Les objets connectés (IoT) dans les entreprises et les organisations

Construisez une base solide pour exploiter tout le potentiel de l'IoT , quel que soit votre secteur d'activité

Fiche solution

Alcatel·Lucent Enterprise

L'IoT : une nouvelle donne pour les organisations

En conjuguant les grandes orientations techniques et commerciales, notamment la mobilité, l'automatisation et l'analyse des données, l'Internet des objets (IoT) a la capacité de transformer les organisations en modifiant profondément la manière dont elles recueillent les données et les informations. L'IoT désigne la mise en réseau d'objets physiques, de capteurs, actionneurs ou autres dispositifs intégrés, qui peuvent recueillir et transmettre en temps réel des informations concernant l'activité sur le réseau. Les données collectées par ces dispositifs peuvent ensuite être analysées pour :

- **Optimiser les processus**, par la réduction des coûts d'exploitation, l'augmentation de la productivité et le développement de nouveaux produits et services
- **En savoir plus sur les besoins et les préférences des clients,** ce qui permet de proposer des produits et des services plus adaptés
- **Améliorer la pertinence et la performance** en surveillant préventivement les infrastructures critiques et en créant des processus plus efficaces
- **Optimiser l'expérience de l'utilisateur,** en proposant de nouveaux produits et services ou en améliorant ceux qui existent déjà pour permettre à une organisation orientée données de se démarquer de ses concurrents

L'essor de l'IoT se poursuit

Les professionnels de l'informatique de différents secteurs anticipent une intensification de l'utilisation des solutions IoT dans un avenir proche. En 2022, le marché de l'Internet des objets devrait connaître une croissance de 18 % pour atteindre 14,4 milliards de connexions actives. D'ici à 2025, avec l'allègement des contraintes d'approvisionnement et une nouvelle accélération de la croissance, quelque 27 milliards d'appareils IoT devraient être connectés.

Source : https://iot-analytics.com/number-connected-iot-devices

Les défis du déploiement de l'IoT

L'IoT génère des flux de données sans précédent, ce qui pose des problèmes de performance, d'exploitation et de gestion au niveau de l'infrastructure réseau, ainsi qu'une augmentation des risques de sécurité à partir de tous les terminaux. Pour relever ces défis, vous devez repenser la conception traditionnelle de vos réseaux afin d'atteindre des niveaux supérieurs de renseignement, d'automatisation et de sécurité.

Elles doivent disposer d'une infrastructure réseau rentable, apte à traiter en toute sécurité de vastes flux de données, mais également simple à gérer et exploiter. L'infrastructure doit :

- **Fournir un processus simple et automatisé pour l'intégration des dispositifs IoT.** Les grands systèmes IoT peuvent regrouper des milliers d'appareils ou de capteurs, or la mise à disposition et la gestion manuelles de tous ces terminaux sont complexes et peuvent être une source d'erreurs. Grâce à une intégration automatisée, l'infrastructure réseau peut reconnaître dynamiquement les appareils et les affecter à un réseau sécurisé et approprié.
- **Fournir les ressources réseau adéquates pour que le système IoT fonctionne correctement et efficacement.** Un grand nombre d'appareils du système IoT transmettent des informations stratégiques qui nécessitent un niveau spécifique de qualité de service (QoS). Par exemple, certains types d'utilisation nécessitent des réservations de bande passante appropriées sur une infrastructure de réseau hautement performante afin de garantir la prestation et la fiabilité du service.
- **Garantir un environnement sécurisé contre les cyberattaques et les pertes de données.** Dans la mesure où l'abondance de dispositifs et de capteurs mis en réseau dans l'IoT multiplie les vecteurs d'attaque potentiels, la sécurité joue un rôle essentiel dans l'atténuation des risques de cybercriminalité. La sécurité est nécessaire à plusieurs niveaux, y compris la segmentation des réseaux IoT mêmes.

L'IoT exacerbe la vulnérabilité à la cybercriminalité

L'essor de l'IoT s'accompagne également d'une explosion des menaces de cybersécurité, car la prolifération des capteurs et des dispositifs connectés amplifie considérablement le champ d'attaque du réseau. L'IoT est particulièrement vulnérable, car de nombreux appareils IoT sont fabriqués sans prendre en compte la sécurité, ou construits par des entreprises qui ne comprennent pas les exigences actuelles en matière de sécurité. De ce fait, les systèmes IoT constituent de plus en plus le maillon faible de la sécurité des entreprises.

