



Sécuriser les solutions de communications unifiées et de collaboration

Quelles mesures prendre dans un monde en pleine mutation ?

Livre blanc

Alcatel • Lucent 
Enterprise

Sommaire

- | Un recentrage fort sur la cybersécurité
- | Six domaines clés pour une cybersécurité de bout en bout
- | Atteindre les objectifs de l'entreprise avec moins de risques
- | Cybersécurité : au coeur des pratiques du fournisseur de technologie

Un recentrage fort sur la cybersécurité

Au cours des dernières années, presque toutes les entreprises et administrations ont modifié la manière dont leurs employés communiquent, collaborent et partagent l'information. Si le virage rapide vers le travail à distance a été fondamental pour garantir la continuité de l'activité pendant la pandémie, il y a eu un prix à payer : le périmètre du réseau s'étend désormais bien au-delà des limites traditionnelles des bureaux, augmentant considérablement la surface potentielle d'attaque.

Les risques associés à l'extension des périmètres des réseaux ne sont pas près de disparaître. D'après Gartner, 39 % des professions intellectuelles dans le monde travailleront en mode hybride à distance et au bureau d'ici à la fin de 2023. Aux États-Unis, ce chiffre s'élèvera à 51 %¹.

Les perturbations géopolitiques ont encore accru les risques de cybersécurité. L'Agence de l'Union Européenne pour la Cybersécurité (ENISA) a qualifié l'invasion de l'Ukraine par la Russie de « changement de donne » pour le domaine cyber mondial.² Selon l'Association of Ukrainian IT Outsourcing Companies, une entreprise sur cinq figurant au classement Fortune 500 a fait appel à des développeurs logiciel en Ukraine en 2022.³

Parallèlement, l'impact sociétal des cyberattaques s'accroît. En 2022, nous avons assisté à des cyberattaques majeures contre des infrastructures civiles essentielles, provoquant une urgence nationale au Costa Rica,⁴ alors que d'autres ciblent sans relâche des établissements de santé.⁵

Les entreprises ne peuvent pas se permettre de différer le renforcement de leur cybersécurité

On estime que la cybercriminalité a coûté à l'économie mondiale 5 500 milliards d'euros en 2021 et que les dommages devraient dépasser les 10 000 milliards d'euros d'ici 2025.⁶ Le problème est si grave que l'Union Européenne est en train de créer une loi sur la cyberrésilience (Cyber Resilience Act) et a publié une version 2 considérablement renforcée de sa directive sur la sécurité des réseaux et de l'information (NIS) afin de protéger les consommateurs et les entreprises qui achètent ou utilisent des produits ou des logiciels ayant une composante numérique.⁷ Les États-Unis mettent également en œuvre des mesures pour renforcer la cybersécurité, notamment le décret 14028, qui encourage les agences à adopter les principes de la confiance zéro en matière de cybersécurité et à adapter les architectures de réseau en conséquence.⁸

Alors que les entreprises et les organismes publics cherchent à opérer une transformation numérique et à prendre en compte sur le long terme des modèles de travail flexibles, ils n'ont pas d'autre choix que de renforcer la cybersécurité. Les solutions utilisées par leurs équipes pour communiquer, collaborer et partager des informations doivent intégrer les bonnes pratiques en matière de cybersécurité, à tous les niveaux et dans tous les aspects concernés.

¹ [Gartner Forecasts 39% of Global Knowledge Workers Will Work Hybrid by the End of 2023](#), Gartner, Mars 2023.

² [La volatilité de la géopolitique ébranle les tendances du paysage des menaces de cybersécurité en 2022](#), Agence de l'Union Européenne pour la Cybersécurité (ENISA) Novembre 2022.

³ [En 2022, une entreprise sur cinq du classement Fortune 500 comptera sur l'Ukraine pour ses besoins en matière de développement logiciel](#), Initiative ukrainienne Hi-Tech, octobre 2022.

