Risque, résilience et sécurité pour les gouvernements et les villes

Les bonnes pratiques et les technologies pour maintenir la continuité de l'activité

Alcatel·Lucent Enterprise

Sommaire

La sécurité et la résilience constituent des priorités impérieuses

Aujourd'hui, les gouvernements et les villes du monde entier sont confrontés à une polycrise, c'est-à-dire une convergence de risques cyber et physiques qui menacent les citoyens, les services essentiels et les données sensibles.

Les citoyens s'attendent désormais à recevoir des services fournis par des sites web sécurisés et à pouvoir compter sur eux. Les employés souhaitent travailler à domicile ou au bureau, en fonction de leurs besoins et de leurs préférences. Ces nouvelles exigences, ainsi que la propagation exponentielle des appareils de l'Internet des objets (IoT), repoussent les limites du réseau à un moment où les tensions géopolitiques et la polarisation politique augmentent le risque de cyberattaques.

En outre, le « dark web » (web caché) a créé un marché rentable pour la vente anonyme de données gouvernementales sensibles, ce qui transforme les systèmes gouvernementaux en des cibles très attrayantes pour le vol d'informations. Il offre également un refuge en ligne pour coordonner les attaques contre les gouvernements.

Le vandalisme, le terrorisme, les émeutes et la criminalité sont également en augmentation, créant des menaces de plus en plus grandes pour les infrastructures civiles et de défense et pour la continuité des activités. À cela, s'ajoutent les phénomènes météorologiques violents et les catastrophes naturelles qui rendent très difficile, voire impossible, la prestation des services publics et le maintien de la sécurité des citoyens lorsqu'ils en ont le plus besoin. Par ailleurs, avec l'inflation mondiale qui pèse sur les budgets, le besoin d'initiatives de numérisation qui augmentent la flexibilité, l'efficacité et la productivité des opérations n'a jamais été aussi élevé.

Ensemble, ces risques font qu'il est plus difficile que jamais pour les gouvernements et les villes de rester en conformité avec les réglementations de plus en plus strictes en matière de souveraineté des données et de protection de la vie privée. Par conséquent, le risque d'amendes et de poursuites pour infraction est considérable.

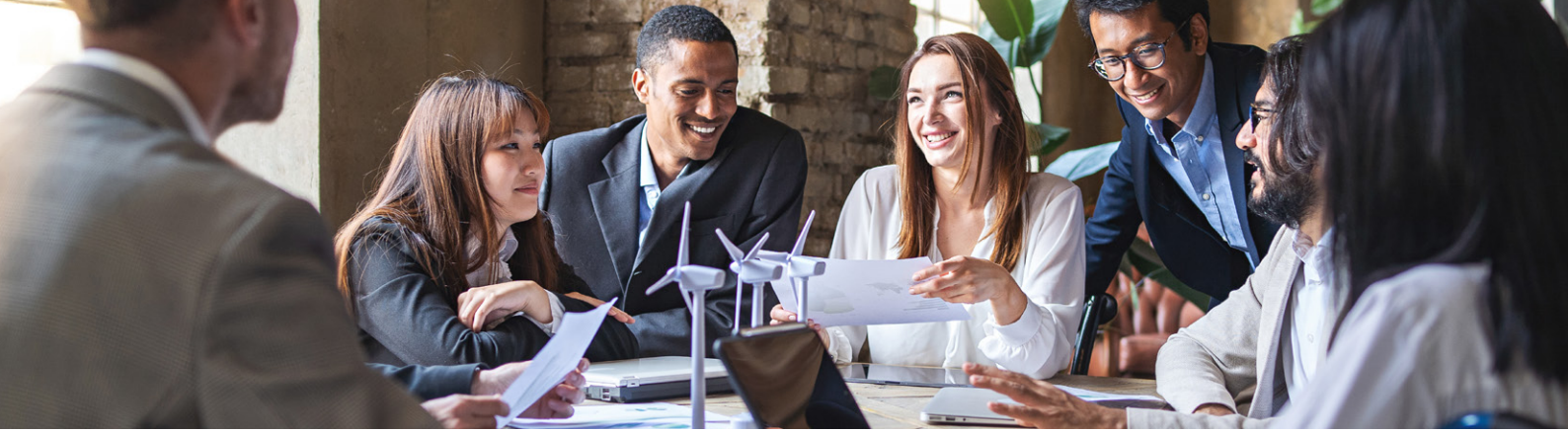
Face à cette nouvelle réalité, les gouvernements et les villes ne peuvent plus s'appuyer sur leurs anciennes stratégies en matière de sécurité et de résilience. Afin d'atténuer ces risques, ils doivent prendre des mesures audacieuses et proactives pour améliorer leur position globale en matière de sécurité. Il devient nécessaire d'adopter une approche nouvelle, innovante et mieux adaptée aux menaces les plus importantes d'aujourd'hui. Grâce à une sécurité renforcée, les gouvernements et les villes seront davantage en mesure de protéger les citoyens et les opérations et de renforcer leur résilience afin d'assurer la continuité de leurs activités en toutes circonstances.

