Le Cloud: Bien plus qu'une affaire de centre de données

Samuel Bonneau – CISA CISSP
Président

FORTICA
CYBERSÉCURITÉ

Samuel Bonneau

- Président de FORTICA Cybersécurité
- Associé du startup IntelliWork
- Président du Comité Innovation de la CCIQ
- Ingénieur en génie informatique
- Informaticien depuis +20 ans
- Expert en cybersécurité depuis +15 ans
- Innovation / Engagement / Dépassement

FORTICA

CYBERSÉCURITÉ

- Depuis 2010: Assure la continuité de vos affaires en déployant les meilleures stratégies de cybersécurité
- Audit & Conformité / Conseil stratégique / Architecture de systèmes
- Spécialistes en sécurité du Cloud
- +60 mandats au privé et au public

Introduction

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

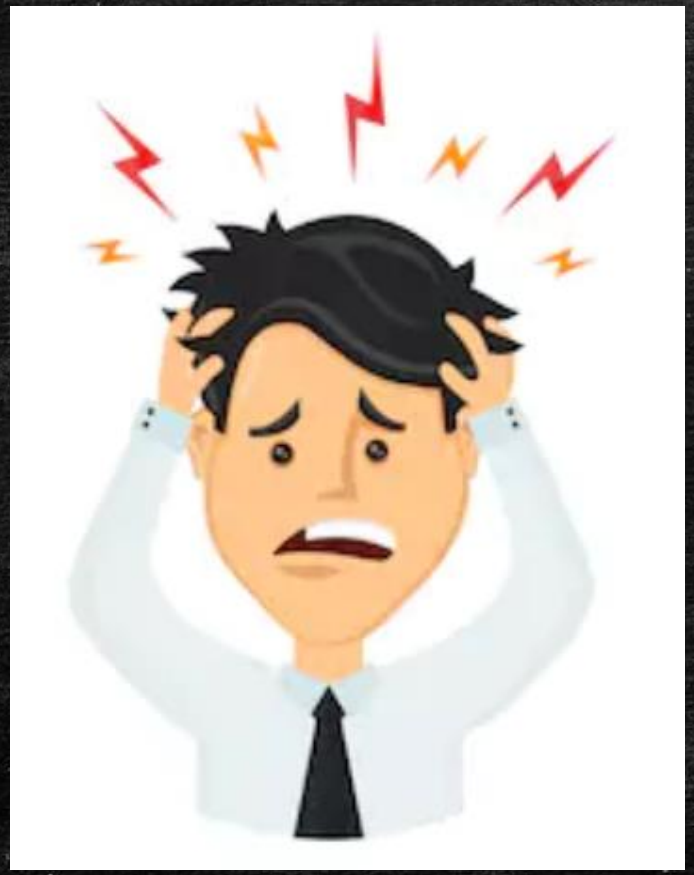
Insight Report

Regional Risks for Doing Business 2018

Top ten risks in North America

1	Cyber-attacks
2	Data fraud or theft
3	Extreme weather events
4	Fiscal crises
5	Energy price shock
6	Asset bubble
7	Failure of critical infrastructure
8	Failure of urban planning
9	Terrorist attacks
10	Failure of climate-change adaptation

Préoccupation des entreprises et consommateurs canadiens



- 87 % des entreprises canadiennes reconnaissent avoir été **victimes d'une cyberattaque** en 2017
  - des données sensibles ont été perdues dans la 50% des cas.
- 77% des canadiens **sont inquiets** de se retrouver victime de vol d'identité.
  - 83% des consommateurs évitent une entreprise ayant subi une fuite de données.
- 90% des canadiens estiment que la cybercriminalité est une **menace pour la sécurité intérieure du pays**.

Cyberattaque: Fatal sur les PME

- PME ciblées pour servir de tremplin vers les multinationales
- 58% des attaques visent les PME
- 66% des incidents envers les PME sont reliés au Cloud
- Dommages moyen: 500 000$

60% ferment dans les 6 mois - Forbes

Une utilisation non-sécuritaire du Cloud peut coûter cher

https://www.kaspersky.com/about/press-releases/2018_costly-cloud-breaches

La plupart des incidents affectent les infrastructures hébergées par un tiers

https://www.kaspersky.com/about/press-releases/2018_costly-cloud-breaches

Les infrastructures se complexifient avec le Cloud

Le Cloud: Oui ou Noui?

