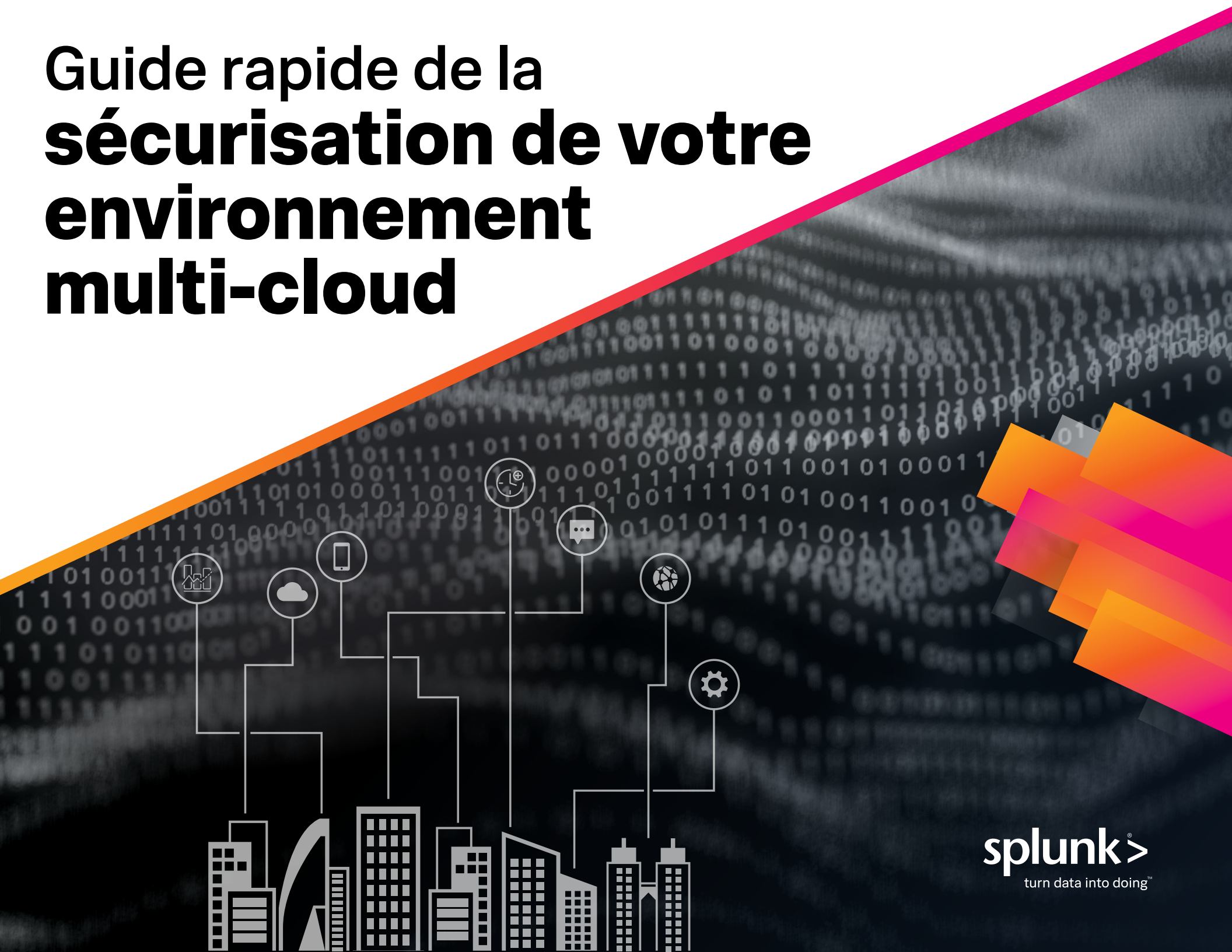
Guide rapide de la **sécurisation de votre environnement multi-cloud**