Steve Turner, analyste chez Forrester, révèle une répartition plutôt uniforme des attaques de ransomwares parmi les secteurs d'activité. Toutefois, ce sont les incidents liés aux ransomwares dans certains secteurs, tels que les infrastructures stratégiques et la santé, qui retiennent généralement l'attention des médias.[1]

Les dispositifs IoT présentent des risques pour les équipements sur l'ensemble du réseau. La création de silos via une segmentation virtuelle du réseau permet d'isoler les appareils IoT et les applications qui les contrôlent, ce qui réduit les menaces et élimine le coût et la complexité des réseaux distincts.

[1]https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond

Mise en place d'une infrastructure de réseau IoT sécurisée

La protection du trafic et des appareils IoT constitue un défi qui ne peut être relevé par une seule et même technologie de sécurité. Cette protection nécessite une approche stratégique qui repose sur plusieurs mécanismes de sécurité.

Pour vous aider à exploiter tout le potentiel du déploiement de l'IoT et à en limiter les risques, Alcatel-Lucent Enterprise (ALE) propose une stratégie de réseau "zero-trust" (ou à confiance zéro), assortie d'une sécurité multi-niveaux.

La stratégie d'ALE assure une protection à chaque niveau de l'infrastructure, de chaque utilisateur et chaque dispositif jusqu'à la couche réseau même. La macro-segmentation et la micro-segmentation du réseau garantissent une approche simple et sûre pour intégrer les appareils en toute sécurité et fournir les ressources réseau adéquates afin d'exploiter le système correctement et efficacement, le tout dans un environnement sécurisé qui protège les entreprises des cyberattaques.

Segmentation de l'IoT

Pour permettre la segmentation de l'IoT, des profils sont attribués à tous les utilisateurs, appareils et applications du réseau ALE. Ces profils, qui définissent les rôles, les autorisations d'accès, les niveaux de qualité de service (QoS) et d'autres informations stratégiques, sont relayés à tous les commutateurs et points d'accès du réseau.

- La macro-segmentation consiste à répartir des dispositifs dans des « segments virtuels », à l'aide de techniques de virtualisation du réseau ; ainsi, plusieurs appareils et réseaux peuvent partager la même infrastructure physique, tout en restant isolés du reste du réseau.
- La micro-segmentation consiste à appliquer différentes règles de QoS et de sécurité aux dispositifs contenus dans chaque segment virtuel. Cette méthode renforce la granularité et la sécurité du réseau, en empêchant les différents types de dispositifs d'un même segment d'interagir les uns avec les autres alors qu'ils ne sont pas conçus pour cela.
- Grâce à la macro-segmentation et à la micro-segmentation du réseau, si un dispositif est attaqué dans une partie du réseau, non seulement cette violation n'affecte pas les dispositifs ou les applications des autres segments virtuels, mais elle ne peut pas se propager à d'autres types de dispositifs au sein du segment infecté
- Lorsqu'un nouveau dispositif IoT est connecté, le réseau reconnaît automatiquement son profil et l'affecte à l'environnement virtuel approprié
- La communication est limitée aux appareils de cet environnement virtuel et à l'application du data center qui les contrôle
- Dans la mesure où tous les utilisateurs ont également des profils au sein du réseau, l'accès aux segments virtuels de l'IoT peut être limité aux personnes et aux groupes autorisés

Sécurité multi-niveaux

- Outre la segmentation de l'IoT, les technologies réseau d'Alcatel-Lucent Enterprise offrent une sécurité stratifiée sur plusieurs niveaux du réseau
- Au niveau des utilisateurs, les profils garantissent que les utilisateurs sont authentifiés et habilités par les droits d'accès appropriés
- Au niveau des appareils, le réseau garantit que les appareils sont authentifiés et conformes aux règles de sécurité établies
- Au niveau des applications, le réseau peut instaurer des règles pour chaque application ou groupe d'applications, notamment le blocage, la limitation de la bande passante et le contrôle de l'accès à chaque application
- Au niveau du réseau, les commutateurs ALE bénéficient d'un code diversifié et sécurisé. Ce code protège les réseaux de toute vulnérabilité intrinsèque, des exploitations de code, des programmes malveillants intégrés et des éventuelles portes dérobées qui pourraient compromettre les commutateurs, les routeurs et tout autre dispositif stratégique.
- Le module Smart Analytics d'ALE utilise une fonctionnalité d'inspection approfondie des paquets ainsi que d'autres technologies, capables de détecter le type de données et d'applications sur le réseau, permettant ainsi d'identifier un trafic réseau inhabituel, des activités non autorisées et des intrusions sur le réseau

