DESCRIPTIF DE LA SOLUTION IDC

la valeur économique des solutions SDN de sécurité pour les centres de données

Sponsorisé par : Cisco

Pete Lindstrom Richard L. Villars
Matthew Marden
18/05/2015

Présentation

Pour fournir un service optimal à leurs clients et améliorer les résultats de l'entreprise, les directeurs informatiques, les responsables des technologies et les architectes d'applications dépendent des systèmes qui gèrent les interactions et les informations au sein de l'entreprise. Disposer d'équipements capables de gérer, dans le centre de données, les nombreuses fonctionnalités de traitement des contenus, d'analyse de larges volumes de données et d'archivage qui sont associées à ces systèmes est donc indispensable. De fait, il faut qu'ils améliorent leurs centres de données existants, qu'ils accélèrent la création de nouveaux centres dans de nouvelles zones géographiques et qu'ils tirent pleinement parti des centres de données de pointe conçus, développés et gérés par des sociétés tierces. Pour IDC, cette transformation des centres de données et des entreprises traduit le passage à une nouvelle et « troisième plateforme ».

Aujourd'hui, cette plateforme est au cœur de presque toutes les innovations avec des centaines de milliers de solutions et de services révolutionnaires qui vont bouleverser l'expérience des clients. Ce changement affecte toutes les fonctions du département informatique, que ce soit au niveau de l'achat de matériel, de la conception, des opérations, du développement, ou de la gestion des ressources ou des données à long terme. Ce nouvel environnement pour centres de données est plus dynamique, plus axé sur les données et plus que jamais en butte à des risques qui doivent être gérés et éliminés. De fait, l'architecture réseau de nouvelle génération devient un élément essentiel.

Ce nouveau modèle architectural doit dépasser les limites technologiques et opérationnelles des architectures réseau traditionnelles pour répondre aux critères exigés par les centres de données et requis par les charges de travail de cette troisième plateforme. Ainsi, l'architecture de mise en réseau définie par logiciel (« software-defined network » ou SDN), qui implique une dissociation du plan de contrôle du réseau du plan de transmission des données a été conçue pour fournir un réseau plus agile et plus flexible aux entreprises qui établissent des environnements cloud.

L'infrastructure axée sur les applications (« application-centric infrastructure » ou ACI) de Cisco a été créée pour répondre aux besoins des opérateurs de centres de données en matière d'automatisation du provisionnement, de programmation de la gestion et d'organisation générale. Plutôt que de dissocier le plan de contrôle du plan de données, l'ACI repose sur un modèle conçu pour tenir compte des besoins des applications et pour automatiser le déploiement sur le réseau, que les applications soient virtualisées ou physiques. Cette approche correspond à ce que Cisco désigne sous le nom de « modèle de gestion déclarative », soit la coopération volontaire d'individus ou d'agents qui présentent

leurs intentions par des engagements les uns envers les autres. Ces intentions sont abstraites. Ainsi, une politique d'application pourrait présenter les besoins de cette dernière, et l'infrastructure sous-jacente (par exemple les commutateurs du centre de données) interpréter les données et déterminer le meilleur moyen de satisfaire à ces exigences en fonction de ses propres capacités.

OpenStack propose une autre option réseau pour le cloud computing. Elle offre un cadre par défaut, appelé Neutron, pour les clients utilisant des services réseau, ainsi qu'un ensemble d'API de communication ascendante ou descendante. OpenStack comprend une architecture modulaire qui offre à chaque client la liberté de sélectionner un système principal qui répond à ses besoins. Certains clients optent tout d'abord pour l'implémentation de référence proposée par défaut, qu'ils complètent ensuite avec des extensions fournies par les prestataires en fonction de leur utilisation et de leurs besoins en matière de réseau.

Les grandes forces de transformation du centre de données

De nombreux facteurs externes affectent directement ou indirectement les opérations et les investissements liés aux centres de données. Ces facteurs sont de différentes natures : commerciale, ou sociale, culturelle ou politique, ou bien encore technologique.

