



JAGUAR NETWORK

A quel point votre infrastructure
dans le cloud est elle sécurisée?

Le dernier rempart entre vous et le cocktail



Jaguar Network : présentation



- **Société créée en 2001**
- **Dédiée aux segments Entreprises, Grands Comptes & Marchés Publics**
- **Expertise reconnue en hébergement, infogérance et réseaux WAN**
 - Certification PCI-DSS
 - Certification ISO 27001 (Q3 2015)
 - ITIL v3
 - Conformité bonnes pratiques ANSSI
- **Une capillarité et une densité qui nous rapproche de nos clients**
 - Suites et cages privées dans 30 Datacenter « Carrier Hotel » interconnectés entre eux
 - Hotline et Support technique en France 24h/24 365j/an
 - Réseau Europe Fibre Optique (extension US, Afrique & Asie)
 - Propriétaire du 2nd Hôtel des Télécoms de l'Europe du SUD (Tiers IV; 4000 M2)
- **Solide financièrement, en forte croissance**
 - Capitaux 100% français
 - Notation Banque de France G3+
 - Croissance à 2 chiffres depuis 2005
 - 5ème Entreprise IT national au classement Deloitte Technology Fast50 depuis 2010



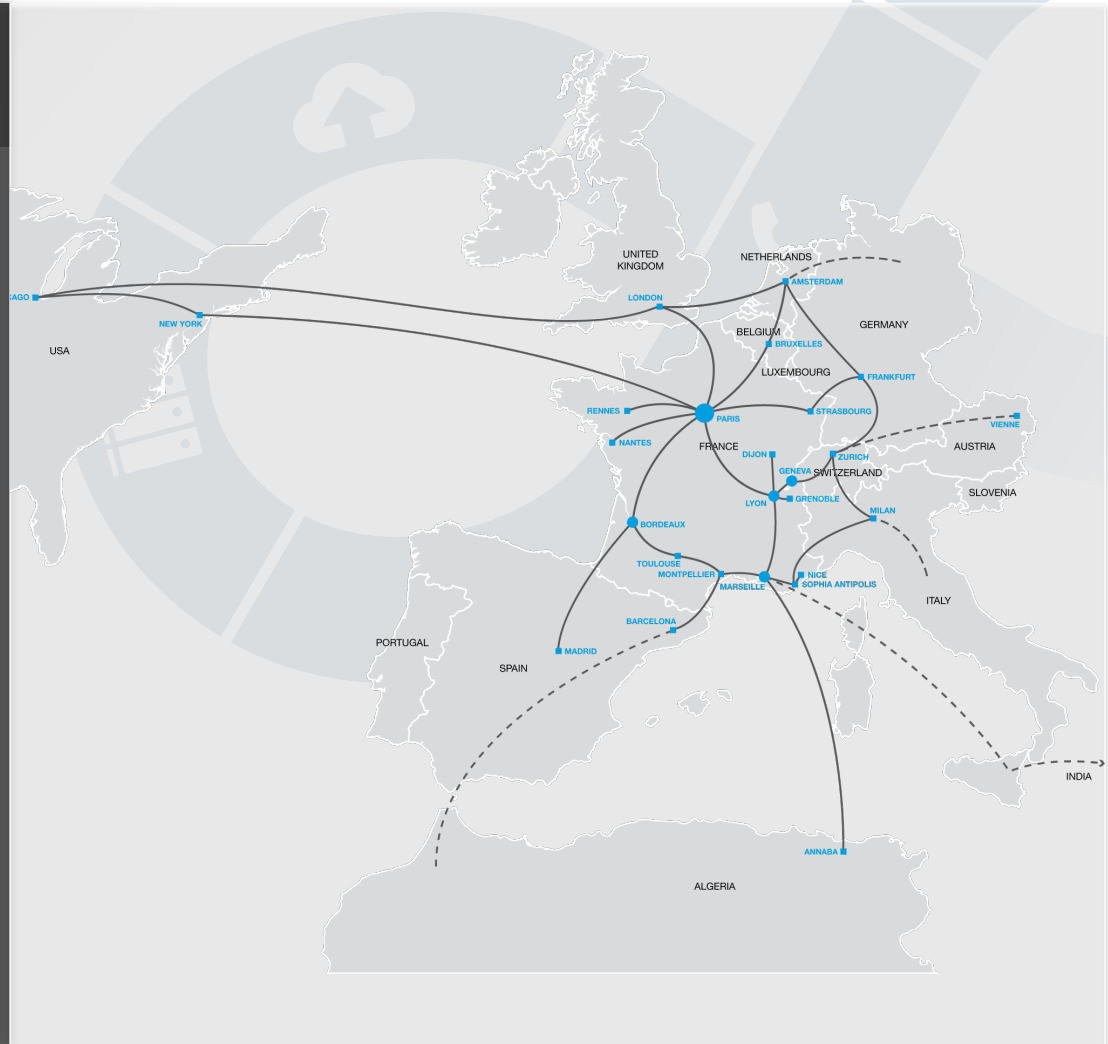
Deloitte.
Technology Fast50

Jaguar Network: un Backbone européen Haute Disponibilité



UN RÉSEAU PERFORMANT À TRÈS HAUT DÉBIT

- ✓ UN RÉSEAU FIBRE OPTIQUE PRIVÉ
- ✓ 360 GB/S DE CAPACITÉ EN IPV4/V6
- ✓ 200 GB/S DE TRANSIT GLOBAL
- ✓ 700+ INTERCONNEXIONS OPÉRATEURS EFFECTIVES
- ✓ 6 500 KMS INTERCONNECTANT L'ENSEMBLE DES DATACENTERS
- ✓ SUPPORT DES SERVICES
 - ✓ CLOUD
 - ✓ RÉSEAU
 - ✓ VOICE
 - ✓ INFRASTRUCTURE
- ✓ SUPERVISION DU RÉSEAU 24X7X365



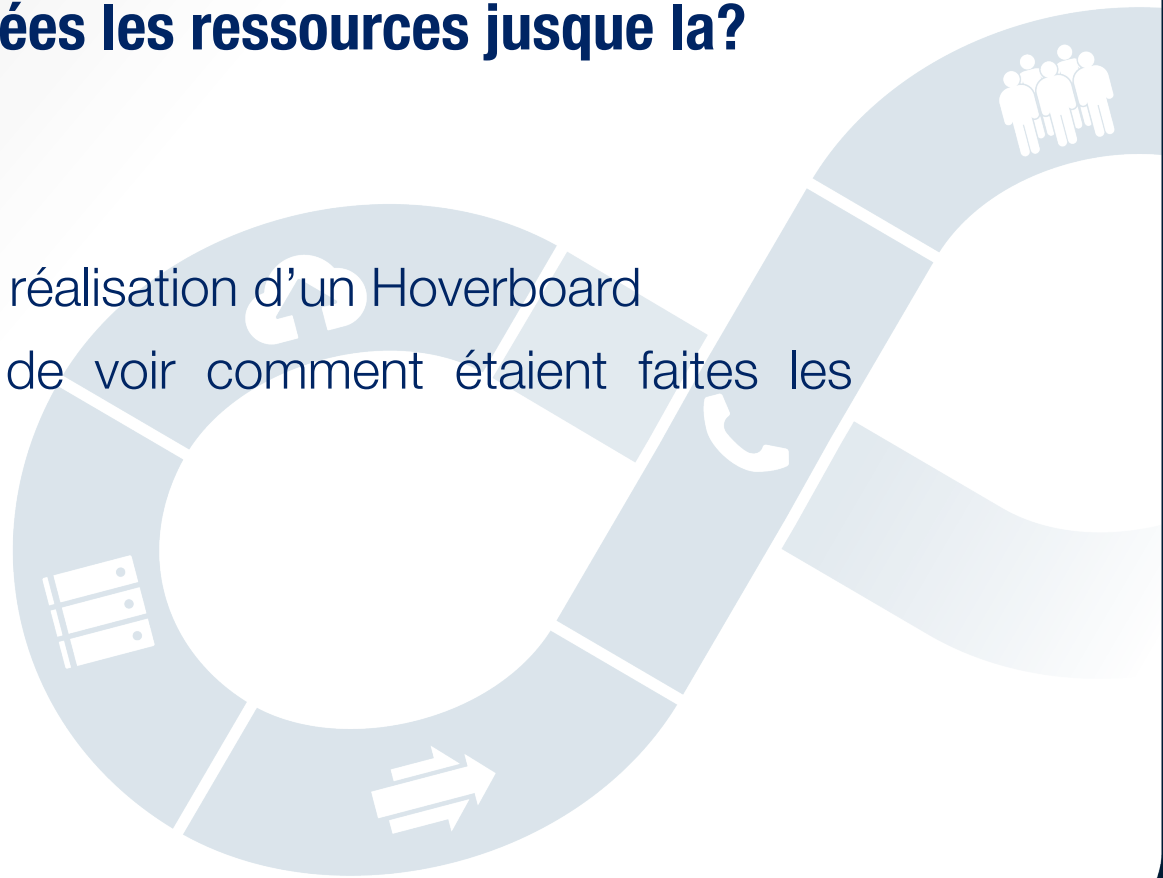
L'informatique en nuage...

