Assurer la sécurité de votre entreprise lorsque vous travaillez à distance

Sébastien Roche, Chief Information Security Officer chez Alcatel-Lucent Enterprise, nous présente l'approche d'ALE en matière de continuité des activités et de sécurité.

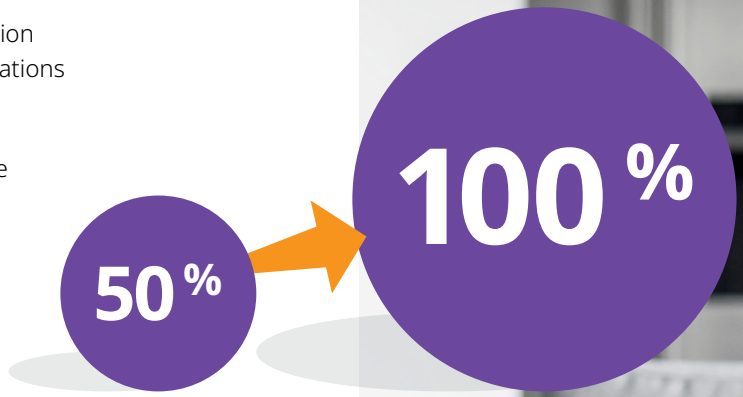
Brochure

Alcatel·Lucent
Enterprise

La nouvelle réalité du télétravail

Depuis 2020, les entreprises qui ne proposaient pas encore l'option du télétravail ont été mises au défi de transformer leurs organisations pour assurer la continuité de leurs activités et la sécurité.

Il y a plus de 15 ans, Alcatel-Lucent Enterprise a lancé une stratégie de télétravail pour plus de 50 % de ses collaborateurs répartis dans 50 bureaux dans le monde entier. Plus de la moitié des collaborateurs d'ALE étant en télétravail, nous disposions déjà du réseau et de l'architecture informatique nécessaires pour favoriser le travail à distance. Le défi consistait donc à savoir comment nous allions procéder pour permettre à 100 % de nos collaborateurs d'être en télétravail.

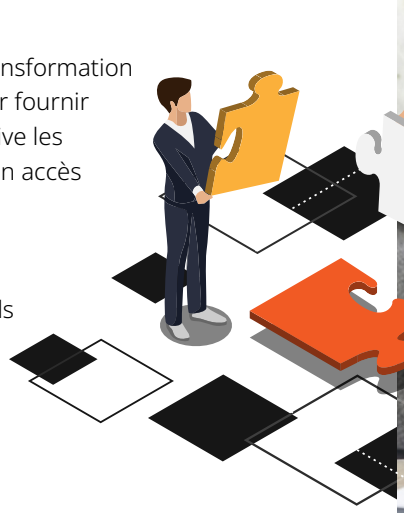


Se préparer à agir plus rapidement

Depuis près de 10 ans, ALE s'est engagée dans une vaste transformation informatique. Une architecture de réseau a été adoptée pour fournir une sécurité du cloud destinée à bloquer de manière proactive les menaces, à identifier les attaques potentielles et à garantir un accès sécurisé aux collaborateurs.

Cette transformation comprenait :

- La sécurité dans le cloud grâce à des points d'accès virtuels
- Le traçage en temps réel
- L'identification des comportements inhabituels afin de détecter les menaces



Brochure
Assurer la sécurité de votre entreprise en situation de télétravail

Brochure
Assurer la sécurité de votre entreprise en situation de télétravail

Préparation = réaction plus rapide en situation de crise

Lorsque la crise a frappé, il a été décidé le vendredi après-midi d'avoir recours au télétravail dès le lundi d'après. Les collaborateurs ont reçu l'instruction d'emporter leur ordinateur portable et leur écran informatique chez eux. Le lundi matin, le travail a débuté comme d'habitude, sans interruption, puisqu'ils ont pu commencer leur journée depuis leurs bureaux à distance. La transformation du réseau effectuée précédemment a ainsi permis d'assurer la sécurité de la connectivité à distance, quelle que soit la localisation des collaborateurs.

Le défi lié à l'accès

Les profils d'utilisateurs ont constitué un défi important pour notre plan de télétravail. En particulier, les équipes de R&D et de support technique ont besoin d'accéder à certains serveurs et plateformes de développement, ce que notre solution d'accès à distance ne permettait pas.

Au démarrage de la transition de tous les collaborateurs vers le télétravail, nous avons adapté notre infrastructure de façon à augmenter notre bande passante et à supporter l'augmentation du nombre de connexions à distance requises par les télétravailleurs.