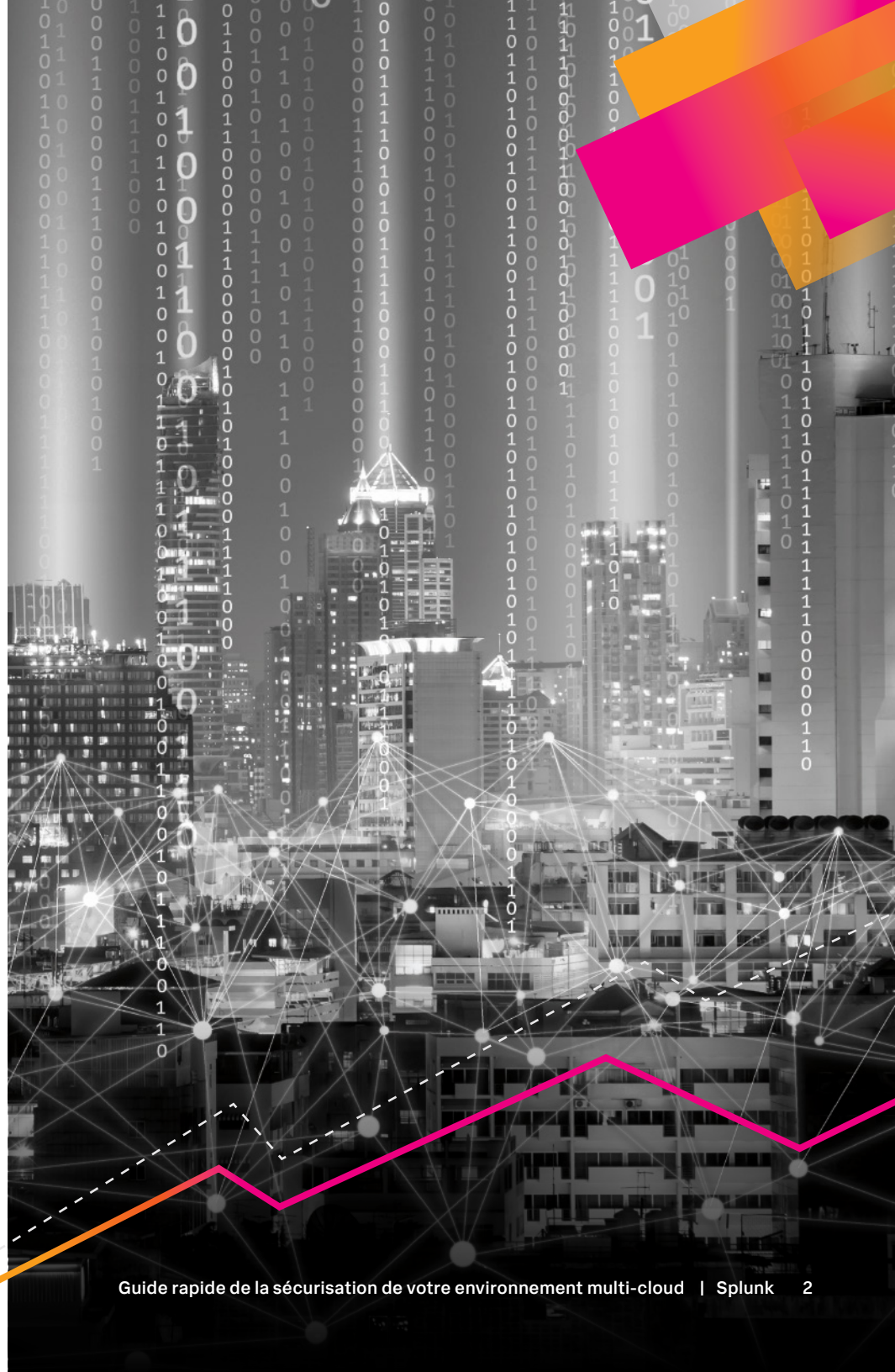
splunk>
turn data into doing™

Guide rapide de la **sécurisation de votre environnement multi-cloud**

La plupart des entreprises migrent leur infrastructure et leurs services dans le cloud, et beaucoup d'entre elles adoptent une stratégie multi-cloud.

Pourquoi ?

Dans ce guide rapide, nous vous expliquons ce qu'est le multi-cloud, les avantages de l'adoption d'une stratégie multi-cloud et, dernier point – et pour nous sans doute le plus important – comment sécuriser votre multi-cloud avec la bonne solution de sécurité.



