



Multi-Cloud

Preventing emerging security risks

EBF Cloud Banking Conference

Benny Bogaerts



“

76% of CEOs surveyed considering migrating apps to the cloud within 18 months...

”

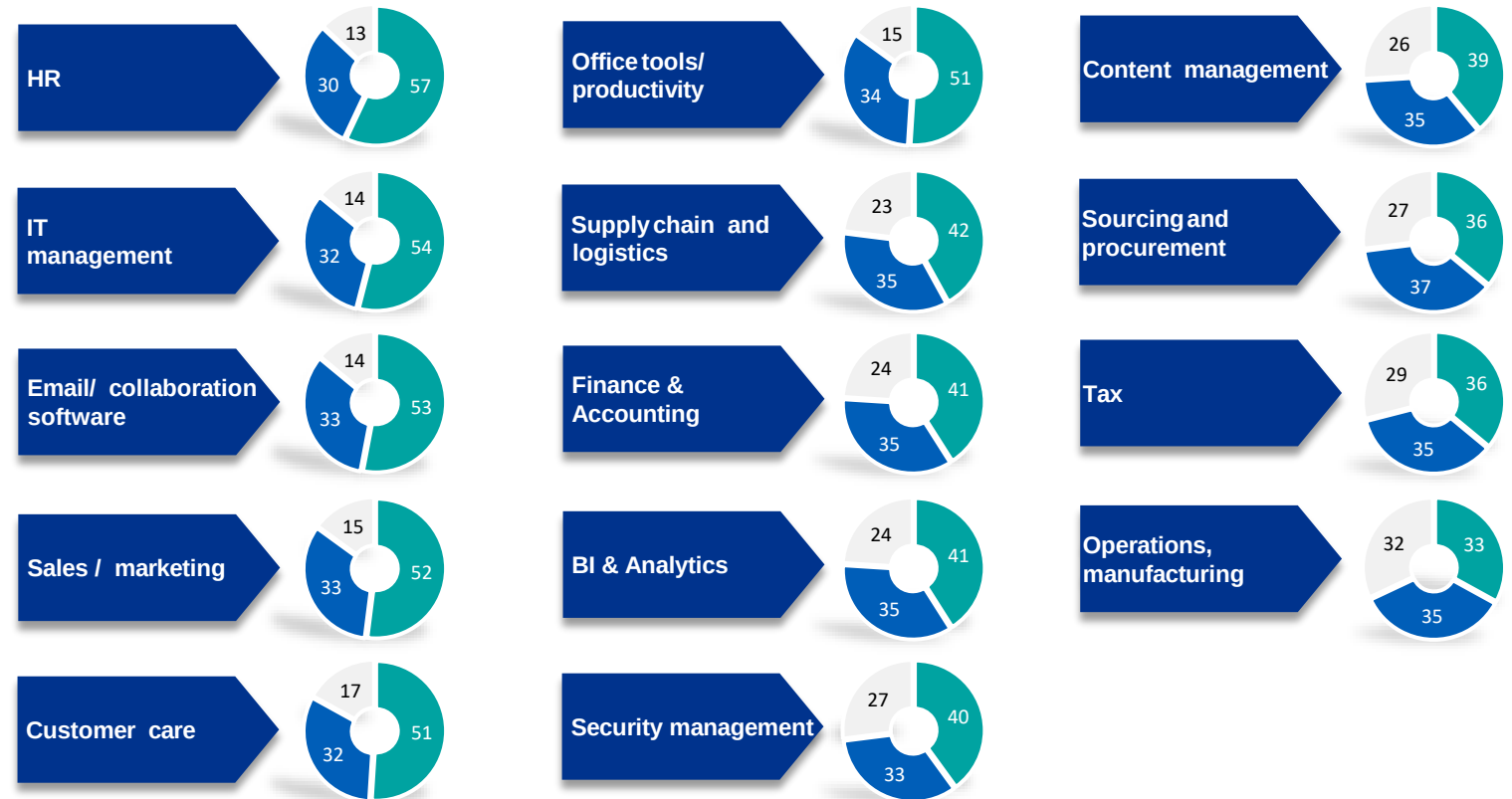
KPMG Global Cloud Survey 2018



Moving to a broader Cloud environment

Global Cloud Survey

■ Now ■ Within 18 month ■ Remaining



Source: KPMG International's Global Cloud survey: The implementation challenge

Total respondents (n = 674)

