Les 3 défis du cloud qui pèsent sur vos équipes IT

Quelles conséquences sur votre business ?

aws | TREND MICRO™

Sommaire

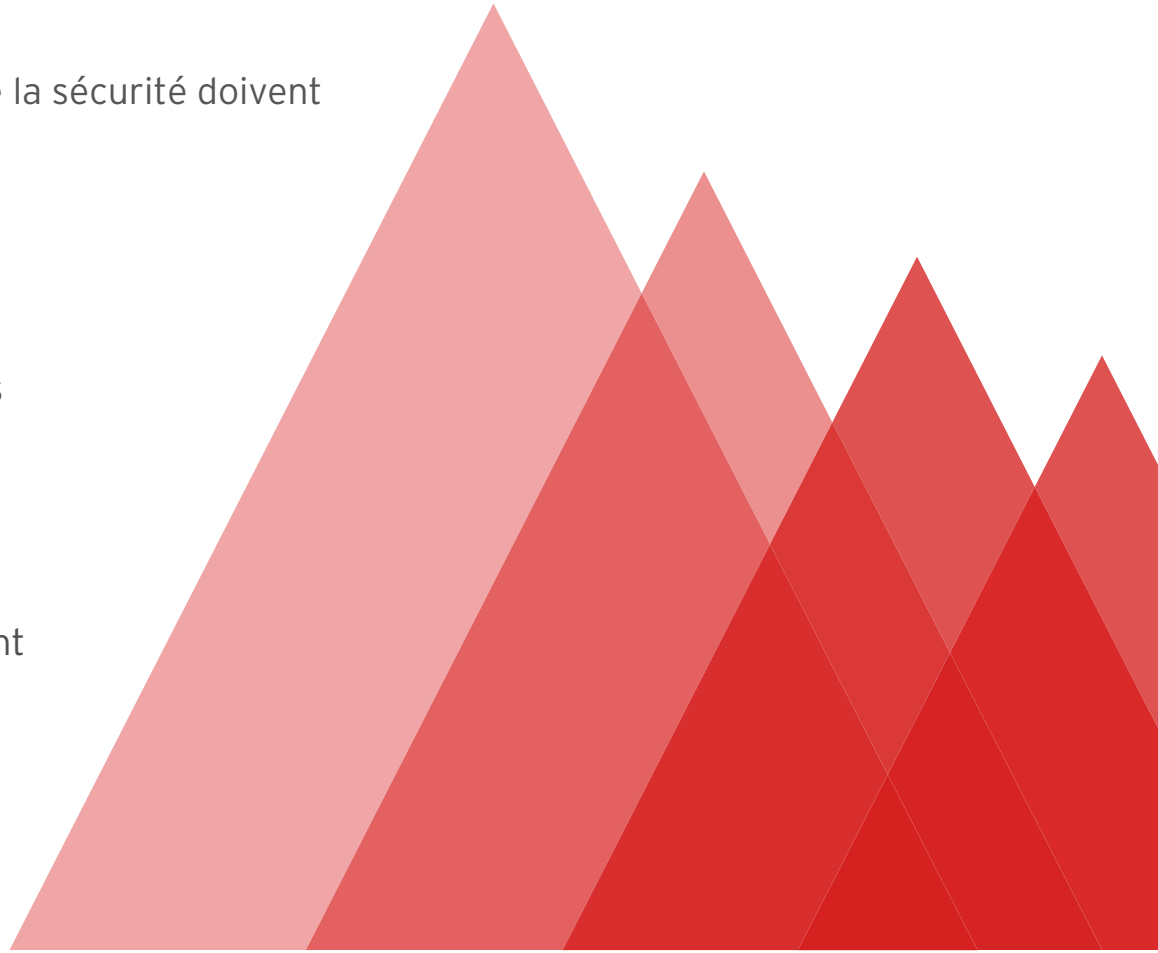
Le constat :

Aujourd'hui, les équipes en charge du cloud et de la sécurité doivent

EN FAIRE PLUS AVEC MOINS

Du point de vue fonctionnel et tarifaire, certaines solutions de gestion de la sécurité s'adaptent à l'adoption généralisée du cloud Amazon Web Services (AWS).