- **Le facteur commercial :**
  - **Le « tout service » :** le changement des modèles de financement des ressources numériques et physiques entraîne une restructuration des pratiques internes en matière de budget, de coût et d'investissements.
  - **La numérisation croissante des entreprises :** la transition d'un modèle commercial physique à un modèle numérique modifie considérablement les taux de croissance des données, les besoins de performances et les exigences fonctionnelles informatiques.
  - **L'enchevêtrement des secteurs d'activité :** l'extension des écosystèmes commerciaux conduit à une normalisation des connexions et des échanges de données entre les entreprises et les différents secteurs d'activité.
- **Le facteur social, culturel et politique :**
  - **Les normes d'utilisation des données :** les opinions individuelles et les lois de chaque pays en matière de collecte, de conservation et d'utilisation des données personnelles et de propriété intellectuelle sont particulièrement fragmentées et volatiles.
  - **L'exploitation des données :** les nations, les entreprises et les organisations criminelles ont institutionnalisé l'existence d'une guerre informatique dans le cyberespace.
  - **L'engagement et l'interaction avec les clients :** les médias sociaux constituent un lieu privilégié d'échange direct entre les entreprises et leurs clients, et entre les clients eux-mêmes, créant ainsi un besoin constant de renouvellement et de mise à jour des informations.
- **Le facteur technologique :**
  - **L'Informatique modularisée :** l'utilisation de modèles de packaging hyperévolutifs définis par logiciel, convergés ou sur le cloud, modifie le mode d'achat et de gestion des unités informatiques de base.
  - **Le poids des données :** les données utilisées pour les interactions avec les clients et les données utilisées pour accroître la visibilité de l'entreprise sont désormais, et de plus en plus, générées, collectées et archivées dans les centres de données des prestataires de service.

- **L'Informatique à géométrie variable :** la demande de prise en charge d'analyses ou de campagnes mobiles éphémères oblige les départements informatiques à acheter, déployer et redéployer des équipements très rapidement et pour de courtes périodes.

Le remaniement et la redéfinition des centres de données et des ressources informatiques causés par ces différents facteurs affectent aussi considérablement les réseaux étendus des entreprises. Ainsi, celles-ci devront modifier leurs connexions existantes reliant les centres de données internes aux équipements des prestataires tiers. Elles devront également s'adapter à des changements importants dans la gestion du trafic, à savoir apprendre à gérer un trafic plus important, plus mobile et moins prévisible.

Le rôle de la sécurité dans les centres de données modernes

Pour accompagner ces changements et l'évolution rapide de leurs charges de travail, les centres de données ont besoin de solutions de sécurité plus agiles et plus souples. Avec chaque type d'utilisation, la sécurité prend un sens différent : intégrité, fidélité, visibilité, contrôle du contenu et des données. Les départements informatiques ont besoin d'une plateforme commune afin de mettre en place de façon rapide et fiable un large éventail de fonctionnalités de sécurité dans les centres de données, et ce, à l'échelle de l'entreprise.

Au niveau du réseau, la fonctionnalité de sécurité intégrée comprend la surveillance (détection des intrusions), la segmentation de l'accès au réseau gérée par des politiques (pare-feu) et le cryptage des communications (réseau privé virtuel). Pourtant, les entreprises traitent souvent les ressources des centres de données de façon globale, ne faisant aucune distinction en termes d'usage ou de niveau de risques. Cette approche leur permet de placer toutes les ressources dans une seule et grande « zone » pour ne concentrer leur protection que sur les seuls points d'entrée et de sortie de ce périmètre (parfois aussi appelés points d'accès « Nord » ou «Sud »).

