Éléments à considérer et solutions pour l’espace de travail numérique des agents publics

Alcatel·Lucent Enterprise

Livre électronique

Sommaire

Présentation

Les agents publics de toutes les organisations publiques accomplissent des tâches essentielles pour les citoyens. Leur rôle ne peut être sous-estimé. Ils ont souvent un impact direct sur la vie de plusieurs milliers de personnes.

La numérisation des services a commencé depuis un certain temps. Outre la pression constante pour améliorer les services publics et réduire les coûts, la pandémie a contribué à accélérer cette tendance. Cependant, il y a deux ans, le monde n'aurait jamais pu prévoir le pourcentage élevé d'agents publics qui adopteraient le télétravail et les équipes distribuées qui en résulteraient. Après l'accord-cadre relatif à la mise en œuvre du télétravail dans les trois fonctions publiques signé le 13 juillet 2021, le premier accord sur le télétravail dans la fonction publique a été publié au Journal officiel le 3 avril 2022.

La demande des outils de travail numériques par les agents et la complexité de la prise en charge des équipes distribuées posent des défis aux organismes publics. En conséquences, ils ont été obligés de remplacer les solutions temporaires par des solutions plus permanentes pour soutenir le travail hybride.

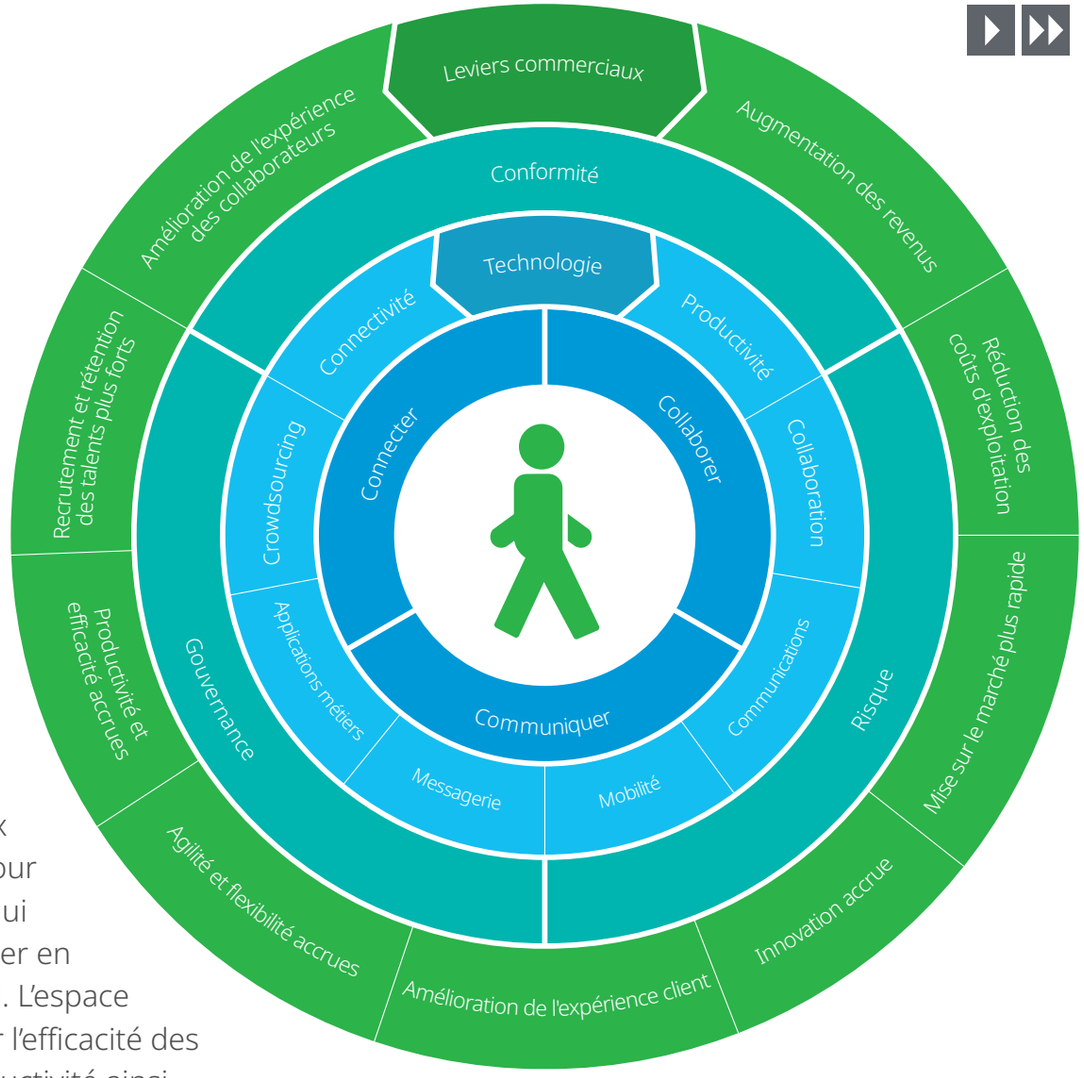
Deloitte[1] a réalisé un excellent graphique qui explique l'intégration de l'espace de travail numérique et les avantages qu'il offre.