Mais nombre d'entreprises tentent de protéger leurs charges de travail dans le cloud mais peinent à s'y investir suffisamment en ressources et en support.



aws | TREND MICRO

Protéger davantage, mais avec moins de ressources

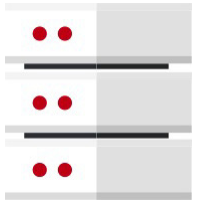
Les entreprises qui migrent vers le cloud s'attendent à ce que leurs équipes IT protègent davantage de serveurs et de ressources que dans le passé - alors que les budgets, formations et outils nécessaires ne sont pas toujours à la hauteur.

Ces équipes sont souvent forcées de jouer les pompiers, au lieu de tirer pleinement parti des innovations d'AWS : les objectifs stratégiques ne sont donc que rarement tenus.

Source : Data Centers in Flux : The IT Optimization Challenge, Q3 2016, IDG Research, 2016

aws | TREND MICRO

Quels sont les défis des équipes en charge du cloud et de la sécurité ?



La gestion des serveurs

Une prolifération des serveurs, applications et données qui pèse sur une gestion efficace de la sécurité

Le facteur humain

Une carence en matière de compétences et de formation spécifiques à la sécurité du cloud

Des outils de sécurité inadaptés

Des technologies inadéquates et obsolètes par rapport aux objectifs de sécurité et métiers

Penchons-nous maintenant sur l'origine de ces défis et sur leur impact sur votre métier.

aws | TREND MICRO

Section 1

La gestion des serveurs

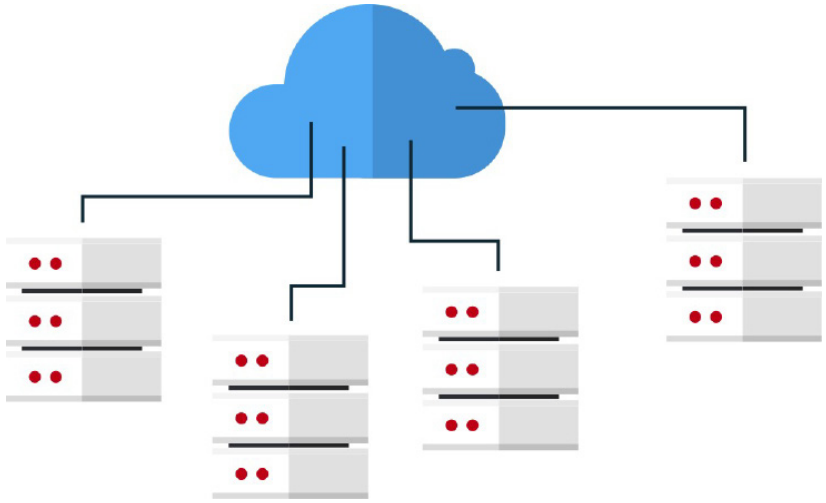
Une prolifération des serveurs, applications et données qui pèse sur une gestion efficace de la sécurité

aws | TREND MICRO

Tout démarre par vos serveurs

Pour accompagner leurs nouveaux projets, les entreprises ont tendance à renforcer leur infrastructure IT de façon incrémentale. De ce fait, elles répondent uniquement à un besoin à court terme. Avec AWS, il est simple d'activer de nouveaux serveurs lorsque nécessaire. En revanche, la tâche est bien plus complexe pour les équipes IT qui doivent les sécuriser.

Environ **30%** des serveurs ne sont pas utilisés – **Soit environ 10 millions de "serveurs en sommeil" dans le monde**



Trop souvent, cette approche résulte en une sous-utilisation coûteuse du réseau qui nuit aux objectifs à long terme.

L'impact métier de la gestion complexe des serveurs

Les entreprises qui souffrent d'une gestion complexe des serveurs :

Ne disposent pas d'une visibilité en temps réel sur leur statut de sécurité.

Consacrent trop de temps à la gestion des serveurs

Peinent à réagir rapidement aux incidents de sécurité

Les menaces de sécurité sont plus fréquentes

La sous-utilisation des serveurs et les carences en matière de fonctions de sécurité ont un coût financier.

