LES 10 MEILLEURES RECOMMANDATIONS EN TERMES DE SÉCURITÉ SUR LE CLOUD PUBLIC

Le passage au cloud public constitue le premier paradigme du secteur informatique depuis le début des années 2000 avec la première explosion d'Internet. D'après 451 Group®, les responsables informatiques des entreprises prévoient que 60 pour cent des charges de travail seront exécutées dans le cloud d'ici 2018.1 Cette croissance est motivée par une agilité et une évolutivité supérieures, de meilleures performances et un accès plus rapide aux technologies innovantes. Autant d'atouts qui offrent aux organisations un avantage sur la concurrence.

Si l'adoption naissante du cloud public présente de nouvelles opportunités, aussi bien en termes de productivité que d'agilité, elle expose également l'organisation à des risques de sécurité potentiels. Il existe deux caractéristiques bien connues du cloud public dont il faut tenir compte. Tout d'abord, l'utilisateur contrôle essentiellement un ensemble de ressources virtualisées (pour le calcul, la gestion du réseau et l'exécution des applications), exécuté sur un système dont vous n'êtes pas propriétaire. Deuxièmement, le cloud public est une extension de votre réseau. Si ces faits sont bien compris de tous, le public est moins conscient du niveau de sécurité dont bénéficient les applications et les données dans le cloud public. Même s'il est probable que l'infrastructure de votre fournisseur de services cloud soit hautement sécurisée, vous devez intervenir pour assurer la protection de vos applications et données dans le cloud public.

Les hackers ne se soucient pas de l'endroit où sont hébergées vos données. Leur but est de compromettre votre réseau pour voler les données utilisateur, vos propriétés intellectuelles et vos ressources informatiques, qu'elles soient situées dans le cloud public, le cloud privé ou un datacenter physique. Vous devez donc prendre les mesures nécessaires pour protéger les ressources qui y sont enregistrées — une évidence qui n'en est pas toujours une pour les groupes d'entreprises et les équipes DevOps chargées du passage au cloud public. Ce livre blanc a pour vocation de fournir aux équipes de sécurité toutes les informations nécessaires pour prendre en amont les mesures nécessaires, poser les questions adéquates et maintenir la même vigilance sur le cloud public que dans les datacenters.

1. h ps://451research.com/blog/764-enterprise-it-execu ves-expect-60-of-workloads-will-run-in-the-cloud-by-2018

Sommaire

10 points à prendre en compte pour sécuriser les charges de travail de votre cloud public

Vous trouverez ci-dessous les 10 points principaux à prendre en compte pour protéger efficacement les données et les applications dans le cloud public contre une multitude de menaces de sécurité en évolution permanente, qui sont souvent similaires à celles touchant les datacenters traditionnels sur site.

Adoptez le modèle de sécurité partagée

Les fournisseurs de services cloud, tels qu'Amazon® Web Services (AWS®) et Microsoft® Azure®, insistent sur le fait que la sécurité relève aussi de la responsabilité de leurs clients Dans ce modèle, le fournisseur doit veiller à ce que la plateforme soit toujours active, disponible, actualisée, etc.

Beaucoup de gens sont persuadés que l'infrastructure générale du datacenter est plus sécurisée que la leur. Ce qu'ils oublient, c'est qu'en tant que clients, il leur incombe de protéger leurs applications et données exécutées dans le cloud public.

L'image 1 présente les responsabilités incombant à chaque partie. La sécurisation de vos charges de travail dans le cloud public (indiquées en rouge à des fins de clarté) n'est pas différente de celle assurée sursite. Vous pouvez entièrement contrôler le niveau de sécurité à implémenter et vous devez prendre des mesures pour protéger votre contenu, qu'il s'agisse de données clients ou de propriétés intellectuelles.