La sécurité est la clé

La sécurité et la protection des données d'entreprise sont extrêmement importantes en période d'incertitude et touchent de nombreuses entreprises qui traitent des données sensibles, comme les organisations du secteur public, les ministères, les villes, grandes et moyennes.

Avant même de commencer à faire référence au télétravail chez ALE, nous avons déployé une infrastructure distribuée et sécurisée, ainsi qu'une solution de connexion privée entièrement basée sur le cloud pour tous les collaborateurs afin de garantir un accès distant sécurisé au réseau. Nous avons conservé la solution VPN existante pour un faible nombre d'équipes ayant des besoins spécifiques, tels que la connexion de téléphones IP dans leurs bureaux distants. Nous avons également fourni des PC professionnels aux collaborateurs, avec la possibilité de gérer les téléchargements et les mises à jour automatiques des logiciels.

Écarter les failles de sécurité

Comme on pouvait s'y attendre pendant ce travail à distance intensif, le nombre d'appels et d'e-mails concernant des e-mails suspects a augmenté, ainsi que les demandes de mise à jour de mots de passe. Les attaques par hameçonnage ont également explosé, tout comme les attaques ciblées sur les logiciels vulnérables.

Bien que l'utilisation de proxies protège ALE contre les problèmes majeurs liés à la cybersécurité, nous ne cessons de constater tous les jours de nouvelles violations, provenant d'e-mails, de téléchargements et de versions de logiciels/OS non mises à jour.

Rester en contact

Chez ALE, nous gardons un lien virtuel permanent avec nos équipes. Nous communiquons régulièrement, partageons des conseils et des bonnes pratiques, et veillons à ce que notre équipe soit disponible pour soutenir tous les collaborateurs.

Recommandations d'ALE pour assurer la sécurité du télétravail :

- N'autorisez ou n'encouragez pas l'utilisation d'appareils personnels (PC) pour échanger et communiquer des données professionnelles
- Mettez en place un accès privé et sécurisé pour les collaborateurs
- Automatisez les mises à jour logicielles sur l'ensemble du réseau de l'entreprise
- Restez vigilants par rapport aux demandes suspectes reçues par e-mails
- N'utilisez que des logiciels certifiés. Les audits et les certifications permettent d'authentifier la sécurité des logiciels
- Simplifiez vos processus décisionnels. Dans les situations d'urgence, un responsable de la sécurité ou un DSI doit prendre rapidement des décisions pour résoudre les problèmes afin d'assurer la continuité des services

Six recommandations d'ALE pour une connexion à distance sécurisée

1. Automatisez les rappels de changement de mot de passe

Aidez les employés à modifier les mots de passe professionnels avant qu'ils n'expirent. Avant leur expiration, les collaborateurs devraient recevoir un e-mail quotidien contenant des instructions les invitant à modifier le mot de passe.

2. Activez la sauvegarde des données dans le cloud

Autorisez et encouragez les collaborateurs à enregistrer régulièrement leurs données afin d'éviter toute perte en cas de problème avec leur ordinateur portable. Mettez en place des espaces de stockage pour la sauvegarde des données et proposez une assistance à distance par le biais d'un service d'assistance informatique.

3. Rappelez aux collaborateurs les meilleures pratiques en matière de protection des appareils

Gardez votre ordinateur portable en parfait état :

- Éteignez l'ordinateur portable à la fin de chaque journée de travail (éviter le mode veille/verrouillage)
- Conservez les ordinateurs portables éloignés des sources de chaleur (comme le soleil ou le chauffage)
- Évitez de manger ou de boire à proximité des ordinateurs portables
- Gardez les câbles hors de portée des enfants et des animaux de compagnie

4. La sécurité avant tout

Sensibilisez les équipes aux risques et aux bonnes pratiques en matière de sécurité :

- Encouragez les employés à bien réfléchir avant de cliquer sur des liens contenus dans un e-mail, même si celui-ci semble avoir été envoyé par une personne de confiance
- Proposez un suivi informatique en cas de doute
- Fournissez des outils de signalement d'e-mails suspects
- Utilisez la gamification pour créer une culture axée sur la sécurité : par exemple en encourageant les collaborateurs à détecter et à signaler les e-mails suspects

5. Communiquez

L'isolement rend les personnes vulnérables aux cyberattaques. Donnez les moyens à vos équipes de garder le contact :

