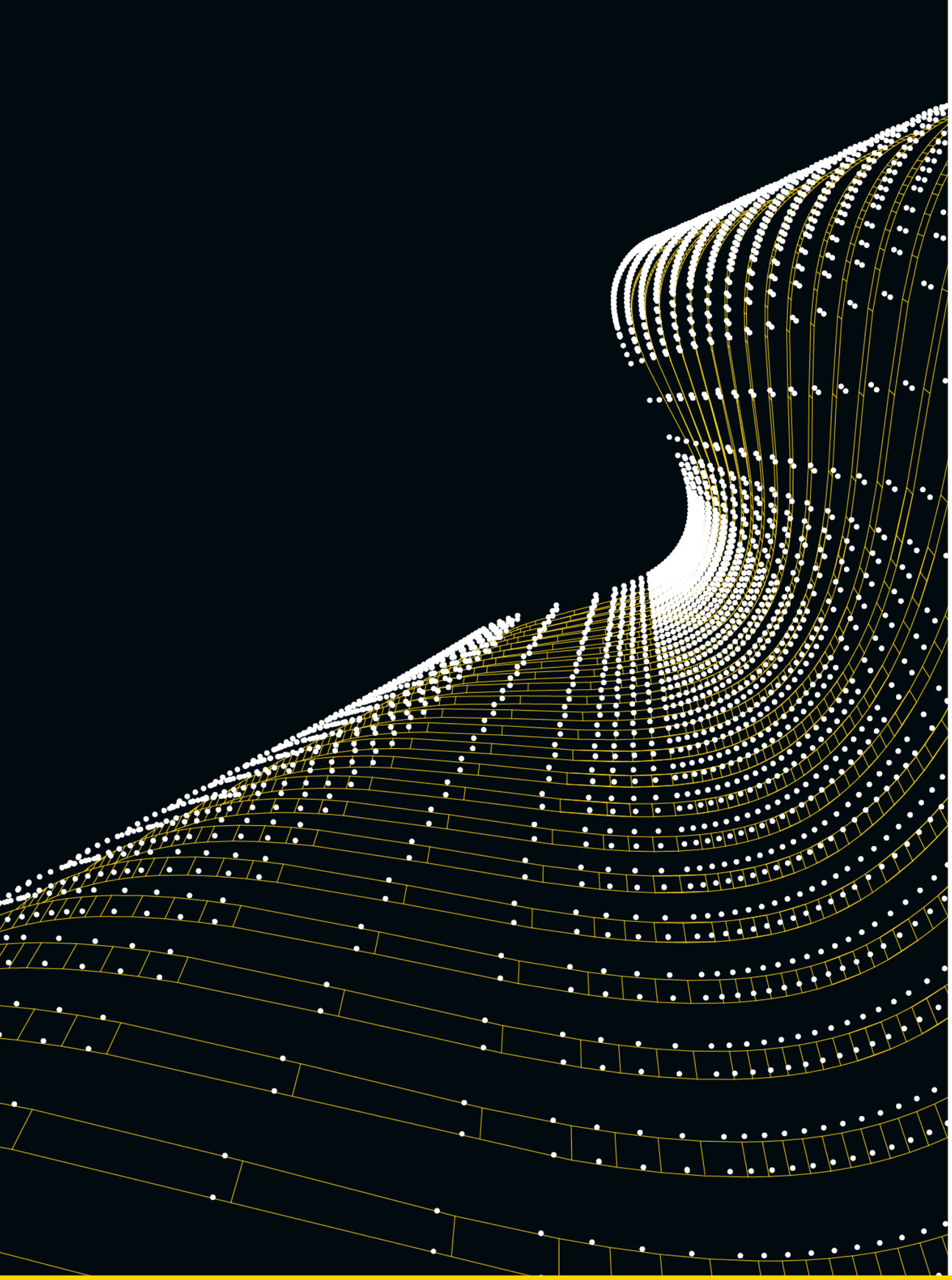
ASSISTÉ PAR LE CLOUD

Surveillance et gestion à distance

LIVRE BLANC

Restez unifié
Restez à jour
Gardez le contrôle

zenitel



Sommaire

1

Introduction

Les systèmes de communication cruciale – tels que les systèmes d'alarme vocale, les interphones, les points d'assistance et les solutions de sonorisation – sont conçus pour protéger les personnes et les biens. Ils doivent fonctionner parfaitement au moment précis où on en a besoin. Garantir que ces systèmes restent pleinement opérationnels à tout moment n'est pas seulement une responsabilité technique – c'est une obligation essentielle en matière de sécurité.

Ce livre blanc explique comment **la surveillance et la gestion à distance (RMM) assistées par le cloud** transforment la manière dont les systèmes de communication cruciale sont entretenus, surveillés et sécurisés. Il souligne les limites des services de gestion traditionnels, décrit le fonctionnement d'une approche assistée par le cloud et met en évidence la valeur opérationnelle et commerciale pour les intégrateurs de systèmes et les clients finaux.