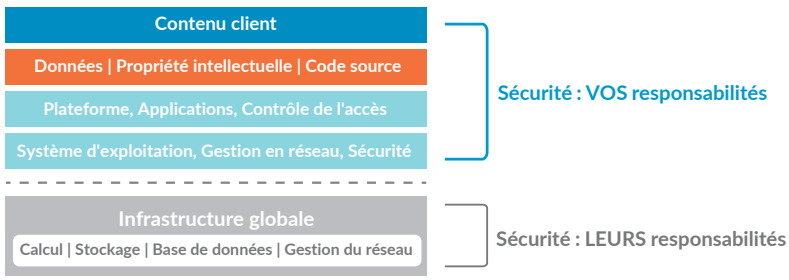


Image 1 : modèle du partage des responsabilités dans le cloud public

Consultez le service commercial et les équipes DevOps en amont

De nombreux projets de cloud public sont menés par les équipes internes des organisations, notamment les équipes DevOps, qui mettent régulièrement au point de nouveaux produits ou prototypes fonctionnels. Les difficultés découlent de deux facteurs : la disponibilité générale des nouvelles approches applicatives et l'implication de l'équipe de sécurité, souvent mise à contribution lors du déploiement. Ces deux services ont alors pour mission d'identifier les failles de sécurité potentielles de l'architecture.

Dans l'idéal, les équipes DevOps et celles chargées de la sécurité doivent travailler en tandem pour comprendre la portée des projets de cloud public et veiller à ce que l'architecture des déploiements applicatifs soit conforme aux besoins en développement, tout en réduisant les risques de sécurité.

Déterminez votre exposition potentielle

L'usage du cloud public relève souvent du « shadow IT » en raison de la facilité d'ouverture des comptes. Les employés pensant agir pour le bien de l'organisation peuvent créer des failles de sécurité si l'environnement n'est pas configuré correctement. Il est impératif d'identifier les utilisateurs du cloud public au sein de votre organisation et de vérifier que votre environnement est configuré correctement.

- **Surveillez l'usage du cloud public :** la manière la plus rapide et la plus fiable de déterminer l'usage consiste à contacter le représentant local de votre fournisseur de cloud public pour lui demander dans quelle mesure votre organisation recourt à AWS ou Azure. Vous pouvez sinon utiliser des outils de visibilité du réseau qui permettent d'analyser l'utilisation en fonction du trafic des applications sur le réseau.

- **Vérifiez que la configuration est adéquate :** configurez l'environnement en appliquant les bonnes pratiques de sécurité. Par exemple, chaque service AWS possède un ensemble d'interfaces publiques pour la programmation des applications (API), qui doivent être désactivées lorsqu'elles ne sont pas utilisées. La plupart des nouveaux utilisateurs d'AWS ne savent pas qu'Amazon Simple Storage Service est un service public et que tout ce qui y est stocké est exposé sur internet en l'absence de verrouillage par une politique. Sur Azure, lors de l'établissement d'un VNet initial au sein d'un groupe de ressources, les utilisateurs doivent comprendre que tous les ports sortants sont ouverts par défaut, ce qui peut présenter une exposition non désirée.
- **Activer l'authentification à deux facteurs :** d'après le dernier rapport annuel Verizon sur les violations de données, 81 pour cent des failles à l'origine d'un piratage exploitaient des informations d'authentification dérobées ou des mots de passe faibles. Pour éviter qu'un hacker n'accède à votre cloud public à l'aide d'informations d'authentification volées, il est nécessaire d'appliquer une authentification à deux facteurs.
- **Verrouillez SSH :** Secure Shell® fait partie des méthodes privilégiées pour contrôler la sécurité des services sur le cloud. Pourtant, ce service reste souvent exposé dans les environnements AWS et Azure. Souvent, les organisations ne comprennent pas les subtilités des clés de chiffrement et des certificats, s'exposant ainsi à des vulnérabilités que les cybercriminels savent parfaitement exploiter. Un cybercriminel possédant un accès SSH peut facilement utiliser l'infrastructure cloud d'une organisation pour lancer ses propres attaques par botnet.

Image 2 : environnement de test d'automatisation du cloud public

Comprenez la stratégie des hackers

Les hackers s'appuient sur l'automatisation pour rechercher des cibles potentielles en quelques secondes. Une fois ces dernières identifiées, ils déterminent les faiblesses en vérifiant les mots de passe par défaut, les mauvaises configuration de SSH, etc.

Pour mettre en valeur les effets des capacités d'automatisation des hackers, un environnement d'essai dans le cloud public a été conçu, avec des instances d'une base de données SQL et un serveur WordPress®. Comme l'indique l'image 2, l'environnement a été testé à partir de plus de 35 pays, avec plus de 25 applications différentes, en moins de huit heures. Contrairement à un datacenter privé, qui présente moins de problèmes en termes d'exposition publique, les ressources du cloud public sont largement exposées. Cet exemple souligne l'importance de la sécurité dans le cloud public.