« Le cloud computing, ou l'informatique en nuage [...], est l'exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet. » © Wikipedia



Comment étaient hébergées les ressources jusque là?

- On est en 2015.
- Lexus vient d'annoncer la réalisation d'un Hoverboard
- Pas de meilleur moyen de voir comment étaient faites les choses avant...



Comment étaient hébergées les ressources jusque là?

- On est en 2015.
- Lexus vient d'annoncer la réalisation d'un Hoverboard
- Pas de meilleur moyen de voir comment étaient faites les choses avant...





■ La « salle informatique »

- 100% de l'infra hébergée sur site
- Gros investissements CAPEX + OPEX
- Peu de flexibilité car ressources environnementale restreintes.
- « Maitrise » du design, de l'architecture et donc, de la sécurité.





■ Le « datacenter »

- Majorité de l'infra hébergée dans un datacenter.
- CAPEX / OPEX réduit sur l'environnement d'hébergement (énergie, clim...)
- Matériel appartenant toujours à l'entreprise. Investissement supplémentaire pour chaque nouvelle machine / service / besoin.
- « Maitrise » du design, de l'architecture et donc, de la sécurité



■ Le «cloud »

- Toute l'infra est outsourcée chez un ou plusieurs fournisseurs de cloud.
- Quasiment plus aucun CAPEX et des OPEX « modulables »
- Flexibilité de la solution.
- Aucune maîtrise du design ou de la sécurité de l'infra (surtout sur un cloud public)

Le cloud et ses travers: les risques réseau

■ Séparation des clients

- Tout le monde dans le même VLAN?
- 1 VLAN par client?
- n x VLAN par client?
- Possibilité d'avoir des pVLAN pour sécurisation des ressources entre elles?