En 2016

82 000

Environ **82 000** incidents majeurs de cybersécurité ont eu lieu en 2016 tandis que le coût moyen d'un piratage de données s'élève à environ **USD 4 millions**

aws | TREND MICRO

Maîtriser l'évolution des environnements cloud

Opter pour une sécurité transversale qui offre davantage de visibilité sur chaque département métier

Renforcer la visibilité sur le cloud pour toutes les équipes grâce à des processus et outils modernes

Automatiser la sécurité dans le cadre de DevOps, pour une sécurité intégrée en natif et pas simplement rajoutée

Trend Micro Deep Security for AWS, optimisé par XGen™ apporte à vos équipes IT une visibilité intégrale. Les équipes en charge du cloud et de la sécurité définissent ainsi des processus proactifs pour gérer les incidents de sécurité sur l'ensemble des départements métiers.

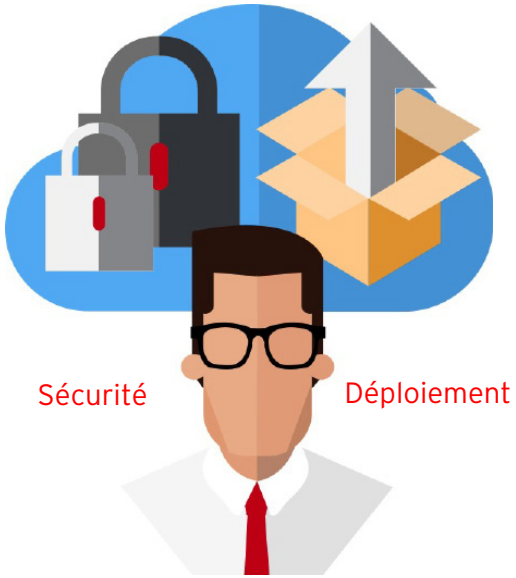
Section 2

Le facteur humain

Une carence en matière de compétences et de formations spécifiques à la sécurité du cloud

Le rôle de l'équipe de sécurité IT s'ouvre à de nouvelles responsabilités.

Des nombreuses entreprises attendent désormais de leurs équipes DevOps qu'elles gèrent les environnements cloud, mais aussi leur sécurité. Sans les compétences et la formation adéquates, ce rôle hybride de “DevSecOps” peut être particulièrement fastidieux, et les professionnels IT le savent.



Le défi N°1 du cloud : la pénurie en ressources et compétences.

Source : State of the Cloud Report, RightScale, 2016

Gérer la sécurité des charges de travail du cloud

Le cloud présente des besoins en sécurité très différents de ceux des data centers physiques sur site. Cette sécurité doit être assurée par des équipes compétentes et formées de manière pertinente.

Vos spécialistes des déploiements et vos développeurs sont peut-être des experts dans leur domaine, mais sans doute pas en matière de sécurité.

En 2016, 46% des entreprises ont connu une pénurie de compétences en sécurité.

Source : Through the Eyes of Cyber Security Professionals, ESG/ISSA, 2016

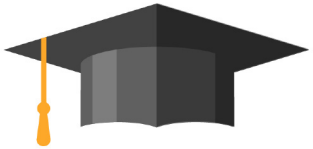
Rechercher les talents nécessaires au sein de votre équipe IT

Pour associer profils généralistes et spécialistes, les équipes IT doivent :

Collaborer avec des organisations professionnelles

Bénéficier de formations spécifiques

Être accompagnées et conseillées dans leur travail (mentorat)



Obtenir des certifications de sécurité supplémentaires

AWS propose toute une gamme de certifications de sécurité pour aider votre équipe à mieux piloter leurs environnements cloud. Ces certifications renforcent l'expertise de votre équipe IT et évaluent leurs compétences vis-à-vis des tendances actuelles et émergentes de la sécurité.

Plus d'automatisation avec AWS

En matière de déploiement et de sécurité.

Sans automatisation

Vos équipes de sécurité et cloud doivent se contenter de processus chronophages et enclins à l'erreur, tandis que le risque de non-conformité est réel

VS

Avec automatisation

Vos équipes cloud et de sécurité déploient et protègent vos environnements à l'aide de modèles et règles normalisées et validées, proposés par Trend Micro : les gains de temps, la sécurité et la conformité réglementaire sont au rendez-vous

aws | TREND MICRO

Section 3

Des outils de sécurité inadaptés

Des technologies inadéquates et obsolètes par rapport aux objectifs de sécurité et métiers

Quel est l'impact de vos outils de sécurité sur votre métier ?

Lorsqu'elles étudient la sécurité de leur cloud, les entreprises doivent arbitrer entre **coût, facilité d'utilisation** et **efficacité**.