La technologie fournit des outils qui permettent d'améliorer la communication et la collaboration, quel que soit le lieu ou l'appareil utilisé. Toutefois, il peut être plus difficile de s'assurer que vous disposez de la bonne technologie pour obtenir le résultat souhaité.

Alcatel-Lucent Enterprise a accompagné des clients du monde entier pour comprendre les nouveaux défis auxquels ils se confrontent et pour proposer des solutions numériques qui permettent à leurs équipes de travailler en tout lieu, avec n'importe quel appareil. L'espace de travail numérique peut augmenter l'efficacité des agents, favorisant une meilleure productivité ainsi que la réduction des déplacements, un réel avantage pour la planète.

Ce livre électronique traite de trois éléments clés de l'espace de travail numérique pour le secteur public :

- Communications et collaboration
- Connectivité
- Sécurité



Nous examinerons ensuite les solutions ALE qui peuvent aider les organismes publics à évoluer vers l'espace de travail numérique, avec flexibilité, agilité et sécurité.

1 - https://www2.deloitte.com/content/dam/Deloitte/be/Documents/technology/The_digital_workplace_Deloitte.pdf

Éléments clés à considérer pour l’espace de travail numérique des agents publics

Communication et collaboration

Grace au nouvel accord de télétravail pour la fonction publique, les agents partagent leur espace de travail entre le domicile, les sites distants et le bureau. Le bureau n’est plus le seul lieu où le travail se déroule. Il devient davantage l’espace privilégié pour les réunions de groupe, les formations et les rencontres avec les citoyens. Travailler et échanger avec les équipes est possible aujourd’hui quel que soit le lieu. Cela a eu un impact considérable sur l’environnement de travail, rendant les communications et la collaboration plus importantes que jamais.

Les communications constituent un élément essentiel de la réussite de l’espace de travail numérique. Le défi consiste à garder les agents engagés, productifs et motivés. Ils ont en effet besoin d’outils de communication qui facilitent leurs activités quotidiennes et leur permettent de communiquer et de collaborer avec leurs collègues, leurs équipes et les citoyens, quel que soit le lieu de travail ou l’appareil utilisé.

Pour garantir des communications connectées, nous vous recommandons :

- Des services de communications avancées pour les agents, notamment : service voix de haute qualité, chat de groupe, messages vocaux et possibilité de passer d’un appel à une vidéo quel que soit l’appareil
- Des services de collaboration tels que le partage d’écran, le contrôle du bureau à distance et le partage de fichiers volumineux
- Des communications et de la collaboration sécurisées avec les contacts externes
- De la continuité des appels dans toute l’organisation grâce à une connexion instantanée et à un répertoire complet de contacts
- Un canal de diffusion d’informations, permettant de tenir tout le monde au courant des dernières annonces ou réglementations
- Communications et collaboration intuitives

Afin de proposer aux agents des outils à la hauteur de leurs besoins, voici quelques recommandations :