⁴ [Les 13 cyberattaques les plus coûteuses de 2022 : rétrospective](#), Security Intelligence, décembre 2022.

⁵ [Bilan de l'année 2022 : une année riche en événements pour la cybersécurité](#), Forbes, décembre 2022.

⁶ [New European Union cybersecurity proposal takes aim at cybercrime](#), Forum économique mondial, septembre 2022.

⁷ [Loi sur la cyberrésilience de l'UE](#), Commission Européenne, septembre 2022.

⁸ [Décret sur l'amélioration de la cybersécurité de la nation](#), Cybersecurity & Infrastructure Security Agency.

Livre blanc

Sécuriser les solutions de communications unifiées et de collaboration





Six domaines clés pour une cybersécurité de bout en bout

Les solutions de communications unifiées et de collaboration doivent mettre en œuvre la cybersécurité de bout en bout, car elle constitue le seul moyen de s'assurer que la sécurité est appliquée de manière exhaustive. Une approche globale de la cybersécurité par les fournisseurs de ces solutions aide les entreprises et les organismes publics à :

- **Prévenir les cyberattaques**, en mettant en œuvre la cybersécurité dans chaque étape de la conception du produit afin de réduire la surface d'attaque
- **Protéger contre les cyberattaques**, en mettant en œuvre les normes de sécurité les plus récentes et les bonnes pratiques dans tous les composants de la solution afin d'accroître leur résistance
- **Réagir aux cyberattaques**, en prenant des mesures rapides et appropriées pour limiter l'impact et améliorer la résilience en cas d'attaque

Pour déterminer si les solutions de communications unifiées et de collaboration mettent en œuvre la cybersécurité de bout en bout, il convient de les évaluer en les confrontant aux domaines décrits ci-dessous. Ces six domaines critiques couvrent les principales vulnérabilités en termes de cybermenaces et permettent une évaluation complète.

1 Sécurité dès la conception

Historiquement, la conception de la plupart des solutions était pilotée par la nécessité d'ajouter de nouvelles fonctionnalités, et la sécurité était une considération importante, mais secondaire. Avec l'évolution du contexte, les priorités traditionnelles en matière de conception se sont inversées et celle-ci doit désormais être guidée par les exigences en matière de cybersécurité.

Les solutions matérielles et logicielles sécurisées dès la conception prennent en compte la sécurité à chaque étape de la définition, du développement et de la livraison du produit. Tout le hardware et les systèmes d'exploitation sont durcis, la protection contre les dénis de service (DoS) est intégrée et les solutions mettent en œuvre les bonnes pratiques en matière de cybersécurité. Par exemple, une solution de communications unifiées et de collaboration destinée aux organisations de sécurité intérieure répondra aux normes très strictes de résilience et de confidentialité exigées par ces organisations.

2 Sécurité ZTNA (Zero Trust Network Access)

Les stratégies de sécurité qui accordent la confiance en fonction de la localisation de l'utilisateur à l'intérieur du pare-feu de l'entreprise, des informations d'identification qu'il saisit ou de l'application ou de l'appareil qu'il utilise ne sont plus suffisantes, même lorsque plusieurs mécanismes de sécurité sont combinés. Aujourd'hui, aucun utilisateur, appareil ou application ne devrait bénéficier d'une confiance implicite.

Les solutions de communications unifiées et de collaboration qui mettent en œuvre un modèle de sécurité ZTNA (Zero Trust Network Access) contribuent à lutter efficacement contre des menaces en constante évolution. Le modèle ZTNA ne fait confiance à aucun utilisateur, appareil ou application, quel que soit l'endroit où il se trouve. Ce modèle repose sur cinq affirmations clés :

- Le réseau est hostile
- Les menaces externes et internes sont omniprésentes
- La localisation et l'identité ne suffisent pas à accorder la confiance
- Chaque appareil, chaque utilisateur et chaque flux de réseau doit être authentifié et autorisé
- Les politiques de réseau et de sécurité doivent être dynamiques et utiliser autant de sources de données que possible



3 Macro et micro-segmentation

La macro et la micro-segmentation permettent une approche granulaire et hautement contrôlée de la cybersécurité pour tous les utilisateurs, appareils et applications qui accèdent au réseau.