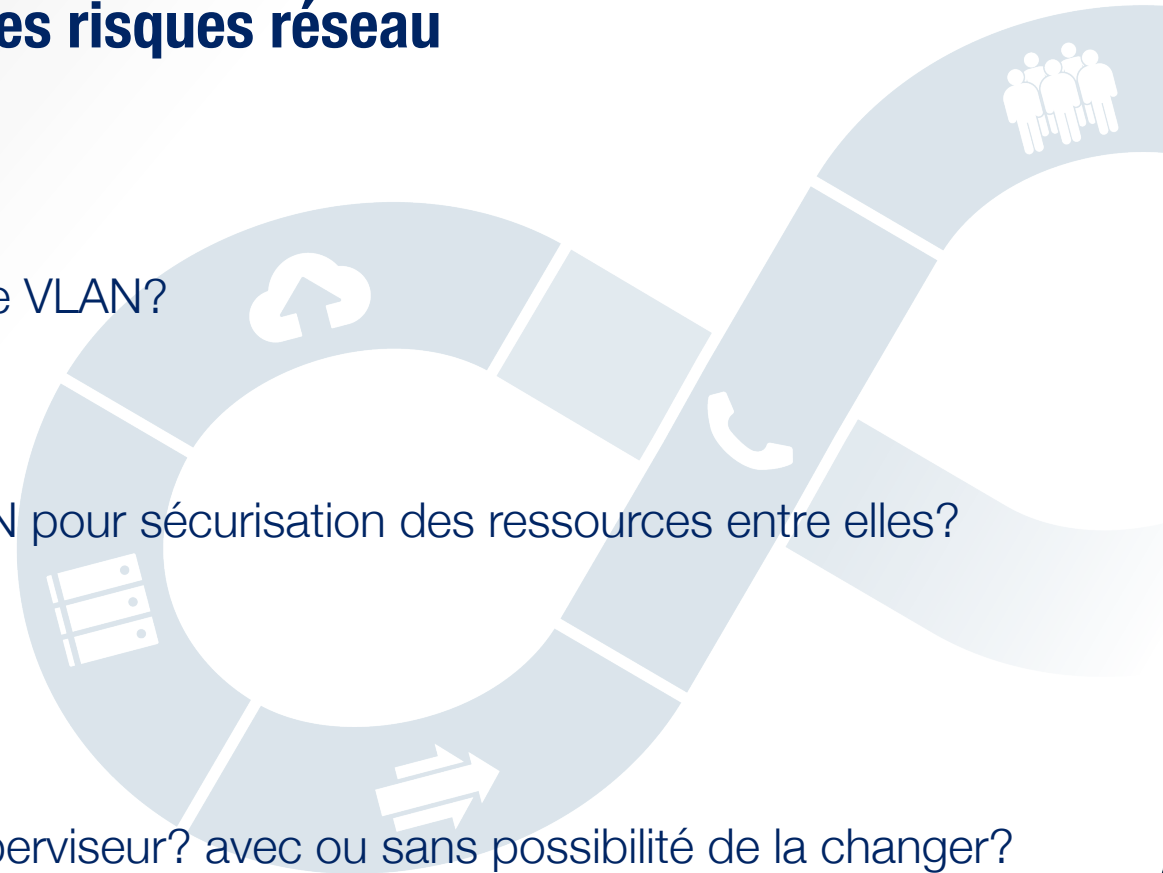
Le cloud et ses travers: les risques réseau

■ Séparation des clients

- Tout le monde dans le même VLAN?
- 1 VLAN par client?
- $n \times$ VLAN par client?
- Possibilité d'avoir des pVLAN pour sécurisation des ressources entre elles?

■ Sécurité du LAN

- MAC fixée sur la VM ou l'hyperviseur? avec ou sans possibilité de la changer?
- QUID du port security sur les switch.
- Quel type de trafic une machine compromise peut intercepter?
- Propagation des politiques de sécurité L2 entre les hyperviseurs / vswitchs.



Le cloud et ses travers: les risques réseau

■ Quid du firewall?

- Possibilité de le choisir suivant vos standards?
- Matériel dédié ou partagé?
- Equipement hardware avec FPGA / ASIC ou VM?
- Firewall dans le sens Internet -> plateforme uniquement ou dans les 2 sens?
- Quid de la possibilité de filtrer en inter VLAN?



Le cloud et ses travers: les risques réseau

■ Quid du firewall?

- Possibilité de le choisir suivant vos standards?
- Matériel dédié ou partagé?
- Equipement hardware avec FPGA / ASIC ou VM?
- Firewall dans le sens Internet -> plateforme uniquement ou dans les 2 sens?
- Quid de la possibilité de filtrer en inter VLAN?

■ L'accès au cloud depuis l'entreprise?

- VPN point à point via Internet?
- Possibilité d'inclure le « cloud » dans un VPN MPLS d'entreprise.
- Quid de la QoS?
- Et les utilisateurs distants / itinérants?

Le cloud et ses travers: les données

■ L'accès aux stockage des données

- En local sur les disques du serveurs ou via une baie de stockage.
- Réservation des ressources (IOPS)
- Garantie de la latence, du jitter et de la perf en général?
- Si je déménage ma VM, les données suivent?
- Quid d'un filesystem full?



Le cloud et ses travers: les données

■ L'accès aux stockage des données

- En local sur les disques du serveurs ou via une baie de stockage.
- Réservation des ressources (IOPS)
- Garantie de la latence, du jitter et de la perf en général?
- Si je déménage ma VM, les données suivent?
- Quid d'un filesystem full?

■ La pérennité de mes données

- Mon fournisseur fait il des backup? A quel intervalle?
- Quid de l'accès à mes backups?
- Est ce que j'ai une réplication synchro / asynchrone?
- Si mes données sont répliquées, est ce sur le même site ou à distance?
- Lors de la résiliation du service, que deviennent mes données / backup?
- Les données que j'externalise sont elles chiffrées? Qui peut y avoir accès?