- Évaluer les profils utilisateurs et les exigences en matière de communications, en fonction des tâches des agents, de la mobilité et du besoin d’accéder aux applications métiers
- Offrir aux agents sur le terrain avec les citoyens des appareils optimisés permettant un accès rapide aux informations et aux communications lorsqu’ils sont en déplacement

- S’assurer que le personnel en contact avec les citoyens dispose d’un accès optimisé à la gestion des appels et des interactions, intégré aux systèmes de gestion des relations clients (CRM) ou aux applications métier
- Permettre la collaboration avec le personnel administratif afin d’améliorer les services offerts aux citoyens et la résolution au premier appel
- Évaluer les exigences légales locales/nationales afin de protéger la confidentialité des données

Pour garantir un télétravail hautement performant, les éléments suivants sont incontournables :

- Un chat de groupe, des capacités de réunions audio et de visioconférences avec le partage d’écran pour collaborer sur n’importe quel appareil
- De la continuité des appels grâce à une seule infrastructure sous-adjacente pour connecter tous les profils
- Un poste téléphonique de bureau pour les agents qui passent plus d’une heure au téléphone et gèrent des appels importants tels que : l’accueil du public, des services de santé ou la gestion des situations d’urgence
- Des communications intégrées aux applications métier afin de faciliter l’adoption par les utilisateurs et d’éviter d’encombrer le bureau de leur PC
- Un accès à distance sécurisé pour accéder en toute sécurité aux informations confidentielles

Connectivité

L'espace de travail numérique repose sur une connectivité de haute qualité, résiliente et sécurisée. Alors que l'on assiste à la normalisation de nouveaux modes de travail et que l'espace de travail numérique prend forme, l'infrastructure numérique permettant de connecter les agents doit être en place. Quel que soit le lieu, certains points essentiels doivent être pris en considération.

- La sécurité doit être une priorité absolue. Il est essentiel de disposer d'une solution réseau à plusieurs couches de sécurité. Un cadre Zero Trust suppose que chaque dispositif ou chaque utilisateur représente un risque pour la sécurité. Le contrôle d'accès au réseau doit être activé
- L'accès sécurisé aux applications en tout lieu rend nécessaire la mise en place d'accès basés sur les profils utilisateur. Les profils utilisateur assurent une connectivité sécurisée et flexible, sans perte de service, quel que soit le lieu.
- Les télétravailleurs avec des exigences élevées en matière de sécurité et de confidentialité des données, doivent pouvoir se connecter au réseau de l'organisation depuis leur domicile ou des différents bureaux. Les politiques de sécurité de l'organisation sont ainsi respectées, et l'équipe informatique est en mesure de garder le contrôle
- Les agents utilisent désormais des ordinateurs portables pour des applications en temps réel (voix, vidéo) tant au bureau qu'à la maison. Il s'agit d'un changement important pour de nombreux organismes publics. Le réseau Wi-Fi doit être capable de prendre en charge une plus grande utilisation des applications en temps réel sur une zone plus étendue. Il convient d'en tenir compte lors de la définition de la portée du réseau
- La résilience du réseau Wi-Fi est devenue une priorité, car de plus en plus d'agents se connectent sans fil. Un réseau sans fil distribué avec une intelligence dans les points d'accès élimine le point de défaillance unique, et qu'en cas de panne d'un point d'accès, d'autres points d'accès dans le réseau prendront le relais. Un réseau intelligent sans fil distribué élimine également la nécessité de dupliquer le réseau, ce qui permet de gagner du temps et de l'argent
- L'accélération du rythme de la transformation numérique crée une pression sur l'équipe informatique qui doit déjà exécuter les tâches quotidiennes. Les gains d'efficacité pouvant être réalisés doivent être pris en compte. La réduction du nombre d'interfaces de gestion et de systèmes d'exploitation dans le réseau permettra de réduire la charge de travail et le temps de formation. En outre, l'automatisation réduira le temps de déploiement et de gestion opérationnelle du réseau
- Un accès de haute qualité est essentiel. L'espace de travail numérique crée des efficacités pour permettre une plus grande productivité, mais si la connectivité est insuffisante, la productivité accrue est perdue

Sécurité

Sécurité des communications

L'administration et les organismes publics représentent des cibles importantes pour les cyberattaques. Hameçonnage, piratage de compte, rançongiciels, violation de données… Dans leurs rapports annuels, l'Anssi et cybermalveillance.gouv.fr constatent que les cyberattaques ont fortement augmenté en 2021.[2] Il est donc essentiel de mettre en œuvre un équipement le plus sûr qui soit. Les outils de gestion intégrés doivent permettre de superviser la sécurité de tous les éléments.