Les risques sont bien réels

Malheureusement, il est trop facile pour les gouvernements et les villes de retarder les mesures d'atténuation des risques, en particulier lorsque les incidents qui font la une des journaux ne se produisent que dans des lieux éloignés. Mais en réalité, chaque organisation gouvernementale est une cible potentielle d'attaques.

Un rappel à la réalité

- Les cyberattaques contre les gouvernements ont fait un bond de 95 % au cours du second semestre 2022.[1]
- L'attaque contre le gouvernement du Costa Rica a été considérée comme l'une des plus coûteuses de l'année[2], les attaques avec demande de rançon étant une méthode privilégiée pour attaquer les services publics[3].
- D'ici 2025, on estime que 30 % des organisations d'infrastructures stratégiques seront victimes d'une faille de sécurité.[4]



Alors que les populations urbaines continuent de croître,[5] les risques pour les gouvernements et les citoyens ne cessent d'augmenter. Ainsi, les Nations Unies conseillent aux gouvernements de faire en sorte que les villes et les établissements humains soient ouverts à tous, sûrs, résilients et durables, comme indiqué dans l'objectif 11.[6]

---

[1] Les cyberattaques contre les gouvernements ont grimpés de 95% durant la dernière moitié de 2022, selon CloudSek. CSO États-Unis, janvier 2023.

[2] les 13 Cyberattaques les plus coûteuses de 2022: un regard en arrière Renseignements de Securité, décembre 2022.

[3] Document d'orientation : Cyberstratégie nationale 2022. U.K Cabinet Office, décembre 2022.

[4] Gartner prédit que 30 % des organisations d'infrastructures critiques connaîtront une faille de sécurité d'ici 2025. Gartner, décembre 2021.

[5] Développement urbain. Banque mondiale, avril 2023.

[6] Objectif 11 : Faire en sorte que les villes et les établissements humains soient ouverts à tous, sûrs, résilients et durables. Nations Unies.

En raison de tous ces facteurs, il est clair que les gouvernements et les villes doivent accorder une attention accrue aux risques, à la résilience et à la sécurité pour :

- **Assurer la continuité des services essentiels et protéger les données sensibles**, en particulier en cas de crise inattendue
- **Minimiser les coûts d'assurance des risques** par la mise en place d'une protection adaptée à chaque type de cyber risques et physiques auquel ils sont confrontés
- **Réduire les pertes financières** dues aux cyberattaques et aux attaques physiques, aux poursuites judiciaires par les citoyens et aux amendes pour violation de données et non-conformité
- **Préserver leur réputation et la confiance de leurs citoyens**, deux éléments qui peuvent être endommagés ou complètement perdus en raison de retards et de pannes de service
- **Protéger les citoyens** en fournissant des informations importantes relatives à la santé, à la sécurité et à la protection

