LIVRE BLANC

Travail hybride : la complexité n'est pas une fatalité

La sécurité doit être omniprésente, où que se trouvent les utilisateurs

Synthèse

Sur les dix dernières années, la technologie a su apporter aux collaborateurs davantage de flexibilité dans le choix des dispositifs qu'ils utilisent, les lieux où ils travaillent et les ressources auxquelles ils accèdent. Le BYOD (Bring your own device) et l'accès aux applications cloud constituaient les premières étapes de cette flexibilité.

Si les entreprises se préparaient déjà à mettre en œuvre une stratégie de travail hybride (WFA pour Work From Anywhere) pour les années à venir, la pandémie de COVID-19 a créé l'urgence. Désormais, les collaborateurs sont demandeurs de ce télétravail et le défi est de savoir comment offrir une expérience de travail hybride qui assure la productivité et la sécurité des collaborateurs.

Selon le rapport sur le panorama mondial des menaces, les incidents par ransomware ont bondi de près de 1 100 % entre juin 2020 et juin 2021.[1]

Sécuriser le travail hybride

Lorsque la récente pandémie a frappé le monde, peu d'entreprises étaient préparées au télétravail. Les collaborateurs se sont retrouvés, du jour au lendemain, obligés de se connecter à distance à leur bureau, à partir de réseaux résidentiels peu ou prou sécurisés. Le contrôle d'accès n'était pas adapté et les dispositifs utilisés vulnérables. Sans surprise, les cybercriminels ont été véloces à tirer parti de ces points faibles. Ainsi, Forrester indiquait récemment que 67 % des entreprises avaient été ciblées par une cyberattaque exploitant les vulnérabilités associées au télétravail.[2]

Pour l'avenir, nombre d'entreprises envisagent de pérenniser le télétravail, tout du moins à temps partiel. Elles ont déjà investi dans des outils et solutions pour aider leurs collaborateurs à rester productifs dans un contexte de télétravail qui a gagné ses lettres de noblesse.

Le collaborateur hybride travaille ainsi de son bureau quelques jours par semaine et de chez lui le reste du temps. Il doit pouvoir naviguer en toute transparence entre ces deux environnements. Où qu'il se situe, il doit pouvoir accéder en toute sécurité aux applications et ressources présentes dans le cloud ou le data center.

Pour accompagner le travail hybride, les entreprises doivent envisager sa sécurité et déployer des solutions capables d'accompagner et de protéger les utilisateurs, où qu'ils se trouvent. La sécurité des terminaux (endpoints) doit être associée au ZTA (zero-trust access) et au ZTNA (zero-trust network access). La sécurité de la connectivité réseau soit être assurée par un SD-WAN (software-defined wide-area networking) sécurisé et par une solution SASE (secure access service edge). Les moteurs de règles doivent permettre un accès sur la base de l'utilisateur, de sa localisation, du type de dispositif utilisé et de sa posture de sécurité.

De nombreuses entreprises envisagent de protéger le travail hybride en utilisant des solutions issues de multiples fournisseurs. Ainsi, un éditeur assurera la protection des terminaux, un autre proposera sa solution EDR (endpoint detection and response), un troisième aura la charge de gérer les identités, et ainsi de suite. On imagine ainsi que des pare-feux différents protègeront le data center, les sites distants et les différentes plateformes cloud utilisées. Face à cette hétérogénéité, définir une solution unique globale, fiable et cohérente relève de la gageure. Tout comme faire collaborer ces différents outils entre eux. Enfin, c'est la maintenance de ces systèmes qui mobilise fortement les équipes IT.

Il est donc préférable de déployer des solutions qui seront toutes intégrées au sein d'une plateforme mesh de cybersécurité. Cette plateforme renforce la sécurité, facilite les tâches de gestion et d'orchestration et se veut plus économique que de faire appel à de multiples solutions cloisonnées.

Une protection omniprésente

Le travail hybride exige une sécurité opérationnelle, que l'utilisateur soit présent au bureau, à son domicile ou en déplacement. Chacun de ces lieux de travail exige une technologie spécifique pour assurer une protection complète.

L'enquête Fortinet Global Ransomware Survey indique que 67 % des entreprises ont été la cible d'un ransomware.[3]

Télétravail à domicile

Puisque les entreprises utilisent nombre d'applications métiers, il devient essentiel de sécuriser en profondeur l'accès à ces applications, les réseaux qui permettent de s'y connecter, ainsi que les dispositifs/équipements qui hébergent ces applications. Les données clients, les serveurs, les applications, les informations d'identité, les identifiants de connexion et les codes sources sont souvent hébergés au niveau des sièges sociaux d'entreprise. La sécurité des utilisateurs, des dispositifs et des serveurs au bureau exige des pare-feu de nouvelle génération (NGFW) en tant que première ligne de défense pour protéger ces informations critiques. Les entreprises doivent associer ces NGFW à des solutions de sécurité des terminaux, zero-trust et de gestion des identités :

- Les NGFW sécurisent les accès externes via une sécurité sophistiquée et cohérente sur les campus corporate, les data centers, les sites distants et les environnements cloud.
- Les agents ZTNA et les services d'identité contrôlent et sécurisent l'accès aux applications et autres ressources. Le ZTNA permet un contrôle interne qui surveille l'accès aux applications, en chiffrant les tunnels au bureau et en validant les utilisateurs.
- Une sécurité des terminaux de type EDR pour protéger les utilisateurs et dispositifs. L'EDR offre les moyens de sécuriser les dispositifs des utilisateurs et interagit avec les données critiques.

