



# Sécurisez vos applications dans le cloud

Nicolas Malaval

Amazon Academy – 8 décembre 2020



# Les bénéfices du cloud sont bien connus



Cessez de deviner la capacité nécessaire



Déployez globalement en quelques minutes



Remplacez les coûts en capitaux par des coûts variables



Supprimez les tâches non différenciatrices



Bénéficiez d'importantes économies d'échelle



Agilité, vitesse et innovation

# Le cloud réconcilie agilité et sécurité



---

Expérimenter  
Etre agile  
Etre productif

ET



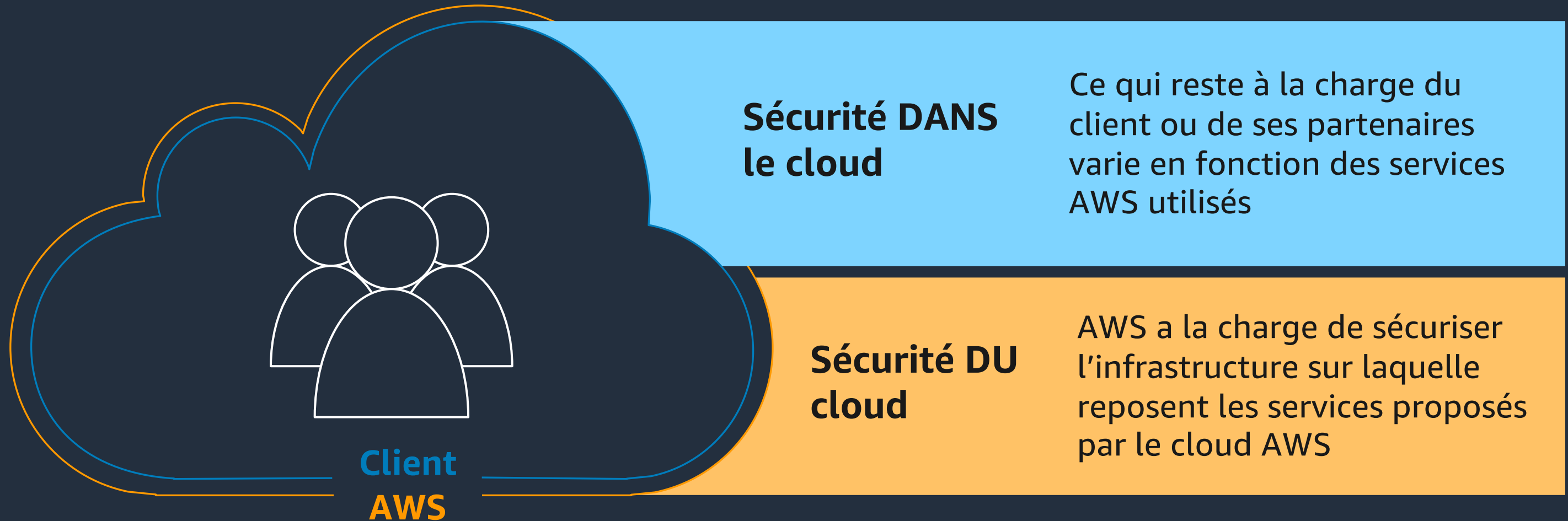
---

Rester sécurisé  
Garder le contrôle

# Agenda

- Modèle de responsabilité partagée
- Sécurité **du** cloud
- Sécurité **dans** le cloud
- Protection des données

# Modèle de responsabilité partagée



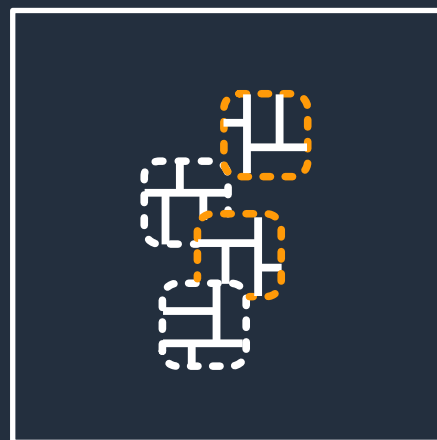
# Renforcez votre sécurité grâce aux services gérés par AWS

## « Lift and Shift »



Amazon EC2, Amazon VPC, AWS Direct Connect...

## Optimisé pour le Cloud



Amazon RDS, Amazon ECS/EKS, Amazon EMR, Amazon EFS, AWS Elastic Beanstalk...

## Conçu pour le cloud



Amazon S3, AWS Lambda, Amazon SQS, Amazon SNS, AWS Glue, Amazon Rekognition...