Cependant, ces entreprises sont encore trop nombreuses à ne pas investir dans les technologies qui assureront leur pérennité.

Pour gérer la sécurité de leurs données, elles se contentent de systèmes en place obsolètes et peu efficaces ou d'un patchwork d'outils hétérogènes.

- d'où un réel danger.

Se contenter de ce qu'on sait est un danger

La visibilité et la vigilance sont essentielles à la sécurité du cloud, mais les outils de sécurité d'hier ne proposent pas de visibilité en temps réel au cœur des charges de travail.

Sécurité en place

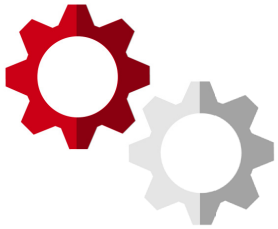
- Ne protège pas les charges de travail cloud et hybrides
- N'offre pas de visibilité au sein des environnements cloud temps-réel

Différentes interfaces de sécurité

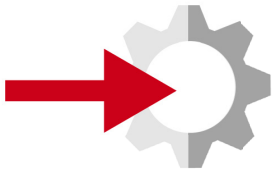
- C'est le résultat d'outils de sécurité rajoutés par incrément au fil du temps
- La multiplicité des outils de gestion et de reporting n'offre pas de visibilité unifiée.

L'impact des systèmes de sécurité obsolètes

Les systèmes de sécurité obsolètes ou peu structurés nuisent à votre productivité.



L'absence d'automatisation force les équipes IT à mettre à jour manuellement les logiciels et règles



L'absence d'intégration avec les logiciels tiers pèse sur la productivité et est source d'erreurs

Les analyses et patchs de sécurité ralentissent vos systèmes

L'impact des budgets IT trop faibles

Les entreprises dont les budgets IT sont restreints courent le risque d'un piratage de données.

Amendes pour non-conformité à PCI DSS

De $5,000 a plus de $100,000 par mois + frais de transaction et bancaires plus importants

Source : *PCI Compliance Guide*, PCI ComplianceGuide.org

Amendes pour non-conformité au RGPD

Jusqu'à 4% du C.A. mondial ou €20 million

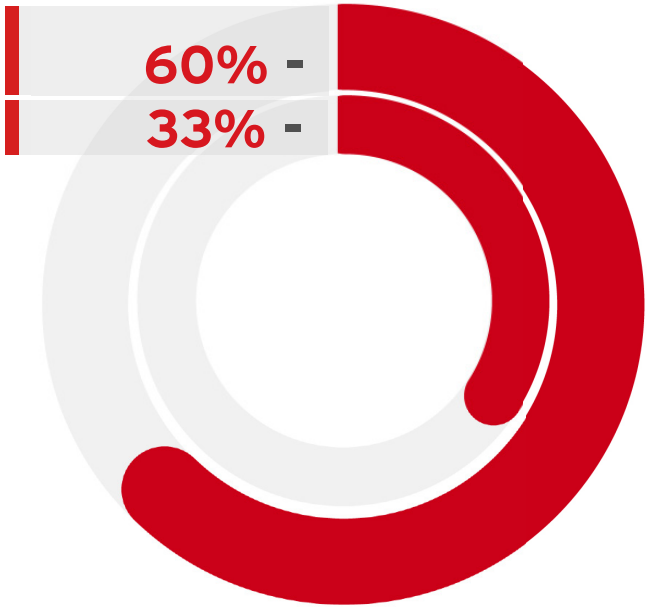
Source : Réglement Général sur la Protection des Données

La refonte intégrale de votre infrastructure peut être un vrai défi. Trend Micro simplifie cette opération en offrant une intégration par API, vous permettant de tirer le meilleur parti de vos outils existants et de remplacer ceux qui sont obsolètes.

Source : *Ga*

aws | TREND MICRO

Plus de visibilité au sein du cloud, moins d'incidents de sécurité



Les analystes estiment qu'en 2018, les **60%** des entreprises qui auront déployé une visibilité cloud pertinente verront leurs incidents de sécurité regresser de **33%**

Source : *Gartner Predicts* 2017: *Cloud Security,* Gartner, 2016

aws | TREND MICRO

Une approche consolidée

aws | TREND MICRO

Trend Micro Deep Security for AWS, optimisé par XGen™

Avec AWS, Trend Micro apporte une solution à la gestion fastidieuse des serveurs, à la pénurie de compétences cloud au sein de votre entreprise et à l'utilisation d'outils inappropriés.

