Best Practices for Managing Risks in Your Cloud Deployment

November 2019

Best Practices for Managing Risks in Your Cloud Deployment

IT teams are embracing the cloud for its scalability, reliability, flexibility, and rapid deployment capabilities, helping them achieve performance and cost-savings goals.

According to Gartner, by the end of 2019, we'll see, "30 percent of the 100 largest vendors' new software investments will have shifted from cloud-first to cloud-only."

But for enterprises transitioning from on-prem architectures, a move to the cloud opens up new and unchartered territory when it comes to managing risk. Complex, distributed resources in the cloud call for an update to the standard risk management and security approach.

For security teams tasked with securing cloud environments, holding on to pre-cloud tools and mindset is no longer going to work, as the challenges and tools needed to secure cloud environments are different from what was required to secure pre-cloud architectures. Even worse, copying pre-cloud solutions means that the drawbacks of pre-cloud architectures are brought into the cloud world. Only by fully embracing the cloud and its values can enterprises take full advantage of its benefits.

Security Challenges in the Cloud

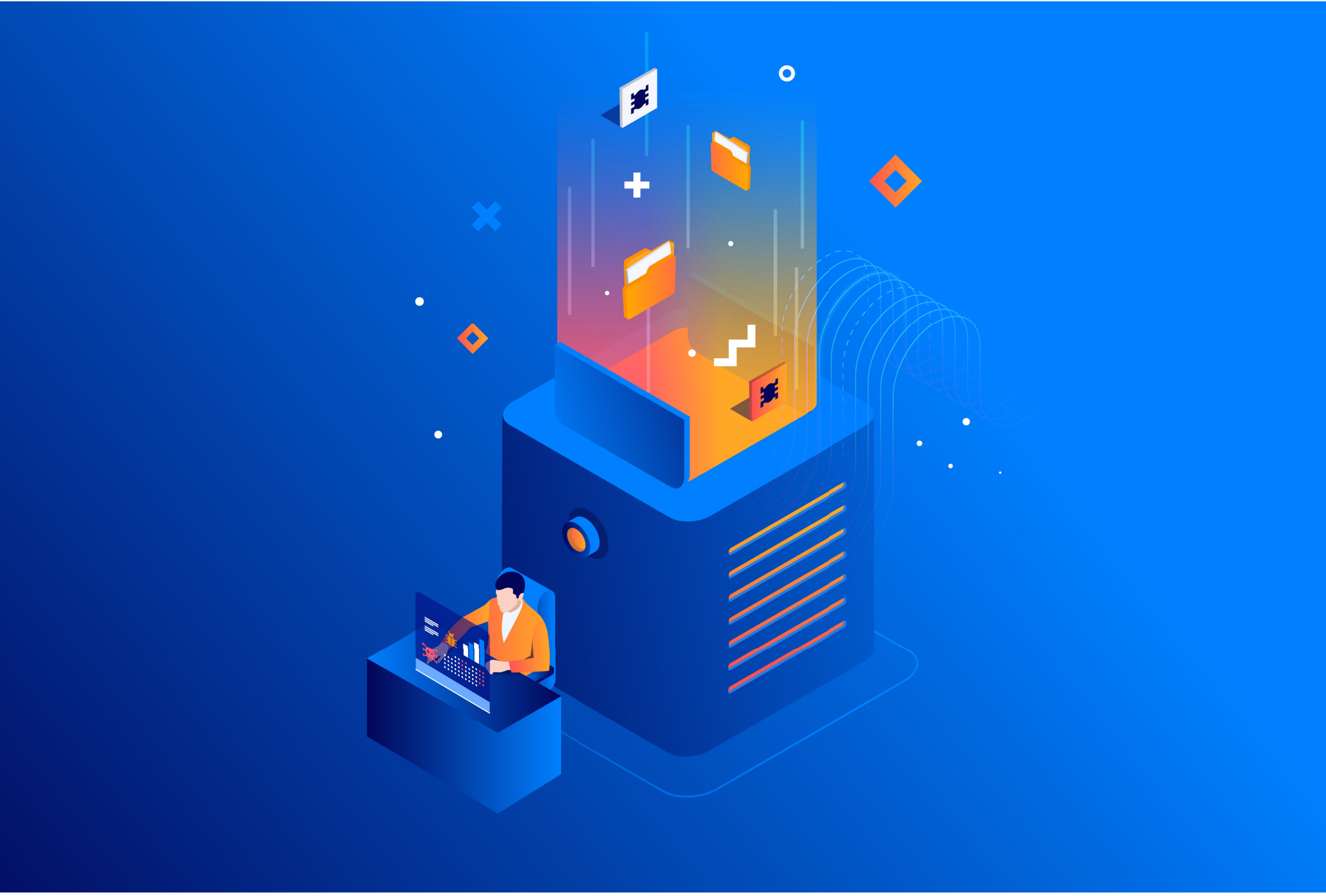
Cloud Challenge 1: Overriding IT and Security