Évaluez vos options de sécurité

Lors de la transition vers le cloud public, vous avez le choix entre plusieurs options de sécurité, dont la plupart sont très similaires à celles disponibles pour les réseaux physiques.

- **Sécurité native du cloud public :** les fournisseurs de cloud public proposent des services de sécurité native, notamment des groupes de sécurité et des pare-feu d'application web. Même si ces outils contribuent à réduire la surface d'attaque, ils comportent des failles de sécurité.
  - Les groupes de sécurité sont essentiellement des listes de contrôle d'accès en fonction des ports offrant des fonctionnalités de filtrage. Toutefois, vous ne pourrez pas identifier ou contrôler efficacement les applications autorisées, empêcher les menaces ni contrôler le mouvement des fichiers.
  - Les pare-feu d'applications web protègent uniquement les applications HTTP et HTTPS et ignorent le reste du trafic. Ils ne sont pas toujours obligatoires, contrairement aux pare-feu, qui eux sont essentiels. Les pare-feu d'application web ne protègent pas les applications telles que Microsoft Lync®, SharePoint® ou Active Directory®, dont le fonctionnement nécessite un large éventail de ports contigus. De plus, ils manquent d'efficacité pour identifier et contrôler les outils de gestion ou d'accès à distance tels que SSH ou Microsoft RDP.
- **Produits dédiés :** l'une des approches les plus courantes pour sécuriser le cloud public consiste à utiliser un produit dédié au niveau de l'hôte pour détecter les menaces et les prévenir. La popularité de cette approche vient du fait que la sécurité native, combinée à un système de détection ou de prévention des intrusions (respectivement désignés par les acronymes IDS et IPS), est suffisante pour protéger votre déploiement. En réalité, un IDS est paradoxal à l'égard de la vitesse et l'agilité du cloud, puisqu'il nécessite une intervention et des réparations manuelles. Un IPS s'intéresse uniquement aux menaces connues, en passant à côté des menaces de type zero-day ou inconnues. Aucun de ces deux systèmes n'offre une vue d'ensemble sur votre environnement de cloud public.
- **Sécurité maison :** certaines organisations choisissent de mettre au point une approche « maison » pour sécuriser leurs charges de travail sur le cloud public et utilisent des scripts et outils de visibilité pour protéger les déploiements. Les inconvénients potentiels de cette stratégie sont le manque de pertinence des ressources, le manque d'expertise pour gérer l'implémentation et les opérations de sécurité, ainsi que l'absence de support en cas de faille de sécurité.

Les organisations qui s'appuient sur leurs ressources humaines internes pour gérer le cloud public et les déploiements de sécurité doivent se préparer à une réduction progressive de leurs effectifs. En général, seuls quelques ingénieurs connaissent l'environnement parfaitement, mais ils n'ont pas toujours le temps de rédiger une documentation correcte ou de partager leurs connaissances. Si un seul de ces ingénieurs quitte l'organisation, celle-ci ne sera peut-être plus en mesure de gérer efficacement ses futurs besoins en matière de sécurité.

- **Appareils virtualisés intégrés :** un appareil virtualisé intégré tel qu'un pare-feu nouvelle génération virtualisé offre une base pour gagner en visibilité sur votre trafic dans votre déploiement de cloud. En employant une sécurité nouvelle génération intégrée, les organisations peuvent améliorer la protection de leurs applications et données dans le cloud public. Elles peuvent pour cela recouvrir à des technologies d'identification en fonction des applications, des utilisateurs et du contenu pour déterminer avec précision les données auxquelles les utilisateurs accèdent et à quelle fin. Grâce à ces connaissances, elles peuvent mettre en place une politique de sécurité dynamique pour autoriser les applications, le contenu et les utilisateurs en toute sécurité, tout en protégeant les données et les applications des déploiements du cloud public contre les menaces ciblées ou aléatoires.

