accenture

THE HEALTHCARE CLOUD SECURITY PARADOX

Public cloud can be significantly more secure than private or on-premise data center strategies.

So why aren't healthcare CIOs taking full advantage of moving to the cloud?

Moving data to the public cloud does not involve a security trade off. To the contrary, experts say that the 60% of enterprises that implement appropriate public cloud security controls will experience one-third fewer security failures.[1] This is good news for US healthcare organizations, which experienced double-digit growth in the number of data breaches from 2016-2017.[2]

Accenture research shows that healthcare CIOs clearly recognize the security benefits of cloud: 60% cite data protection and management as the principal strategic priority advanced by moving to the public cloud. And 66% are in the process of shifting to a cloud services model—enabled through migrating existing applications and/or building natively on new cloud platforms.

Yet the research also reveals that more than two thirds of organizations have retained 80% or more of their estate on-premise. So, what's holding CIOs back from moving to the public cloud?

[1] Gartner, "Is the Cloud Secure?", March 27, 2018 https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

[2] Accenture analysis of publicly available data from the U.S. Department of Health & Human Services

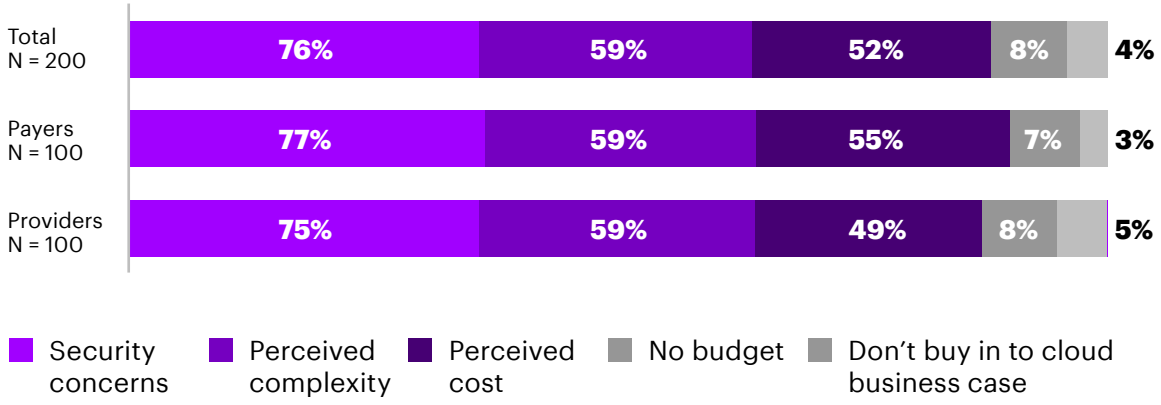
COMPLACENCY IS CONTAGIOUS

Accenture research shows that "security concerns" trump both complexity and cost as the key reason for caution among slow cloud adopters (see Figure 1). However, the same survey also revealed that many healthcare CIOs (40%) acknowledge that the public cloud is more secure than either private cloud (35%) or on-premise data centers (25%). This strongly suggests that the issue is more about mindset than technology. Security concerns revolve around how to leverage public cloud as a platform to improve security rather than whether cloud is inherently more secure if leveraged correctly.

The skills and knowledge gap in developing mature public cloud security strategies and the tools and processes that enable them is creating roadblocks to rapid public cloud adoption. The uncertainty about how to translate existing on-premise security practices to public cloud and where to adapt or change to benefit from new approaches or capabilities that public cloud provides translates into long delays in design and implementation.

Figure 1: Security concerns and perceived complexity and cost are the top reasons for slow public cloud adoption in the healthcare industry.

For those [business functions] that have been slower to adopt cloud, what were the reasons?*



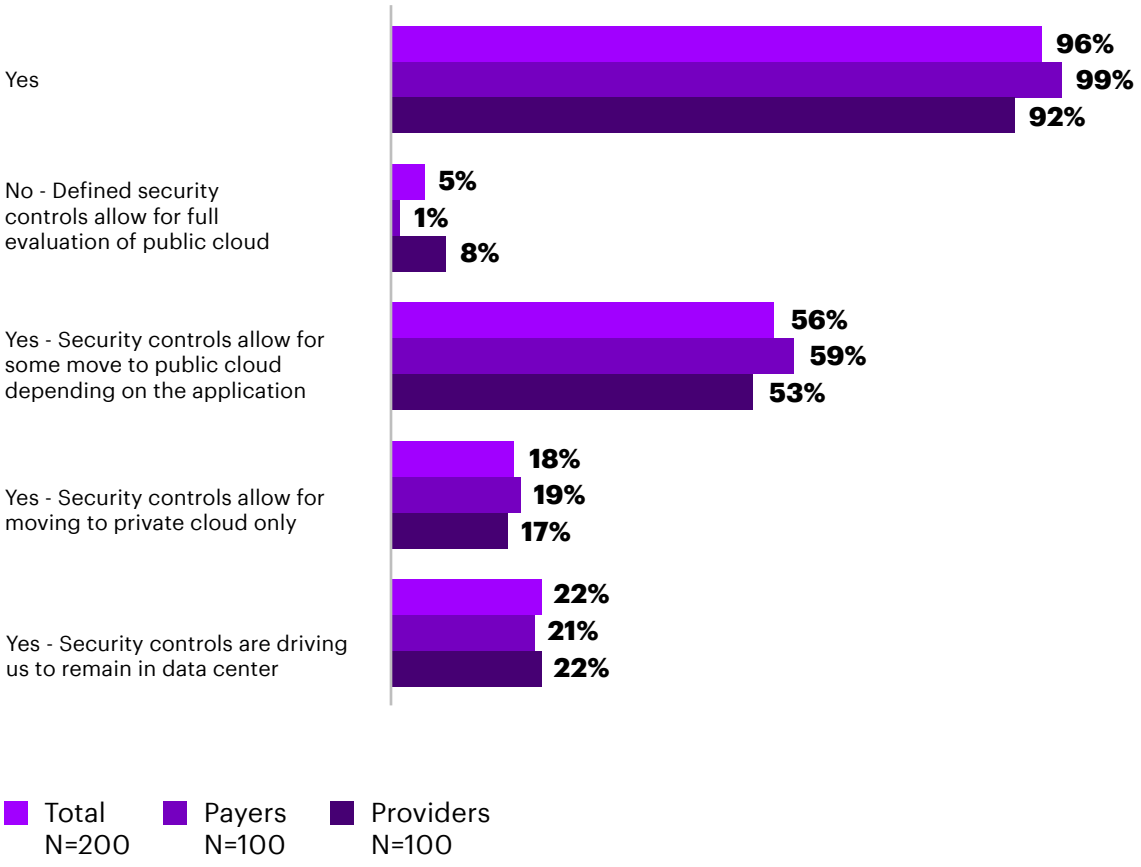
* Respondents could choose multiple options