Qu'est-ce que le **multi-cloud ?**

L'adoption d'une stratégie multi-cloud n'est pas un concept difficile à appréhender. Cela consiste simplement, pour une entreprise, à exploiter au moins deux services cloud au sein d'une même architecture afin de relever différents défis.

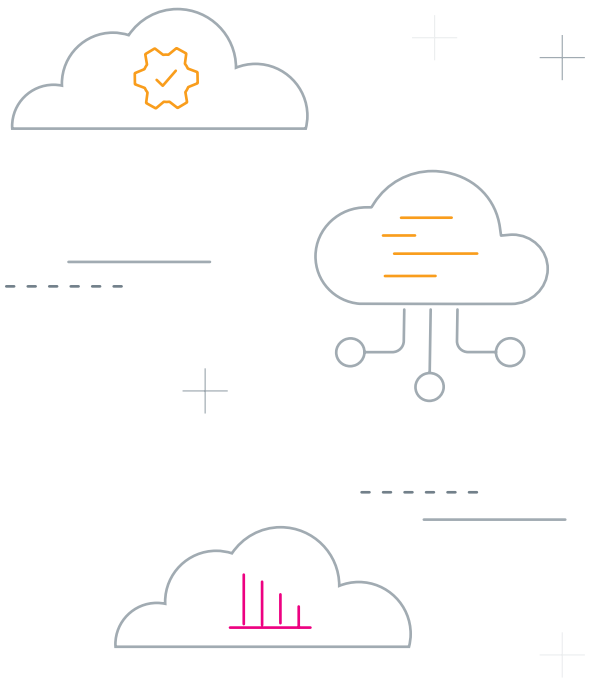
Certaines nuances méritent tout de même d'être comprises. En particulier, le multi-cloud peut être composé de différents types de services. Commençons par le cloud public. On pense à Amazon Web Services, Microsoft Azure ou à la plateforme Google Cloud. Le cloud privé, ensuite, est similaire au cloud public mais son accès est réservé à une entreprise spécifique ou hébergé localement par une société. Enfin, le multi-cloud comprend souvent toutes les solutions SaaS (logiciel en tant que service) actuellement utilisées par les entreprises. Pensez aux services tels que G Suite, Workday, Salesforce, Adobe Creative Cloud et Office 365. Et la liste continue.

La stratégie multi-cloud n'est pas la même chose que l'approche de cloud hybride, qui désigne les modèles de déploiement sur plusieurs clouds publics, privés ou les deux. C'est notamment le cas quand une entreprise base son infrastructure sur un cloud privé local et un cloud public tiers. Cette approche de l'infrastructure est parfois requise pour des questions de conformité, ou pour compartimenter certaines parties de l'activité comme les finances.

Six avantages des **environnements multi-cloud**

L'adoption d'une stratégie multi-cloud offre bien plus de six avantages mais, pour aller droit au but, nous avons réuni les six plus importants :

1. Économies
2. Flexibilité et agilité
3. Fiabilité accrue
4. Optimisation des performances
5. Indépendance vis-à-vis des fournisseurs
6. Réduction des risques d'attaques par déni de service



Toujours pour faire court, donnons un peu de contexte à cette liste.

Une stratégie multi-cloud permet de réaliser des **économies** de plusieurs manières, notamment grâce à la **flexibilité et l'agilité** qu'elle apporte. Par exemple, il est plus difficile pour des pirates de faire tomber tous les services d'une entreprise s'ils sont distribués sur plusieurs clouds. De plus, une stratégie multi-cloud peut considérablement **améliorer les performances**. Les clouds passifs servent de solution de repli en cas de défaillance ou de problème de performance des clouds principaux (que cela soit le fait d'un acteur malveillant ou d'une modification des opérations). Cette **fiabilité renforcée** des services dans leur ensemble contribue à réduire et/ou éliminer les interruptions en attendant que le cloud principal soit à nouveau opérationnel.

Pour prendre un exemple concret, pensez aux attaques par **déni de service distribué (DDoS)** au cours desquelles les pirates utilisent plusieurs systèmes informatiques ou appareils connectés pour attaquer et surcharger un serveur, un site web ou un fournisseur cloud. Lorsque l'attaque réussit, les réseaux tombent en panne et les coûts explosent pour l'organisation visée.

