HEALTHCARE AND CLOUD ADOPTION IN 2021

John Grange, OpsCompass CTO

Marc Johnson, Impact Advisors, Senior Advisor

OpsCompass

OpsCompass
11422 Miracle Hills Drive
Suite 300
Omaha, NE 68154

TABLE OF CONTENTS

INTRODUCTION

Healthcare providers are relying on cloud resources at an astounding rate to keep up with digital transformation and control costs. According to Nutanix, 87% of healthcare companies surveyed cited hybrid cloud as an ideal IT operating model to meet demands such as personalized healthcare and data from AI assistants[1].

Cloud computing plays a valuable role in helping healthcare providers make patient care more portable and accessible. With the rise of at-home care and more remote options, researchers and providers are creating new ways to track patient outcomes and treatments. New applications that heavily rely on the cloud are becoming more and more prevalent. Healthcare facilities across the nation are beginning to seamlessly connect their resources and data.

While exciting, these advancements also bring the risk of unchecked and mismanaged growth. If left unmonitored, this growth can threaten the safety of EMR applications, accelerate costs, and put patient data at risk.

Unstructured, unmanaged healthcare clouds can undermine the very purpose of their existence.

Do you have the visibility and resources needed to manage the delicate balance of modern healthcare?

Purpose of this paper

With this paper, we'll discuss:

- How to manage and control a multi-cloud environment.
- How to identify security gaps before they cause real damage.
- How to simplify compliance and audits with comprehensive visibility.
- How to control costs and scale your cloud infrastructure without exceeding budgets.

[1]https://www.nutanix.com/press-releases/2020/healthcare-organizations-deem-data-security-and-compliance-as-leading-factors-in-hybrid-cloud-adoption

MULTI-CLOUDS PILE UP FAST

Concerns over security and compliance have left many healthcare providers like hospitals, clinics, and treatment centers clinging to on-premises servers and storage. Historically, healthcare providers have avoided new technologies, including the cloud, for fear of putting patient data at risk and jeopardizing compliance with IT regulations. There has been a move, however, to increased remote patient management. As in-house equipment costs continue to rise, many healthcare providers are trying to save costs by expanding their presence to a multi-cloud environment.

According to the CEO of Ambra Health, hybrid cloud deployment among healthcare providers may grow 37% this year, up from 19% in 2019[2].

If you are setting up an environment for a healthcare provider, your experience with the cloud might start with a Software as a Service (SaaS) like Office 365. Then one might progress to Disaster Recovery as a Service (DRaaS). These services might then be followed by Amazon Web Services (AWS) and possibly Azure. In no time, you are in a multi-cloud environment that co-mingles with your networks and critical EMR solutions. But do you have the tools needed to manage these environments?

"Healthcare providers can be tempted to prematurely move on-premises applications and data to the cloud," said Marc Johnson, CISO with Impact Advisors, a nationally recognized healthcare consulting firm in Illinois. "And that's where I see a lot of healthcare organizations struggling today. They want to take that simple route of lift and shift everything, which is absolutely not the right thing to do because it leads them down the wrong path for security and cost, for what appears to be agility."

> *"Healthcare providers can be tempted to prematurely move on-premises applications and data to the cloud… this leads them down the wrong path for security and cost."*

Healthcare multi-cloud environments can be dangerous, costly, and extremely difficult to monitor. Costs for unused or underutilized cloud resources can quickly add up and unchecked permissions can lead to unauthorized access to critical resources. When it comes to audits for HIPAA and other regulations, you might find yourself assigning a small army of IT resources to track down information.

Management also becomes an issue when healthcare organizations move the wrong applications and data to the cloud. Even in an age of "cloud now," some things should never be moved or connected to the cloud.

[2]https://www.entrepreneur.com/article/363124

KEEP YOUR MULTI-CLOUD HOUSE IN ORDER

To keep your multi-cloud environment from putting your critical data at risk, you need complete visibility to know when resources and applications are added to your cloud.

With the right level of visibility into your multi-cloud environment, you can sort and see by providers, accounts, resource types, and regions from a single pane of glass. You can reduce wasted cloud resources, anticipate your cloud activities' costs, and receive alerts before they exceed budgets. Visibility enables complete control over your multi-cloud.

A higher level of control also means an increased ability to rein in costs. If you know when resources like SaaS-based applications and storage are no longer being used, you can eliminate them to save money. Control gives you the ability to make configuration changes when and where needed, preventing others from taking those actions upon themselves.

According to Johnson, healthcare organizations can experience a 30% cost savings by moving to the cloud – but only if it's managed appropriately.

"We can see both AWS and Azure with consistent measurement and can monitor cost, rigor, and performance in one location," Johnson shares about his OpsCompass cloud management experience with CIO Magazine, "Without OpsCompass, our FTE [full-time equivalent] costs would have doubled."

COMPLIANCE CAN CHANGE IN A HEARTBEAT

Visibility and control are critical components of ensuring you are following HIPAA and other industry guidelines.

Cloud subscription-based applications can be easily added to your multi-cloud environment by anyone with a credit card, producing a new level of Shadow IT. These applications might hit the mark in terms of delivering services needed at the moment, but do you know how they stack up against your internal policies and industry regulations?