Gestion d'exploitation et du réseau de bout en bout

Les solutions réseau d'Alcatel-Lucent Enterprise offrent également des avantages considérables en matière d'exploitation et de gestion.

- ALE permet d'exploiter plusieurs réseaux virtuels distincts sur une seule infrastructure commune, ce qui évite d'avoir à investir dans plusieurs infrastructures physiques
- La solution d'accès unifié d'ALE permet aux technologies filaires et sans fil de constituer un réseau unique et robuste, doté de services réseau communs, d'un cadre stratégique, d'un schéma d'authentification commun et d'une base de données d'authentification unique
- Les solutions réseau d'Alcatel-Lucent Enterprise disposent également d'un système de gestion unique pour tous les éléments de l'infrastructure, notamment la gestion unifiée des réseaux LAN (filaires) et WLAN (sans fil). Les systèmes de gestion de réseau dans le cloud Alcatel-Lucent OmniVista® 2500 Network Management System et Alcatel-Lucent OmniVista® Cirrus Network Management as a Service proposent une interface unique pour gérer les environnements virtuels, les commutateurs, les points d'accès et tous les autres composants du réseau.

Un portefeuille de réseaux performants

Les commutateurs, points d'accès et contrôleurs ALE supportent la dernière génération de capacités à large bande passante et à faible latence, et peuvent gérer un grand nombre de dispositifs dans des environnements à haute densité. Les produits et solutions de réseau ALE répondent aux besoins de réseau des entreprises de toutes tailles. ALE propose également une sélection de commutateurs, de points d'accès et de routeurs renforcés pour les déploiements de réseaux en extérieur ou dans des environnements difficiles.

Scénarios IoT dans les secteurs clés

Les solutions IoT promettent aux entreprises de gagner en intelligence et en efficacité. Ces avantages sont particulièrement remarquables dans certains secteurs d'activité.

Santé

L'IoT a le potentiel de transformer le secteur de la santé en remaniant profondément la collecte et l'utilisation des données par les hôpitaux, les cliniques et autres établissements de santé, en conjuguant les grandes tendances techniques et commerciales que sont la mobilité, l'automatisation et l'analyse des données afin d'améliorer la délivrance des soins aux patients. Les données recueillies à partir de ces dispositifs peuvent ensuite être analysées par l'établissement pour :

- Améliorer les soins aux patients, en proposant des services et une prestation de soins inédits ou enrichis qui permettent à un établissement de santé orienté données de se démarquer de ses concurrents
- Optimiser les processus, en développant de nouveaux services, flux de travail et solutions qui augmentent l'efficacité et réduisent les coûts d'exploitation
- En savoir plus sur les besoins et les préférences des patients, permetant aux établissements de santé d'offrir des soins et une expérience plus adaptés
- Renforcer l'intelligence des réseaux des hôpitaux, en surveillant préventivement les infrastructures critiques et en automatisant le déploiement et la gestion de l'infrastructure informatique

L'essor de l'IoT dans le secteur de la santé s'accompagne également d'une explosion des menaces de cybersécurité, car la prolifération des capteurs et des dispositifs connectés amplifie considérablement le champ d'attaque du réseau.
L'IoT dans le secteur de la santé est particulièrement vulnérable, car de nombreux appareils IoT sont fabriqués sans prendre en compte la sécurité, ou construits par des entreprises qui ne comprennent pas les exigences actuelles en matière de sécurité. Par conséquent, les systèmes IoT peuvent potentiellement représenter le maillon faible de la cybersécurité des hôpitaux, des cliniques et des établissements de santé.