La macro-segmentation sépare les utilisateurs, les appareils et les applications en fonction de leur domaine fonctionnel, de sorte qu'ils ne peuvent pas communiquer avec les éléments d'autres macro-segments. Par exemple, les applications de communications unifiées et de collaboration d'un macro-segment ne peuvent pas communiquer avec les technologies de sécurité, telles que les caméras de vidéosurveillance et les systèmes de verrouillage des portes d'un deuxième macro-segment, ni avec les capteurs et les commandes d'éclairage, de chauffage et de climatisation d'un troisième macro-segment.

La micro-segmentation définit la manière dont les utilisateurs, les appareils et les applications au sein d'un macro-segment peuvent interagir les uns avec les autres ; elle est généralement régie par des politiques de sécurité très spécifiques. Par exemple, une caméra de surveillance pourrait ne pas être autorisée à s'interfacer avec un verrou de porte, bien qu'ils fassent partie du même macro-segment du point de vue de la sécurité.

4 Chiffrement natif de bout en bout

Dans les organisations globales, les employés, les clients, les partenaires et les fournisseurs peuvent être n'importe où dans le monde. Les solutions qu'ils utilisent pour communiquer et collaborer peuvent être installées dans le bâtiment où ils travaillent, à l'autre bout de la ville ou dans un centre de données à l'autre bout du monde. Dans tous les cas, les échanges d'informations doivent être sécurisés et confidentiels, que ce soit à travers des communications voix, vidéo et texte.

Pour que seuls les participants à la conversation puissent accéder aux informations échangées, chaque conversation doit être entièrement chiffrée, de l'origine à la destination. Cela signifie que chaque élément matériel et logiciel impliqué dans les communications de bout en bout doit incorporer nativement des mécanismes de chiffrement approuvés par les agences de sécurité.

5 Certifications et accréditations en matière de sécurité et de protection de la vie privée

Il y a quelques années à peine, les certifications et accréditations les plus strictes en matière de sécurité n'étaient exigées que pour les produits de sécurité, tels que les pare-feux, ou dans des secteurs particuliers, tels que la défense. Aujourd'hui, des normes de sécurité spécifiques doivent être appliquées à tous les produits technologiques, dans tous les secteurs d'activité.

Il est extrêmement important de vérifier que les affirmations en matière de cybersécurité sont étayées par des certifications et des accréditations reconnues. Voici quelques exemples de conformité à valider :

- **Normes mondiales de sécurité et de protection de la vie privée**, telles que ISO 27001 pour la sécurité de l'information, ISO 27017 pour des environnements cloud plus sûrs, ISO 27018 pour la protection des informations personnelles identifiables dans les environnements cloud, et la certification Critères Communs EAL (Common Criteria Evaluation Assurance Level - EAL) 2 et supérieure pour la sécurité des systèmes informatiques
- **Normes sectorielles de sécurité et de protection de la vie privée**, telles que la loi HIPAA (Health Insurance Portability and Accountability Act) aux États-Unis et la certification HDS (Hébergeurs de Données de Santé) en France
- **Normes régionales de sécurité et de protection de la vie privée**, telles que le Règlement Général sur la Protection des Données (RGPD) dans l'Union Européenne

6 Tests de sécurité continus et spécialisés

À l'instar des normes de sécurité, les processus de test de sécurité spécialisés, autrefois réservés aux produits de sécurité, sont désormais obligatoires pour les solutions de communications unifiées et de collaboration.

Les tests de pénétration en sont un bon exemple. Ces tests simulent des cyberattaques afin de révéler les vulnérabilités en matière de sécurité et d'y remédier de manière proactive avant que les problèmes ne surviennent. Pour garder une longueur d'avance sur les cybermenaces dans un paysage en constante évolution, les tests de pénétration, qui sont uniquement motivés par des exigences de cybersécurité, doivent être effectués de façon continue.