En outre, les appareils mobiles transforment le paysage des communications et renforcent le besoin de sécurité, car les cyberattaquants exploitent les volumes croissants de code contenus à chaque point d'accès. Le chiffrement de niveau défense, la confidentialité des données et les environnements de communications hautement confidentielles nécessitent une infrastructure sécurisée, disponible, efficace et facile à gérer.

Nos recommandations sont les suivantes :

Mettez à jour votre système de communications et surveillez-le :

- Les mises à jour du système sont d'une importance capitale en termes de cybersécurité. Elles permettent de maintenir vos systèmes de communication à jour et de les protéger contre les vulnérabilités des logiciels
- Activez la surveillance de votre système de communications afin de repérer les activités suspectes en configurant des seuils d'utilisation et des alarmes dans le système de gestion du réseau

Authentifiez et chiffrez :

- Activez l'authentification mutuelle entre tous les appareils (téléphones et passerelles) et le système de communications
- Chiffrez la signalisation afin d'éviter les attaques de protocole et les attaques de type « Man-in-the-Middle »
- Chiffrez les communications IP afin d'éviter les écoutes illicites

Rendez vos systèmes redondants et ajoutez un élément de sécurité :

- Le risque ne peut jamais être égal à zéro. Si une passerelle ou le système de communications principal tombe en panne, un système de secours peut prendre le relais de manière transparente en cas de redondance spatiale
- Ajoutez les composants nécessaires à la protection de votre système de communications, tels qu'un contrôleur de session en périphérie ou un proxy inverse, tandis que les serveurs de notifications servent à alerter les personnes nécessaires

Éduquez :

- Sensibilisez les utilisateurs et les administrateurs ; appliquez les meilleures pratiques au sein de vos équipes, notamment en rappelant la mise à jour des mots de passe, en formant les utilisateurs à la lutte contre la cybercriminalité et en leur apprenant à reconnaître un appel chiffré grâce à l'icône de cadenas sur le téléphone

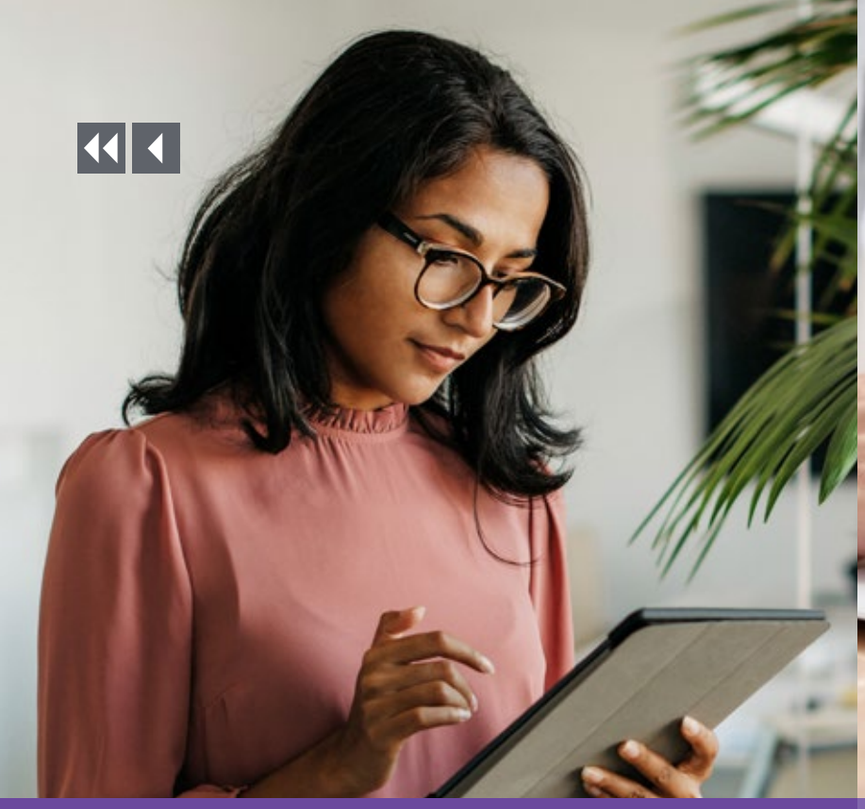
2 - https://www.vie-publique.fr/en-bref/284654-les-cybermalveillances-en-forte-hausse-en-2021

