Modèle de sécurité AWS

Julien Simon, Principal Technical Evangelist, AWS

julsimon@amazon.fr
@julsimon

© 2015, Amazon Web Services, Inc. ou ses affiliés. Tous droits réservés.

Agenda

- AWS et la sécurité
- Modèle de sécurité partagée
- Conformité
- Bonnes pratiques et outils
- Obtenir de l'aide

AWS et la sécurité

Plus d’un million de clients actifs

2008

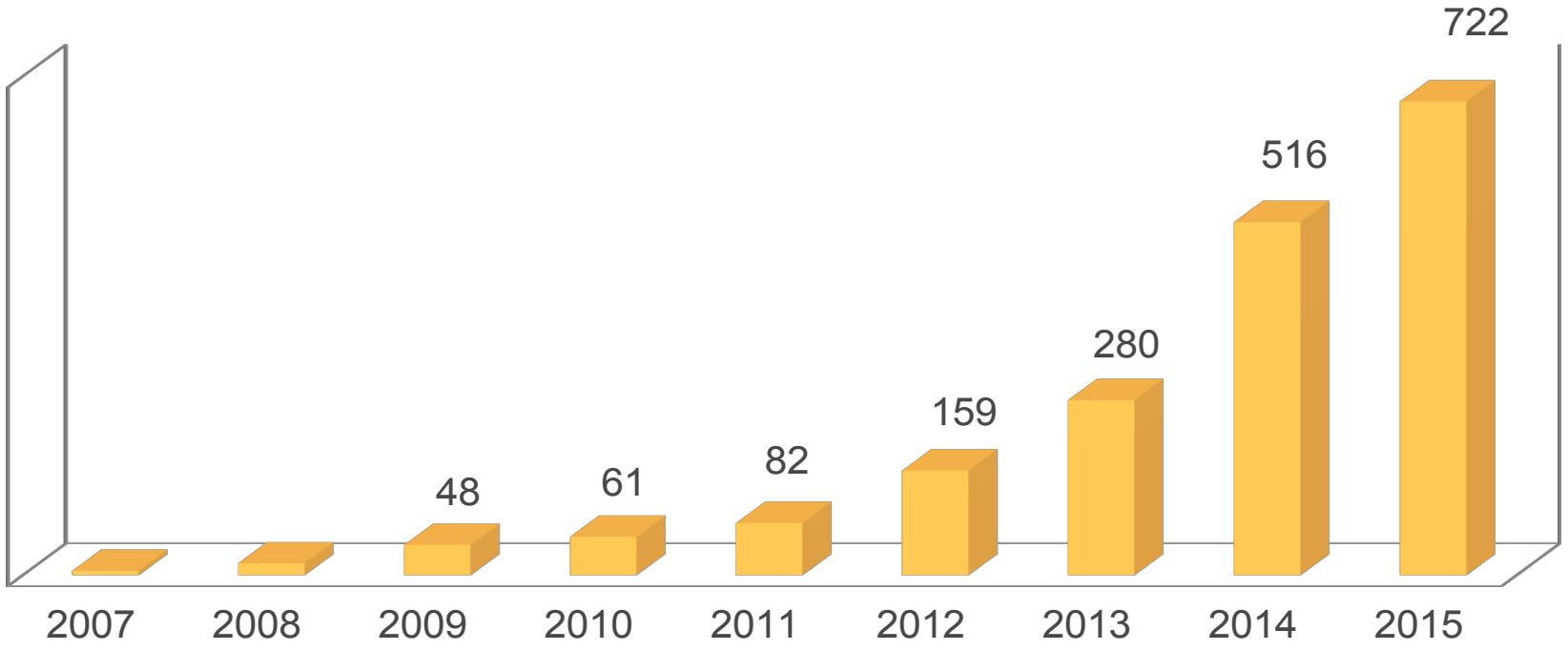
2015

amazon web services | Webinars

Chaque secteur a ses exigences de sécurité et de conformité

NASDAQ
VEOLIA
NETFLIX
SOCIETE GENERALE
CANAL+
FORTUNEO BANQUE
Pfizer
vodafone

Innovation constante, y compris sur la sécurité



Au 30 Septembre 2016 : 709 nouvelles fonctionnalités

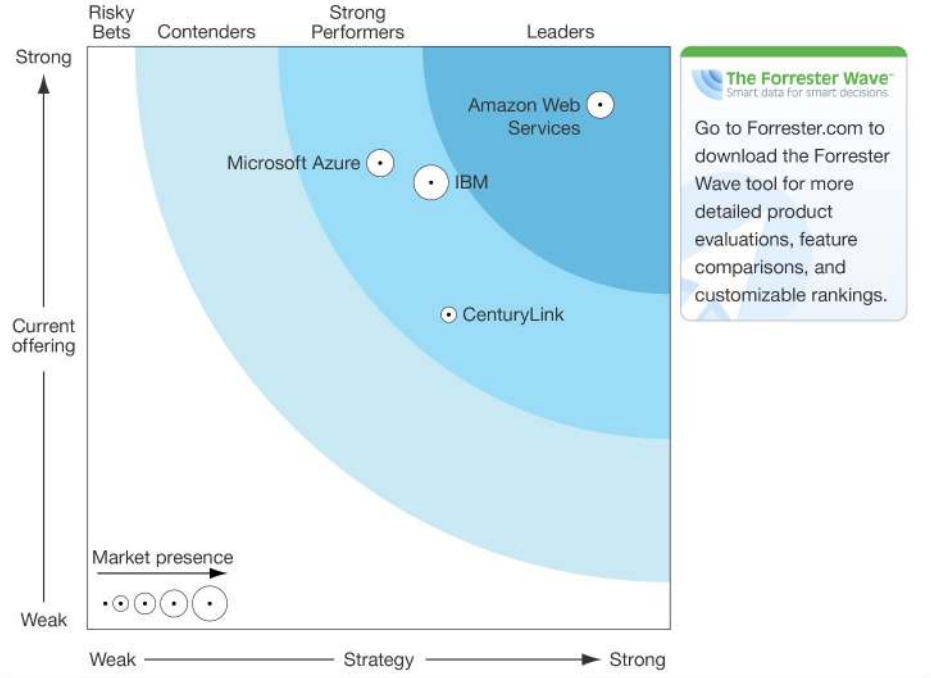
AWS Marketplace : outils de sécurité

Analyse avancée des menaces	Sécurité des application	Gestion des identités et d	Protection des serveurs et points de	Sécurité du réseau	Gestion des clés et du	Tests de vulnérabilité et de pénétration
ALERTLOGIC	IMPERVA	CIPHERGRAPH networks	TREND MICRO	SOPHOS	SafeNet	tenable network security
ALIEN VAULT	FORTINET	SECUREAUTH	intel Security	Check Point We Secure the Internet.	Vormetric Data Security Simplified	QUALYSGUARD
	Barracuda	M-Pin SSO Authentication for Enterprises		paloalto networks.	HYTRUST Cloud Under Control	

FORRESTER RESEARCH | SECURITY & RISK PROFESSIONALS

Forrester Wave™: Public Cloud Service Providers' Security, Q4 '14

The Forrester Wave™: Public Cloud Platform Service Providers' Security, Q4 2014