Le secteur de l'education

Les établissements d'éducation ne font pas exception dans le monde du tout IoT. Un monde dans lequel les technologies sont intégrées à tous les produits imaginables. L'IoT présente de nombreux avantages pour les universités et les écoles, en proposant une nouvelle génération d'objets intelligents, susceptibles d'améliorer considérablement l'expérience d'apprentissage ainsi que la protection et la sécurité des campus. Qu'ils soient aussi petits qu'un capteur de lumière ou aussi grands qu'un tableau intelligent, les dispositifs IoT remanient en profondeur la gestion de l'environnement pédagogique et les méthodes d'apprentissage des élèves. Les appareils IoT :

- Permettent d'établir des méthodes d'apprentissage inédites en favorisant une expérience pédagogique plus adaptée et plus dynamique, telles que les manuels numériques interactifs et l'apprentissage par les jeux
- Modifient les méthodes d'enseignement et de contrôle des résultats grâce à des équipements audiovisuels intelligents et des systèmes d'enregistrement vidéo numérique pour les cours ainsi que l'évaluation en ligne
- Simplifient les tâches des directeurs d'établissement par une surveillance préventive des infrastructures critiques et l'élaboration de processus plus efficaces et plus rentables pour la gestion des systèmes de chauffage, de ventilation et de climatisation, de l'éclairage et de l'aménagement du paysage
- Offrent un environnement plus sûr aux élèves et aux enseignants grâce à des caméras de surveillance numériques, des verrous de porte intelligents et des bus scolaires connectés

Dans ces écoles et ces universités repensées, les administrateurs peuvent recueillir, stocker et analyser d'énormes quantités de données sur l'environnement et les performances des étudiants. Les établissements disposent ainsi des renseignements nécessaires à l'amélioration des processus de réussite des élèves et peuvent identifier les lacunes à combler.

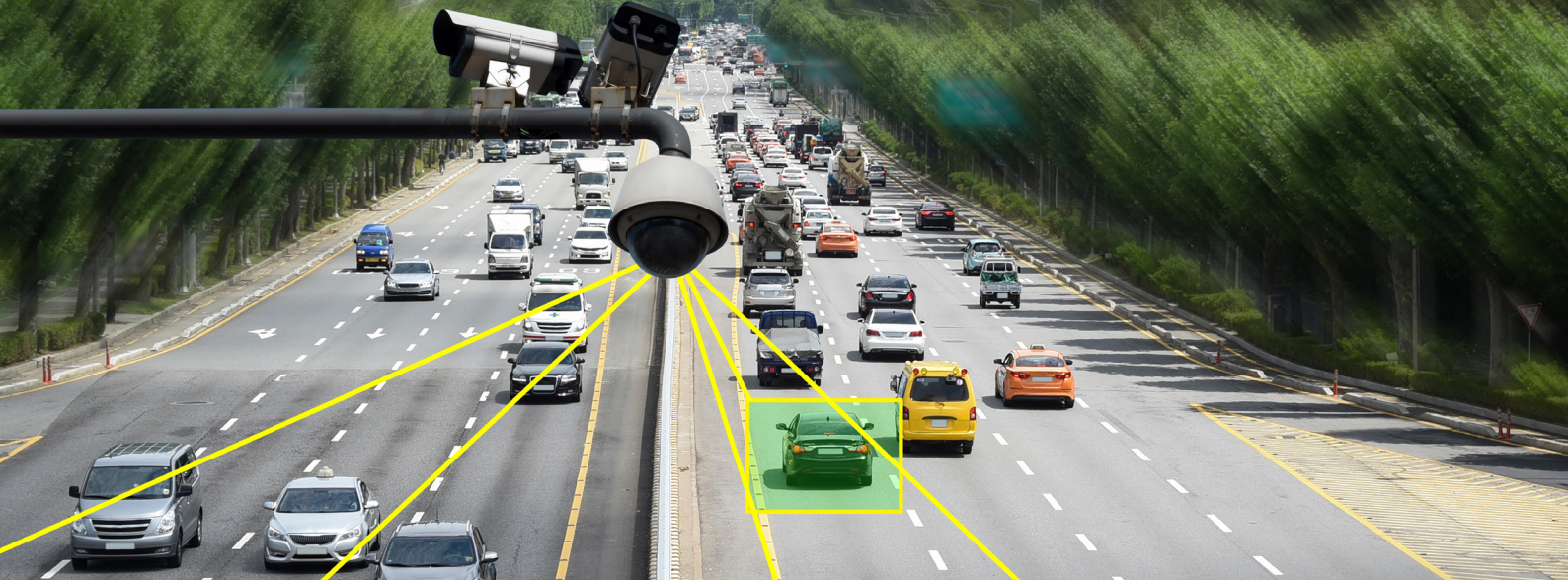
Ces changements transformateurs sont source à la fois de perspectives et de menaces. Il est impératif d'appliquer une stratégie de défense en profondeur qui garantit des connexions sécurisées aux dispositifs IoT et prévient les violations susceptibles de porter atteinte à la confidentialité des données des étudiants et à la sécurité de la recherche, ou de mettre en danger l'authenticité et l'intégrité des données.