Le cloud et ses travers: les risques juridiques

■ Le bypass de la DSI et du RSSI

- Hébergement clandestin de projets, sandbox, plateformes de tests...
- Echappe à toute politique de sécurité ou d'audit.
- Données confidentielles ou code source produit par l'entreprise sortie sans contrôle.



Le cloud et ses travers: les risques juridiques

■ Le bypass de la DSI et du RSSI

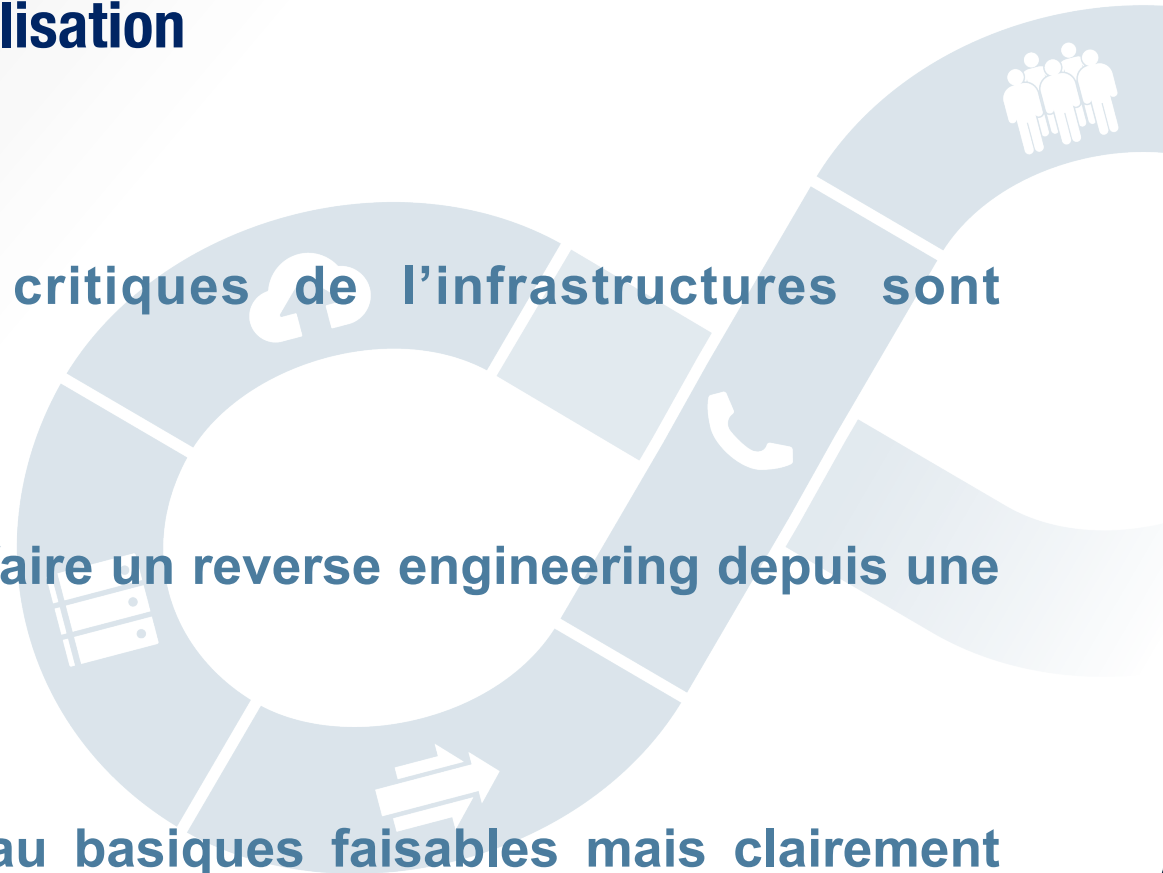
- Hébergement clandestin de projets, sandbox, plateformes de tests...
- Echappe à toute politique de sécurité ou d'audit.
- Données confidentielles ou code source produit par l'entreprise sortie sans contrôle.

■ La confidentialité et responsabilité de mes ressources

- Suis je sous patriot act?
- Mes données sont hébergées dans un pays tiers, suis je en accord avec la réglementation de ce pays?
- En cas de litige, quel juridiction est compétente pour traiter mon différent?
- Ais je un risque d'espionnage industriel en mettant certaines données sensibles dans le cloud?