La numérisation présente des avantages et des risques

Dans le monde numérique d'aujourd'hui, les personnes, les objets et les processus sont connectés. Ces connexions permettent aux gouvernements et aux villes de :

- Tirer parti de la technologie de l'IoT et des informations qu'elle fournit
- Automatiser les flux de travaux afin d'améliorer l'efficacité et d'accélérer les réponses aux citoyens
- Utiliser des données précises en temps réel afin d'accroître la visibilité et de prendre des décisions éclairées
- Mettre en œuvre des applications de bâtiments intelligents qui permettent des opérations plus durables, plus rentables et plus résilientes

Si ces améliorations sont essentielles pour permettre aux gouvernements et aux villes d'atteindre leurs objectifs, les technologies mises en œuvre introduisent également un nouvel ensemble de risques cyber et physiques qu'il convient de prendre en compte.

De nouvelles façons de réfléchir aux vulnérabilités

Avec la numérisation, les vulnérabilités sont plus faciles à mettre en évidence et les menaces peuvent rapidement se répercuter sur les systèmes, appareils et applications interconnectés :

- La défaillance d'un système peut tout affecter
- Les pirates peuvent exploiter les connexions entre les infrastructures pour étendre leur champ d'action
- Les virus peuvent profiter des connexions pour se propager au sein d'une organisation

La numérisation renforce également le lien entre les risques cyber et physiques. Par exemple, des personnes malveillantes peuvent pirater à distance des centres de données gouvernementaux ou obtenir un accès physique en compromettant le verrouillage électronique d'une porte. De même, les caméras de sécurité peuvent être désactivées, déconnectées ou reconnectées à des flux vidéo préenregistrés à la suite d'une attaque cyber ou physique, ce qui, dans les deux cas, les rend inutiles du point de vue de la protection.

La convergence entre les technologies de l'information (IT) et les technologies opérationnelles (OT) crée de nouvelles possibilités d'attaques. Aujourd'hui, les pirates peuvent compromettre un capteur IoT pour accéder au réseau et aux systèmes et ressources d'information de grande valeur qui y sont connectés. Inversement, ils peuvent s'introduire directement dans le réseau et utiliser ce dernier comme passerelle pour attaquer les systèmes critiques du bâtiment tels que les ascenseurs, les détecteurs de fumée, les alarmes incendie et les systèmes d'arrosage.

Les nouvelles technologies peuvent également être utilisées pour ou contre les organisations gouvernementales. Prenons l'exemple de l'intelligence artificielle (IA). L'IA permet de prévenir les cybermenaces et les menaces physiques, de s'en protéger et d'accélérer les réponses, mais elle permet aussi à des acteurs malveillants de déchiffrer les mots de passe des systèmes gouvernementaux. À l'avenir, nous pouvons nous attendre à une situation similaire avec l'informatique quantique, qui aidera les gouvernements à résoudre des problèmes complexes, mais facilitera également le décryptage d'informations sensibles.

Des considérations et défis uniques

Les risques spécifiques liés à la numérisation dépendent des technologies déployées. Les réseaux modernes et les technologies de communication comportent trois risques principaux :

- **Pannes** : les défaillances matérielles et logicielles peuvent survenir à tout moment, sans avertissement. Les incendies, les inondations, les conditions météorologiques extrêmes et d'autres facteurs imprévus peuvent également provoquer des pannes, tandis que les pannes d'électricité peuvent affecter la qualité et la stabilité de la fourniture d'électricité, entraînant des dysfonctionnements et des défaillances.
- **Cyberattaques** : des données confidentielles peuvent être perdues ou volées, et les réseaux et systèmes peuvent être corrompus, ralentissant ou arrêtant complètement les services et opérations du gouvernement. Les attaques par logiciel de rançon peuvent prendre en otage des réseaux et des systèmes entiers, rendant inaccessibles les données et les fonctionnalités critiques.
- **Obsolescence** : les fournisseurs de technologie peuvent mettre fin au support pour le matériel et les logiciels, tandis que les pénuries de la chaîne d'approvisionnement peuvent rendre logistiquement impossible ou trop coûteuse la poursuite de l'utilisation des solutions. L'évolution des exigences en matière de conformité réglementaire peut également rendre les solutions technologiques obsolètes.