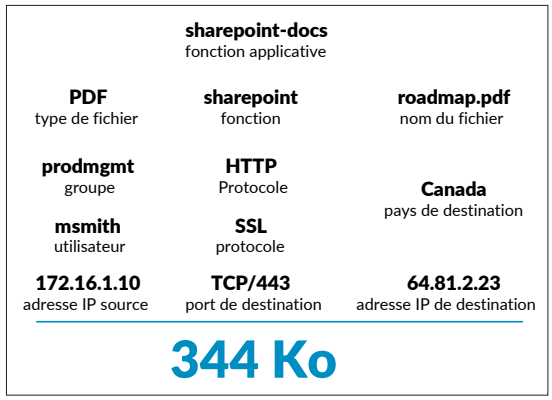


Image 3 : contexte complet des flux de trafic

Savoir, c'est pouvoir

John Antonios, consultant en image de marque, affirme que « le pouvoir est le résultat combiné des connaissances et de l'action ». En matière de sécurité sur le cloud public, les connaissances commencent par assurer la sécurité du trafic dans votre environnement (mobile, réseau physique et cloud).

Les données numériques traversant ces environnements atteignent des volumes faramineux. En utilisant un pare-feu nouvelle génération virtualisé dans le cadre d'une plateforme de sécurité complète intégrée nativement, les organisations obtiennent le niveau d'analyse nécessaire sur l'identité et les caractéristiques du trafic et peuvent ainsi prendre des décisions plus éclairées pour protéger les applications et les données contre les menaces.

Les outils de cloud public natifs offrent peu de visibilité au niveau de la couche applicative. De plus, dans certains cas, il est nécessaire d'acquérir des connaissances approfondies en gestion de réseau pour interpréter correctement les données. Même si l'interprétation est précise, il n'est guère utile de savoir qu'un port utilise telle adresse IP source pour transmettre 344 Ko de données à une adresse de destination sur le port TCP 443 alors que des centaines d'applications peuvent utiliser le port TCP 443.

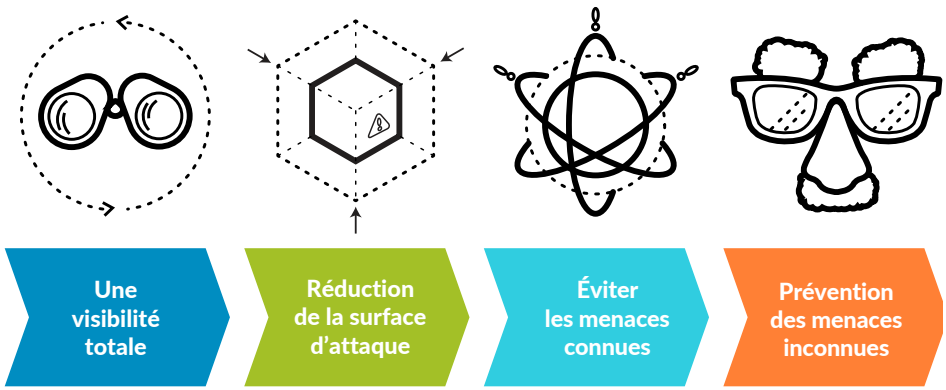
Dans certains déploiements hybrides dans lesquels le cloud public est connecté à l'entreprise via un VPN IPSec, l'utilisation de contrôles en fonction des ports pour limiter l'accès aux ports TCP 80 et TCP 443 est considéré comme suffisant, au motif que cette exposition se borne aux données provenant de l'entreprise. C'est une stratégie fondamentalement inefficace.

- Au moins 500 applications, pour la plupart associées à des outils d'accès à distance, des applications évasives et des proxys peuvent utiliser les ports TCP 80 et TCP 443.
- Souvent, les applications utilisées nécessitent d'autres protocoles et services (DNS, NetBIOS et éventuellement SSH), chacun d'entre eux nécessitant l'ouverture d'un port spécifique.
- Chef et Puppet, outils de développement les plus courants, nécessitent l'ouverture d'un large éventail de ports :
  - Ports ouverts pour Chef : 80, 112, 443, 4321, 5432, 5672, 8000, 8983, 9683, 9090, 15672, 16379, 7788–7799
  - Ports ouverts pour Puppet : 25, 443, 8081, 8140, 61613

En réalité, s'ils assurent un niveau de contrôle initial, les contrôles des ports ne permettent pas d'identifier contextuellement le trafic lié à l'application, son contenu ou son utilisateur. Comme l'indique l'image 3, la prise de décisions informées en matière de politique de sécurité nécessite de comprendre l'ensemble du contexte dans lequel s'inscrit le trafic, notamment les adresses IP et les pays source/de destination, les protocoles, l'utilisateur ou le groupe d'utilisateurs à l'origine de l'activité, la catégorie d'URL, l'identité de l'application, les fonctions applicatives spécifiquement utilisées ainsi que le nom et le type du fichier concerné.