113065

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

https://aws.amazon.com/fr/resources/forrester-pc-learn-more-emea/

Jet Propulsion Laboratory
California Institute of Technology

"Based on our experience, I believe that we can be even more secure in the AWS cloud than in our own data centers"

Tom Soderstrom, CTO, NASA JPL

Inspiring Innovation in the Cloud @ NASA/JPL and Beyond: https://www.youtube.com/watch?v=JrTs4tjxlOY

amazon web services | Webinars

"The financial service industry attracts some of the worst cyber criminals. We work closely with AWS to develop a security model, which we believe enables us to operate more securely in the public cloud than we can in our own data centers"

Etude de cas: https://aws.amazon.com/solutions/case-studies/capital-one/

la Nouvelle République.fr

"Notre projet aurait pris des semaines, voire des mois dans nos data centers pour atteindre le même niveau de service et de sécurité que propose AWS"

Hugues Gendre, DSI

SAP

Etude de cas : https://aws.amazon.com/fr/solutions/case-studies/nrco/
SAP sur AWS: https://aws.amazon.com/fr/sap/

PayPlug

Comment la start-up PayPlug a pu concurrencer les banques grâce à AWS

par
Yann Serra
LeMagIT

PayPlug propose aux e-commerçants une alternative à la page de paiement que les banques glissent sur leurs sites. Il fallait une infrastructure hautement disponible et certifiée par les organismes financiers que la start-up aurait été incapable de fournir sans AWS.