Chacun de ces risques peut entraîner les autres. Une panne ou une technologie obsolète peut ouvrir la porte à des cyberattaques, lesquelles pouvant provoquer une panne ou mettre en évidence l'obsolescence d'une technologie.

Ensemble, ces risques signifient que les gouvernements et les villes doivent améliorer leur capacité à prévenir les menaces, à s'en protéger et à y réagir. Ne rien faire n'est plus une option. Continuer à s'appuyer sur des réseaux et des technologies de communication obsolètes et isolés alors que les risques continuent à se multiplier n'est pas une approche viable, quel que soit le point de vue.

Une approche globale et un processus normalisé

Chaque gouvernement et chaque ville se doit d'élaborer une approche stratégique et tactique de la sécurité et de la résilience adaptée à son profil de risque unique, à sa situation géographique, à son mandat, à son budget et à d'autres exigences. Toutefois, même si les résultats de leurs efforts diffèrent, il est utile d'adopter une approche normalisée et de partager les bonnes pratiques afin d'obtenir de meilleurs résultats.

Une approche globale de l'atténuation des risques permet aux gouvernements et aux villes d'accroître la sécurité et la résilience dans trois domaines clés de leur mandat, à savoir :

- **Citoyens** : protéger la sécurité des personnes et les données contre toutes les menaces
- **Opérations** : maintenir des fonctions, des transactions et des services sûrs et fiables en toutes circonstances
- **Bâtiments** : rendre les lieux de travail et les espaces publics plus intelligents et plus sûrs

Quatre étapes pour renforcer la sécurité et la résilience

En tenant compte des points avancés ci-dessus, les étapes suivantes peuvent aider les gouvernements et les villes à déterminer leur profil de risque et à choisir les solutions de réseau et de communication adaptées à leur situation spécifique.

1. **Évaluer** : identifier les risques cyber et physiques, les zones d'exposition et les conséquences potentielles, ainsi que les différentes options pour prévenir, protéger et réagir aux attaques dans chaque cas. Commencer par un audit, puis évaluer les risques et les pertes potentielles pour chaque vulnérabilité identifiée. Cela permet d'identifier les actions et les solutions appropriées dans chaque cas.

   Si l'évaluation est la première étape, elle n'est pas une activité ponctuelle. Afin de contrer l'évolution rapide du paysage des menaces, il est important de réévaluer régulièrement les risques et de surveiller en permanence les ressources cyber et physiques pour détecter de nouvelles vulnérabilités.
2. **Prévenir** : choisir des solutions qui permettent d'éviter ou de contenir les risques cyber et physiques tels que :
   - D'un point de vue cyber, rechercher des solutions dotées de fonctions de sécurité intégrées qui n'ont pas besoin d'être achetées séparément ou renouvelées. Les solutions doivent prendre en compte la sécurité à chaque étape de la définition, du développement et de la livraison du produit, et contribuer à une architecture et à un environnement technologique Zero Trust (confiance zéro). Elles doivent également prendre en charge la sauvegarde et la récupération automatisées et fournir des informations à des fins d'audit.
   - D'un point de vue physique, identifier les solutions qui augmentent la visibilité et rendent l'accès aux équipements plus difficile. Les solutions de vidéosurveillance, de contrôle d'accès, de suivi des équipements, de détection d'intrusion et d'alarme, de services de géolocalisation et de reconnaissance faciale en sont de bons exemples.
3. **Protéger** : choisir des solutions qui vous aident à vous protéger contre les risques cyber et physiques, par exemple :
   - Sur le plan cyber, il convient de s'assurer que les solutions sont certifiées conformes aux normes de sécurité, qu'elles intègrent des capacités de chiffrement natif et des mécanismes d'authentification avancés, et qu'elles limitent la propagation des cyberattaques et des virus
   - Pour renforcer la protection physique, il ne faut pas se contenter d'utiliser la vidéosurveillance, mais il convient aussi de prendre en compte le rôle des communications, des alertes et des notifications, ainsi que des solutions qui permettent de protéger les travailleurs dans les lieux isolés
4. **Réagir** : choisir des solutions qui permettent une récupération efficace en cas de violation de la sécurité, par exemple :
   - Les solutions cyber doivent être prises en charge par une équipe de réponse aux incidents de sécurité des produits, fournir une piste de vérification et des procédures de récupération, et prendre en charge la restauration des données
   - Les solutions physiques doivent prendre en charge les opérations de commande et de contrôle (C2) et les communications essentielles.

