

PwC China and Hong Kong Cloud Security Enablement Services

2018





You might be taking steps to enable a new business/ operation model using cloud...

We are here to help you enable necessary protections on your chosen cloud solutions, to match your expected level of protection

“Cloud migration” is no longer a Go or No-Go decision, but a matter of when and how

Behind the rapid and increasing adoption of cloud services (e.g., IaaS, PaaS, SaaS etc.), we have identified the following key common drivers:

1. Global decision of Multinational corporations
2. Business decision
 - Time To Market
 - Need to share
3. Improved operation effectiveness and cost efficiency

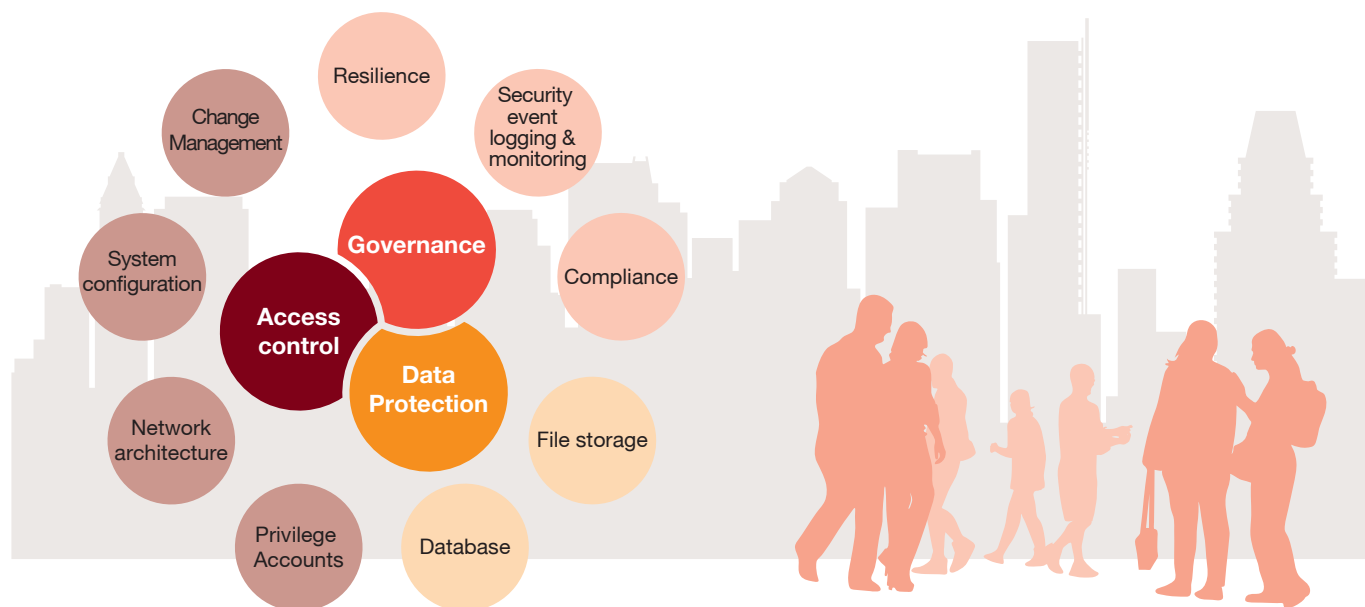
However, a successful cloud migration does not necessarily lead to seamless and secure operations. In recent months, PwC’s Dark Lab researchers have witnessed and responded to a large number of cyber attacks where victims had been using a variety of cloud services and its security has been questioned by many. We beg to disagree.

Cloud Security must be ‘enabled’

In most cases, our on-the-ground experience suggests that ‘cloud security’ was already available from the first day of migration. However, these were never enabled and PwC’s Dark Lab sees this as the primary issue.

The focus is not “am I safe on cloud”, but rather, “how do I enable the required security features on cloud?”

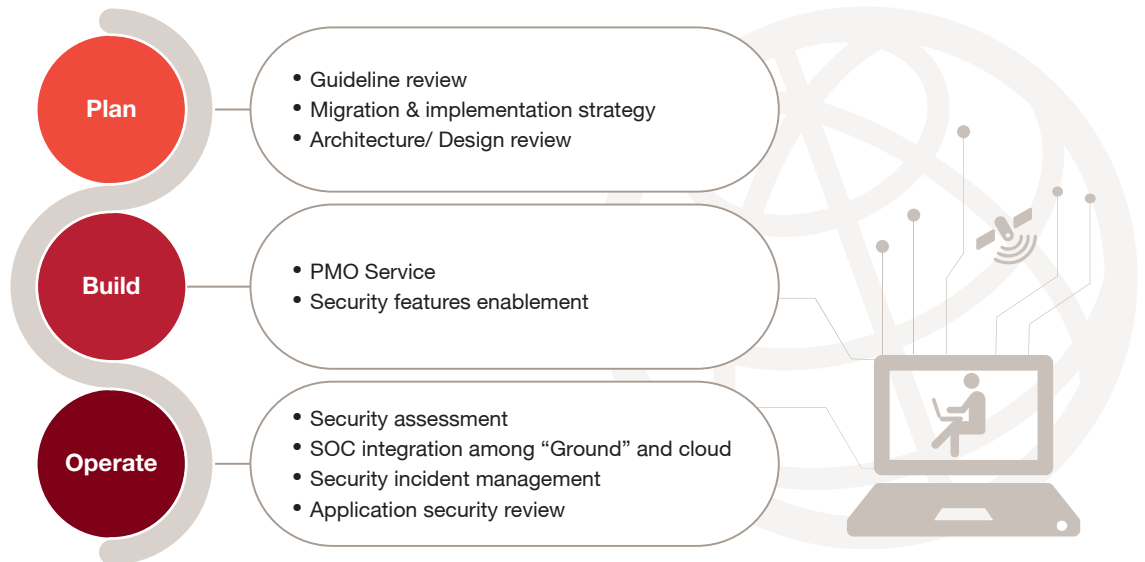
It is time to unleash the security power of the cloud services you are using for IaaS



