be embedded consistently. Too often, it is added at the end of the cloud-first journey and can delay business outcomes—or result in having to do the work all over again.

Cloud needs different tools and skills to on-premise. Cloud needs to be treated like the rest of the software development lifecycle. Changes need to be made in the same way as any application—by checking in and checking out code.

If we fail to "move security to the left", poor alignment, weak governance, manual processes, legacy tools and skills gaps will encourage executives to look upon security as the function holding the business back.

> **In reality, in the race to the cloud, security leaders are its greatest champion.**

"We need a single sheet of glass for visibility into our vulnerabilities but right now many enterprises with multi-cloud instances are looking through a mosaic."

Kris Burkhardt
Accenture CISO

Secure cloud can enable better business outcomes

Cloud security can enable better business outcomes by being:

Fast

Use cloud service provider native accelerators that enable security capabilities and controls to be deployed in minutes or hours, rather than months.

Frictionless

Embed security into existing solutions, business processes, and operational teams.

Scalable

Apply automation and self-healing processes to reduce manual steps and break the resourcing model of adding headcount to enable organizations to scale.

Proactive

Establish pre-emptive controls to block accidental or malicious security incidents from happening in the first place.

Cost effective

Bake-in security from the outset to avoid the additional costs incurred by having to re-do work.

Case study: Accenture

A massive 95% of Accenture applications are in the cloud and supported by the platform economy. Compared with traditional vendor-heavy security solutions of the past, Accenture's new cloud-native focused security offerings enable:

Workforce and team strategy to optimize the current onshore-offshore operating model

Smart working using Infrastructure as Code reduces employee travel to client sites and deployment lengths

Digital ways of working to drive collaboration, innovation, flexibility and value-driven purpose

Reduced talent acquisition spend through better attraction and retention of talent

70%
Reduction in build costs

30-70%
Savings versus previous SIEM as-a-Service offerings

3x
Speed of build and go-live run operations vs legacy security tools

20-40%
Reduction in run operations costs versus legacy approach

50%
Average time reduction to go-live operations

1 Day
Time taken to start onboarding and realize client value

In addition to our experience in undertaking a cloud-first journey we have announced a US$3B investment to help our clients shape, move, build and operate their businesses in the cloud and realize the cloud's business value, speed, cost, talent and innovation benefits.[5]

Empowering the CISO

Consider the progress of your secure cloud journey by asking yourself:

- Where should we focus our investments in the public cloud? (consider: cloud native, identity, data governance, networks security and so on)
- How has COVID-19 affected our priorities and objectives with respect to our eCommerce and online presence—and what impact has that had on the demand to scale in the cloud?
- Do we want to move in a “lift and shift” model or modernizing/refactoring to modern application architectures, like microservices, at the same time?

Cloud's silver lining

In our experience, the following four steps can guide any cloud-first journey and introduce security at speed and scale from the outset.

Know your cloud security posture

Rapidly identify gaps and establish a risk-aligned architecture and roadmap for baseline cloud security that optimizes current technology investments.

Automate native security

Get faster time to value and automate deployment of security guardrails with pre-built accelerators for cloud native services including AWS, Microsoft Azure and Google Cloud.

Be proactive with compliance

Optimize detection and streamline cloud security operations. Mitigate risk with self-healing functions executed natively within cloud service providers (CSPs) or through third-party services to enforce policies in alignment with regulatory requirements and enterprise standards.

Employ security monitoring and response

Monitor public cloud estate cost effectively and at scale by using cloud native security insights tools and a library of use cases that are continuously updated to address evolving threats and complex regulatory requirements.

Contacts

Daniel W. Mellen
Managing Director,
Accenture Security Cloud

Rex Thexton
Senior Managing Director,
Applied Cybersecurity Services

Harpreet Sidhu
Managing Director,
Managed Security Services

Andrew Winkelmann
Managing Director,
Accenture Security

References

1. Navigating the barriers to maximizing cloud value, Accenture, 2020; https://www.accenture.com/us-en/insights/technology/maximize-cloud-value
2. Perspectives on cloud outcomes: Expectation vs reality, Accenture, 2020; https://www.accenture.com/us-en/insights/cloud/cloud-outcomes-perspective
3. Mitigating Cloud Vulnerabilities, National Security Agency, January 2020; https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF
4. Innovate for Cyber Resilience, Accenture, 2020; https://www.accenture.com/gb-en/insights/security/invest-cyber-resilience
5. Accenture Cloud First Launches with $3 Billion Investment to Accelerate Clients' Move to Cloud and Digital Transformation, Accenture, 2020; https://newsroom.accenture.com/news/accenture-cloud-first-launches-with-3-billion-investment-to-accelerate-clients-move-to-cloud-and-digital-transformation.htm

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, Interactive, Technology, and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 506,000 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 **www.accenture.com/security**