pci Certified
Level 1 Service Provider

http://www.lemagit.fr/etude/Comment-la-startup-PayPlug-a-pu-concurrencer-les-banques-grace-a-AWS

amazon web services | Webinars

La sécurité est notre priorité n°1

PERSONNES et PROCESSUS

SYSTEME

RESEAU

PHYSIQUE

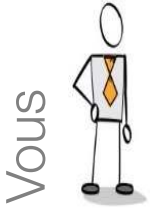
Modèle de sécurité

Taille de l'équipe sécurité d'AWS

Profite à tous les clients

Le modèle de sécurité partagée

Le modèle de sécurité partagée



Applications et contenu client

Identité | Données | Infrastructure

Services de base AWS

Calcul | **Stockage** | **Base de données** | **Mise en réseau**

Infrastructure globale AWS

Zones de disponibilité

Régions

Edge Locations

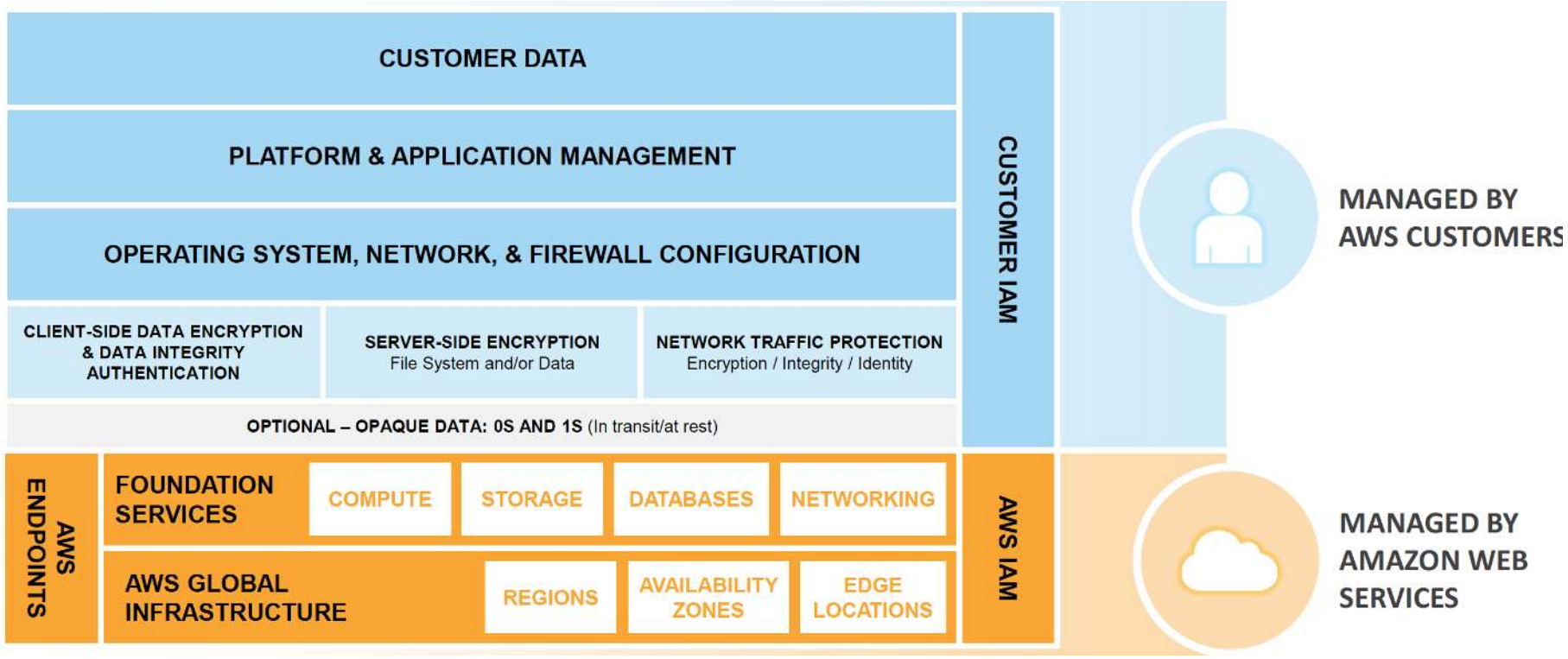
amazon web services

Vous devez définir vos contrôles **DANS** le cloud : *"security in the cloud"*

AWS se charge de la sécurité **DU** cloud : *"security of the cloud"*

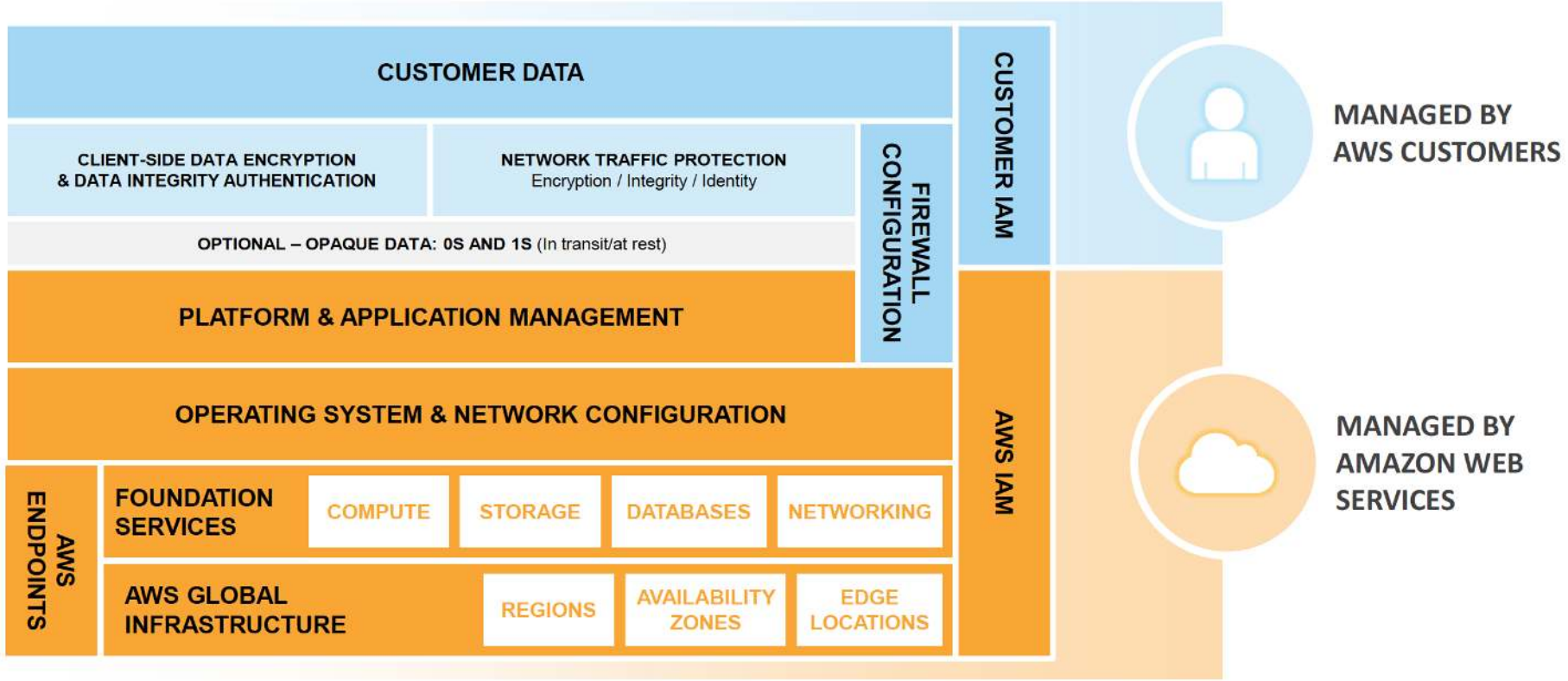
Services d'Infrastructure

Comme Amazon EC2, Amazon EBS ou Amazon VPC



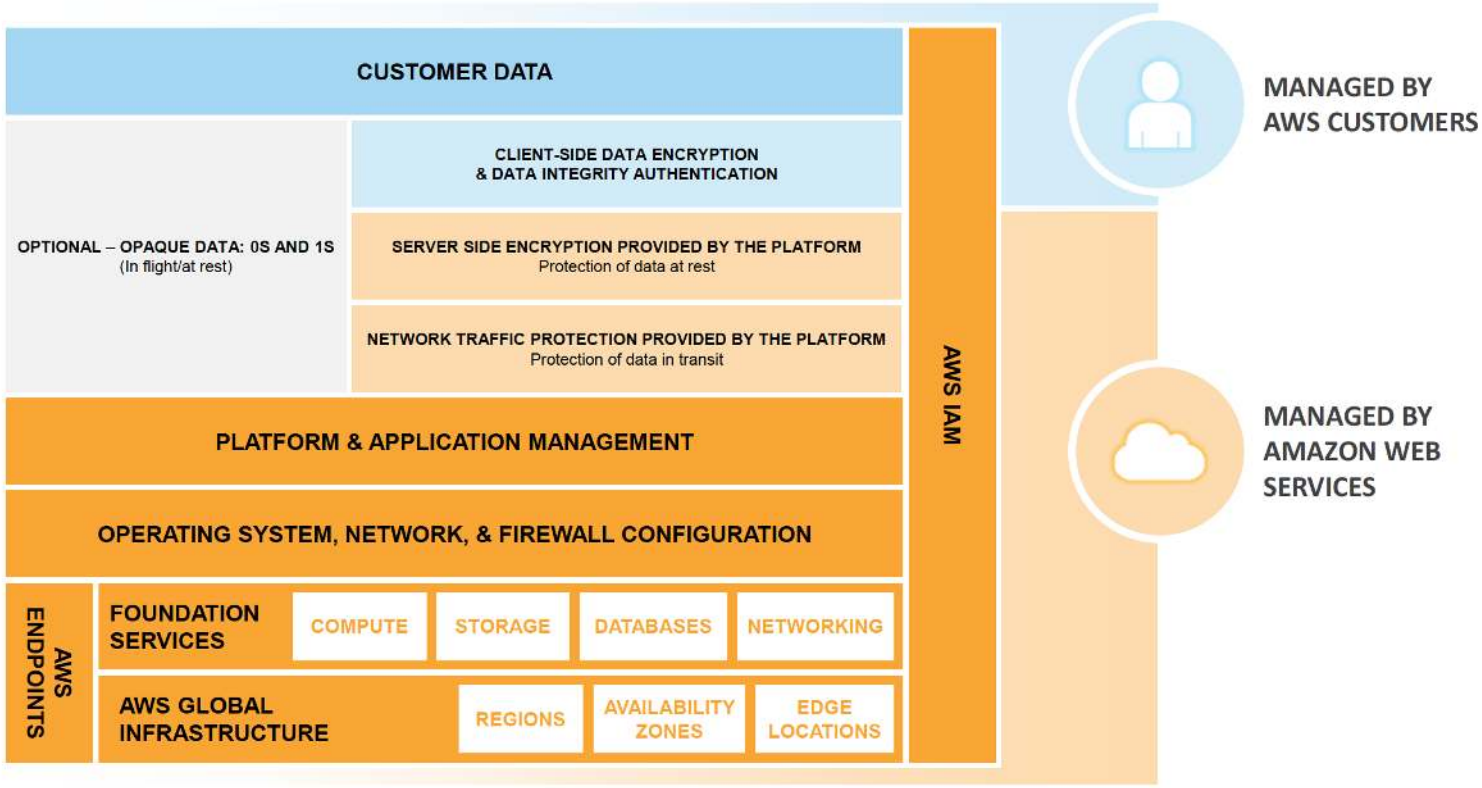
Services basés sur des instances EC2

Comme Amazon RDS, AWS Elastic Beanstalk ou Amazon EMR