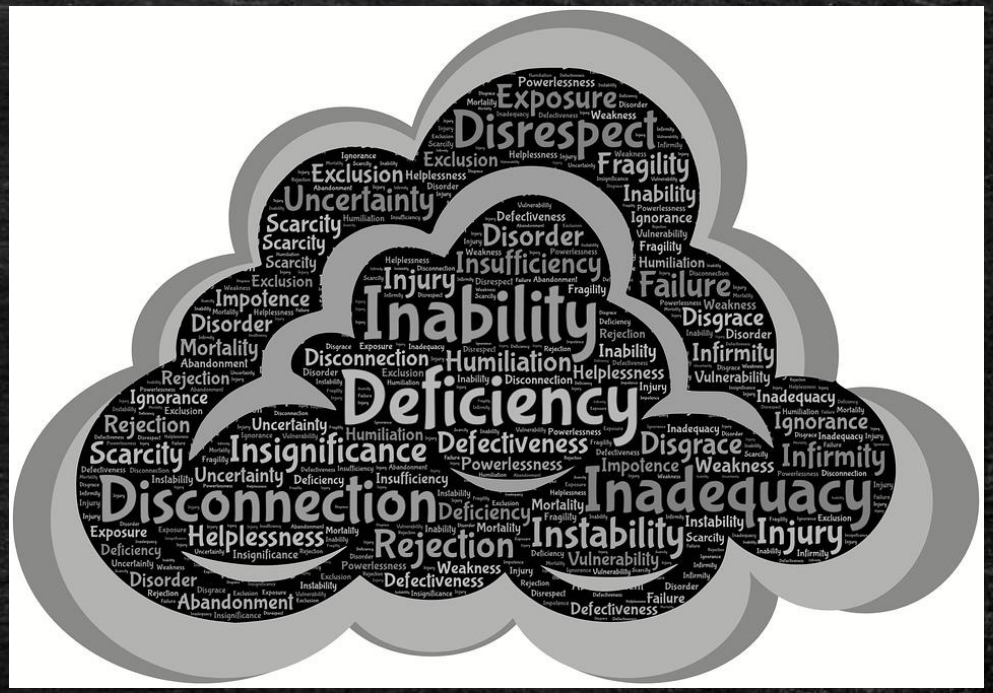
CIO: HURRY UP!!!

LA grande question des CIO…

… et leurs attentes

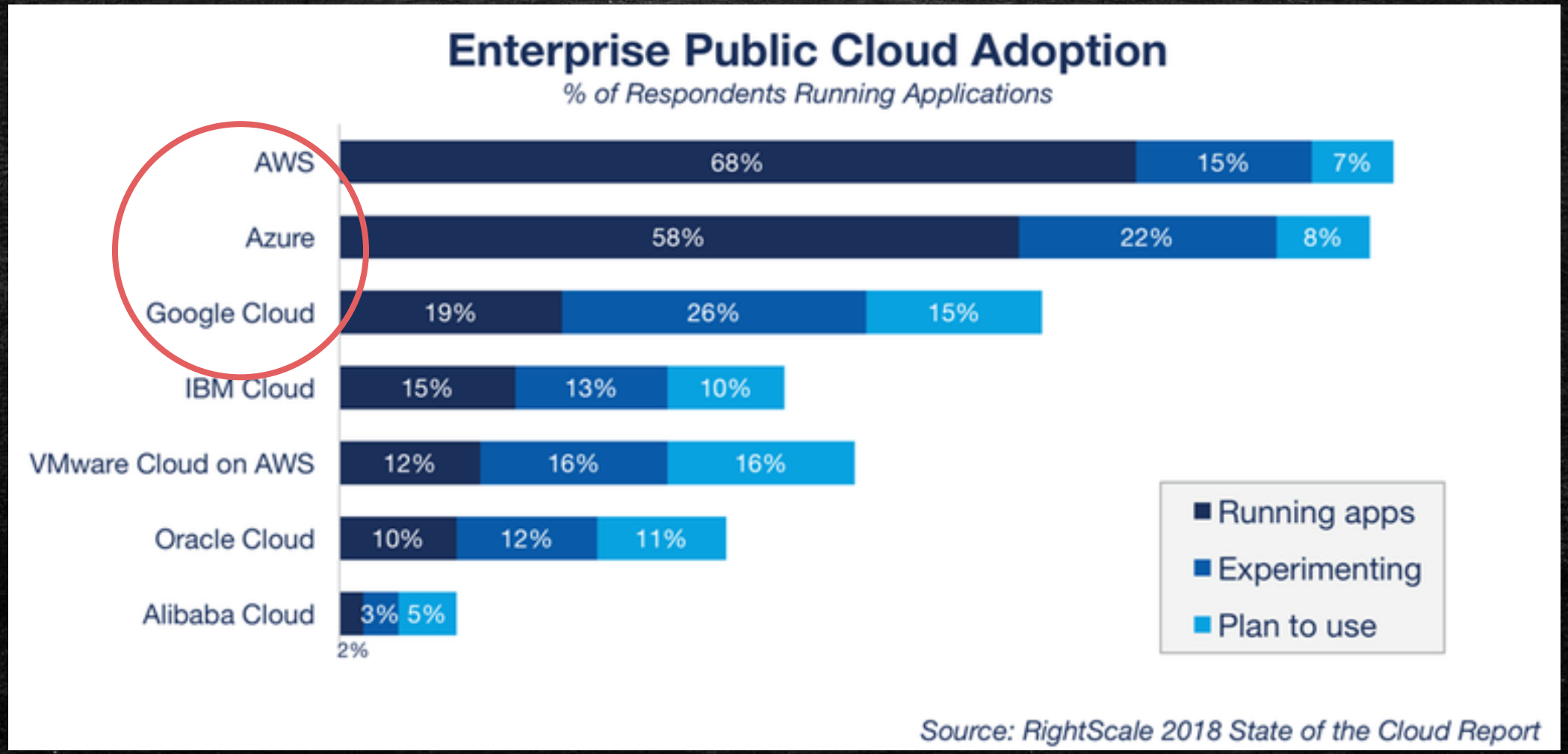
La réalité du Cloud est souvent décevante…