Cadre de risque, de résilience et de sécurité pour le secteur public, les gouvernements et les villes

	1 Évaluer	2 Prévenir	3 Protéger	4 Réagir
Sécurité	✓	✓	✓	
Résilience	✓	✓		✓
Cyber	• Identification des risques • Évaluation • Mappage des équipements • valorisation • Surveillance continue	• Sécurité dès la conception • Évaluation/audit des risques • Conseil avant-vente • Formation des utilisateurs • Détection des fraudes • Procédure de sauvegarde • Mise en place d'une piste de vérification • Renforcé pour les environnements difficiles • Redondance	• Certification de sécurité • Chiffrement • Authentification	• PSIRT/CERT • Piste de vérification • Gestion des incidents • Procédures de récupération • Rétablir
Physique	• Identification des risques • Évaluation • valorisation • Surveillance continue	• Vidéosurveillance • Contrôle d'accès • Suivi des équipements • Détection et alarme • Services de localisation • Reconnaissance faciale • Redondance	• Vidéosurveillance • Communications • Alerte et notification • Protection du travailleur isolé	• Contrôle et commande • Communications essentielles

Les mesures de résilience et de réponse souples sont essentielles pour prospérer face aux risques

« La résilience ne se limite pas à la capacité de se rétablir rapidement. Dans le monde des affaires, la résilience consiste à faire face à l'adversité et aux chocs, et à s'adapter en permanence à la croissance. Les organisations véritablement résilientes ne se contentent pas de mieux rebondir, elles prospèrent dans des environnements hostiles... La souplesse leur permet de réagir de manière adaptée à chaque crise, plutôt que d'appliquer des solutions uniques et rigides. »

— McKinsey & Company

Renforcer la sécurité et la résilience

Les gouvernements et les villes qui suivent l'approche globale et le processus recommandés dans la section précédente ont de nouvelles possibilités d'exploiter les solutions de réseau et de communication pour accroître la sécurité et la résilience des citoyens, des opérations, des bâtiments et des espaces.

Protéger la sécurité des citoyens

Grâce à des solutions de vidéosurveillance de pointe, les fonctionnaires et les responsables de la sécurité publique disposent d'une visibilité en temps réel des événements et des situations d'urgence au fur et à mesure qu'ils se déroulent, ce qui permet d'améliorer considérablement la connaissance de la situation. Ils peuvent ensuite utiliser une plateforme d'orchestration de la sécurité publique et de gestion des flux de travaux pour partager ces connaissances et coordonner les réponses. Les équipes des ministères, des agences et des sites gouvernementaux peuvent facilement partager des informations contextuelles et des réflexions en temps opportun en utilisant une combinaison optimale de communications vocales, vidéo et textuelles pour permettre une prise de décision plus efficace, plus efficiente et plus collaborative.

Les systèmes de notification de masse permettent d'alerter rapidement les personnes et les processus en cas d'urgence afin qu'ils puissent prendre les mesures appropriées plus rapidement. Les appels des fonctionnaires sur le terrain sont acheminés en priorité vers les centres de contact du gouvernement, et les capacités de préservation des appels permettent aux fonctionnaires et aux citoyens de rester en contact en toutes circonstances avec le personnel du centre de contact. Les solutions de communication pour les travailleurs isolés, les situations d'homme à terre et la recherche de contacts accélèrent encore les réponses et renforcent la sensibilisation aux situations potentiellement dangereuses.