Services gérés

Comme Amazon S3 ou Amazon DynamoDB



amazon web services | Webinars

La conformité

Programmes de conformité et certifications

https://aws.amazon.com/fr/compliance/

Conformité

Sur site

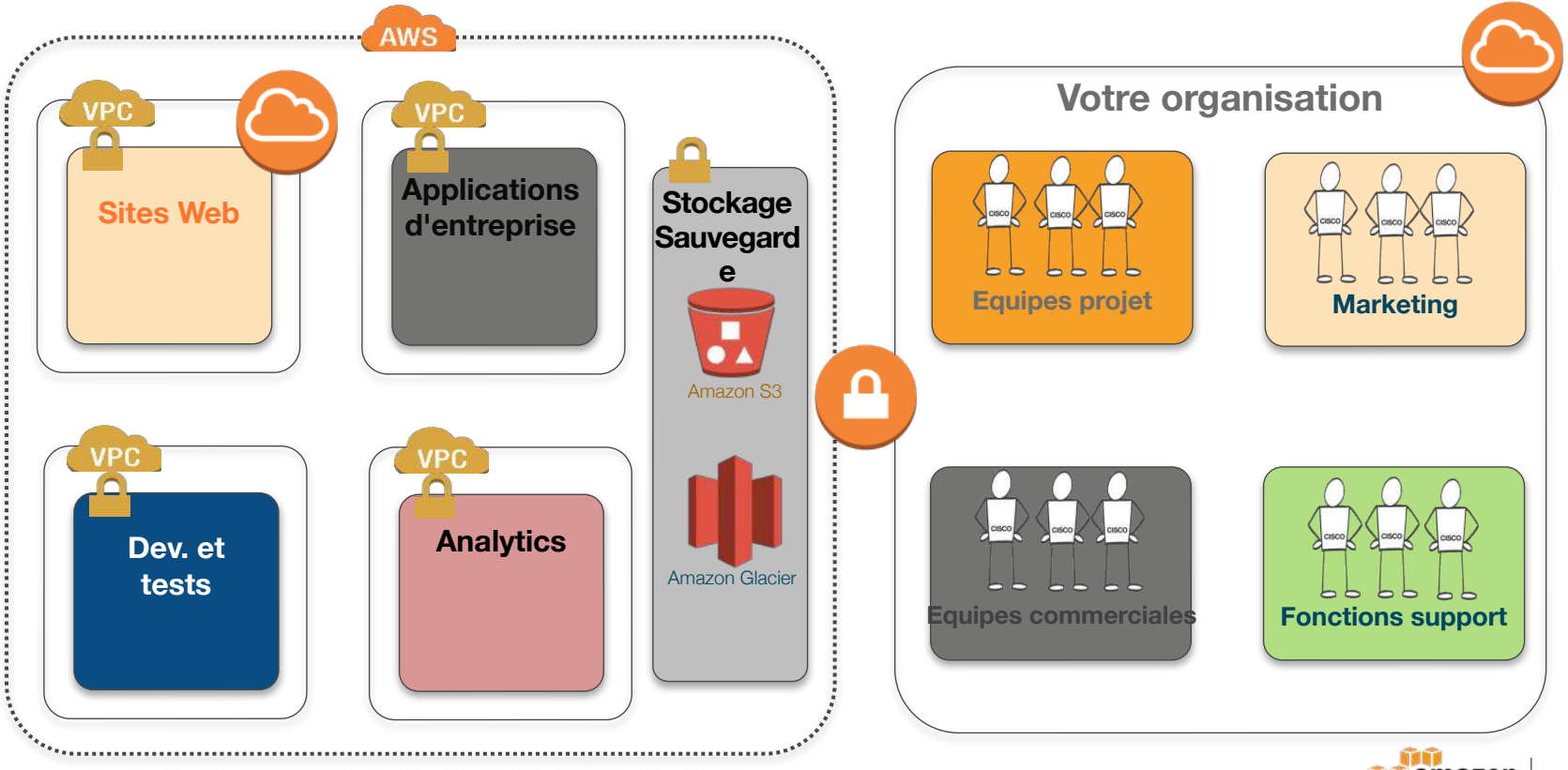
1. Partez de zéro
2. Facultatif sur le plan fonctionnel
3. Audits effectués par une équipe interne
4. Imputable à vous-même
5. Généralement, vérifiée une fois par an
6. Vérification de conformité spécifique à la charge de travail
7. Doit suivre le rythme de l'innovation et nécessite des investissements dans la sécurité