Sécurité du réseau

La cybersécurité est depuis longtemps considérée comme une priorité absolue pour les organismes gouvernementaux et les services publics. Cependant, en raison de la transformation numérique en cours, les exigences en matière de cybersécurité évoluent. Au fur et à mesure de l'accélération de la transformation, les anciennes méthodes de sécurité des réseaux sont désormais obsolètes. En tant qu'élément fondamental de l'architecture du réseau, la sécurité doit être intégrée dès le départ et appliquée universellement à tous les accès au réseau, qu'ils soient filaires ou sans fil. Voici quelques éléments à prendre en compte pour sécuriser votre réseau à tous les niveaux :

- **Au niveau des utilisateurs :** vérifiez qu'ils sont toujours authentifiés et autorisés avec les droits d'accès appropriés (en utilisant les politiques et les profils)
- **Au niveau des terminaux :** vérifiez qu'ils sont authentifiés et conformes aux règles de sécurité établies par le service informatique. Cet objectif peut être atteint par la présence de logiciels installés au niveau des terminaux qui effectuent une analyse de sécurité rapide avant que ces derniers ne se connectent au réseau. Par exemple, l'analyse peut consister à vérifier que les terminaux se connectant au réseau disposent bien d'un logiciel antivirus à jour et de la dernière version du système d'exploitation
- **Au niveau de l'application :** définissez des règles associées à des applications spécifiques (notamment le blocage, la limitation de la bande passante ou l'identification des utilisateurs)
- **Analyse intelligente :** les capacités d'analyse des commutateurs réseau et des points d'accès ALE permettent de fournir une visibilité et des informations détaillées sur le réseau, les utilisateurs, les terminaux et les applications utilisés sur le réseau. Elles peuvent également fournir des fonctionnalités d'inspection approfondie des paquets qui détectent le type de données et d'applications se déplaçant dans le réseau, permettant d'identifier des modèles de trafic réseau inhabituels, ainsi que des activités non autorisées et une intrusion réseau
- **Techniques de segmentation de réseau** : la mise en place de terminaux IoT dans des conteneurs virtuels permettent à plusieurs terminaux et réseaux d'utiliser la même infrastructure physique, tout en restant isolés du reste du réseau. Si une brèche se produit dans une partie du réseau virtuel, elle n'affecte pas les autres zones du réseau et des applications.

Ces techniques de sécurité contribuent à la mise en place d'un cadre d'architecture « Zero Trust », le niveau suivant de l'architecture de réseau qui fonctionne selon le principe « Ne jamais faire confiance - Toujours vérifier », où tous les utilisateurs doivent en permanence être authentifiés, autorisés et validés avant de pouvoir accéder aux applications et aux données.



Espace de travail numérique

Modèles cloud flexibles

Connectez tout

Solutions ALE pour l’espace de travail numérique des agents publics

Communications et collaboration

Les communications de l’ère numérique (DAC) d’Alcatel-Lucent Enterprise fournissent des solutions et des services complets de communications et de collaboration sur site et dans le cloud. L’espace de travail numérique évolue vers un environnement de travail distribué où le télétravail est devenu normal, rendant les communications en temps réel essentielles pour connecter les collègues, les citoyens et les partenaires. Les solutions de communications d’Alcatel-Lucent Enterprise permettent la continuité des appels en tout lieu, dans n’importe quelle situation, et à partir de n’importe quel appareil.