# Sécurité DU cloud





# Matériel spécialement conçu pour les besoins du cloud



Routeurs



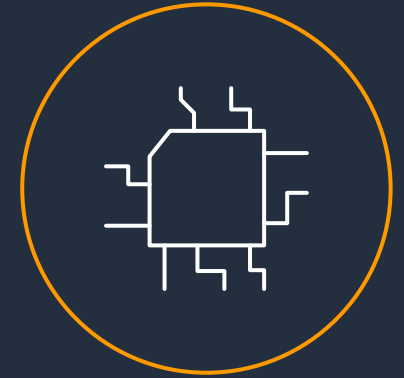
Equilibreurs de charge



Serveurs spécifiques



Logiciels spécifiques



















Puces spécifiques



















**AWS Nitro  
System**

# Programmes de conformité

















## Certifications et attestations


C5	
Cyber Essentials Plus	
DoD SRG	
FedRAMP	
FIPS	
IRAP	
ISO 9001	
ISO 27001	
ISO 27017	
ISO 27018	
MLPS Level 3	
MTCS	
PCI DSS Level 1	
SEC Rule 17-a-4(f)	
SOC 1, SOC 2, SOC 3	
HDS	

## Lois et réglementations

CISPE	
GDPR	
FERPA	
GLBA	
HIPAA	
HITECH	
IRS 1075	
ITAR	
My Number Act	
Data Protection Act – 1988	
VPAT / Section 508	
Data Protection Directive	
Privacy Act [Australia]	
Privacy Act [New Zealand]	
PDPA - 2010 [Malaysia]	
PDPA - 2012 [Singapore]	
PIPEDA [Canada]	
Agencia Española de Protección de Datos	

## Cadres / adéquation

CIS (Center for Internet Security)	
CJIS (US FBI)	
CSA (Cloud Security Alliance)	
Esquema Nacional de Seguridad	
EU-US Privacy Shield	
FISC	
FISMA	
G-Cloud	
GxP (US FDA CFR 21 Part 11)	
ICREA	
IT Grundschutz	
MITA 3.0 (US Medicaid)	
MPAA	
NIST	
Uptime Institute Tiers	
Cloud Security Principles	

 = standard global ou spécifique à une industrie

# En savoir plus sur la sécurité DU cloud

Infrastructure AWS: <https://infrastructure.aws>

Nos centres de données: <https://aws.amazon.com/compliance/data-center/>

Portail conformité AWS: <https://aws.amazon.com/compliance/>

Rapports de conformité AWS: <https://aws.amazon.com/artifact/>

# Sécurité DANS le cloud

# Un large choix de services dédiés à la sécurité



## Identities et permissions

AWS Identity & Access Management (IAM)  
AWS Single Sign-On  
AWS Organizations  
AWS Directory Service  
Amazon Cognito  
AWS Resource Access Manager



## Détection

AWS Security Hub  
Amazon GuardDuty  
Amazon Inspector  
Amazon CloudWatch  
AWS Config  
AWS CloudTrail  
VPC Flow Logs



## Protection d'infrastructure

AWS Firewall Manager  
AWS Shield  
AWS WAF – Web application firewall  
Amazon Virtual Private Cloud (VPC)  
AWS PrivateLink  
AWS Systems Manager



## Protection des données

Amazon Macie  
AWS Key Management Service (KMS)  
AWS CloudHSM  
AWS Certificate Manager  
AWS Secrets Manager  
AWS VPN  
Server-Side Encryption



## Réponse aux incidents

Amazon Detective  
CloudEndure DR  
AWS Config Rules  
AWS Lambda

# Automatisez le traitement des incidents de sécurité



## Exemple

Détection d'un changement de configuration des règles de filtrage réseau

Une des règles ne correspond pas aux exigences du client

Déclenchement d'un évènement lorsque la règle Config change d'état

Une fonction Lambda corrige automatiquement la non-conformité

# Soyez accompagnés

Pour automatiser la configuration des bases de votre environnement AWS



AWS Control Tower



AWS Systems Manager Explorer

Pour appliquer les bonnes pratiques et concevoir des applications sécurisées et résilientes



AWS Well-Architected Framework / Tool

Par nos partenaires pour construire et opérer vos applications sur AWS



# En savoir plus sur la sécurité DANS le cloud

Portail AWS Security : <https://aws.amazon.com/security/>

AWS Well-Architected Framework : <https://aws.amazon.com/architecture/well-architected/>

Partenaires AWS avec la compétence Sécurité :  
<https://aws.amazon.com/security/partner-solutions/>

AWS re:Inforce : <https://reinforce.awsevents.com/>



# Protection des données

# La confiance des clients est notre priorité absolue



Vous gardez l'entière propriété et le contrôle de vos données sur AWS



Vos données restent dans la région de votre choix, sauf si vous décidez de les répliquer

# En savoir plus sur la protection des données

RGPD : <https://aws.amazon.com/compliance/gdpr-center/>

CLOUD Act: <https://aws.amazon.com/compliance/cloud-act/>

Demandes d'informations adressées à Amazon (dont AWS):  
<https://aws.amazon.com/compliance/amazon-information-requests/>

# Merci !