Sur AWS

1. Démarrez sur la base de services agréés
2. Incluse dans les fonctionnalités
3. Audits effectués par des experts tiers
4. Imputable à tous
5. Vérification continue
6. Approche de la conformité basée sur des scénarios pour toutes les charges de travail
7. L'innovation en matière de sécurité favorise une conformité large

Bonnes pratiques et outils

Segmentez vos environnements

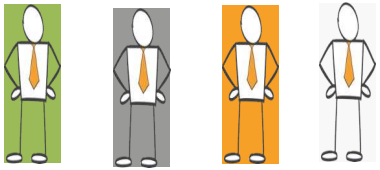


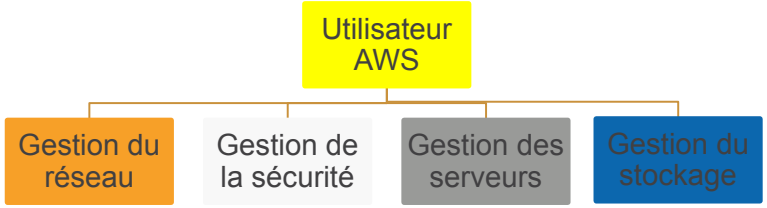
Identité : contrôlez l'accès et séparez les rôles

Vous devez contrôler qui peut faire quoi dans votre environnement AWS, quand et à partir d'où

Contrôle encore plus strict de votre cloud à l'aide de l'authentification multi-facteur