Administrations

Les administrations publiques et les municipalités se joignent au flux de l'IoT. Les villes intelligentes présentent des débouchés économiques majeurs et de nouvelles possibilités de servir et protéger leurs habitants. Dans ces villes connectées, les entreprises de services publics utilisent des compteurs intelligents pour créer des systèmes de tarification adaptables, et les constructeurs déploient des capteurs et des composants d'automatisation dans les nouvelles constructions. Les parkings intelligents représentent un gain de temps et d'efficacité pour les habitants. Les poubelles intelligentes déclenchent un appel à l'action lorsqu'elles atteignent le seuil de débordement. L'IoT facilite la collecte par les municipalités et les administrations d'informations sur la mobilité et les tendances en matière de données, ce qui permet de réaliser des analyses essentielles à la formulation de stratégies et à la planification urbaine à long terme. L'IoT présente les avantages suivants :

- Des citoyens et des organismes publics mieux connectés peuvent fournir des services et des ressources de qualité, sécurisés et réactifs qui renforcent l'interaction et la confiance entre les administrations et les résidents, grâce à l'optimisation de l'habitabilité, l'aptitude au travail et la durabilité
- Une sécurité renforcée des transports en commun induite par une meilleure compréhension de l'exploitation du système de transport, grâce à des capteurs qui tracent toutes les données, des anomalies de la vitesse des trains légers sur rail aux températures des routes, en passant par la localisation en temps réel des bus publics
- La réduction des encombrements et de la consommation d'énergie grâce aux technologies de la ville intelligente, qui exploitent les données en temps réel pour améliorer l'ajustement des ressources à la demande. Ces technologies garantissent aussi l'agilité nécessaire pour réagir rapidement à l'évolution des modèles de circulation en constante mutation, aux variations de la consommation d'eau ou d'électricité, ou aux modifications de la qualité de l'air
- L'amélioration des performances d'exploitation et de maintenance grâce à une surveillance préventive des infrastructures publiques critiques et à la création de processus plus efficaces pour réduire les coûts d'exploitation et améliorer la capacité du système
- Renforcement de la sécurité publique grâce à des interventions plus rapides et plus efficaces en situation d'urgence

Cependant, la barre de la cybersécurité doit être placée haut, voire très haut. Dans les villes connectées où certaines applications, capteurs et appareils ne sont pas tous conçus dans un souci de sécurité, une infrastructure intelligente et automatisée est indispensable pour répartir ces appareils dans des catégories distinctes et les empêcher de communiquer avec des dispositifs qui leur sont interdits. Ce cloisonnement renforce considérablement la sécurité et engage l'entité publique dans une démarche de confiance zéro par la création de plusieurs couches de protection dans une stratégie de défense en profondeur.



Transports

L'internet des objets (IoT) est en passe de transformer le secteur des transports en remaniant profondément la collecte de données et d'informations par les systèmes, grâce à la combinaison de l'automatisation et de l'analyse des données. Des capteurs, actionneurs ou autres dispositifs peuvent recueillir et transmettre en temps réel des informations concernant l'activité sur le réseau. Ces données peuvent ensuite être analysées par les sociétés de transport afin d'améliorer l'expérience et la sécurité des usagers, réduire les encombrements et la consommation d'énergie, tout en optimisant les performances d'exploitation.