"When a cloud application is added to your environment, your compliance score can change in a heartbeat without your knowledge," Johnson said. "Cloud providers claim they're operating within regulatory standards. But when it comes to an audit, the burden of proof is on you."

> *"When it comes to an audit, the burden of proof is on you."*

That is why it is crucial to have the visibility and control to enforce your policies and industry regulatory standards. You need to know your compliance score at any given time, not just before an audit.

Enforce Standards and Always Know Your Compliance Score

Point-in-time visibility into your healthcare multi-cloud is critical to confirming compliance with your internal baselines and specific regulatory benchmarks. OpsCompass provides visibility tools that can make life easier for dedicated IT compliance experts, automatically benchmarking every change against compliance standards including HIPAA, Center for Internet Security (CIS), and National Institutes standards.

SECURITY GAPS IN THE CLOUD

Alerts to changes in your compliance score can also serve as an indicator of potential security exposures. Healthcare is no longer considered sacrosanct to cybercriminals, even in the middle of a global pandemic. Unchecked cloud solutions can offer new entry points for hackers to attack healthcare organizations.

One of the largest attacks last year involved Blackbaud, a U.S. based cloud computing provider, which experienced a ransomware attack that reached colleges, universities, foundations, and other non-profits across the U.K., U.S., and Canada. This put people's data at risk – a risk that healthcare providers cannot afford[3].

"When a cloud resource joins your multi-cloud without your knowledge, any number of exposures can occur. Even if they're approved, outside cloud resources can still introduce elements that can wreak havoc with your network and data," Johnson said.

Healthcare providers who move to the cloud rely on management, configuration, and automation tools, all of which can be misconfigured and exploited. This creates new attack opportunities. But proper monitoring of your compliance score and cloud health can easily identify and mitigate those kinds of risks.

Build a Better Security Posture for your Healthcare Cloud

To help prevent cloud vulnerabilities, strive for improvements to your Cloud Security Posture Management (CSPM). CSPM gives IT operations and cloud engineering teams the visibility needed to determine their multi-cloud environments' evolving security and compliance posture. A good security posture will provide alerts and tools to improve the security of your healthcare data and patient information.

[3]https://www.securitymagazine.com/articles/93857-blackbaud-sued-after-ransomware-attack

OPSCOMPASS GIVES YOU CONTROL AND VISIBILITY

To help you meet the digital demands ahead, OpsCompass gives clear visibility and management to make sure your healthcare multi-cloud environment is safe, secure, and able to grow without putting your customers at risk.

With a healthy cloud environment, you will be flexible and resilient to reduce costs without sacrificing security and reliability.

A Better View of Your Cloud

Your road to a healthy multi-cloud environment starts with a comprehensive snapshot to understand what is inside your cloud. This includes a look from a single pane of glass at the different clouds, your accounts, and resources. We can determine when new resources are added, what is causing configuration drifts or exceeding budget, and what is unnecessary based on your consumption models.

Up Your Compliance Score

Upon reviewing your cloud, we can help you determine how well you are meeting internal and regulatory compliance requirements with a proprietary score and graphs over your dashboard. You can then drill down to identify compliance problems and determine how to fix them. Our software remediates the issues and logs when your configuration goes in and out of compliance. This information is then easily exported to use during your next audit.

Automate Your Cloud Platform Security

You can still benefit from the cost savings, speed, and agility of your cloud without sacrificing the safety and security of your apps and data. OpsCompass can help you maintain a healthy security posture by proactively identifying risky configurations across multiple clouds over a single dashboard. We'll help you be aware of cloud configurations and settings that can violate your compliance standards and stop them before they cause harm.

LET'S TALK

With OpsCompass, we can help you meet today's modern healthcare demands with a multi-cloud environment that is safe, secure, and able to scale without exceeding budgets or falling out of compliance with industry regulations. To find out how you can gain clear visibility and management across your entire cloud, contact us or start a free trial or demo today.

About John Grange

jgrange@opscompass.com

John Grange is a seasoned entrepreneur and is currently co-founder and CTO at OpsCompass, a leading SaaS product for managing compliance and security in clouds like Azure, AWS, and GCP. He has 15 years of experience building products and companies including co-founding a top 5 global Microsoft ASP.net hosting provider (now Managed.com) and creating SaaS products in areas diverse as healthcare (Layered Health) and marketing tech (Layeredi). John's passion is identifying those mega trends that truly impact how technology can be leveraged and then building the necessary tools to help real customers use that technology to create business value.

About Marc Johnson

marc.johnson@impact-advisors.com

Marc is an experienced CIO, CTO, CISO, and CCO. Marc has led many organizations in various industries. Most recently, healthcare has been the industry in the greatest need. Regulations and transformation have become the battle cry within healthcare. Marc has championed the transformation of traditional Healthcare IT. Transformation from business as usual to more progressive but tempered outcomes. Marc is leading a Healthcare provider currently while providing input into a SaaS startup.

Additional Resources:

[1] https://www.nutanix.com/press-releases/2020/healthcare-organizations-deem-data-security-and-compliance-as-leading-factors-in-hybrid-cloud-adoption

[2] https://www.entrepreneur.com/article/363124

[3] https://www.securitymagazine.com/articles/93857-blackbaud-sued-after-ransomware-attack