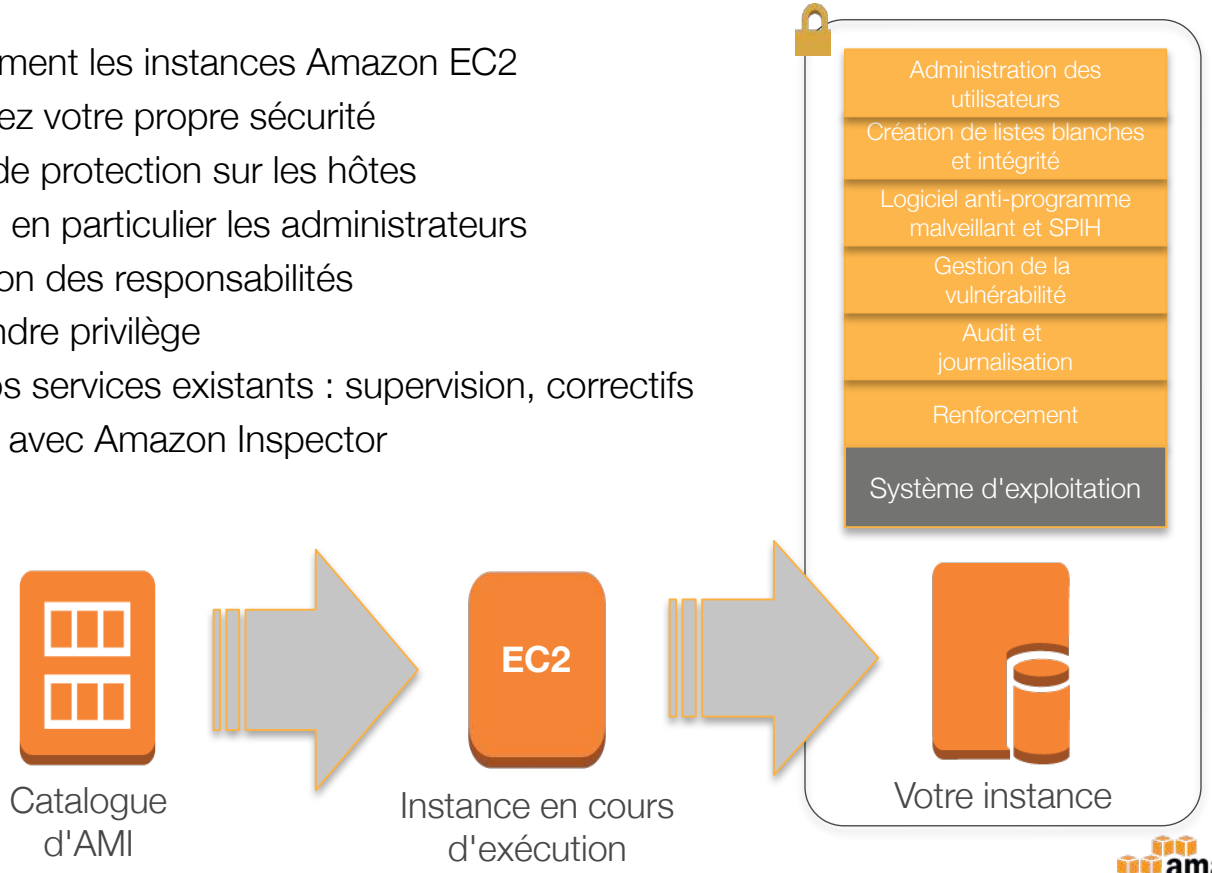
Intégration à votre annuaire d'entreprise existant à l'aide de SAML 2.0 et de l'authentification unique (SSO)





Serveurs : appliquez une sécurité cohérente sur les hôtes

- Vous contrôlez totalement les instances Amazon EC2
- Configurez et renforcez votre propre sécurité
- Utilisez des logiciels de protection sur les hôtes
- Gérez les utilisateurs, en particulier les administrateurs
- Appliquez la séparation des responsabilités et le principe du moindre privilège
- Connectez-vous à vos services existants : supervision, correctifs
- Auditez les instances avec Amazon Inspector



Données : chiffrez tout

Chiffrez vos volumes Elastic Block Storage comme vous le souhaitez

- Chiffrement en un clic
- Chiffrez vous-même à l'aide d'un système de fichiers ou d'utilitaires tiers

Amazon S3 offre un chiffrement côté serveur ou client

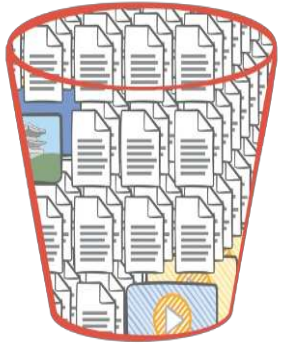
- Gérez vos propres clés ou laissez AWS le faire pour vous

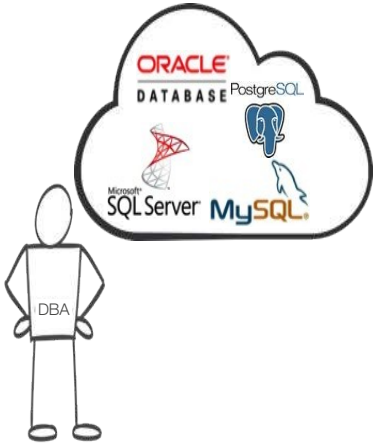
Amazon Redshift propose un chiffrement en un clic

- Chiffrez vos analyses de données
- Vous pouvez fournir vos propres clés

Amazon RDS prend en charge le chiffrement

- Chiffrez vos bases de données MySQL ou PostgreSQL à l'aide de clés que vous gérez via AWS Key Management Service (KMS)
- Prend en charge le chiffrement TDE (Transparent Data Encryption) dans SQL Server et Oracle





Supervision : obtenez une visibilité cohérente

Entière visibilité de votre environnement AWS

AWS CloudTrail consigne l'accès aux appels d'API et enregistre les journaux dans Amazon S3, quelle que soit la manière dont les appels d'API sont effectués

Qui a fait quoi, quand et à partir de quelle adresse IP ?