Les environnements de bureau doivent également intégrer des solutions réseau et de sécurité, à l'instar d'un SD-WAN sécurisé, qui offre des outils réseau sophistiqués conçus pour opérer dans le cadre d'une plateforme de sécurité unifiée, capable d'optimiser la connectivité WAN entre les data centers, les clouds, les sites distants et les campus d'entreprise.

Télétravail du domicile

Les collaborateurs distants et hybrides se connectent généralement depuis un bureau résidentiel, à l'aide d'un PC portable, d'un moniteur et d'une webcam. Ces réseaux résidentiels sont souvent peu sécurisés car faisant appel à des routeurs grand public et hébergeant nombre d'objets connectés vulnérables face à des hackers. Les collaborateurs qui utilisent des réseaux résidentiels rencontrent également des défis dans leur activités exigeant une bande passante importante, à l'image des visioconférences. Celles-ci peuvent être perturbées si d'autres membres du foyer utilisent conjointement la bande passante pour du streaming vidéo ou des jeux en ligne. Les télétravailleurs à la maison ont besoin des éléments suivants :

- Une sécurité des terminaux, de type EDR, pour protéger l'utilisateur et ses dispositifs.
- Des agents ZTNA et des services d'identité pour contrôler et sécuriser les accès aux applications et autres ressources
- Une sécurité professionnelle des réseaux résidentiels pour sécuriser l'accès aux réseau corporate et aux applications dans le cloud ou le data center. Cette sécurité doit pouvoir prioritiser le trafic métier par rapport au streaming vidéo ou au jeu en ligne.

Une solution dédiée aux réseaux résidentiels doit pouvoir étendre les fonctions du pare-feu corporate à la totalité des réseaux résidentiels. Elle doit également segmenter le réseau résidentiel pour offrir une visibilité sur le trafic corporate, optimiser la bande passante allouée aux applications métiers, tout en assurant la confidentialité des collaborateurs dans le activités privées.

Télétravail en déplacement

Les utilisateurs en déplacement ou travaillant en dehors de leur bureau ou de leur lieu principal de télétravail s'exposent souvent à des menaces. Lorsque les utilisateurs mobiles se connectent aux applications et ressources nécessaires à leur travail, ils sont susceptibles d'utiliser des réseaux et points d'accès inconnus et non-sécurisés pouvant mettre en péril le réseau. Les utilisateurs nomades ont besoin des éléments suivants :

- Une sécurité des terminaux, de type EDR, pour l'utilisateur et ses dispositifs.
- Des agents ZTNA et des services d'identité pour contrôler et sécuriser les accès aux applications et autres ressources
- Des solutions SASE de sécurité des réseaux distants pour offrir un pare-feu cloud et sécuriser les collaborateurs hors du réseau corporate ou résidentiel

Une solution de réseau mobile doit offrir une authentification multifactorielle, une passerelle de sécurité web basée dans le cloud et une solution CASB (cloud access security broker)

Une sécurité intégrée du travail hybride associée à une veille sur les menaces

En support du travail hybride, les entreprises doivent identifier une plateforme mesh de cybersécurité qui fonctionne en tant que système intégré et proposant une veille décisionnelle sur les menaces. Cette veille apporte aux produits de sécurité des informations essentielles d'identification des menaces et de protection, sur l'ensemble des lieux de travail. Cette approche orientée plateforme unifier la sécurité zero-trust, des terminaux et réseau grâce à des API et passerelles d'intégration, permettant à l'utilisateur de se déplacer en toute transparence d'un lieu à un autre, de manière totalement sécurisée.
La cybersécurité simplifie la création et l'application des règles, assure des configurations uniformes, centralise les fonctions de gestion et permet de surveiller les utilisateurs, dispositifs, données, applications et workflows.

Le travail hybride s'est généralisé dans le contexte de la crise sanitaire, mais cette dernière n'a fait qu'accélérer une tendance déjà perceptible. Ce mode de travail s'annonce pérenne et les entreprises doivent s'assurer d'être prêtes à l'adopter en toute sécurité.

[1] "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," Fortinet, août 2021.

[2] "Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work," Forrester, 2021

[3] "The 2021 Ransomware Survey Report," Fortinet, 3 novembre 2021.

FORTINET

www.fortinet.com/fr

mai 6, 2022 1:24 PM
1400814-0-0-FR