©2019 KPMG Advisory, a Belgian CVBA/SCRL and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The cloud ecosystem is maturing and scaling



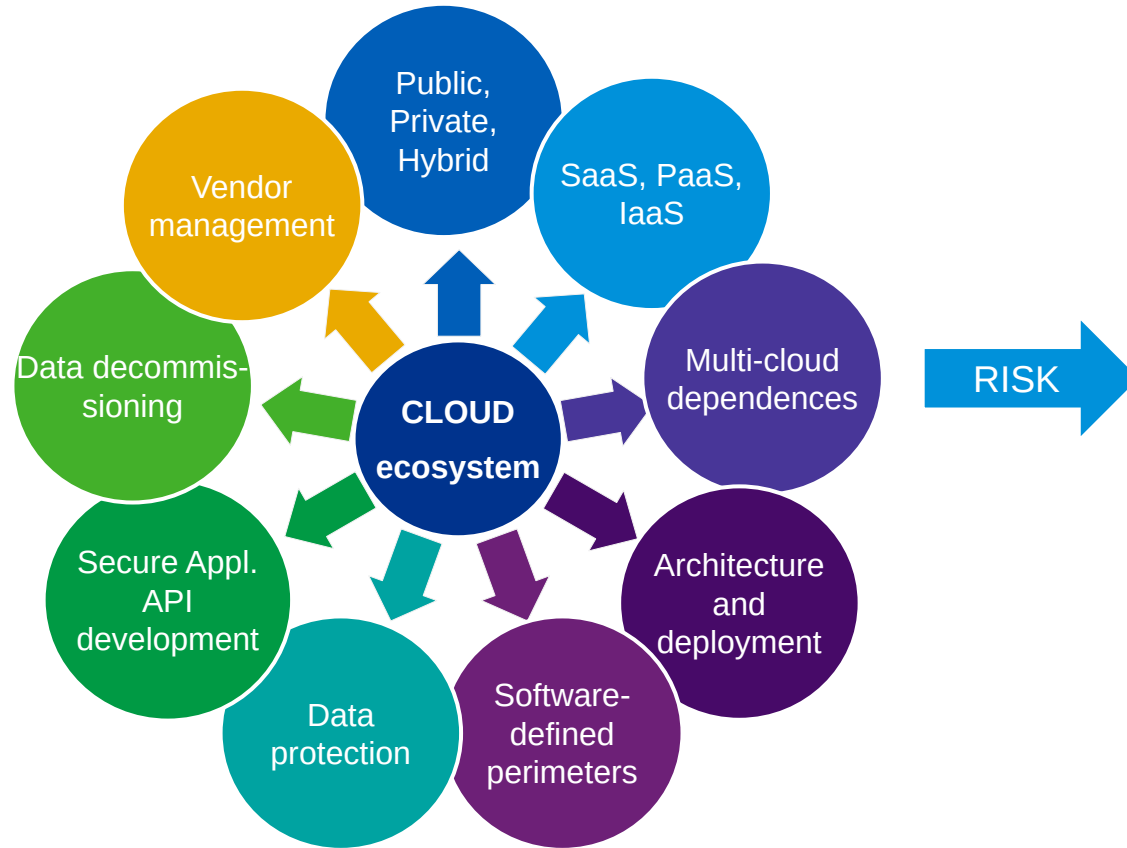
Source: The 2018 Harvey Nash/KPMG CIO Survey

82%...
have more
confidence in
cloud
technology
than the last 3
years

HARVEY NASH / KPMG CIO SURVEY 2019



The change of your ecosystem



New models, architectures and relationships		New and existing threats	
Threat actor		Threat objective	
Organized crime		— Financial gain — Corporate espionage	
Competitor		— Financial gain — Competitive advantage	
Nation state		— Economic advantage — Financial gain — Intelligence	
Hacker		— Fame — Notoriety — Embarrassment — Financial gain	

Sharing Responsibilities with Others....

1. The adoption of cloud introduces a shared responsibility model for security
2. Consumers have the most responsibility with IaaS and least with SaaS cloud models
3. This shared responsibility model can create confusion and risk exposures for cloud consumers if not properly understood and addressed

Organizations should clearly define cloud security roles and responsibilities and ensure cloud vendor contracts, cloud vendor implementations, and control operations address gaps.