Fonctions de communications principales :

- **Connexion transparente** à l’intérieur et à l’extérieur de l’organisation. L’infrastructure de communications sous-jacente connecte les agents à distance ou dans les bureaux aux agents de terrain, aux équipes administratives, quel que soit leur appareil, par le biais d’une multitude de technologies standards telles que PSTN, TDM, IP, SIP, VoWIFI, DECT et fournissent également des données à l’équipe informatique pour surveiller la qualité de service (QoS)
- Le **routage d’un numéro unique** sur le téléphone professionnel et le softphone convient parfaitement au travail hybride. Que les agents travaillent chez eux ou au bureau, les appels aboutissent toujours : aucun appel n’est perdu et aucun renvoi d’appel n’est nécessaire

- Les DeskPhones ALE offrent une **qualité HD et le son 3D Symphonic**, et les combinés robustes et applications pour smartphone destinés au personnel mobile, comprenant des notifications et des alarmes actives pendant l'itinérance sur site
- Un **accès facile** aux messages d'accueil déstinés aux clients et aux fonctions d'agent tels que les groupes d'appels et les files d'attente permettent au personnel du service citoyen de répondre à tous les appels
- Les **conférences en cas d'urgence ou de crise** permettent de faire participer automatiquement des contacts prédéfinis, d'un simple appui sur un bouton
- **Le chiffrement de bout en bout** offre la sécurité et la garantie de confidentialité requises par les organismes publics
- Les communications et la collaboration dans l'espace de travail numérique sont facilitées grâce à un **appel par un simple clic** à un contact ou au lancement d'une conférence, ou à des fonctionnalités plus avancées comme le chat de groupe, le partage d'écran et de fichiers, les réunions audio et les visioconférences, le tout dans une seule application, disponible en tant que client web. Aucune installation n'est requise. Des applications sont disponibles pour les appareils Android et IoS ainsi que pour les PC. Les clients disposant de solutions ALE peuvent utiliser des combinés existants dotés de la technologie WebRTC
- Les connecteurs pour Microsoft® Teams et Google permettent aux agents de **communiquer facilement** avec l'ensemble de l'organisation depuis leur espace de travail numérique. Grâce aux connecteurs pour SaaS CRM et ITSM, les agents peuvent communiquer et collaborer à partir de leurs applications métier

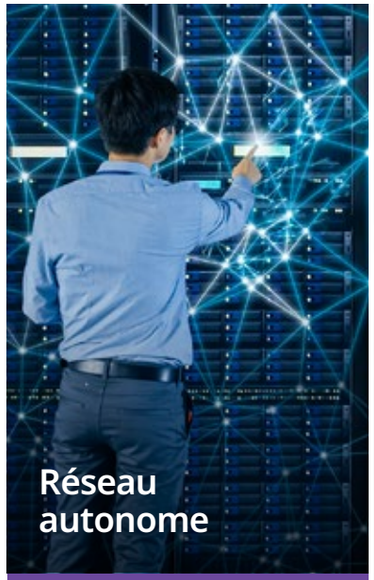
Livre électronique
Éléments à considérer et solutions pour l'espace de travail numérique des agents publics

Connectivité

Le Digital Age Networking d'Alcatel-Lucent Enterprise fournit un réseau autonome qui offre une expérience de connexion fluide et résiliente aux réseaux d'Alcatel-Lucent OmniSwitch® (LAN) et Alcatel-Lucent OmniAccess® Stellar (WLAN), alliée à une convergence ultra-rapide, un contrôle fiable des accès au réseau et une QoS garantie. Le Wi-Fi professionnel de nouvelle génération avec système de contrôle WLAN incorporé aux points d'accès rend superflus les contrôleurs physiques centralisés. Les solutions ALE peuvent être gérées sur site ou dans le cloud.

