Le travail hybride, de nombreuses variables Ã surveiller et protÃ©ger
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 16/12/2022 13:00:00

Depuis plus de deux ans, lâheure est au travail hybride, les collaborateurs pouvant effectuer leurs tÃ¢ches depuis leur domicile, comme au bureau. AprÃ¨s un tÃ©lÃ©travail Â« forcÃ© Â» par la pandÃ©mie, ce nouveau modÃ¨le satisfait aujourdâhui de plus en plus dâemployÃ©s, qui peuvent Ã©quilibrer leur vie professionnelle et privÃ©e Ã leur guise.

Toutefois, l'emplacement du bureau n'est pas la seule variable ajustable dans cette nouvelle normalitÃ©. Les appareils, les applications, jusquâaux identitÃ©s et aux structures organisationnelles sont dÃ©sormais hybrides, ce qui conduit Ã l'Ã©mergence de nouveaux dÃ©fis de sÃ©curitÃ©.

Pour Julien Fournier, VP Southern Europe chez Netskope, toutes ces variables doivent Ãªtre prises en compte et Ã©tudiÃ©es pour une sÃ©curitÃ© optimale, quel que soit le lieu oÃ¹ le collaborateur se trouve.

Â« Aujourd'hui, les approches hybrides sont motivÃ©es par des exigences de flexibilitÃ© et d'agilitÃ©, et, si elles sont correctement implÃ©mentÃ©es, les environnements de travail hybrides ont le potentiel de crÃ©er un avantage concurrentiel significatif. Pour ce faire, quatre grands piliers sont Ã prendre en compte : lâemplacement, les appareils, les applications et les services, et la main dâÅuvre.

â¢ Lâemplacement hybride : câest le pilier le mieux apprÃ©hendÃ© et compris actuellement par les entreprises et les collaborateurs. Une rÃ©ticence existe en effet Ã retourner au bureau cinq jours par semaine, ce qui pousse Ã lâhybridation du lieu de travail.

Pour les professionnels de la sÃ©curitÃ©, un environnement fixe permet de mettre en place une protection de pÃ©rimÃ¨tre physique et oÃ¹ les rÃ©seaux sont connus et fiables. Or, lorsque les employÃ©s accÃ¨dent Ã des systÃ¨mes en dehors de cet environnement hautement provisionnÃ© et sÃ©curisÃ©, des exigences potentiellement supplÃ©mentaires peuvent Ãªtre nÃ©cessaires pour sÃ©curiser les rÃ©seaux.

â¢ Appareils hybrides : avant la pandÃ©mie, les problÃ¨mes de sÃ©curitÃ© concernant les appareils Ã usage mixte se concentraient sur le "bring your own device" (BYOD). Mais, depuis deux ans, les appareils professionnels ont Ã©tÃ© de plus en plus utilisÃ©s Ã des fins personnelles - pour de l'enseignement Ã domicile ou des appels vidÃ©o notamment.

Certaines organisations ont effectivement dÃ» Ã©quiper rapidement leurs employÃ©s d'ordinateurs portables et d'appareils mobiles pour maintenir lâactivitÃ© au moment des restrictions sanitaires. Ainsi, de nouvelles habitudes se sont formÃ©es et il faut dÃ©sormais prendre en compte que ces appareils servent Ã©galement pour un usage personnel, et en dehors des heures de travail.

â¢ Applications et services hybrides : auparavant, les applications professionnelles Ã©taient diffÃ©rentes de celles utilisÃ©es Ã domicile. De nos jours, les logiciels non managÃ©s, ainsi que les services cloud non gÃ©rÃ©s, sont utilisÃ©s quotidiennement Ã des fins professionnelles et personnelles, par de nombreux collaborateurs.

En effet, selon nos recherches, 97 % des applications et services cloud utilisÃ©s par les organisations moyennes sont identifiÃ©s comme Ã©tant du "shadow IT", et donc non gÃ©rÃ©s. Ce surplus de complexitÃ© existe car les applications managÃ©es, utilisÃ©es dans une entreprise (telles que les applications cloud Microsoft et Google, ou les services SaaS et IaaS comme Box ou AWS) sont Ã©galement disponibles en tant que produits grand public.

Or, si le mÃªme appareil est utilisÃ© pour accÃ©der aux instances professionnelles et personnelles du mÃªme service cloud, la grande majoritÃ© des systÃ¨mes de sÃ©curitÃ© traditionnels sont incapables de le dÃ©tecter ou de le contrÃ´ler.

â¢ Main-d'Åuvre hybride : pour rester compÃ©titives, les organisations doivent souvent rÃ©duire ou augmenter rapidement leurs effectifs, externaliser, se dÃ©velopper sur de nouveaux marchÃ©s par le biais de fusions et d'acquisitions, ou mÃªme abandonner certaines activitÃ©s non essentielles par le biais d'une cession.

La main-d'Åuvre n'est donc plus une entitÃ© unique qui peut facilement Ãªtre rÃ©gie par des politiques uniformes. Il s'agit d'un mÃ©lange de types de contrats divers et soumis Ã diffÃ©rentes lÃ©gislations. Chacun de ces segments de la main-d'Åuvre nÃ©cessite diffÃ©rents niveaux d'accÃ¨s aux systÃ¨mes et potentiellement des privilÃ¨ges d'accÃ¨s qui changent Ã©galement rÃ©guliÃ¨rement.

Ainsi, l'hybride va plus loin que le simple bureau, et chaque pilier indique qu'il est nÃ©cessaire de repenser la sÃ©curitÃ©, afin d'attÃ©nuer les risques et de soutenir la productivitÃ©. Pour protÃ©ger ces nouveaux modÃ¨les de travail hybrides, le Security Service Edge (SSE) semble Ãªtre la solution adaptÃ©e.

Ce dernier est une pile de sÃ©curitÃ© native du cloud centrÃ©e sur les donnÃ©es, et pilotÃ©e par une politique cohÃ©rente avec des rapports unifiÃ©s. Il comprend donc tous les services requis pour activer et sÃ©curiser les donnÃ©es partout oÃ¹ elles s'aventurent : dans des applications cloud, sur internet et dans des datacenters privÃ©s.

L'emplacement des employÃ©s, sous-traitants et partenaires, les appareils qu'ils utilisent, ainsi que les applications non managÃ©es, sont observÃ©s et ces informations sont utilisÃ©es pour mettre en place les politiques de sÃ©curisation des donnÃ©es de maniÃ¨re appropriÃ©e.

GrÃ¢ce Ã une architecture de sÃ©curitÃ© capable de protÃ©ger les donnÃ©es oÃ¹ qu'elles se dÃ©placent ainsi que dâagir en temps rÃ©el, lâentreprise est alors Ã mÃªme de rÃ©pondre aux dÃ©fis et opportunitÃ©s auxquels elle est confrontÃ©e.

Les modÃ¨les de travail hybrides entraÃ®nent donc une rÃ©architecture complÃ¨te de la sÃ©curitÃ© pour qu'elle soit native du cloud et centrÃ©e sur les donnÃ©es ; ce qui permet in fine aux entreprises de pouvoir sâadapter Ã toute Ã©volution technologique facilement ! Â»