- 84% des entreprises estiment que leurs solutions de sécurité actuelles sont insuffisantes pour gérer la sécurité dans le *cloud*.
- 48% des entreprises ont connu une attaque dans le Cloud, celles-ci ont entraîné une perte de clients dans 44 % des cas



Les fournisseurs de services Cloud

Les grands gagnants



Les autres ☺

Où se situent plusieurs entreprises québécoises au niveau Cloud

- À l'étape de la prise de connaissance
- Passage vers le Cloud avec peu d'expertise
- Gestion du changement mal planifiée et pénible
- Sécurité est souvent de base et moins sécuritaire que sur site

Qu’en pensent les avocats sur l’emplacement des données?

Commission d’accès à l’information du Québec

General Data Protection Regulation

PRIVACY SECURITY

Canadian mandatory breach notification starts November 1, no regulations yet

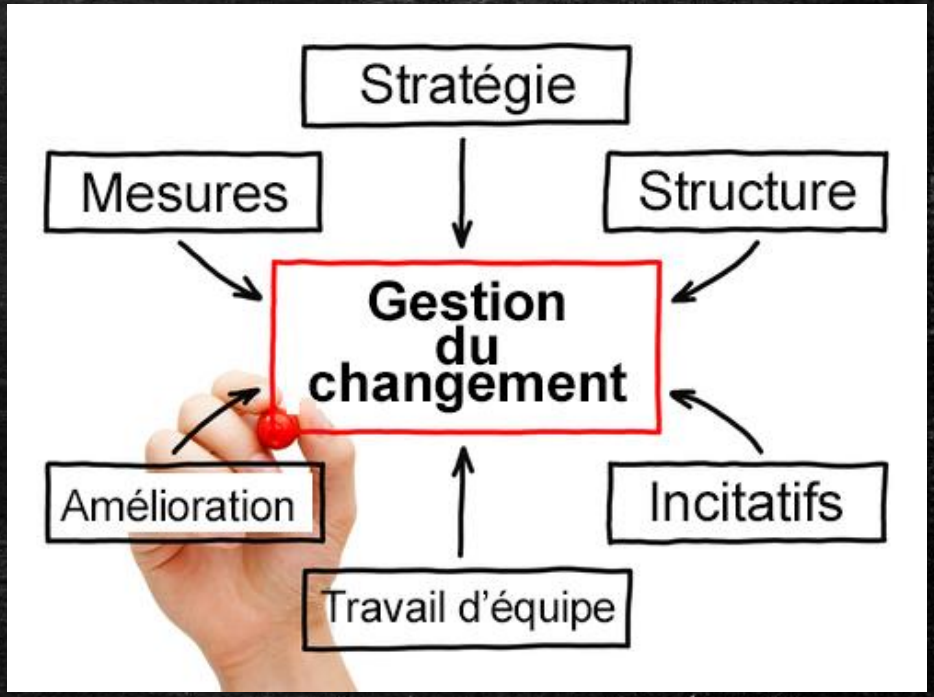
Les pires erreurs à ne pas commettre

1. Voir le Cloud comme un projet technologique
2. Ne pas valider les promesses des vendeurs
3. Croire que le Cloud est sécuritaire par défaut
4. Approcher la sécurité Cloud comme *on premises*

Quelques conseils pratiques

Conseil #1: Voir le Cloud comme un projet complexe

- Stratégie
- Expertise (interne, externe, fournisseurs)
- Gestion du changement
- Preuve de concept