Les fournisseurs de technologie qui s'engagent à aider leurs clients à maintenir une cybersécurité maximale doivent fournir les ressources, les outils et l'expertise nécessaires pour effectuer ces tests de pénétration en continu.



Atteindre les objectifs de l'entreprise avec moins de risques

Les solutions de communications unifiées et de collaboration qui mettent en œuvre l'ensemble des mesures de cybersécurité décrites dans la section précédente offrent aux entreprises et aux organismes publics la liberté et la souplesse nécessaires pour développer leurs activités tout en minimisant les risques et en garantissant d'être en conformité. Ces solutions ont la capacité de :

- **Équiper les employés** avec les moyens adaptés pour collaborer et partager des informations en toute sécurité et en toute confidentialité sur n'importe quel support et n'importe quel appareil, où qu'ils se trouvent
- **Améliorer l'expérience client** grâce à des communications enrichies, pertinentes et contextuelles, offrant la capacité d'une prise de décision plus rapide, la possibilité de processus métier automatisés et permettant de détecter de manière proactive les problèmes avant qu'ils n'affectent le client
- **Accroître l'excellence opérationnelle et l'agilité** en utilisant une infrastructure numérique déployée là où elle est la plus judicieuse pour l'organisation — sur site ou dans un cloud hybride, privé ou public — tout en adhérant à des politiques strictes en matière de confidentialité des données et en garantissant la conformité avec les réglementations relatives à la confidentialité des données

Les cas d'usage décrits ci-dessous mettent en évidence quelques-unes des possibilités offertes et qui peuvent facilement être adaptées à d'autres besoins et à d'autres secteurs d'activité.

Créer un espace de travail numérique flexible pour renforcer l'autonomie des employés

Avec une combinaison adéquate de solutions de communication et de collaboration sécurisées, les employés peuvent travailler de manière plus rapide et plus flexible, tout en respectant totalement les réglementations en vigueur dans leur secteur d'activité.

- **Dans le secteur de la santé**, un effectif très mobile peut collaborer et partager des informations tout en respectant les normes de sécurité des données des patients. Les équipes peuvent facilement se transmettre des informations pour assurer la continuité des soins et obtenir rapidement l'assistance requise. Le personnel médical peut utiliser des communications sécurisées en temps réel pour améliorer l'efficacité du flux des tâches médicales et la disponibilité des résultats pour les patients. Le personnel non médical peut accélérer les processus et les réponses aux problèmes de maintenance susceptibles d'affecter la sécurité des patients et des soignants.
- **Dans le secteur de l'éducation**, les enseignants peuvent proposer des expériences d'apprentissage à distance plus riches et plus attractives, avec davantage de possibilités pour les élèves et étudiants de participer à des activités, de collaborer à des projets et d'interagir en utilisant le support de leur choix. Grâce à un contrôle d'accès complet et automatisé, l'intégrité des données est préservée alors que les ressources du réseau sont hiérarchisées suivant le degré d'importance des communications.
- **Dans les administrations**, le personnel peut échanger des informations en toute sécurité au sein d'équipes dispersées. La collaboration peut être améliorée avec le partage d'écran, le contrôle à distance du bureau du PC et l'échange de fichiers volumineux. Le personnel peut également interagir en toute sécurité avec les citoyens sur des applications web ou mobiles utilisant la voix, la vidéo, le chat ou la messagerie instantanée.
- **Dans les transports**, un espace de travail numérique permet aux employés d'utiliser leurs propres appareils, de rendre les processus plus efficaces et de fournir aux passagers des services à valeur ajoutée, tels que la possibilité de travailler pendant leur voyage. Les données sont protégées partout sur le réseau grâce à des protocoles de communication sécurisés, des systèmes durcis et un code diversifié.