Au fur et à mesure que les centres s'étoffent et se transforment en larges ensembles de ressources qui fournissent toute une gamme de fonctionnalités à des départements différents de l'entreprise, à des utilisateurs et des plateformes multiples et variés, la sécurité doit aussi évoluer pour protéger ces ressources toujours plus dynamiques et riches contre des menaces plus ciblées. Les entreprises doivent réfléchir à la façon dont elles gèrent le partage des ressources, la surveillance et le cryptage des communications à un niveau plus détaillé.

Les centres de données modernes doivent déterminer comment déployer leurs systèmes de prévention et de détection des intrusions et la segmentation de leur pare-feu afin de savoir où redéployer les contrôles existants et si de nouvelles fonctionnalités sont nécessaires pour couvrir les communications « Est » et « Ouest » entre les serveurs et les autres ressources. L'exercice implique notamment d'identifier de plus petits ensembles de ressources, généralement au niveau des applications, mais sans pour autant exclure d'autres niveaux, et d'insérer plus de contrôles et de surveillance pour gérer le trafic entre les applications.

Avec l'augmentation des contrôles déployés dans les centres de données, le recours à des fonctionnalités de gestion centralisée devient indispensable. En outre, les ressources protégées étant plus dynamiques et plus mobiles, les fonctions de sécurité doivent s'adapter aux nouvelles architectures.

Cette analyse IDC repose sur les études réalisées par IDC auprès des utilisateurs des produits de sécurité dans le paysage en pleine mutation des centres de données. Elle chiffre les bénéfices potentiellement réalisables, soit un gain de productivité de 33,5 % pour les activités liées à la sécurité

informatique, une baisse de 80,7 % des temps d'arrêt non planifiés dus aux attaques et aux menaces pour la sécurité, et un déploiement 63,3 % plus rapide des nouvelles applications et des nouveaux services de sécurité. Annuellement, pour une entreprise de 1 000 utilisateurs, les gains liés à une meilleure fiabilité se chiffrent à 48 700 dollars, les gains liés à la performance du département informatique à 71 700 dollars, et ceux liés à l'amélioration des opérations à 92 600 dollars.

Les bénéfices des solutions de sécurité pour les centres de données de nouvelle génération

Les solutions de sécurité pour les centres de données de nouvelle génération doivent permettre aux entreprises d'optimiser au mieux leurs investissements dans ces centres. Pour ce faire, ces solutions doivent être intégrées, robustes, agiles, évolutives et basées sur des politiques. Bien conçues et implémentées, les solutions de sécurité pourvues de ces caractéristiques créent de la valeur : elles simplifient et accélèrent la gestion et le provisionnement des solutions de sécurité, elles réduisent l'impact commercial et opérationnel des menaces pour la sécurité et elles garantissent que la sécurité n'entrave pas la capacité des centres de données à soutenir et dynamiser l'activité des entreprises. De telles solutions de sécurité offrent aux centres de données de nouvelle génération les avantages suivants :

- **Elles sont intégrées pour offrir de meilleures performances et réduire les risques.** Les solutions de sécurité qui s'intègrent à la fois aux solutions prenant en charge les environnements de centres de données traditionnels des entreprises et aux autres produits de sécurité utilisés dans l'environnement des centres de données de nouvelle génération permettent de gagner du temps et de réduire les risques. En outre, l'intégration réduit le temps nécessaire aux équipes de sécurité pour recréer les politiques et éliminer les silos de sécurité informatique inefficaces et coûteux. Elle réduit enfin le temps d'exposition des applications et des services aux éventuelles menaces pour la sécurité.
- **Elles sont simplifiées pour faciliter les opérations de gestion.** Les produits de sécurité des centres de données de nouvelle génération sont employés dans des environnements qui reposent sur l'automatisation et l'orchestration. Pour s'adapter à ce type d'environnement, ces produits de sécurité doivent donc aussi utiliser des politiques pour activer leur provisionnement en tant que service. Ils accompagnent ainsi l'architecture globale des centres de nouvelle génération et optimisent également la productivité des équipes de sécurité informatique qui passent moins de temps à gérer et administrer les paramètres, la configuration et le déploiement des solutions de sécurité.
- **Elles sont dotées de fonctionnalités robustes permettant de réduire l'impact des menaces pour la sécurité.** Les produits de sécurité dans les centres de données de nouvelle génération doivent fournir une gamme complète de fonctionnalités sécuritaires qui couvrent tout le trafic entrant ou sortant, et les déplacements au sein du centre. Cela permet aux entreprises de réduire l'impact des menaces sur les utilisateurs et leurs activités. Les utilisateurs disposent de plus de temps pour être performants et l'entreprise bénéficie de la réduction des interruptions d'activité.
- **Elles sont agiles et évolutives pour soutenir l'activité de l'entreprise grâce à leurs applications.** Les centres de données de nouvelle génération sont configurés pour soutenir les opérations commerciales en simplifiant la gestion des applications et en accélérant leurs cycles de développement. Pour atteindre cet objectif, les produits de sécurité doivent pouvoir être déployés à tout moment et le plus rapidement possible pour réduire les délais de commercialisation.