Conseil #2: Former une équipe de travail multidisciplinaire

Affaires, Légal, TI, Sécurité, PO, Gestion changement

Conseil #3: Adapter l'architecture de sécurité

Les réseaux, les applications et le stockage n'est plus ce qu'il était

L'approche d'isolation en 3-tiers et la défense en profondeur perd de son sens

Zero Trust Architecture

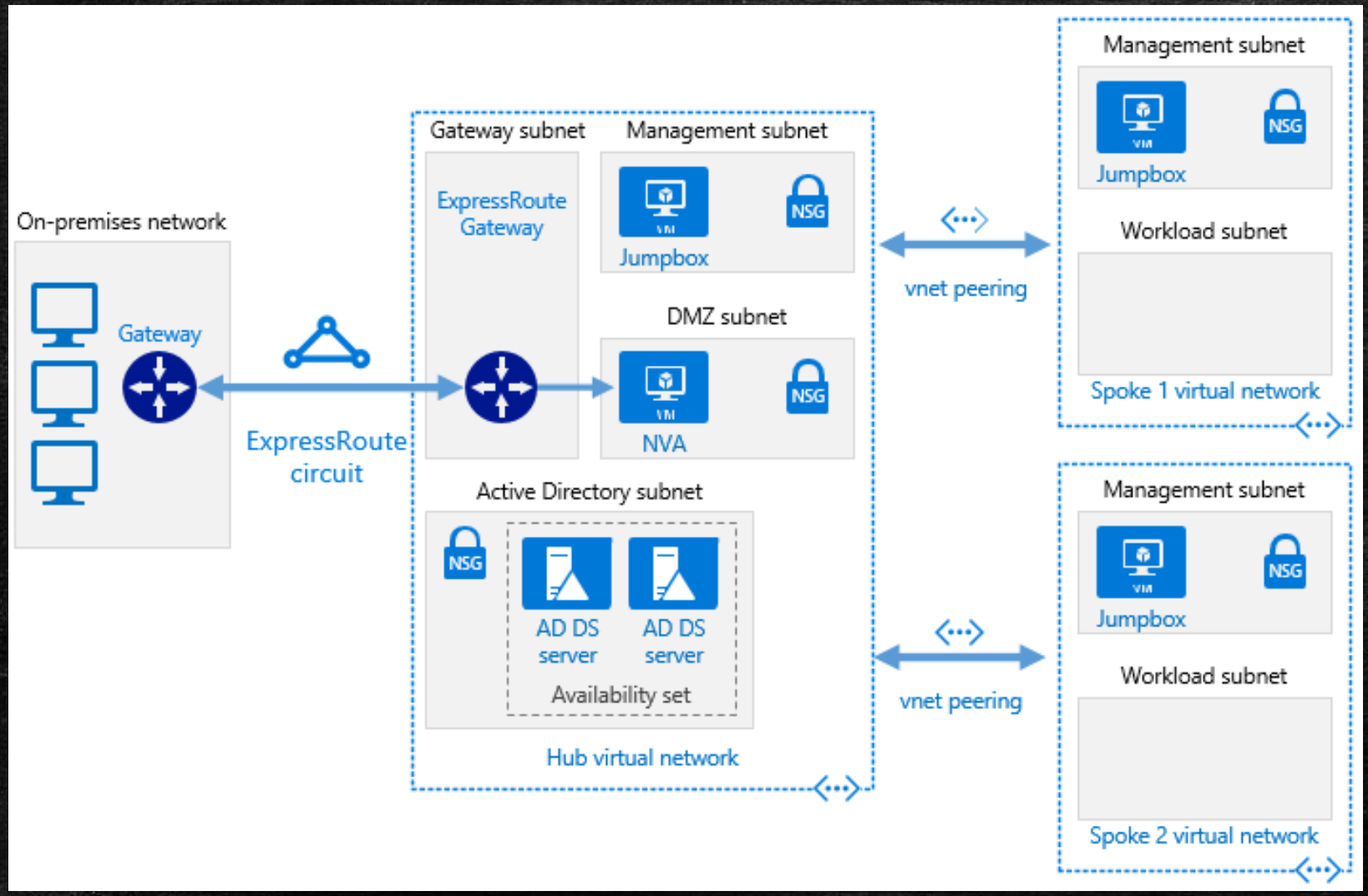
L'identité est le nouveau périmètre de sécurité

Considérations de sécurité technique

#1: Ajouter une protection accrue autour de l'identité

- Centraliser l'authentification (synchronisation des comptes et fédération d'accès)
- Définir des règles d'accès et d'authentification conditionnelles basées sur le niveau de risque
- Analyser les comportements des utilisateurs
- Détecter et bloquer les anomalies