According to Symantec, 93% of security decision-makers report issues with keeping tabs on all their cloud workloads, and only 27% believe that they are capable of addressing all cloud security threats.

The way enterprises deploy technology has fundamentally changed. In the pre-cloud era, any enterprise IT initiative or digital project required hands-on, end-to-end involvement from the internal IT team and respective security personnel. With the cloud, spinning up servers and applications, managing them, and keeping them running on a day-to-day basis is done seamlessly and with a click of a button. Business users no longer rely on IT departments and technical expertise to push ahead with cloud services and security isn't always built-in or baked into the process.

As a result, security and IT professionals are increasingly losing track of workloads in the cloud. A recent survey by Gartner illustrates that approximately 40% of all IT spending at a company occurs outside the IT department. Since cloud applications often do not require internal IT support to deploy, the number of applications used by employees without the explicit approval, or even the knowledge of the IT department is growing.

This opens up a pandora's box of vulnerabilities and security holes as sensitive corporate data is often uploaded to these apps and services, putting the enterprise at risk of a data breach.



Cloud Challenge 2: The Agility/Security Tradeoff

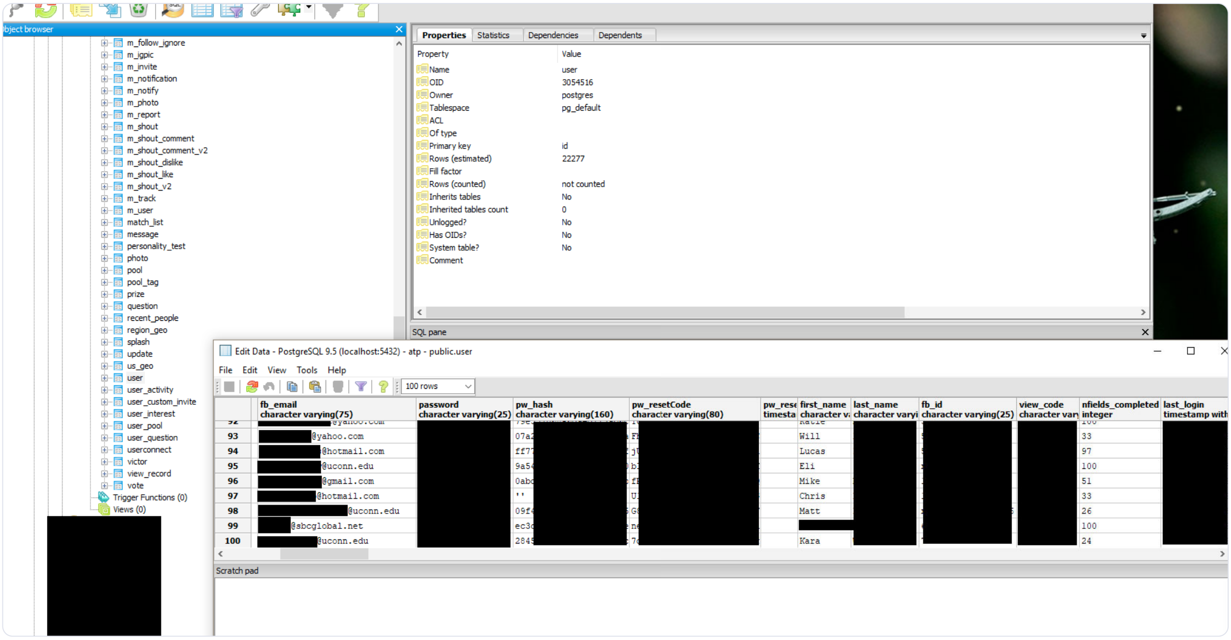
One of the undisputed strengths of cloud deployments - the unprecedented agility that speeds up innovation - comes at a cost.