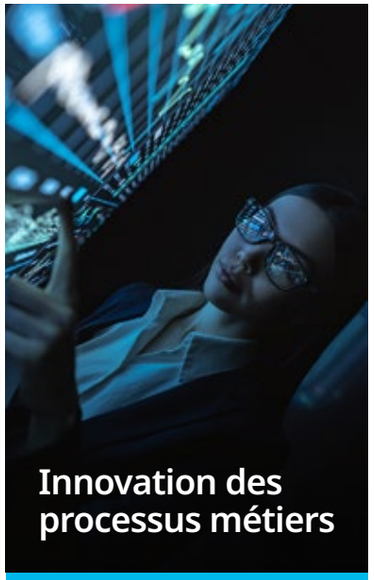
Caractéristiques de connectivité clés des solutions ALE :

- **Un système de gestion du réseau unique** offre un niveau supplémentaire d'intégration entre les réseaux filaires et sans fil, ce qui réduit la charge de travail du responsable informatique, lequel ne doit pas gérer deux systèmes de gestion avec deux ensembles de politiques et de règles de configuration. Le système de supervision de réseau Alcatel-Lucent OmniVista®. Network Management System (NMS), permet une gestion unifiée et une visibilité à l'échelle du réseau, pouvant améliorer l'efficacité et l'agilité des équipes informatiques
- L'**approvisionnement automatisé** d'une infrastructure réseau sécurisée simplifie les ajouts, les déplacements et les modifications tout en réduisant le temps nécessaire à la maintenance et à l'exploitation du réseau.
- Le **Shortest Path Bridging (SPB)**, conçu pour prendre en charge la création et l'exploitation d'un réseau moins complexe, construit et maintient dynamiquement la typologie du réseau entre les nœuds. La charge SPB répartit et utilise toutes les connexions physiques disponibles en libérant davantage de bande passante
- **Fonctionnalités de travail hybride (option 1). L'accès distant sécurisé** est activé grâce au point d'accès distant (RAP). Le réseau de l'organisation peut être facilement étendu en dehors du site principal, offrant une connectivité aux télétravailleurs comme s'ils étaient dans le réseau local. Selon le modèle, le RAP peut également fournir une connectivité filaire pour les téléphones IP ou pour d'autres appareils IoT. L'accès est pris en charge par des politiques de sécurité centralisées et unifiées sur les réseaux filaires et sans fil, ce qui garantit une gestion facile et une sécurité extrêmement robuste et cohérente
- **Fonctionnalités de travail hybride (option 2) SD-WAN et SASE**. Le Secure Access Service Edge (SASE) permet de connecter en toute sécurité les sites distants, les succursales et les télétravailleurs. La solution SASE pour les télétravailleurs consiste en un logiciel installé dans l'ordinateur portable de l'utilisateur qui fournit un accès sécurisé aux applications du data center de l'organisation, que ce soit des centres de données privés, Internet ou des clouds publics, avec une gestion centralisée et sans nécessiter de matériel supplémentaire sur le site du travailleur. SASE offre une sécurité avancée avec un pare-feu de nouvelle génération (NGFW), comprenant le filtrage des URL et le pare-feu applicatif, et une gestion unifiée des menaces (UTM), comprenant un système de prévention des intrusions de nouvelle génération (NGIPS), un antivirus et une fonctionnalité contre les éléments malveillants.



Automatisez les opérations critiques du réseau et améliorez l'expérience utilisateur

Développez la numérisation grâce à l'intégration et à la gestion sécurisées des IoT



Accélérez la transformation grâce à des flux de travail automatisés

Sécurité

Sécurité des communications

Que vous soyez responsable d'un petit organisme public local ou d'un grand organisme public national, votre réseau de communications risque d'être la cible de pirates informatiques.