- Prise en charge de nombreux services AWS et plus à venir – inclut EC2, EBS, VPC, RDS, IAM et Redshift
- Agrégation aisée de toutes les informations consignées

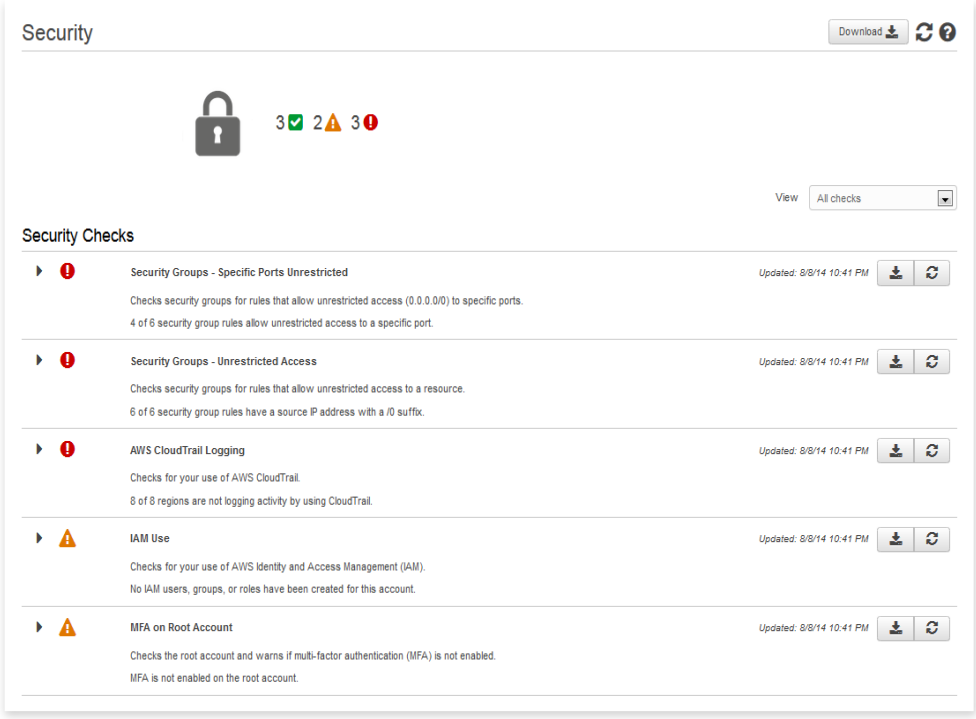
Intégration à des outils d'analyse de journaux de partenaires AWS, notamment Splunk, AlertLogic et SumoLogic

Obtenir de l’aide

Obtenir de l'aide : Amazon Trusted Advisor

Effectue une série de vérifications de sécurité sur votre environnement AWS :

- Ports ouverts
- Accès illimité
- Utilisation d'IAM
- Journalisation CloudTrail
- Autorisations S3
- Authentification multi-facteur
- Stratégie de mot de passe
- Risque d'accès aux bases de données
- Enregistrements DNS
- Configuration de l'équilibreur de charge



Obtenir de l'aide : Support Technique

Equipe de compte

- Votre gestionnaire de compte défend votre cause
- Les architectes solutions possèdent une grande expertise

Quatre niveaux de support

- **Gratuit** – Support basé sur les forums et la vérification de l'état
- **Développeur** – Support par e-mail et assistance sur les bonnes pratiques
- **Professionnel** – Support par téléphone/chat/e-mail, délai de réponse d'1 heure
- **Entreprise** – Délai de réponse de 15 min, gestionnaire technique de compte dédié

Obtenir de l'aide : Services Professionnels

Services professionnels AWS

- Architecture de sécurité d'entreprise
- Définition des contrôles et des stratégies
- Conception SOC

Réseau de partenaires AWS

- Plus de 600 partenaires consultants AWS certifiés dans le monde

En résumé

- La sécurité est la priorité n°1 d'AWS : vous profitez d'un environnement créé pour les organisations les plus exigeantes en matière de sécurité
- AWS se charge de la sécurité **DU** cloud : vous bénéficiez de plus de 700 services, outils et fonctionnalités fournis par AWS et ses partenaires
- Vous définissez vos contrôles **DANS** le cloud
- Vous conservez la possession, le contrôle et la visibilité sur votre plate-forme et vos données

Ressources

https://aws.amazon.com/security
https://aws.amazon.com/compliance

https://aws.amazon.com/fr/whitepapers/overview-of-security-processes/
https://aws.amazon.com/fr/whitepapers/aws-security-best-practices/

https://aws.amazon.com/blogs/security/

Merci !

Julien Simon, Principal Technical Evangelist, AWS

julsimon@amazon.fr
@julsimon