- Organisez des sessions d'avancement régulières, des réunions virtuelles, des événements, des espaces de collaboration, des « happy hours »
- Encouragez les personnes à communiquer régulièrement avec leurs équipes
- Envoyez régulièrement des e-mails destinés à informer les collaborateurs que l'équipe informatique se tient à leur disposition et à leur rappeler les meilleures pratiques en matière de sécurité

6. Encouragez l'adoption d'habitudes saines

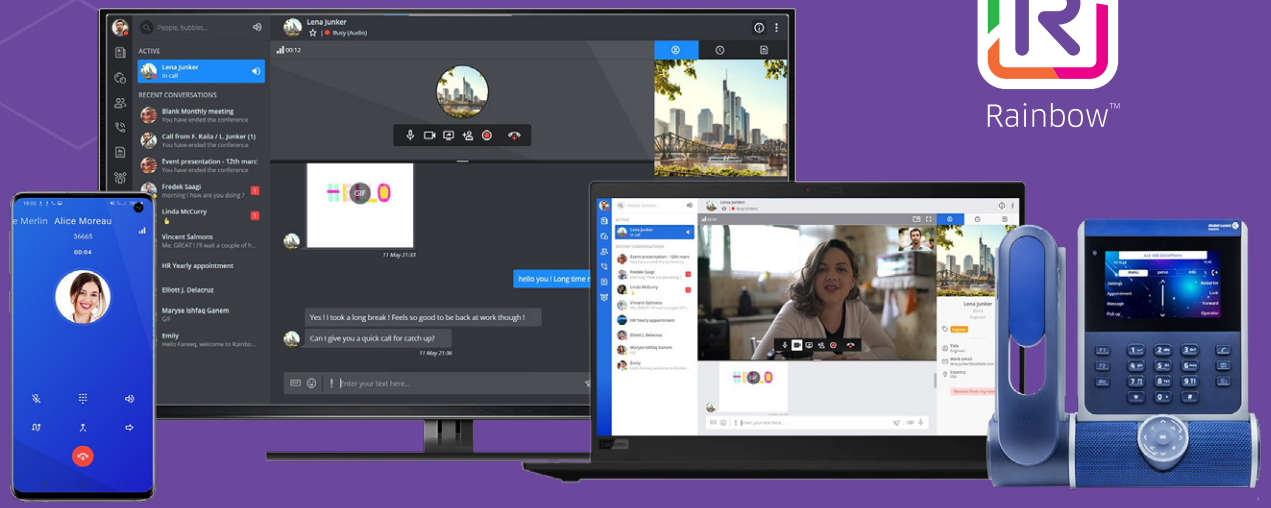
Le télétravail ne doit pas être synonyme de journées de travail de 12 heures avec une connectivité continue ou des réunions consécutives. Encouragez les collaborateurs à s'éloigner de leur écran, à se déconnecter, et à passer du temps en famille ou à l'extérieur.

Rainbow™ d'Alcatel-Lucent Enterprise pour une collaboration connectée

Rainbow : une plateforme cloud pour la collaboration en équipe avec le chat, les appels vidéo et audio, le partage d'écrans et de documents, qui fournit aux employés les services dont ils ont besoin pour rester connectés. La plateforme est largement utilisée par tous les employés pour chez ALE collaborer avec leurs collègues, leurs clients et leurs partenaires commerciaux, et elle est connectée au système téléphonique pour les appels externes.

En outre, nos partenaires et nos clients du secteur public ont également adopté Rainbow comme solution de collaboration en interne. Rainbow répond en effet aux exigences de sécurité du secteur public, de la défense, de la santé et d'autres secteurs spécifiques. Notre produit respecte les réglementations de sécurité les plus strictes, notamment le RGPD et le HDS. Rainbow est certifié ISO 27001 et CSPN par l'ANSSI.

Rainbow™



Brochure
Assurer la sécurité de votre entreprise en situation de télétravail

Travailler à distance en toute sécurité

Alors que les entreprises autorisent un nombre croissant d'employés à télétravailler, les analystes du secteur confirment les risques accrus de cyberattaques.

Chez ALE, nous utilisons en interne les applications et services de communication et de collaboration que nous déployons chez nos clients. Ces solutions sont développées dans un souci de cybersécurité, quelles que soient les conditions d'utilisation - au bureau, à distance ou en déplacement. Outre le fait que ces solutions sont certifiées par des agences de sécurité internationales et conformes aux réglementations en vigueur, la meilleure garantie que nous puissions offrir à nos clients, c'est que des milliers d'employés d'ALE dans le monde entier les utilisent tous les jours en toute confiance.

Pour plus d'informations, visitez notre site Web.

Alcatel·Lucent Enterprise