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Network controls	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Host infrastructure	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Physical security	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer

Source: Microsoft what does shared responsibility in the cloud mean
<https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/>

Sample top cloud security risks

Top risks in 2016, did it change?

ENISA Top Cloud Security Risks by Likelihood & Impact

Effectiveness of Risk Management Lever (Consumer)

Sample Risk	Summary Description	Policy	People	Process	Technology	Legal
Lock-In	Inability to move data and processes from one provider to another.	●	●	●	●	●
Loss of Governance	Lack of access to provider tools to control and monitor your data & environment. For example in-ability to back-up and remove data.	●	●	●	●	●
Isolation Failure	Underlying shared resource is compromised.	●	●	●	●	●
Compliance Risks	In-ability to demonstrate compliance across cloud environments (e.g. PCI, HIPAA, GDPR, etc.).	●	●	●	●	●
Management Interface Compromise	Cloud administrative and management consoles are accessible from anywhere and most any device.	●	●	●	●	●
Data Protection	In-ability to know where your data is, how it is being shared and used, who has access to it, and who has accessed it.	●	●	●	●	●
Insecure or Incomplete Data Deletion	Risk that data is not properly deleted or removed.	●	●	●	●	●
Malicious Insider	Internal human resources gaining un-authorized or inappropriate access to sensitive information and / or otherwise altering or making un-available.	●	●	●	●	●

There have been several cloud related incidents



by Joe Panettieri • Feb 28, 2019

Dow Jones, parent of The Wall Street Journal, is the latest company to misconfigure Amazon Web Services (AWS) and expose mission critical data on the public cloud. The issue apparently involved a contractor.

Independent security researcher Bob Diachenko discovered the massive [Dow Jones Watchlist dataset](#), sitting on a public Elasticsearch cluster. It was 4.4GB in size and available for public access to anyone who knew where to look, the researcher says.

The database, he notes, contained 2.4 million records detailing such extremely sensitive information as:

- global coverage of senior Politically Expose Persons, their relatives, close associates, and associated companies;
- national and international government sanction lists and categories;
- persons officially linked to, or convicted of, high-profile crimes; and
- profile notes from Dow Jones including citing federal agencies and law enforcement sources.

Over 540 million Facebook records found on exposed AWS servers

Leak originated at two third-party companies that had collected Facebook data on their own servers.
By Catalin Cimpanu for Zero Day | April 3, 2019 — 18:32 GMT (02:32 GMT+08:00) | Topic: Security

Ad closed by Google

Stop seeing this ad

Why this ad? (i)



Data breach hunters have found two Amazon cloud servers storing over 540 million Facebook-related records that have been collected by two third-party companies. The number of affected users is believed to be in the range of millions and

SEE ALSO

10 dangerous app vulnerabilities to watch out for (free PDF)