L’infrastructure Cisco axée sur les applications

Les réseaux définis par logiciel (SDN) séparent les fonctionnalités de plan de contrôle des fonctionnalités de plan de données et sont souvent définis en termes très précis. La sécurité définie par logiciel reprend la philosophie et l’architecture fondamentale des réseaux SDN, mais en élargit les possibilités en s’intégrant à un plus grand nombre d’environnements. Le modèle SDN de « réseau en étoile » lie un contrôleur où les politiques de sécurité sont définies et évaluées à des nœuds qui appliquent ces politiques, le tout de façon dynamique et en temps réel. L'utilisation d'un langage de politique au niveau de la couche applicative permet aux politiques applicables d'être déployées dans les nœuds appropriés afin de garantir une certaine flexibilité et l'alignement avec les composants de l'application en cours d'utilisation. Le résultat est une architecture réseau plus facile à gérer et une efficacité optimisée.

L'infrastructure axée sur les applications (ACI) de Cisco a été conçue pour répondre aux besoins des centres de données modernes en matière de sécurité et de données. Elle est gérée par un contrôleur central, l'APIC (« Application Policy Infrastructure Controller »). Le module APIC contrôle l'ensemble des périphériques de sécurité du centre de données, virtuels ou physiques. De fait, ces périphériques sont étroitement surveillés et associés aux ressources qu'ils protègent. Ce contrôleur peut provisionner et gérer des périphériques de sécurité et réseau Cisco, et prendre en charge un écosystème de prestataires de sécurité tiers. En outre, il intègre des fonctionnalités supplémentaires pour la prise en charge d'autres sociétés tierces.

Sachant tirer profit de l’architecture de sécurité existante d’une entreprise, l’ACI Cisco permet aux entreprises d’exploiter les contrôles de sécurité physique existants tout en augmentant le nombre de contrôles fonctionnels dans les machines virtuelles ou physiques afin de protéger les communications « Est-Ouest » de plus en plus importantes. Pour gérer les ressources dynamiques d’une entreprise moderne, il est possible de créer des politiques, de les associer à un profil d’application, puis de les distribuer dans un environnement. De cette façon, les ressources se déplacent avec la politique appropriée.

L'infrastructure ACI offre ainsi aux entreprises qui ont investi massivement dans les solutions de sécurité Cisco et qui disposent d'un ensemble établi de politiques de sécurité la possibilité d'éviter une restructuration complète de l'architecture de leur centre de données et d'opter pour une évolution en toute sécurité et en douceur. Elle permet également de répondre aux nouveaux besoins des architectures virtualisées et distribuées garantissant que l'entreprise bénéficie d'un niveau de sécurité approprié.

Les bénéfices chiffrés des solutions de sécurité pour les centres de données de nouvelle génération

Le tableau 1 présente une mesure des bénéfices potentiels pour les entreprises utilisant des solutions de sécurité dans les centres de données de nouvelle génération, selon une étude IDC en cours.