Afin d'aider à prévenir les situations d'urgence et à accélérer les réponses, les solutions d'IA connectées à de multiples sources de données peuvent être utilisées pour identifier les risques et les événements potentiellement gênants, et pour automatiser les flux de travaux.

Accroître la fiabilité des opérations

Un réseau d'entreprise sécurisé et résilient prend en charge les communications stratégiques ainsi que les technologies IoT, de cybersécurité et de sécurité physique qui sont essentielles à la fiabilité des opérations.

Les solutions de réseau idéales comprennent des caractéristiques indispensables pour protéger l'accès au réseau et aux informations qu'il contient, notamment :

- **Un code source et des logiciels renforcés sur les commutateurs de réseau** : le code source est délibérément varié afin de rendre l'exploitation des vulnérabilités beaucoup plus difficile pour les attaquants potentiels. En outre, le code et les logiciels sont vérifiés et validés de manière indépendante afin de garantir leur intégrité et leur sécurité.
- **Macro- et micro-segmentation** : dans le contexte « Zero Trust », la segmentation fait l'objet d'une attention particulière aux niveaux macro et micro. La macro-segmentation divise le réseau en zones distinctes basées sur des facteurs tels que la fonction, l'application ou le groupe d'utilisateurs, afin d'isoler les ressources et les équipements critiques du reste du réseau. La micro-segmentation adopte, quant à elle, une approche plus granulaire, segmentant le réseau au niveau de l'utilisateur ou de l'appareil pour permettre un contrôle plus fin de l'accès au réseau et de l'application de la politique de sécurité.
- **Opérations autonomes** : l'automatisation du placement des équipements et des ressources dans des macro-segments et l'application de politiques au niveau de l'utilisateur et de l'appareil contribuent à réduire le risque d'erreurs humaines, une cause fréquente d'atteintes à la cybersécurité.
- **Équipements renforcés** : les équipements de réseau peuvent résister à des conditions difficiles telles que des températures extrêmes et de fortes vibrations. L'équipement prend en charge la redondance de l'alimentation à partir de deux sources afin d'assurer la continuité des opérations en cas de panne de courant. Un temps moyen entre les défaillances (MTBF) élevé peut garantir la fiabilité, en minimisant les temps d'arrêt imprévus et les perturbations causées par les pannes et les défaillances.

Les gouvernements et les villes obtiennent également la souplesse requise pour déployer des solutions de réseau et de communication dans leurs locaux ainsi que dans des environnements de clouds publics et privés. Ces options de déploiement permettent d'appliquer des stratégies de redondance géographique et spatiale qui sont essentielles pour maintenir la continuité des activités en cas de défaillance ou d'urgence, même sur des sites distants.

Renforcer la sûreté et la sécurité dans les bâtiments et les espaces

Un réseau multiservice sécurisé est requis pour prendre en charge les applications et les processus nécessaires à la protection contre les risques et au maintien de la disponibilité du service à tout moment. Afin de prendre en compte le nombre croissant d'appareils sans fil connectés au réseau Wi-Fi, les gouvernements et les villes auront besoin d'un réseau sans fil robuste et fiable qui fonctionne sans encombrement susceptible d'en réduire l'efficacité.

Les solutions de vidéosurveillance avancées qui contribuent à la protection des citoyens permettent également d'assurer la sécurité des bâtiments et des espaces publics. Ces solutions sont complétées par le suivi des équipements qui permet de retrouver plus rapidement et plus facilement les personnes et les équipements essentiels lors d'événements inattendus et de situations d'urgence.

Les gouvernements et les villes disposent désormais des capacités d'automatisation nécessaires pour mettre en œuvre et gérer efficacement les solutions IoT pour les applications de sûreté et de sécurité, telles que le contrôle d'accès et le suivi des équipements. Ils peuvent intégrer automatiquement et en toute sécurité un grand nombre de nouveaux appareils IoT avec l'identification des empreintes numériques des dispositifs, la classification et la conteneurisation des appareils, sans risquer que le personnel informatique distrait introduise des vulnérabilités par inadvertance.