#2: Revoir l'architecture de sécurité

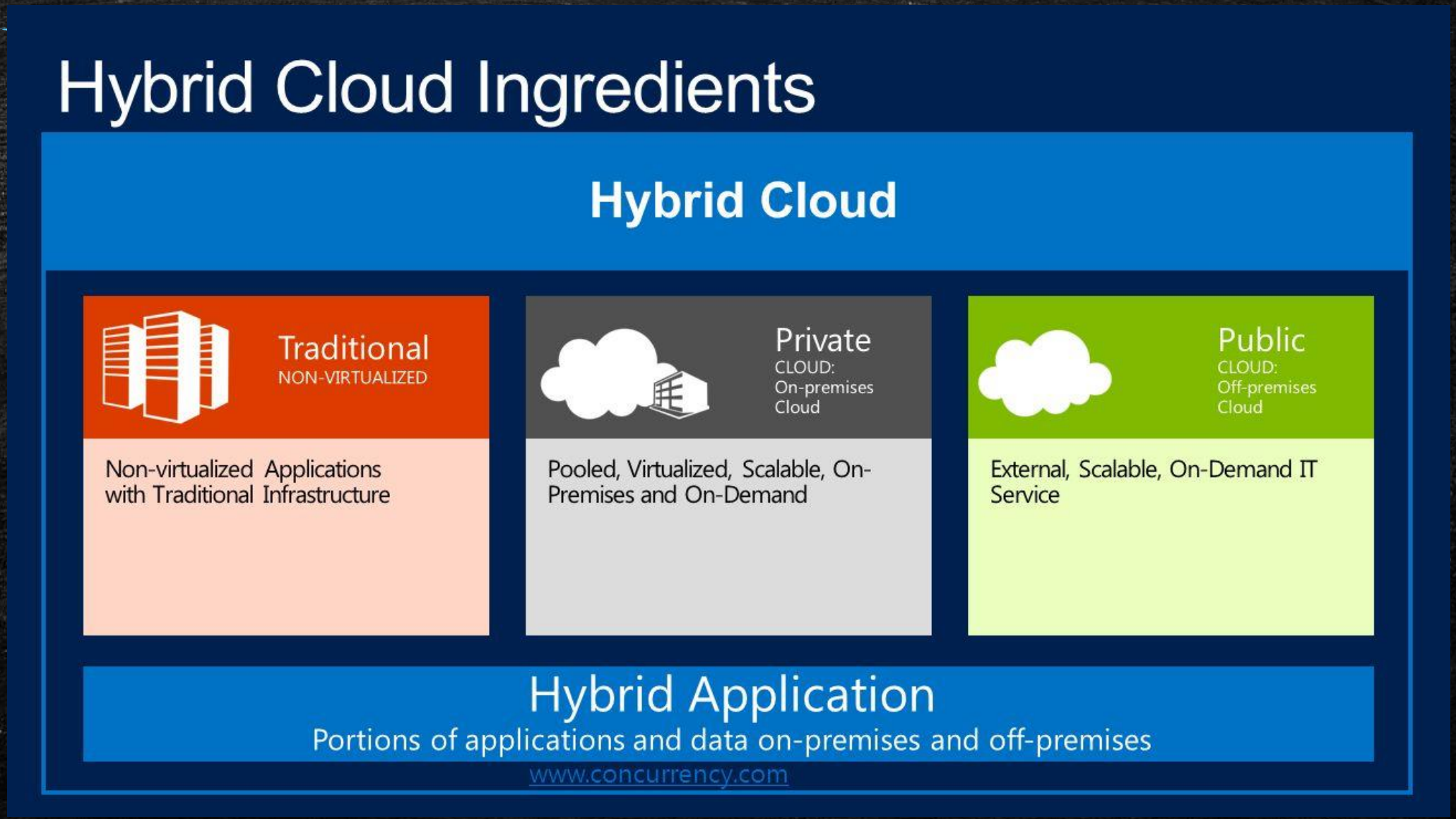


- Centraliser les communications
- Un seul point d'entrée et sortie internet
- Hub-Spoke
- NVA