Misez sur la prévention

Ceux qui partent du principe que les hackers ont déjà gagné optent pour une approche basée sur la détection et la remédiation. Certes, une parfaite compréhension de votre environnement permet en effet l'adoption d'une telle philosophie. La prévention des cyberattaques sur le cloud public nécessite quatre capacités essentielles :



Une visibilité totale

Si elles sont appliquées correctement, les connaissances constituent un puissant outil de sécurité. Il est essentiel d'identifier les applications sur le réseau et dans le cloud public — indépendamment du port, du protocole, de la tactique d'évasion ou du chiffrement— mais aussi les caractéristiques de chaque application, les fonctions qu'elles utilisent spécifiquement et le risque relatif qu'elles présentent. Sur la base de telles connaissances, vous pouvez alors déployer une politique de sécurité plus cohérente sur l'ensemble du réseau pour le protéger contre les attaques connues et inconnues.

Réduction de la surface d'attaque

L'utilisation de l'identité de l'application pour appliquer un modèle de sécurité positive réduit la surface d'attaque, puisque seules les applications spécifiquement identifiées sont autorisées, tandis que toutes les autres sont interdites. Vous pouvez adapter l'usage des applications en fonction des besoins de votre organisation, contrôler les fonctions applicatives (par exemple, autoriser les documents SharePoint pour tous les utilisateurs, mais limiter l'accès administratif de SharePoint au groupe informatique) ou encore empêcher les menaces d'accéder à votre réseau et de s'y déplacer latéralement.

Éviter les menaces connues

La mise en œuvre de politiques de prévention de menaces spécifiques à certaines applications constitue une étape essentielle pour inciter les utilisateurs à respecter la politique de prévention. Les politiques de prévention des menaces spécifiques aux applications sont efficaces pour bloquer les menaces connues, notamment les exploits de vulnérabilité, les logiciels malveillants ainsi que le trafic généré par les logiciels malveillants et les systèmes de command-and-control.

Prévention des menaces inconnues

Les fichiers inconnus et potentiellement malveillants sont analysés en fonction de centaines de comportements. Si un fichier est considéré malveillant, un mécanisme de prévention est appliqué en cinq minutes. Ensuite, les informations obtenues à l'issue de l'analyse du fichier sont utilisées pour renforcer en continu toutes les autres fonctionnalités de prévention.

Adoptez une approche centrée sur le cloud

Le cloud public permet à votre organisation de surmonter les difficultés grâce à une approche agile et plus évolutive. Pour profiter pleinement du cloud, il est recommandé « d'appliquer à votre déploiement les mêmes concepts qu'à un datacenter en abandonnant les approches traditionnelles ». Les organisations peuvent ainsi améliorer leur disponibilité et leur capacité d'évolution.

Si on prend l'exemple de la haute disponibilité traditionnelle sur deux appareils, on peut considérer que son principe peut être appliqué au déploiement de votre cloud public. Toutefois, l'avantage de l'accélération matérielle pour un basculement en moins d'une seconde est perdu dans le cloud public puisqu'on utilise alors des ressources tierces. Pour exécuter le basculement à partir d'une instance d'appareil vers une autre, le processus est réalisé en software. Cette opération peut nécessiter jusqu'à 60 secondes en fonction de l'environnement et ne peut pas être appliquée dans plusieurs régions simultanément. L'approche centrée sur le cloud utilise le tissu du fournisseur de cloud et ses fonctionnalités de résilience, telles que l'équilibrage de charge, pour offrir une haute disponibilité, rapidement et en toute transparence.