	AWS	Microsoft Azure	Office 365	Alicloud
Compute	EC2, Lambda, ECS, Lightsail	Azure VM, Azure Container Service, Azure Function	N/A	Elastic Compute Service , Container Services
Network	VPC, ELB, CloudFront, Security Group, Route53, DirectConenct	Virtual Network, Content Deliver Network, NSG, DNS, Traffic Manager, Load Balancer, Application Gateway, ExpressRoute	N/A	VPC, CDN, , SLB, WAF
Privilege accounts		Azure AD Privilege Identity Management	Azure AD Privilege Identity Management	
Storage	S3, Glacier, EBS, Storage Gateway	Azure Storage (Blobs, Tables, Queues, Files), Azure StorSimple, Azure File Storage	OneDrive, SharePoint	Object Storage Service, NAS, Table Store
Database	RDS, DynamoDB	Azure SQL database, Azure DocumentDB, Cosmos DB, Table Storage		ApsaraDB for RDS, Aspara for MongoDB
Security and Compliance	IAM, CloudHSM, KMS, Shield , WAF	Azure AD, Azure Key Vault, WAF	Advanced Threat Protection, Mobile Device Management	RAM, KMS, Anti-DDoS, Server Guard, WAF
Logging & Monitoring	CloudWatch, CloudTrail	Activity Log, Diagnosis Logs, Azure AD Reports, OMS, Azure Log Integration	Azure AD Reports, User Activity Reports, Mailbox audit logging	Cloud Monitor, ActionTrail
Security features you can enable:	>90	>90	>60	>80

Disclaimer: Please note that the above information is for reference only. Please refer relevant cloud provider's website for latest information and details

Building your end-to-end cloud journey



Case Study



Business issue

- Client encountered a security incident in which the data was locked.
- The normal business operations were interrupted at that time as all of the data cannot be retrieved and processed during working hours.



What PwC did

- Unlocked the data and resumed business operations.
- Analysed the existing IT environment and helped the client to define short term and long term IT strategies.
- Redesigned whole IT infrastructure from security perspectives.
- Migrated public website to Microsoft Azure with a number of infrastructure security controls.
- Migrated customer email accounts from on-premises to Office 365.
- Completed the whole migration process within 2 months.



Value delivered

The results and value of the project that were delivered:

- Customer data is handled in a more secure and systematic way.
- Customer can focus more on generating new profit with business innovation while sharing some of IT infrastructure and security responsibilities to the cloud provider.

Talk to our Cloud Security team in Hong Kong and China

Our cyber security professionals across the globe have access to over 60+ technical and forensics labs, technologies and business partners, and provide incremental or supplemental support as needed. We also have a leading team in the local market, with deep technical expertise and the ability to service your immediate needs.

We're particularly proud of our managed security services capabilities – a unique combination of on-premise and centrally coordinated capabilities designed to free your IT and security teams to focus on improving your business security.

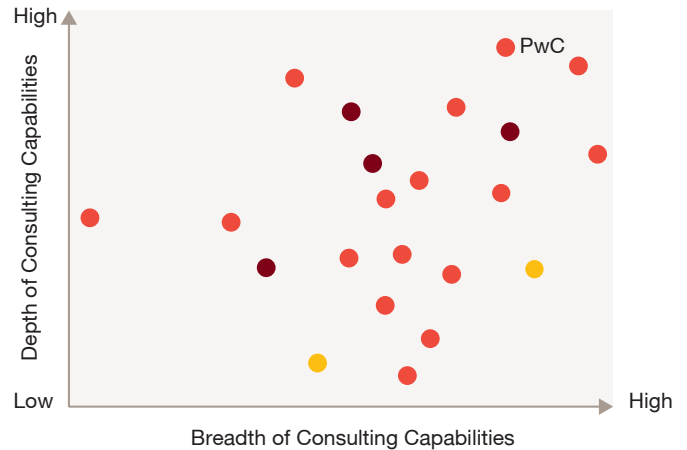
PwC provides security and incident monitoring, analysis, reporting and remediation tracking.

scan the QR code below to book an appointment



Vanguard Leader by ALM Intelligence (2016)

ALM Intelligence Vanguard™ of Cloud Consulting Providers



- Advancing Service Breadth or Depth
- Neutral
- Diminishing Service Breadth or Depth

Source: Cloud Consulting, ALM Intelligence



Kenneth Wong

Partner, Cybersecurity and Privacy National Practice
Leader – China / Hong Kong
+852 2289 2719
kenneth.ks.wong@hk.pwc.com



Kok Tin Gan

Dark Lab
+852 2289 1935
kok.t.gan@hk.pwc.com



Felix Kan

Dark Lab
+852 2289 1970
felix.py.kan@hk.pwc.com



Cyril Luk

Dark Lab
+852 2289 2972
cyril.ct.luk@hk.pwc.com



Dennis Lam

Dark Lab
+852 2289 8515
dennis.cw.lam@hk.pwc.com



Jenius Shieh

Dark Lab
+852 2289 4522
jenius.hc.shieh@hk.pwc.com



Martin Leung

Dark Lab
+852 2289 8542
martin.yc.leung@hk.pwc.com



Tony Lam

Dark Lab
+852 2289 3509
tony.kh.lam@hk.pwc.com



www.pwchk.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2018 PricewaterhouseCoopers Limited. All rights reserved. PwC refers to the Hong Kong member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. HK-20180312-5-C1