Livre blanc

Sécuriser les solutions de communications unifiées et de collaboration

Tout connecter pour améliorer l'expérience client

La connexion sécurisée de personnes, d'objets et d'applications avec des communications en temps réel permet aux entreprises et aux organismes publics de :

- Équiper leurs employés des appareils, des technologies et des informations nécessaires pour assister les clients, tout en réduisant le risque que l'erreur humaine ou la méconnaissance des risques de sécurité ne la compromette.
- Utiliser des appareils intégrés et sécurisés pour communiquer et collaborer avec les clients en mobilité, grâce à un accès complet à leurs solutions de gestion de la relation client (CRM)
- Accroître la protection, le contrôle et la visibilité sur une gamme variée d'appareils de l'Internet des objets (IoT), dont l'utilisation se développe constamment.
- Maintenir les systèmes de communication et de collaboration à jour afin d'éviter que des applications obsolètes n'augmentent la surface d'attaque et n'exposent les vulnérabilités.
- Mettre en place des contrôles d'accès efficaces et un chiffrement de bout en bout sur toutes les plateformes.

La gestion unifiée du réseau permet de gérer de manière holistique l'ensemble des plateformes de communication, des applications et des appareils IoT. Ainsi, elle permet de :

- Simplifier les tâches de gestion sur les réseaux filaires et sans fil et les appareils IoT afin de réduire les coûts de gestion du réseau, d'optimiser les performances et d'augmenter l'efficacité opérationnelle.
- Accélérer le dépannage dans des environnements technologiques de plus en plus diversifiés afin de réduire le risque d'interruption de service et de temps d'arrêt.

La gestion unifiée des réseaux dans tous les secteurs d'activité offre de nombreux avantages. Voici quelques exemples :

Dans le secteur de la santé, les solutions IoT permettent de localiser les équipements critiques tels que les bouteilles d'oxygène, les brancards, les moniteurs de surveillance, les perches à perfusion et les fauteuils roulants, afin d'améliorer la sécurité des patients et l'efficacité du personnel. La connectivité entre les personnes, les objets et les applications peuvent également servir à déclencher des alarmes qui notifient le personnel médical des appels des patients, des dysfonctionnements des équipements médicaux, et qui peuvent alerter tous les membres de l'établissement en cas de danger.

Dans le domaine de l'éducation, il est possible de connecter les appareils et les applications des campus intelligents à plusieurs niveaux de sécurité afin d'empêcher des appareils insuffisamment sécurisés d'accéder au réseau. Les établissements scolaires peuvent également utiliser l'empreinte digitale des appareils IoT à connecter à leur réseau pour identifier les caractéristiques des appareils telles que le type, le fabricant, le modèle et le système d'exploitation, afin de simplifier et d'accélérer la configuration du réseau IoT et l'intégration des appareils.

Livre blanc

Sécuriser les solutions de communications unifiées et de collaboration



Accroître l'excellence opérationnelle et l'agilité

Grâce à la possibilité de déployer en toute sécurité des solutions de communications unifiées et de collaboration sur site ou dans un cloud hybride, privé ou public, les entreprises et les organismes publics peuvent bénéficier des technologies numériques de la manière qui correspond le mieux à leurs objectifs et à leur mission. Chaque organisation peut atteindre de nouveaux niveaux d'excellence opérationnelle, tout en répondant aux exigences spécifiques à son secteur, en adoptant des modèles de cloud qui améliorent les opérations et amènent de l'agilité telles que dans :

- **Le secteur de la santé**, où les dossiers numérisés des patients contribuent à améliorer les soins et à renforcer l'efficacité des soignants, avec la certitude que les données personnelles de santé sont stockées dans un centre de données sécurisé et certifié dans le cloud.
- **L'éducation**, où les enseignants, le personnel administratif et les étudiants bénéficient d'un accès sécurisé et confidentiel à des applications et services dans le cloud, où qu'ils se trouvent. Les services IT peuvent ainsi réduire le temps et les coûts associés au déploiement, à l'assistance et à la mise à jour de la grande variété des applications utilisées dans l'enseignement.
- **L'administration**, où les communications confidentielles doivent offrir une haute disponibilité et être protégées par des mécanismes DoS natifs, ainsi que par du hardware et des systèmes d'exploitation durcis.
- **Les transports**, où les solutions de communication sont critiques en termes de résilience et de souveraineté des données, l'altération des capacités de communication pouvant conduire à des situations dangereuses pour les voyageurs et le personnel.