L'IoT est au cœur des forces qui redessinent les transports pour garantir une sécurité renforcée, des déplacements plus performants, une meilleure maintenance des véhicules et des avions et une gestion plus judicieuse du trafic. Citons quelques exemples d'applications de l'IoT dans le secteur des transports :

- Gains d'efficacité pour accroître la capacité du système et améliorer la sécurité et le confort des usagers tout en réduisant les coûts et les risques
- Panneaux à messages dynamiques en bordure de route, pour systèmes de transport intelligents, qui affichent en temps réel l'état des routes, les tarifs de péage, les fermetures de voies et la circulation
- Véhicules autonomes, capables de détecter leur environnement, prévoir les comportements, communiquer avec les autres véhicules et leur environnement et réagir instantanément à des scénarios réels sur l'autoroute
- Vidéosurveillance pour sécuriser les déplacements de personnes et de foules, automatiser et fournir une détection précoce des comportements suspects et des bagages abandonnés

Les cyberattaques peuvent avoir un impact sur les opérations quotidiennes pendant une période prolongée. Non seulement le service est perturbé, mais l'exposition de données hautement sensibles constitue également un risque considérable dans ce secteur. Si certaines cyberattaques ont pour objectif le paiement d'une rançon, d'autres visent à semer le chaos et le désordre en paralysant des systèmes entiers. Perturbation des feux de circulation, blocage de l'accès à des fichiers et des données importants, interruption des services de paie et violation des distributeurs de titres de transport et des guichets automatiques ne sont que quelques exemples de ces cyberattaques.

- En 2018, la société Bay & Bay Transportation a été victime d'une attaque massive de ransomware qui a verrouillé les systèmes qu'elle utilise pour gérer son parc de 300 camions
- En 2018, des pirates informatiques ont mis hors service 2 000 ordinateurs appartenant au ministère des Transports du Colorado, perturbant ainsi son exploitation pendant des semaines. Plus récemment, des cybercriminels ont infiltré trois des 18 systèmes informatiques de la régie métropolitaine des transports de la ville de New York.
- Le premier semestre de 2020 a révélé une augmentation stupéfiante des incidents liés aux ransomwares, avec une hausse globale de 715 % d'une année sur l'autre.
- En 2020, 9 millions d'adresses e-mail et de documents de voyage de clients d'EasyJet ont été volés. Parmi les passagers escroqués, 2 208 ont été victimes d'un piratage des données de leur carte de crédit. Cette cyberattaque, associée au choc de la pandémie mondiale, a fait perdre à la compagnie aérienne 45 % de la valeur de ses actions, entraînant ainsi sa première perte annuelle en 25 ans d'existence.

Les réseaux et les stratégies IoT sécurisés sont disponibles dès aujourd'hui

Les produits et solutions d'Alcatel-Lucent Enterprise constituent une base de réseau sécurisée pour vous accompagner dans le déploiement de systèmes IoT susceptibles d'apporter un éclairage. Notre mission : optimiser produits et processus, vous faire gagner en efficacité, et améliorer l'expérience client. Les stratégies de cloisonnement de l'IoT et de sécurité multi-niveaux développées par ALE réduisent les risques et simplifient la mise en place des réseaux IoT : elles facilitent l'intégration des appareils, optimisent les opérations et renforcent considérablement la sécurité. ALE peut vous aide à exploiter pleinement les avantages potentiels de l'IoT en fournissant des niveaux supérieurs de données, d'automatisation et de sécurité du réseau.

Pour en savoir plus

Pour plus d'informations sur les solutions IoT d'ALE, consultez le site ALE IoT Security.

www.al-enterprise.com/fr-fr Le nom et le logo d'Alcatel-Lucent sont des marques commerciales de Nokia utilisées sous licence par ALE. Pour en savoir plus sur les autres marques déposées utilisées par les sociétés affiliées de la Holding ALE, veuillez consulter le site www.al-enterprise.com/en/legal/trademarks-copyright. Toutes les autres marques déposées appartiennent à leurs propriétaires respectifs. Les informations présentées peuvent faire l'objet de modifications sans préavis. ALE Holding et ses sociétés affiliées ne sauraient être tenues responsables d'inexactitudes éventuelles dans les informations contenues dans le présent document. © Copyright 20XX ALE International, ALE USA Inc.
Tous droits réservés dans tous les pays. DID22080801FR (septembre 2022)

Alcatel·Lucent Enterprise