As code is being deployed at an increasingly neck-breaking speed, bugs and security holes abound, and human errors are becoming both more likely and more devastating. Even the smallest error, for example adding an extra “/ “sign could have severe consequences.

In the pre-cloud era, both the security and application owners, needed to drop the ball to make enterprise data records public. Nowadays, databases are often managed at a single touchpoint, making critical mistakes more probable and more frequent.

Large scale breaches resulting from human error are the hallmark of the cloud era. Here are just a few examples from 2019:

- Over 540 million Facebook interaction records left exposed by third parties using Amazon's cloud services
- Amazon AWS error exposes info on 31,000 GoDaddy servers
- 24 million financial documents related to US mortgages and banking on an exposed database
- Cloud database removed after exposing details on 80 million US households
- 1TB of police body camera videos found lounging around public databases



m_follow_ignore
m_igpic
m_invite
m_notification
m_notify
m_photo
m_report
m_shout
m_shout_comment
m_shout_comment_v2
m_shout_dislike
m_shout_like
m_shout_v2
m_track
m_user
match_list
message
personality_test
photo
pool
pool_tag
prize
question
recent_people
region_geo
splash
update
us_geo
user
user_activity
user_custom_invite
user_interest
user_pool
user_question
userconnect
victor
view_record
vote
Trigger Functions (0)
Views (0)

[redacted]

Property	Value
Name	user
OID	3054516
Owner	postgres
Tablespace	pg_default
ACL	
Of type	
Primary key	id
Rows (estimated)	22277
Fill factor	
Rows (counted)	not counted
Inherits tables	No
Inherited tables count	0
Unlogged?	No
Has OIDs?	No
System table?	No
Comment	

Edit Data - PostgreSQL 9.5 (localhost:5432) - atp - public.user

	fb_email character varying(75)	password character varying(25)	pw_hash character varying(160)	pw_resetCode character varying(80)	pw_rese timesta	first_name character va	last_name character varyi	fb_id character varying(25)	view_code character vary	nfields_completed integer	last_login timestamp with
93	[redacted]@yahoo.com	[redacted]	[redacted]	[redacted]		Will	[redacted]	[redacted]	[redacted]	33	[redacted]
94	[redacted]@hotmail.com	[redacted]	[redacted]	[redacted]		Lucas	[redacted]	[redacted]	[redacted]	97	[redacted]
95	[redacted]@uconn.edu	[redacted]	[redacted]	[redacted]		Eli	[redacted]	[redacted]	[redacted]	100	[redacted]
96	[redacted]@gmail.com	[redacted]	[redacted]	[redacted]		Mike	[redacted]	[redacted]	[redacted]	51	[redacted]
97	[redacted]@hotmail.com	[redacted]	''	[redacted]		Chris	[redacted]	[redacted]	[redacted]	33	[redacted]
98	[redacted]@uconn.edu	[redacted]	[redacted]	[redacted]		Matt	[redacted]	[redacted]	[redacted]	26	[redacted]
99	[redacted]@sbcglobal.net	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	100	[redacted]
100	[redacted]@uconn.edu	[redacted]	[redacted]	[redacted]		Kara	[redacted]	[redacted]	[redacted]	24	[redacted]

'Example of breached PostegreSQL database'

Cloud Challenge 3: Pre-cloud Solutions Are No Longer Effective

In the physical world, creating a new network or spinning up a new server was a lengthy and complicated process that involved many people and required hardware installation and physical cabling. Today, everything happens with a script. Securing virtual networks and virtual servers is also a different animal altogether, and perimeter-based security solutions that rely on physical firewalls, switches and routers are losing their relevance.