Cybersécurité : au coeur des pratiques du fournisseur de technologie

Si de nombreux fournisseurs de technologie mettent l'accent sur la cybersécurité, tous ne disposent pas de l'expertise nécessaire pour mettre en œuvre une sécurité de bout en bout.

Alcatel-Lucent Enterprise va plus loin que les autres fournisseurs en mettant en œuvre toutes les bonnes pratiques requises pour une cybersécurité de bout en bout. Nous appliquons ces bonnes pratiques à nos solutions :

- Suivi des recommandations du National Institute of Science and Technology (NIST) lors de l'évaluation des risques liés aux nouvelles fonctionnalités et lors de la mise en œuvre de fonctions de cybersécurité, telles que le chiffrement natif
- Renouvellement de la certification Critères Communs EAL2+
- Respect des normes ISO 27001 appliquées à toutes nos solutions basées sur le cloud
- Support du modèle ZTNA, correspondant à la segmentation granulaire du réseau et à des politiques de sécurité très spécifiques afin de réduire le risque d'activités non autorisées
- Exécution de tests hautement spécialisés et spécifiques à la sécurité, tels que des tests de pénétration, sur tous nos produits
- Obtention de certifications clés dans certaines industries, telles que HDS, HIPAA et FERPA (Family Educational Rights and Privacy Act) comme Rainbow d'Alcatel-Lucent Enterprise.

En tant qu'experts reconnus en matière de cybersécurité, nous contribuons aux propositions de directives de l'Union Européenne dans le domaine. Nous mettons également à profit notre expertise pour aider nos clients à choisir et à mettre en œuvre la combinaison de solutions de communications unifiées et de collaboration sécurisées la mieux adaptée à leurs besoins et à former leurs employés aux bonnes pratiques en matière de cybersécurité.

En savoir plus

Pour savoir comment nous pouvons aider votre organisation à tirer pleinement parti des solutions sécurisées de communications de l'ère numérique, [visitez notre site web](#) ou [contactez-nous dès aujourd'hui](#).

Les solutions Alcatel-Lucent Enterprise sont reconnues dans le monde entier pour leur fiabilité

De grands noms dans tous les secteurs d'activité s'appuient sur nos solutions sécurisées de communications de l'ère numérique pour atteindre leurs objectifs :

- [La métropole et la ville de Perpignan](#) en France, où les autorités publiques mettent en œuvre un plan stratégique de transition numérique qui comprend la visioconférence et les communications voix pour les employés, le support des applications IoT, ainsi que de nouveaux contenus et services pour les habitants de Perpignan, les touristes et les employés municipaux.
- [Newman University](#) aux États-Unis, une université catholique d'études interdisciplinaires d'art, qui a doté son personnel de fonctionnalités de téléphonie mobile ne nécessitant pas de numéros de téléphone directs. Son équipe informatique utilise une plateforme unique, intuitive et basée sur le cloud pour gérer, provisionner et surveiller l'ensemble de l'infrastructure réseau.
- [Kingsway Hospitals](#) en Inde, qui a mis en œuvre des solutions d'infrastructure de communication en temps réel qui permettent au personnel médical et administratif de rester connecté afin d'optimiser le parcours de soins et d'améliorer l'expérience des patients.
- [J. Malucelli Group](#) au Brésil, qui a modernisé son réseau avec une solution convergée voix et données comprenant la téléphonie dans le cloud ainsi que des réseaux LAN et Wi-Fi avec gestion dans le cloud, afin de simplifier et de réduire le coût des communications entre plusieurs entreprises du groupe.