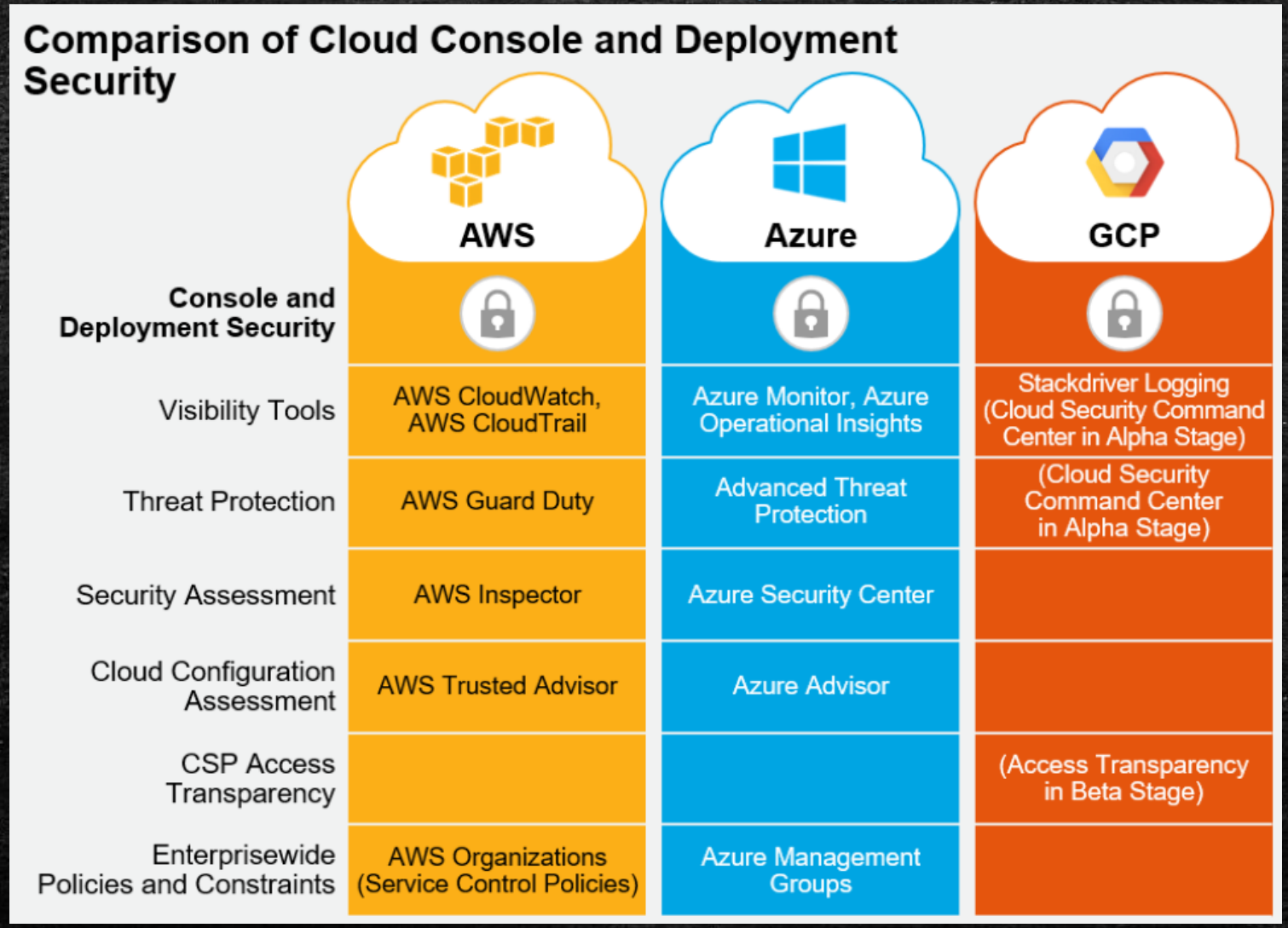
#3: CASB (*Cloud Access Security Broker*) et IDaaS – seulement en cas de besoin

- Offrir une visibilité sur tous les services Cloud consommés par l'organisation
- Centraliser l'authentification et les accès (fédération des identités et SSO)
- Centraliser la gestion de la sécurité du Cloud
- Optimiser la détection d'indicateurs de compromission et de fuite de données

#4: Prévoir dès le départ qu'il y aura des interactions entre On Premises, IaaS, PaaS et SaaS



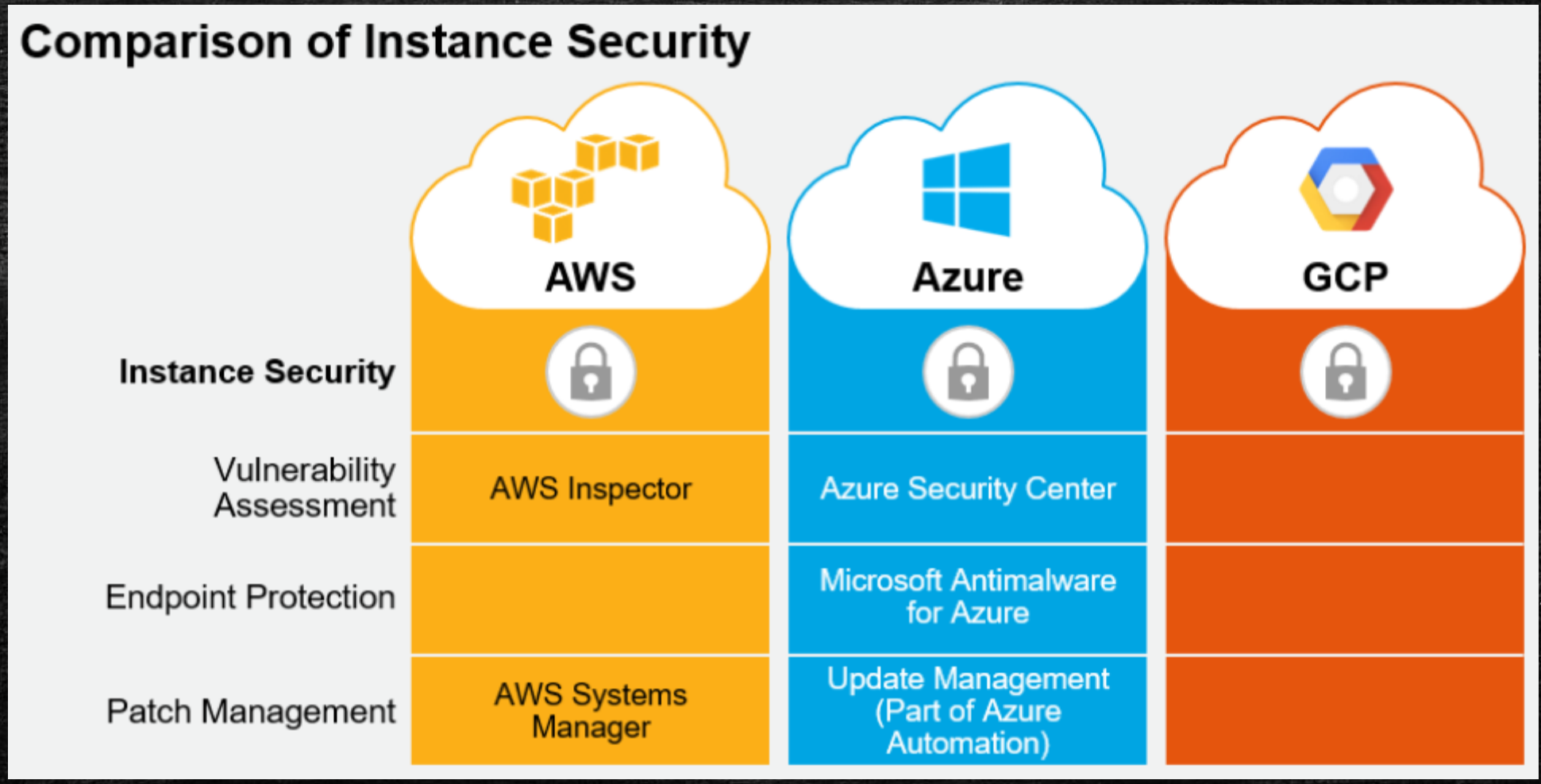
#5: Utiliser les services de sécurité des fournisseurs Cloud