Cloud Challenge 4: Poor Visibility

One of the biggest security challenges in the cloud is lack of visibility into applications, users and network traffic. Enterprises overwhelmingly have low visibility into their public cloud environments, and the tools and data supplied by cloud providers remain insufficient. Cloud visibility is multi-faceted and requires the ability to penetrate all four layers of cloud environments:

- **Cloud infrastructure level:** Clear visibility here provides answers to the following questions: which assets are running on which networks, who is allowed to access them, etc.
- **Operating system level:** Visibility into this layer provides information on which OS is in use, its configuration and setup (including user privileges, and latest updates and patches to the OS) and when it was last updated or patched. Since the remote code execution vulnerabilities inhabit this layer, it is a crucial piece of the puzzle when it comes to cloud security.
- **Application level**: It is vital to see which applications are installed, their configurations, and whether they are patched.
- **Data stack level:** Contains visibility into all data inventory and where it is housed. Clear visibility into this layer is critical in order to determine where the organization's crown jewels are, and which servers include sensitive data such as PII or payment info.

According to the aforementioned survey by Gartner, cloud professionals report the following issues caused by inadequate cloud visibility:

- Lack of cloud visibility is obscuring security threats to their organization
- Visibility problems lead to application and network performance issues
- Insufficient visibility is a key factor in application and network outages

Nearly half of companies have performance issues from a lack of cloud visibility

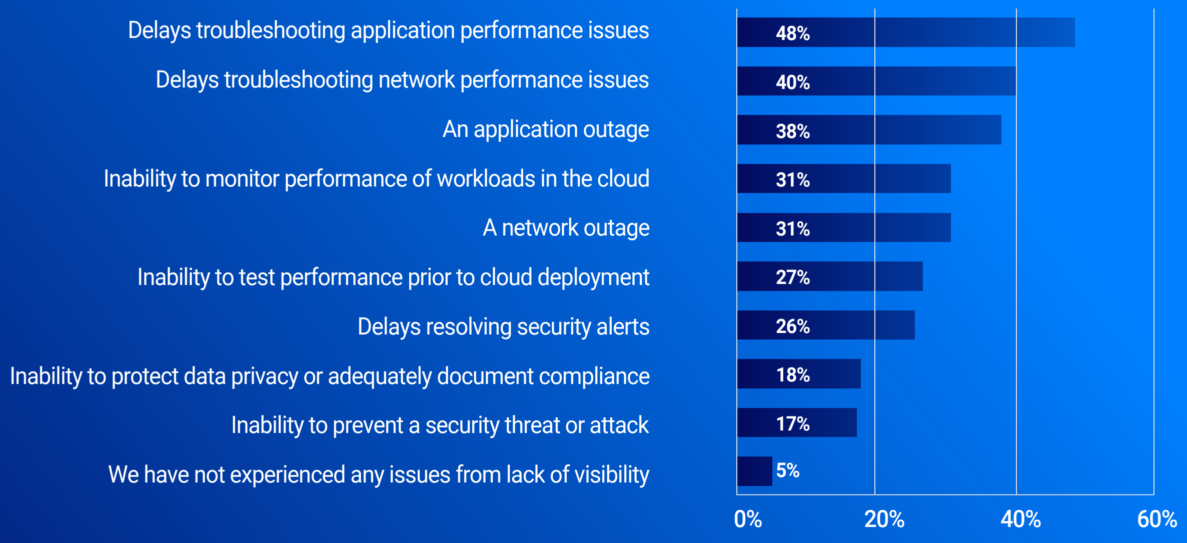


Image source: https://www.ixiacom.com/resources/state-cloud-monitoring

Cloud Challenge 5: Pre-cloud Security Troubles Did Not Go Anywhere

Hackers are infrastructure-agnostic; they don't care if your architectures are based on-prem or in the cloud. Traditional security concerns such as critical vulnerabilities, malware, phishing, social engineering and ATO attacks are as relevant for cloud environments are they are for hybrid or on-prem deployments. Vulnerabilities in cloud containers have increased by 46 percent compared to the same period in 2018 and by 240 percent compared to 2017.