Source: Accenture research

Another significant challenge to public cloud adoption is that nearly all healthcare organizations (96%) still have traditional policies and controls in place that prevent material public cloud adoption (see Figure 2). This is often because policies and controls name specific technologies or products rather than focusing on the desired security outcome. It is commonplace to see vendor names or capabilities in policies that limit the application to public cloud or lack the flexibility to accommodate newer capabilities born in the cloud. Often compounding this problem in healthcare are the customer-specific and regulatory requirements that have been translated into on-premise security practices over the years, which need to be refreshed for the public cloud.

Figure 2: Nearly all healthcare organizations have security policies or controls that prevent public cloud adoption.

Are there existing security policies or controls within your organization today that prevent material cloud adoption (private or public)?



Source: Accenture research

Accenture experience suggests that few existing security policies are in direct conflict with public cloud-based platforms as the primary landing zone for healthcare applications and data—it's more about understanding new shared responsibility models inherent with large platform providers and vendors and building out a new set of security controls that are easily consumable by application teams building new capabilities in the cloud. And if CIOs had a better understanding of why the public cloud is so secure the necessary shift in mindset might be accelerated. (See below.)

GRANULAR AND ROBUST: WHY THE CLOUD IS MORE SECURE BY DEFAULT

Modern, well architected applications leveraging the public cloud are innately more secure than their on-premise or private hosted counterparts. With public cloud, the default posture is to deny access; users and services need to be explicitly granted permission to access resources.

This is the inverse of on-premise environments that are open by default and where policies are manually applied to limit access. The fine grained "deny by default" posture in the public cloud greatly increases an organization's security posture and minimizes the inherent risks of inadvertent malicious access when applied consistently.

MAKE SECURITY EVERYONE'S RESPONSIBILITY— AND FOCUS ON OUTCOMES

Plainly, CIOs need to revise the way they think about cloud security. By aligning with other enterprise stakeholders—especially CISOs—and agreeing on desired outcomes, they can refresh their security controls that deliver on those outcomes.

Five considerations are key:

01 **Take a public cloud-first mindset.** Leverage new security capabilities, born in the cloud. Don't simply reapply existing security practices, processes and tooling in the cloud.

02 **Collaborate early across all stakeholders, especially the CISO.** Accenture research shows that only 21% of CIOs have completely aligned their cloud strategies with their CISO. This is a problem given the work required to build proper foundational cloud security capabilities that can be operated in the public cloud at scale.

03 **Ensure that you go beyond IT.** Draw in legal, compliance, vendor management and others and make it a conversation about why security in the public cloud reduces risk for the organization over time.

04 **Empower application owners and developers** as the stakeholders responsible for architecting capabilities differently so that they are secure in the public cloud. Provide them with pre-approved security guardrails by which they can easily integrate security into their development processes achieving speed and security.

05 **Leverage partners differently.** Maintaining security compliance in the public cloud requires a new set of cloud management capabilities. Leverage partners and public cloud providers with robust policy enforcement and compliance monitoring built for the nuances of healthcare/HIPAA.

For more information:

AUTHORS

David Wood
david.e.wood@accenture.com

Kimberly Wolf
kimberly.wolf@accenture.com

FOLLOW US

@AccentureHealth

AccentureHealth

ABOUT THE ACCENTURE 2018 HEALTHCARE CIO CLOUD SECURITY SURVEY

Accenture commissioned a survey of 100 healthcare payer executives and 100 healthcare provider executives in the US to assess healthcare organizations' cloud strategy, positioning, maturity, drivers and organizational readiness. The survey was conducted online by McGuire in May 2018 and has a confidence level of 95%.

ABOUT ACCENTURE INSIGHT DRIVEN HEALTH

Insight driven health is the foundation of more effective, efficient and affordable healthcare. That's why the world's leading healthcare providers and health plans choose Accenture for a wide range of insight driven health services that help them use knowledge in new ways—from the back office to the doctor's office. Our committed professionals combine real-world experience, business and clinical insights and innovative technologies to deliver the power of insight driven health. For more information, visit: **www.accenture.com/insightdrivenhealth.**

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions–underpinned by the world's largest delivery network–Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 477,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com.**