#5: Utiliser les services de sécurité des fournisseurs Cloud

Network Security	AWS	Azure	GCP
VPN Gateway	VPC-to-Site IPSEC	Azure VPN Gateway	Cloud VPN
Dedicated Network	Amazon Virtual Private Cloud (VPC)	Azure VNet	Cloud VPC
Transit Network	Requires Cisco Cloud Service Router (CSR)	Transit VNet	
User-Defined Routes	VPC Route Tables	Part of VNet Functionality	Cloud Router
Cloud Security Groups at Subnet Level		Azure Network Security Groups (NSGs)	Firewall Rules
Cloud Security Groups at VNIC Level	AWS Security Groups	NSGs	
IPv6 Security Groups	AWS Security Groups		
Attribute-Based Cloud Security Groups		Application Security Groups	Source and Target Tags
Subnet Access Lists	Network ACLs	Endpoint ACLs	
Dedicated DDOS-Free Connection	AWS Direct Connect	Azure Express Route	Dedicated Interconnect
DDOS Protection	AWS Shield, AWS Shield Advanced	Azure DDOS Protection (in Preview)	CloudArmor (Not Scrubbing)
Traffic Tracking	Flow Logs	Flow Logs	
WAF (OWASP Top 10 Core)	AWS WAF	Azure Application Gateway	
WAF (Managed Third-Party Rules)	AWS WAF		
WAF Policy Language (Bespoke Rules)	AWS WAF		