7 Best Practices for Managing Risks in your Cloud Deployments

Cloud deployments demands security architectures that are designed for the cloud, not copied from the pre-cloud workloads. Here are 7 best practices to make that happen:

1. Design your Security for the Cloud

Cloud security is to a large extent a balancing act. On the one hand, IT teams must minimize friction and inter-company dependencies. On the other hand, they need to ensure that the right processes and security procedures are followed. Finding the right balance between usability and security is key, as even the best policy won't be effective if the people in your organization are not working together with your security team. That is why beyond policy and procedures, cloud security must be supported by ongoing awareness training, collaboration, processes and advanced security technologies that were made for the cloud.

2. Think of Security Dependencies as a "Graph"

Whether your architecture is on-prem or in the cloud, hackers always look for the weakest link. In the majority of cases, breaches happen through the 'back alleys' of the environment and not through the fortified front gates. Hackers often breach a network by accessing a less high-profile spot and then move laterally through the network until they reach a high value asset, their jackpot. Instead of prioritizing your assets and concentrating on protecting your "crown jewels", **think of cloud assets as a network of security dependencies, where every piece of the puzzle, no matter how small, contributes to the overall security posture**. In a way, the key is to think of your attack surface as a graph and carefully monitor connections between assets.

3. Bring Back the Separation of Duties

The purpose of having a separation of duties is to prevent a single person or team from having ‘Godlike’ powers within an environment. Your development team will always be requested to immediately deliver new product and/or organizational capabilities. They can not be expected to always prioritize security over agility and rapid deployment. There must be a policy in place that enables security teams to be effective auditors and approvers for all deployments released by the application and development teams.

4. Beware of Phantom Data Copies

One of the dirty secrets of many multi-cloud deployments is the fact that the data needs to be available simultaneously in multiple environments, mainly due to performance and cost considerations. In order to run your application on a multi-cloud environment, you need to make sure that the data is locally available on each cloud. These copies are often created ad-hoc without proper security procedures, abandoned after use and left completely neglected from a security perspective, making them an easy target for an attack. While copying data is not a recommended practice, many developers feel as if they have no other choice. In these particular instances, IT personnel should remain vigilant as phantom data copies are often an easy target for attackers.

5. Prioritize Visibility

Poor visibility is one of the major contributing factors to lack of security in the cloud. However, there isn’t much of an excuse for having poor visibility into cloud workloads anymore. Today, it’s a matter of finding the right tools, putting them into place and making sure that security teams have both the toolsets and the training they need to attain the level of visibility necessary.

6. Consider your TCO

Choose tools that integrate easily and work seamlessly with your cloud environments and entire technology stack. Integration projects can easily get out of hand and become big investments. The key to managing your cloud TCO risks is to never depend on manual integrations; this approach didn’t really work in the pre-cloud era, and certainly won’t work in the multi-cloud world with many moving parts.

7. The Accounting Department is Your Friend

Your accounting department is your best ally when it comes to securing the cloud. It's difficult for IT teams to keep track even of their own usage and spending. Since as much as 40% of all enterprise IT spending occurs outside the IT department, your accounting department essentially has the map to all the hidden cloud environments, throughout your entire organization, including ones that you forgot about or even never heard of. Credit card bills are the best paper trail you can use to track down forgotten cloud assets. Make sure to use it.

Getting Cloud Security Right

Full-stack visibility into your cloud environments is a crucial piece of the puzzle. While CISOs and their teams are held accountable for the organization's ever expanding cloud footprint, current tools don't provide the visibility needed to effectively and efficiently secure the ever expanding cloud deployments. Orca Security delivers instantaneous, scalable, hassle and impact free full stack visibility so you can:

- Detect vulnerabilities, malware and compromised assets
- See your entire full stack cloud inventory
- Discover and see previously missed assets
- Get full, hassle-free visibility at a fraction of the cost offered by alternative solutions

For more information on the Orca Security Platform,
Contact: info@orca.security.

Request a demo