Lâ□□argument financier en faveur de la sÃ©curitÃ© dans le cloud
Internet
PostÃ© par : JulieM
PubliÃ©e le : 15/4/2022 13:00:00

D'aprÃ¨s Gartner, d'ici Ã 2025, 51 % des dÃ©penses IT des dÃ©partements informatiques d'entreprise qui pourront migrer dans le cloud seront consacrÃ©es au cloud.

A lâ□□Ã©poque oÃ¹ le Cloud sâ□□est imposÃ© comme un nouveau modÃ¨le opÃ©rationnel pour le secteur IT, son faible coÃ»t total de possession (CTP) Ã©tait lâ□□un des principaux arguments de vente.

Pourtant, aujourdâ□□hui, nombreux sont ceux qui, lorsquâ□□ils envisagent de transfÃ©rer la sÃ©curitÃ© dans le Cloud, craignent que cela nâ□□entraÃ®ne une augmentation des coÃ»ts ou, tout du moins, un investissement initial difficile Ã justifier Ã moyen terme.

Selon Stanley Nabet, Regional Director France chez Netskope, la rÃ©alitÃ© est telle quâ□□une architecture Secure Service Edge (SSE) native du Cloud offre un solide retour sur investissement avec un faible coÃ»t total de possession. La capacitÃ© Ã justifier ces Ã©lÃ©ments permet dâ□□obtenir plus facilement un budget pour la mise en Å□uvre dâ□□un projet de transformation de la sÃ©curitÃ© :

Â« Les entreprises peuvent rÃ©duire les coÃ»ts grÃ¢ce Ã lâ□□utilisation dâ□□une infrastructure Cloud partagÃ©e et au paiement de ce qui est nÃ©cessaire uniquement. Ã□volutivitÃ© Ã la demande, sans nÃ©cessitÃ© de rÃ©organisation, câ□□est le modÃ¨le Ã©conomique classique du cloud.

Les entreprises ne doivent pas financer de surcapacitÃ©, ni parier sur la croissance ou le recul, ni risquer dâ□□Ãªtre perturbÃ©es par des fusions-acquisitions ou des rÃ©ductions dâ□□effectifs difficiles Ã prÃ©voir.

Avec le Cloud, les organisations ont la possibilitÃ© de sâ□□adapter Ã des modÃ¨les de travail en constante Ã©volution, tels que le travail Ã distance ou hybride, sans avoir Ã Ã©laborer des politiques destinÃ©es Ã tirer profit des dÃ©cisions dâ□□achat antÃ©rieures.

Lorsque la sÃ©curitÃ© dâ□□une organisation se trouve dans le Cloud, elle peut ajouter des effectifs et les rÃ©orienter sans se soucier de la flexibilitÃ© et de la valeur de lâ□□infrastructure existante.

De plus, la rapiditÃ© du dÃ©ploiement, ainsi que lâ□□Ã©limination des problÃ¨mes et des coÃ»ts liÃ©s Ã lâ□□approvisionnement physique sont des atouts majeurs. Au dÃ©but de la pandÃ©mie, les Ã©quipes ont dÃ» apporter des changements rapides aux infrastructures pour prendre en charge une relocalisation complÃ¨te des employÃ©s.

Et, au moment oÃ¹ la demande Ã©tait pressante, les fournisseurs de matÃ©riel informatique Ã©prouvaient eux aussi des difficultÃ©s Ã fabriquer et Ã expÃ©dier les appareils requis. Pour lâ□□essentiel, nous nous sommes relevÃ©s des effets initiaux de cette crise, mais de nouvelles menaces pÃ¨sent dÃ©sormais sur les chaÃ®nes de production et dâ□□approvisionnement mondiales, apportant leur lot dâ□□instabilitÃ© et de prix Ã©levÃ©s.

La sÃ©curitÃ© dans le cloud se dÃ©ploie dâ□□un simple clic et ne repose pas sur des expÃ©ditions coÃ»teuses ou des formalitÃ©s douaniÃ¨res, un argument de taille dans le contexte

actuel.

Par ailleurs, le routage du trafic vers le centre de donnÃ©es pour y appliquer les politiques de sÃ©curitÃ© est devenu trÃ¨s illogique Ã partir du moment oÃ¹ la main-dâÅuvre sâest dispersÃ©e et oÃ¹ la majeure partie du trafic sâest orientÃ©e vers les applications Cloud plutÃ´t que vers les applications du centre de donnÃ©es.

Si les utilisateurs travaillent Ã distance par exemple, le flux de trafic Ã destination et en provenance du centre de donnÃ©es ne sert plus quâÃ une seule chose, lâapplication des contrÃ´les de sÃ©curitÃ©, avec des rÃ©percussions nÃ©gatives sur lâexpÃ©rience et la productivitÃ© des utilisateurs.

Par le passÃ©, de nombreuses organisations ont investi dans des lignes MPLS onÃ©reuses pour connecter leurs bureaux, mais ce coÃ»t est considÃ©rablement rÃ©duit lorsque le trafic est dirigÃ© directement vers le rÃ©seau via un Security Service Edge.

Avec une approche intÃ©grÃ©e de la sÃ©curitÃ© dans le Cloud fournie par le SSE, les entreprises ont lâopportunitÃ© dâÃ©laborer des politiques de sÃ©curitÃ© homogÃ¨nes qui peuvent Ãªtre appliquÃ©es de maniÃ¨re cohÃ©rente dans lâensemble de leur infrastructure.

Les Ã©quipes se concentrent alors sur les Ã©lÃ©ments les plus importants, gÃ©rer les alertes et les Ã©vÃ©nements, puis ajuster leurs contrÃ´les de sÃ©curitÃ© afin quâils soient les plus efficaces possible, rÃ©duisant ainsi le risque de compromissions de donnÃ©es.

Enfin, la rÃ©duction des coÃ»ts liÃ©s Ã la consommation dâÃ©nergie est Ã©galement un argument clÃ©, souvent nÃ©gligÃ©. La migration vers le Cloud entraÃ®ne en effet une rÃ©duction du nombre de racks dâappareils de rÃ©seau et de sÃ©curitÃ©, fonctionnant tous en mode Ã haute disponibilitÃ©, dans le centre de donnÃ©es.

Lâutilisation dâune infrastructure partagÃ©e et la rÃ©percussion des coÃ»ts de consommation dâÃ©nergie sur le fournisseur de sÃ©curitÃ© dans le cloud permettent ainsi de rÃ©duire considÃ©rablement les charges, tout en contribuant Ã la mise en place dâun programme Ã©cologique visant Ã exploiter les services de la maniÃ¨re la plus efficace possible.

De nombreuses ressources et un budget important seront investis au cours des prochains mois au nom de la transformation. Si une majoritÃ© de DSI et de RSSI font dÃ©jÃ Ã©tat d'Ã©conomies rÃ©sultant du passage de la sÃ©curitÃ© dans le Cloud, les entreprises doivent prendre la mesure de lâintÃ©rÃªt de ce transfert.

Il permet en effet de rÃ©duire le coÃ»t total de possession en matiÃ¨re de sÃ©curitÃ© tout en augmentant leur capacitÃ© Ã protÃ©ger leurs actifs ; un enjeu majeur alors que les cybermenaces sont omniprÃ©sentes. Â»