Caractéristiques de sécurité clés des solutions ALE :

- **Connectivité sécurisée** entre le système de communications sur site (PBX et téléphones) et l'infrastructure cloud, entièrement développée et exploitée par Alcatel-Lucent Enterprise, avec authentification mutuelle, chiffrage et éléments de frontière de sécurité (SBC)
- **Haute disponibilité** avec des architectures redondantes, sur site, dans des clouds privés ou publics, protection contre les attaques par déni de service (DoS), sécurité intégrée avec du matériel durci et des systèmes d'exploitation sécurisés
- **Confidentialité des communications** : un chiffrement puissant, respectant les normes du secteur, mises en œuvre de façon native dans la solution, sans aucun impact sur la qualité et les performances vocales, fournissant l'expérience attendue par les citoyens et les agents
- **Confidentialité et protection des données** avec un contrôle d'accès basé sur les rôles et le chiffrement des données stockées. Cela permet de garantir que toutes les données cruciales sont entièrement protégées de bout en bout et sous votre contrôle
- **Conformité aux réglementations et aux normes** telles que (sans s'y limiter) le Règlement général sur la protection des données (RGPD), la norme ISO 27001, Critères communs EAL2+, la certification HDS (« Hébergeur Données Santé » des services cloud d'ALE pour la conformité à la protection des données des patients en France)
- **Sécurité en tant que processus** avec PSIRT (Product Security Incident Response Team) pour la gestion active des vulnérabilités, la mise à jour régulière des logiciels et de la plateforme de politiques de sécurité

CERTIFICATIONS

ANSSI CSPN

Sécurité du réseau

La transformation numérique a profondément modifié les exigences en matière de cybersécurité en raison de l'augmentation du nombre d'appareils connectés, de la disparition du périmètre réseau et de l'accélération continue des changements. La solution Digital Age Networking d'Alcatel-Lucent Enterprise permet de sécuriser vos équipements et données informatiques. Cette solution vous permet de gérer de près l'accès des utilisateurs, de réduire les vulnérabilités créées par les appareils IoT, mobiles et réseau, d'empêcher des inévitables brèches de fournir un point d'attaque et d'offrir un écosystème de confiance.

Les solutions ALE sont sécurisées depuis leur conception avec :

- Un **code diversifié et sécurisé** qui favorise la sécurité au niveau des dispositifs du réseau en utilisant la vérification et la validation par des tiers indépendants, notamment :
  - Une analyse du code source, des tests en boîte blanche et boîte noire par une société spécialisée dans la cybersécurité afin d'éliminer les vulnérabilités, dont :
    - ¬ Menaces back-door
    - ¬ Logiciel malveillant intégré
    - ¬ Vulnérabilités exploitables
    - ¬ Exposition d'informations exclusives et/ou classifiées
- **Diversification des logiciels :** le logiciel ALE met en œuvre la randomisation de l'espace d'adressage (ASLR). Chaque démarrage de commutateur génère dynamiquement une disposition unique de la mémoire afin d'entraver ou d'empêcher l'exploitation du logiciel
- **Sécurité de type « Zero Trust » (micro et macro-segmentation) :** le cadre de type « Zero Trust » suppose la présence de pirates informatiques. L'organisation n'est plus considérée comme une zone de confiance implicite. Cela implique des actions telles que l'authentification de toutes les connexions. Aucun équipement et aucun utilisateur ne sont entièrement fiables
- **Sécurité par défaut :** l'accès à distance sur l'OmniSwitch doit être activé, ce qui est le contraire de la plupart des autres commutateurs où tous les accès aux commutateurs/routeurs sont activés par défaut et où les administrateurs doivent se débrouiller pour sécuriser le dispositif
- **Protection intégrée contre les dénis de service (DoS) :** protection du système d'exploitation et du module de gestion contre une multitude d'attaques DDOS qui sont généralement utilisées pour faire passer le processeur à 100 % d'utilisation
- **Aucun logiciel** à acheter et à suivre : toutes les fonctions et capacités, même le code sécurisé ALE, sont inclus dans le prix du commutateur - aucun module à ajouter, aucune mise à niveau à acheter. Tous les logiciels sont inclus
- **Intégration automatisée et sécurisée de l'IoT :** par le biais des empreintes numériques, de la classification et de la mise en conteneur des appareils

RGPD européen

En savoir plus

En savoir plus sur les solutions d'Alcatel-Lucent Enterprise pour le secteur public pour le lieu de travail numérique ou contactez-nous afin de discuter de vos besoins.

https://www.al-enterprise.com/fr-fr/secteurs-activite/secteur-public

Alcatel·Lucent Enterprise