Les résultats peuvent avoir un large spectre de répercussions allant des pertes financières pour les entreprises à la mise en danger des personnes dans les services de santé. Une récente étude a chiffré ce risque. Elle a révélé que, pour 98 % des entreprises, une seule heure d'interruption coûte en moyenne plus de 100 000 $, et 33 % des sociétés interrogées ont indiqué qu'une interruption pouvait leur coûter jusqu'à 5 millions $.

Une stratégie multi-cloud contribue à réduire l'impact des attaques DDoS en répartissant le trafic et les services sur plusieurs clouds, éliminant ainsi les risques associés au point de panne unique.

Une stratégie multi-cloud permet également de conserver son **indépendance vis-à-vis des fournisseurs**. Au lieu de tout miser sur un fournisseur, les organisations multi-cloud peuvent comparer les offres similaires et sélectionner celle qui les sert le mieux, quel que soit le fournisseur. D'autre part, cela stimule la compétition entre les prestataires qui savent que les entreprises ont le choix entre de multiples clouds et options. Les fournisseurs doivent rester compétitifs sur le plan des services et des coûts car ils savent que leurs clients peuvent changer à tout moment en fonction des besoins de leur architecture SaaS ou cloud.

Les défis de la sécurisation d'une **stratégie multi-cloud**

Si les avantages d'une stratégie multi-cloud sont nombreux, ils s'accompagnent néanmoins de plusieurs défis. En particulier, il peut être difficile de sécuriser une stratégie multi-cloud en raison du manque de visibilité sur les hôtes et les services. Dans un tel environnement, des acteurs malveillants peuvent détecter, au sein de l'infrastructure d'une entreprise, des vulnérabilités exploitables possiblement ignorées de ceux qui la gèrent.

Plus encore que le manque de visibilité, des défauts de gestion et de configuration présents dès le départ peuvent avoir de coûteuses répercussions en aval. Lors de la mise en place d'un environnement multi-cloud, il est essentiel de prévoir une gestion solide des identités et des accès (IAM), qui constitue un pilier fondamental de la sécurité globale de l'infrastructure d'une entreprise. En effet, c'est elle qui va accorder l'accès aux ressources du cloud sans l'exposer à des acteurs malveillants ou des incidents malheureux.

La complexité est également un enjeu. Si le cloud simplifie la gestion de l'infrastructure, il introduit également une nouvelle complexité en multipliant les services et en induisant une perte de contrôle sur les données exportées vers le cloud ainsi qu'un manque de visibilité, comme on l'a déjà mentionné.

Comment **sécuriser un environnement multi-cloud**

Fort heureusement, il existe une solution. Les écosystèmes multi-cloud sont divers et englobent une multiplicité de fournisseurs, d'applications et de systèmes. Les entreprises qui adoptent une stratégie multi-cloud ont besoin de visibilité et de contrôle sur les modifications de l'ensemble de l'infrastructure pour mieux comprendre qui fait quoi et où sur une myriade de services cloud, afin d'éviter les interruptions de service, voire pire.

Le portefeuille de sécurité de Splunk, qui comprend plusieurs applications destinées aux services cloud, apporte cette visibilité en fournissant des renseignements instantanés sur la sécurité et les opérations des services cloud les plus populaires tels qu'AWS, Azure et la plateforme Google Cloud.

Le portefeuille de sécurité de Splunk aide les entreprises qui ont fait le choix d'une stratégie multi-cloud à superviser la fonctionnalité et la disponibilité de leurs nombreux services cloud au sein d'une interface unique, pour garantir la sécurité et la conformité de leur environnement multi-cloud. La plateforme permet également de déployer des services cloud tiers en toute confiance.

Lancez-vous.

Prêt à découvrir comment acquérir une meilleure visibilité et renforcer la sécurité de votre environnement multi-cloud ? Découvrez pourquoi utiliser Splunk comme SIEM permet d'éviter les interruptions de service et de détecter les vulnérabilités avant qu'elles ne deviennent problématiques.

En savoir plus

splunk> turn data into doing™