Trend Micro est Advanced Technology Partner du programme AWS Partner Network (APN), avec une solution adaptée à la nature dynamique du cloud AWS.

Avec Deep Security for AWS, votre équipe IT dispose d'une solution automatisée et évolutive, sécurisée de manière optimale mais à moindre effort. La solution permet aux équipes IT de garder la main sur des menaces en forte évolution et de se libérer du temps pour se repositionner sur des projets plus stratégiques.

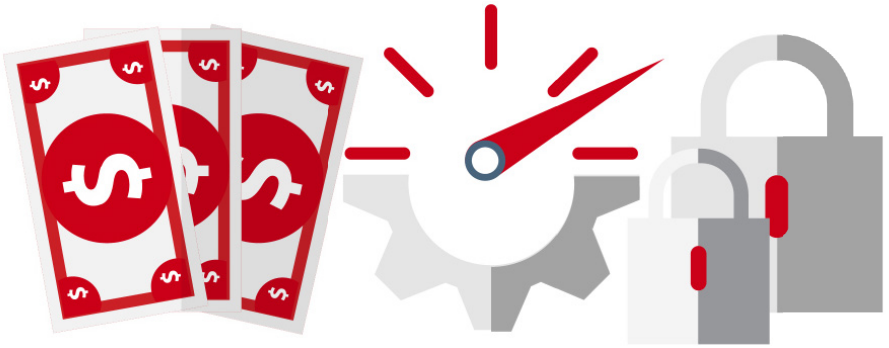
aws | TREND MICRO

La gestion des serveurs

Une sécurité automatisée pour protéger les données, applications et serveurs.

Deep Security for AWS, optimisé par XGen™ simplifie la gestion des serveurs. La visibilité sur les charges de travail cloud, associée à une solution de sécurité multi-fonction, déploie une visibilité granulaire sur la sécurité de chacun de vos départements métiers.

Tirez parti de Deep Security for AWS et bénéficiez de processus proactifs de prise en charge des incidents de sécurité sur l'ensemble de vos départements.



aws | TREND MICRO

Le facteur humain

Renforcer votre sécurité du cloud sans renforcer vos équipes

Avec la bonne technologie en place, vos équipes cloud et de sécurité peuvent se recentrer sur les projets stratégiques d'entreprise. **Deep Security for AWS, optimisé par XGen™ propose les outils dont vous avez besoin pour déployer une solution de sécurité automatisée.** Une sécurité automatisée libère du temps pour vos équipes. Ces dernières peuvent déployer des modèles normalisés et validés et ainsi accélérer le déploiement de vos environnements AWS et les protéger.

Conçu dans une optique de sécurité du cloud, Deep Security for AWS s'intègre en toute transparence avec votre environnement, pour protéger vos charges de travail, en parfaite collaboration avec vos équipes DevOps.

aws | TREND MICRO

Deep Security for AWS tire parti de nombreux services AWS pour renforcer votre expérience du cloud :

Amazon Relational Database Service (Amazon RDS)

- Automatisation des tâches, comme le provisioning matériel
- Installation, exploitation et évolutivité d'une base de données relationnelle

Amazon Simple Storage Service (Amazon S3)

- Stockage pérenne et évolutif des objets
- Stockage et récupération de données vers et à partir du cloud

Amazon Elastic Compute Cloud (Amazon EC2)

- Cloud computing sécurisé et évolutif
- Activation rapide et sécurisée de nouvelles instances

Amazon Elastic Load Balancing (Amazon ELB)

- Routage automatique du trafic entrant
- Tolérance aux pannes applicatives

Auto Scaling

- Dimensionnement automatique des capacités d'Amazon EC2
- Haute-disponibilité des applications

aws | TREND MICRO

Premiers pas

Associé à ces services d'AWS, Deep Security for AWS vous apporte la sécurité temps-réel, évolutive et orientée cloud qu'il vous faut pour vos environnements cloud en évolution, sans avoir à renforcer l'effectif de vos équipes de sécurité.

Deep Security for AWS est disponible à l'achat sur :
La marketplace AWS

Évaluez gratuitement Trend Micro Deep Security for AWS sur 30 jours :
Evaluation gratuite sur 30 jours