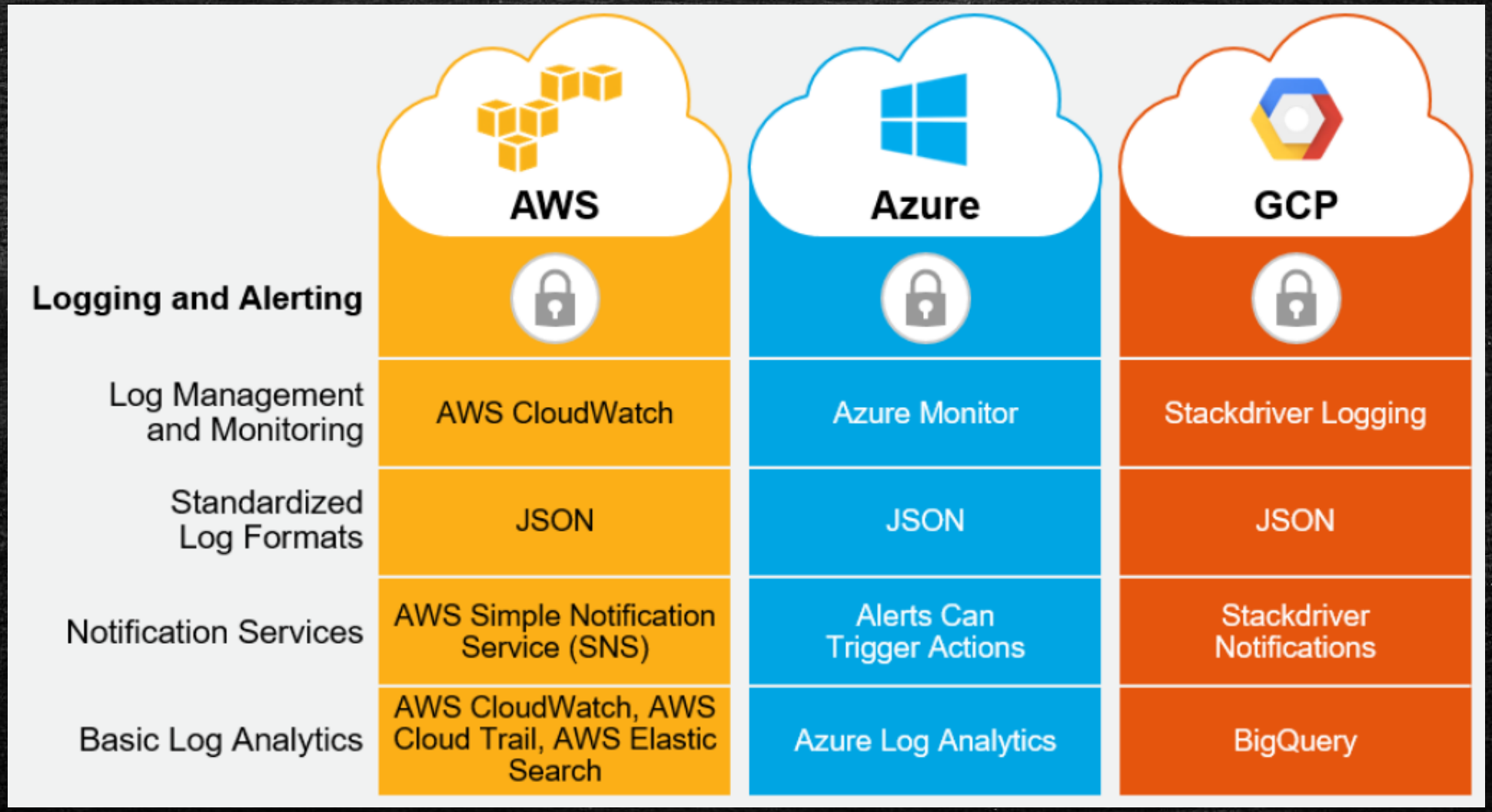
#5: Utiliser les services de sécurité des fournisseurs Cloud



#5: Utiliser les services de sécurité des fournisseurs Cloud

Data Protection	AWS	Azure	GCP
FIPS Validated Key Management	AWS KMS	Azure Key Vault	
Transparent Data at Rest Encryption	Server-Side Encryption	Azure Storage Service Encryption	Default
Transparent Object Storage Encryption	Server-Side encryption	Azure Storage Service Encryption	Default
Generalized Secret Management	AWS Secrets Manager	Azure Key Vault	Cloud KMS
Certificate Management	AWS Certificate Manager	Azure Key Vault	Google App Engine SSL Certificate Service
Bring Your Own Key	AWS KMS	Azure Key Vault	Cloud KMS
Application Endpoint Encryption SDK	Java, .NET, Python, Ruby	Azure Storage Client Libraries (.NET)	
Key Management Service	AWS KMS	Azure Key Vault	Cloud KMS
Exposure of Intel SGX or AMD SEV		(Azure Protected Computing in Preview)	
Client-Managed HSM	AWS Cloud HSM	(In Preview)	(In Preview)
Data Discovery	AWS Macie	(In Preview for Azure SQL Service)	DLP API
Data Masking		Azure SQL Dynamic Data Masking	DLP API

#5: Utiliser les services de sécurité des fournisseurs Cloud



	AWS	Azure	GCP
Logging and Alerting			
Log Management and Monitoring	AWS CloudWatch	Azure Monitor	Stackdriver Logging
Standardized Log Formats	JSON	JSON	JSON
Notification Services	AWS Simple Notification Service (SNS)	Alerts Can Trigger Actions	Stackdriver Notifications
Basic Log Analytics	AWS CloudWatch, AWS Cloud Trail, AWS Elastic Search	Azure Log Analytics	BigQuery

#6: Ajouter des périphériques de sécurité tiers

Azure Marketplace – Market Leading Solutions

#7: Utiliser un centre de sécurité (SOC) adapté au Cloud

#8: Mettre à jour les plans de continuité d’activité, de relève et de gestion des incidents

Conclusion

Êtes-vous prêts pour le Cloud?

- 94% des TI seront dans le Cloud d'ici 2021 et 75 % sous la forme de SaaS
- Le budget mondial pour la sécurité du Cloud va augmenter de 51% en 2019 - Gartner

Vous pouvez compter sur les experts de FORTICA pour vous aider dans la sécurité du Cloud (Office365, Azure, Amazon, Google, Salesforce, etc)

FORTICA
CYBERSÉCURITÉ

Merci Beaucoup de votre présence

Contactez-nous pour vous aider dans vos défis Cloud

Samuel Bonneau – CISA CISSP

sbonneau@fortica.ca

418-564-7143

FORTICA

CYBERSÉCURITÉ