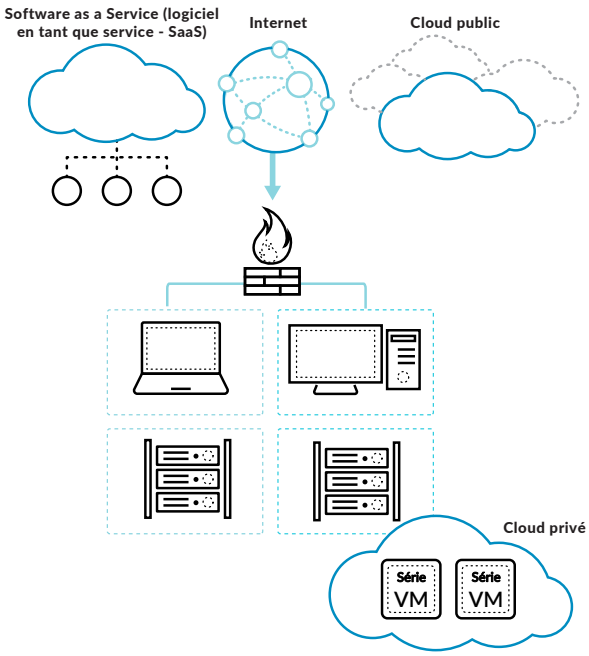


Image 4 : une approche centrée sur le cloud

Recourez à l'automatisation pour éviter les goulots d'étranglement

L'automatisation est un principe fondamental du cloud public, dans lequel les changements sont souvent très rapides. Lorsqu'on applique les pratiques éprouvées en matière de contrôle du changement, le délai inévitable peut induire des frictions, ralentir les déploiements et, pire, affaiblir la sécurité si le déploiement « n'attend pas » que le contrôle du changement soit opérationnel. En automatisant la sécurité dans le cloud public, les organisations peuvent éliminer les frictions induites par la sécurité tout en profitant de la flexibilité et de l'agilité du cloud public. Les organisations doivent vérifier que leur fournisseur de cloud public leur offre les outils d'automatisation suivants :

- **Déploiements sans contact :** Les fonctionnalités telles que le bootstrapping permettent, en quelques minutes, de déployer un pare-feu entièrement configuré, pour isoler efficacement les environnements de réseau virtuel dans le cloud public (par exemple, les groupes de ressources Azure et les clouds privés virtuels AWS).
- **Intégration bidirectionnelle avec des ressources tierces :** l'intégration via les API avec des outils tiers et les données contribue à rationaliser les opérations de sécurité. Par exemple, l'intégration avec ServiceNow® est possible pour assurer la génération de tickets de service et de processus.
- **Mises à jour des politiques « sans validation » :** Les fonctionnalités d'automatisation telles que l'API XML et les groupes d'adresses dynamiques permettent l'application dynamique des mises à jour de la politique de sécurité en fonction des charges de travail. Les organisations peuvent fonctionner à la vitesse du cloud en déployant des mises à jour plus précises en fonction des évolutions de l'environnement.

Assurez la cohérence des politiques grâce à la gestion centralisée

La cohérence de la politique est essentielle à l'efficacité de la sécurité pour les données et les applications dans le cloud public. Le contrôle à partir d'un emplacement central de votre réseau distribué de pare-feu, physiques et virtualisés, et l'application d'une règle de sécurité cohérente entre le réseau et le cloud public sont essentiels pour maintenir les fonctions de sécurité. La gestion centralisée permet d'analyser le trafic et les menaces sur l'ensemble du réseau, en simplifiant la gestion et en minimisant le délai d'application de la politique de sécurité en fonction des changements affectant le cloud public.

Résumé

Les organisations adoptent le cloud public pour accélérer leurs délais de mise sur le marché, améliorer leur activité générale et maintenir leur avantage sur la concurrence. Toutefois, cette adoption étant menée par des groupes centrés sur l'activité, les équipes de sécurité ne sont pas toujours impliquées dans le processus. L'expérience rapportée ici et les recommandations formulées ont des fonctions éducatives et informatives. Elles visent idéalement à encourager le dialogue entre les équipes chargées de la sécurité et les équipes internes des organisations, dans le but de bâtir une architecture de cloud public et d'assurer un déploiement répondant aux besoins de toutes les parties prenantes.

Pour de plus amples informations, consultez les ressources suivantes :

- **Page web :** Sécurisation de votre cloud public
- **Livre blanc :** Comment mettre en œuvre un cloud hybride dans Microsoft Azure en toute sécurité
- **Livre blanc :** Directives de déploiement du pare-feu VM-Series pour cloud hybride AWS

4401 Great America Parkway
Santa Clara, CA 95054, États-Unis

Accueil téléphonique : +1 408 753 4000
Service commercial : +1 866 320 4788
Assistance : +1 866 898 9087

www.paloaltonetworks.com

top-10-public-cloud-security-recommentation-eg-080217