Un partenaire pour soutenir vos stratégies

Les risques auxquels sont exposés les gouvernements et les villes ne cessent de croître, d'où la nécessité de disposer d'un partenaire technologique expert.

Alcatel-Lucent Enterprise, innovateur technologique depuis plus de 100 ans, a développé un cadre de risque, de résilience et de sécurité (RRS) qui s'aligne sur les exigences des gouvernements et des villes. Le cadre RRS comprend les processus, les bonnes pratiques et les solutions dont les gouvernements et les villes ont besoin pour prévoir, surveiller, éviter et contrer l'exposition aux cyber risques et aux risques physiques.

L'équipe d'ALE, composée de spécialistes gouvernementaux extrêmement compétents, travaille en partenariat avec le gouvernement et les responsables municipaux pour les aider à :

- Identifier l'ensemble des risques qui leur sont propres et choisir des solutions pour y faire face
- combler l'écart entre la cybersécurité et la sécurité physique, et la résilience
- Faire valoir ses arguments pour l'approbation du budget

Des solutions flexibles et entièrement conformes

ALE intègre la sécurité dans ses solutions de réseau et de communication dès les premières étapes de la conception. Pour garantir une sécurité et une résilience maximales, les solutions :

- Sont conçues avec des mesures de sécurité approuvées par les gouvernements et les organisations de défense du monde entier
- Sont testées à l'aide de techniques spécialisées et spécifiques à la sécurité, telles que les tests de pénétration
- Respectent les normes mondiales, sectorielles et régionales en matière de sécurité des données et de protection de la vie privée, notamment les principales normes de sécurité du secteur, telles que les Critères communs EAL2+.
- Peuvent être déployées dans n'importe quelle combinaison de modèles sur site et dans le cloud afin de répondre aux exigences les plus complexes
- Prennent en charge les normes ouvertes afin de réduire les complexités d'intégration et les incompatibilités entre les solutions et les fournisseurs

Outre les modèles d'achat traditionnels, ALE propose des plans d'abonnement qui permettent aux clients d'accéder aux dernières technologies avancées en matière de sécurité tout en respectant les contraintes budgétaires. Une gamme complète de services est également disponible pour aider les gouvernements et les villes à chaque étape de leur parcours.

Expérience + expertise

Les experts et les solutions d'ALE bénéficient de la confiance des organisations gouvernementales et municipales du monde entier. Voici quelques exemples :

- L'Eurométropole de Metz en France, où ALE a aidé l'agglomération à assurer la continuité des services essentiels et des communications, à rendre rapidement disponibles les services d'urgence et à relier en toute sécurité les utilisateurs et les objets connectés à travers les bâtiments.
- Le gouvernement écossais, où les solutions ALE fournissent une infrastructure cohérente, sûre et fiable et un contrôle d'accès au réseau, ainsi qu'une sécurité des données renforcée, pour plus de 40 agences gouvernementales.
- Le département de la Défense des États-Unis, où des solutions modernes et robustes prennent en charge de manière fiable les communications et les applications stratégiques tout en répondant à toutes les exigences en matière d'environnement et de chocs, ainsi qu'aux exigences du Trade Agreement Act (TAA) et de la certification en matière de défense..
- Les écoles publiques du Comté de Gwinnett aux États-Unis, où les solutions ALE prennent en charge la sécurité physique, la vidéosurveillance, l'E-911, l'informatique sécurisée et bien d'autres choses encore dans un grand district scolaire où la sûreté et la sécurité sont primordiales.

En savoir plus

Pour découvrir comment Alcatel-Lucent Enterprise peut aider votre entreprise à réduire les risques et à renforcer la sécurité et la résilience, visitez le site Web ou contactez-nous dès aujourd'hui.

DID23061901FR (Decembre 2023)

Alcatel·Lucent Enterprise