La figure 1 présente les gains de productivité sur un an des employés et du département informatique résultant de l'utilisation de solutions de sécurité dans les centres de données de nouvelle génération pour une entreprise de 1 000 utilisateurs.

TABLEAU 1

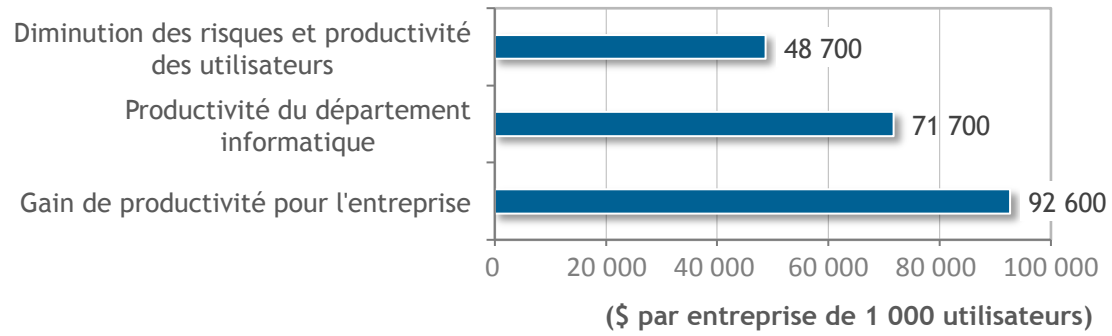
Gains résultant de l'utilisation de produits de sécurité dans les centres de données de nouvelle génération

	(%)
Gains de productivité du département informatique	
Temps en moins consacré à la gestion de la sécurité	33,5
Augmentation du nombre de menaces pour la sécurité détectées de façon proactive	50,9
Temps en moins consacré à la gestion des menaces pour la sécurité	82,1
Bénéfices en termes de diminution des risques et de productivité de l'entreprise	
Réduction des temps d'arrêt non planifiés	80,7
Gains de productivité pour l'entreprise	
Temps en moins consacré au déploiement des solutions de sécurité	63,8

Source : IDC, 2015

FIGURE 1

Bénéfices représentatifs sur un an pour une entreprise comptant 1 000 utilisateurs appliquant des solutions de sécurité dans les centres de données de nouvelle génération



Source : IDC, 2015

Annexe : méthodologie employée pour l'étude

Les données utilisées dans ce document ont été recueillies par IDC au cours d'entretiens menés chaque année au sein d'entreprises utilisant des solutions de sécurité pour leurs centres de données. Nous avons exprimé les résultats en dollars pour une entreprise type qui compte 1 000 utilisateurs. Pour chiffrer les bénéfices liés aux activités du département informatique, IDC a multiplié les gains de temps et de performances par un salaire annuel moyen de 100 000 dollars. Un salaire de 70 000 dollars a été utilisé pour chiffrer les gains de temps et de productivité pour les utilisateurs ne faisant pas partie du département informatique.

À propos de IDC

International Data Corporation (IDC) est le premier fournisseur mondial d'informations commerciales, de services consultatifs et d'événements pour les marchés des technologies de l'information, des télécommunications et des technologies grand public. IDC aide les professionnels de l'informatique, les dirigeants d'entreprise et les investisseurs à prendre des décisions fondées sur des faits en matière d'achats technologiques et de stratégie d'entreprise. Plus de 1 100 analystes IDC effectuent une expertise mondiale, régionale et locale sur les opportunités et tendances des secteurs technologiques et industriels dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC fournit des analyses stratégiques pour aider ses clients à atteindre leurs objectifs d'entreprise importants. IDC est une filiale d'IDG, le leader mondial en supports de technologie, de recherche et d'événements.

Siège mondial

5 Speen Street
Framingham, MA 01701
États-Unis
508.872.8200
Twitter : @IDC
idc-insights-community.com
www.idc.com