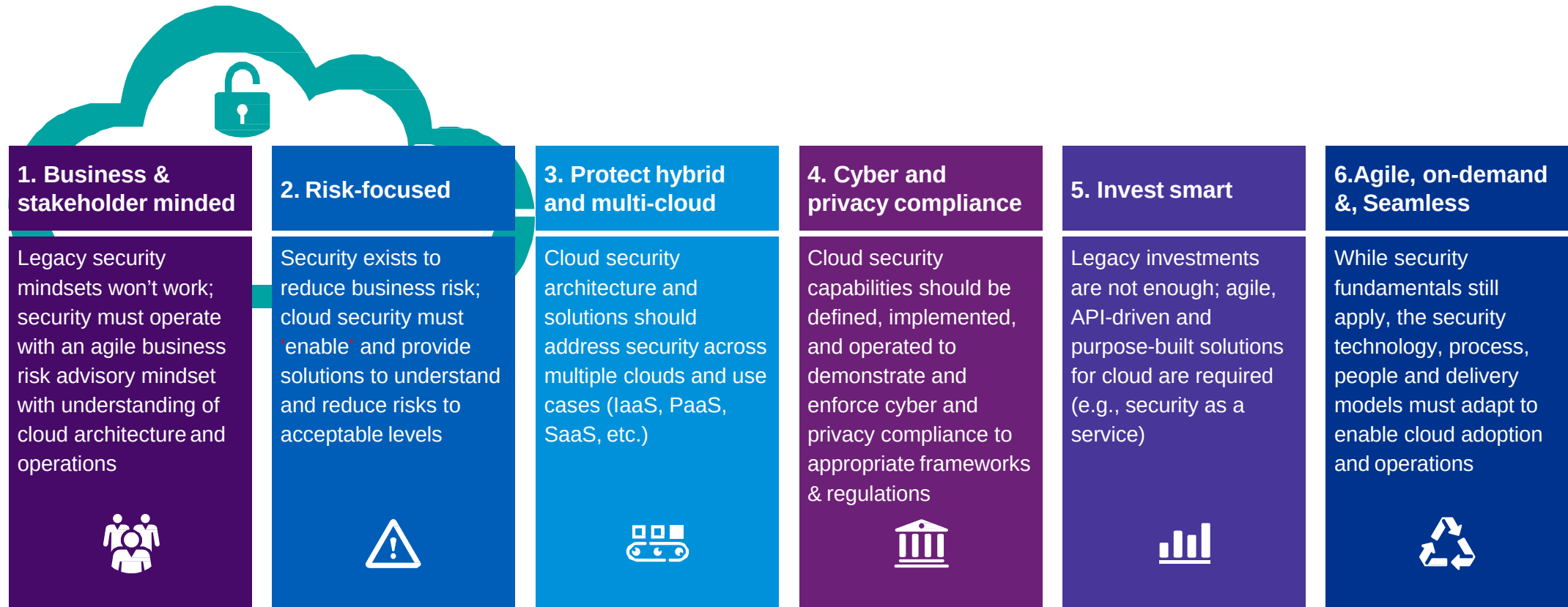
ENTER AND CONSENT TO APPLY



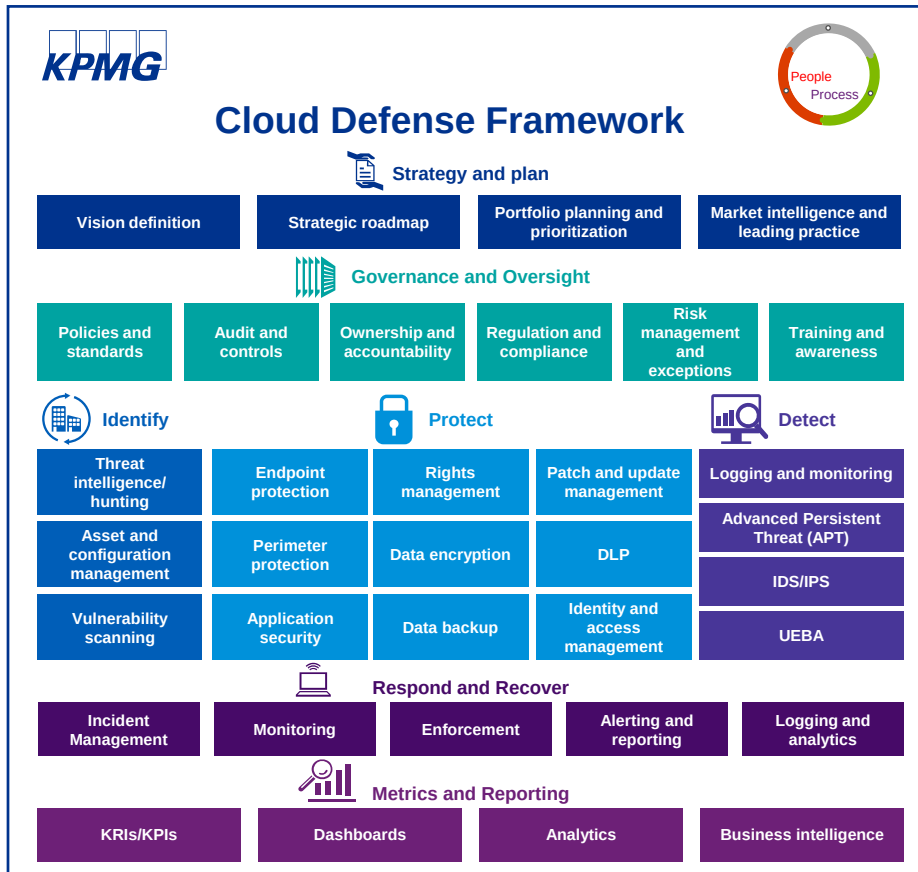
Apply now

MORE FROM CATALIN CIMPANU

Guiding principles for Cloud Security, Privacy and Compliance

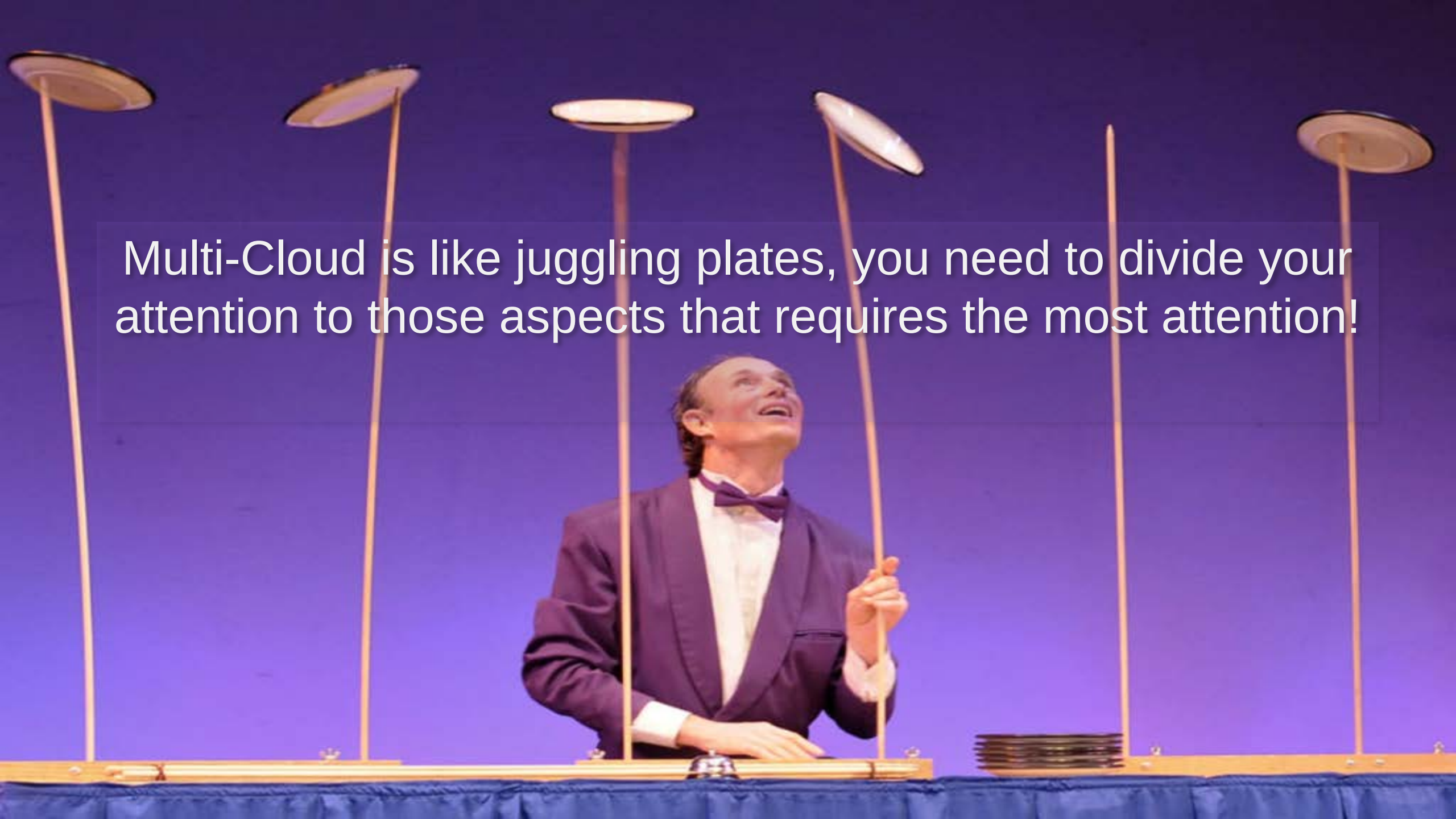


Leverage a Cloud Defense Framework to manage risks



Capabilities to Achieve Security Visibility
...from initiation through a sustainable program

Multi-Cloud is like juggling plates, you need to divide your attention to those aspects that requires the most attention!



Panel discussion