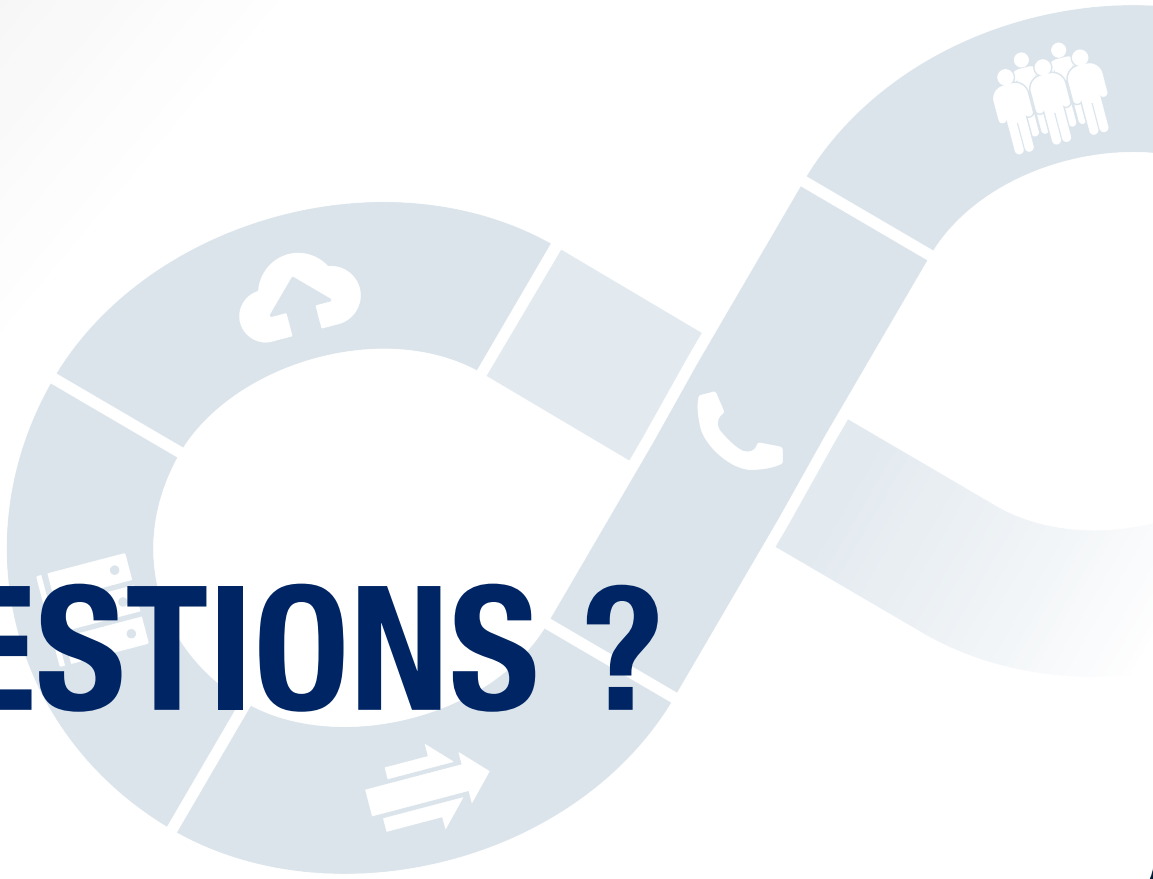
Le brouillard de la virtualisation

- Toutes les couches critiques de l'infrastructures sont cachées / virtualisées.
- Quasi impossibilité de faire un reverse engineering depuis une VM.
- Tests de sécurité réseau basiques faisables mais clairement insuffisants pour valider la sécurité d'une infrastructure.



Que faire vis à vis du cloud?

- **Eduquer!** (les ingénieurs, votre DSI, le département juridique...)
- **Evaluer le risque pour vos données. Méritent elles un cloud privé ou un cloud publique?**
- **Eplucher les CGV de votre fournisseur cloud et lui poser les bonnes questions techniques.**



QUESTIONS ?



@Mat0a



<https://www.linkedin.com/in/matoa>