2

Les limites des services de gestion traditionnels

De nombreuses organisations s'appuient sur des intégrateurs de systèmes ou des partenaires de services pour assurer la maintenance et la surveillance de leurs solutions de communication dans le cadre de contrats de gestion de service.
Historiquement, cela impliquait :

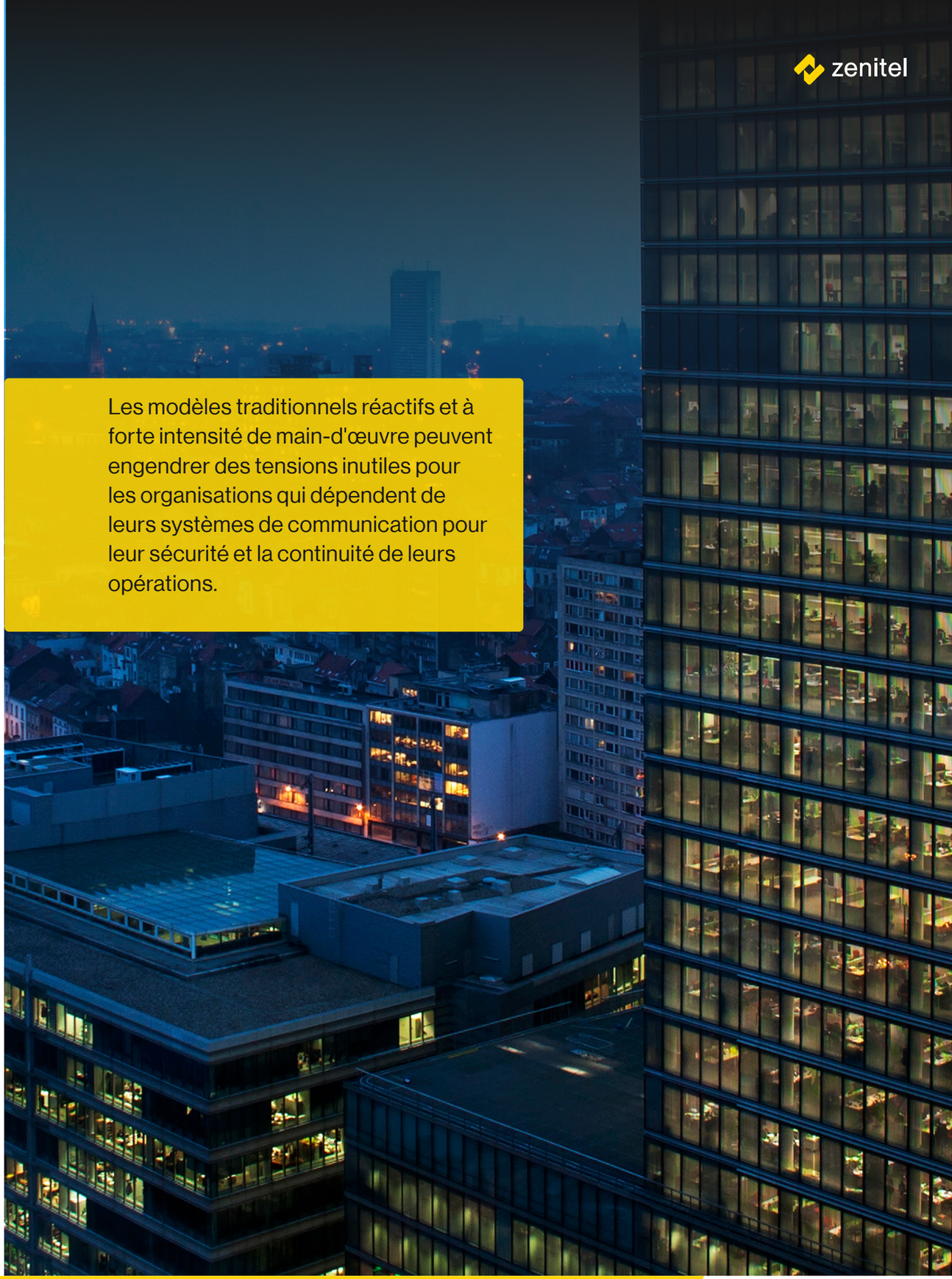
- **Visites régulières sur site**
- **Vérifications manuelles du système**
- **Maintenance réactive lorsque des pannes sont signalées**

Bien que cette approche ait permis d'assurer le bon fonctionnement des opérations pendant de nombreuses années, elle présente trois faiblesses majeures.

Les défaillances passent souvent inaperçues entre les inspections
Des problèmes peuvent survenir peu après une visite programmée et passer inaperçus jusqu'à la prochaine inspection, ou jusqu'à ce que le système tombe en panne lors d'une urgence. Pour la communication cruciale, ce manque de visibilité est inacceptable.

La maintenance est réactive, et non proactive
Les interventions de maintenance sont généralement déclenchées par des problèmes visibles ou des rapports manuels, et non par des alertes précoces provenant du système lui-même. Par conséquent, les organisations réagissent souvent aux incidents plutôt que de les prévenir...

La mise à l'échelle sur plusieurs sites est inefficace
À mesure que les organisations se développent et multiplient leurs sites, le maintien d'un même niveau de service exige davantage de déplacements, de temps et de main-d'œuvre.



Les modèles traditionnels réactifs et à forte intensité de main-d'œuvre peuvent engendrer des tensions inutiles pour les organisations qui dépendent de leurs systèmes de communication pour leur sécurité et la continuité de leurs opérations.

3

RMM assisté par le cloud : **De réactif à proactif**

La surveillance et la gestion à distance assistées par le cloud (RMM) modifient fondamentalement les limites des modèles traditionnels de gestion de service.

Au lieu de dépendre de vérifications manuelles périodiques, les organisations bénéficient d'une visibilité continue et en temps réel sur l'état et les performances de tous les systèmes de communication connectés. Les appareils et sous-systèmes communiquent leur état à une plateforme cloud sécurisée, où les intégrateurs et opérateurs peuvent :

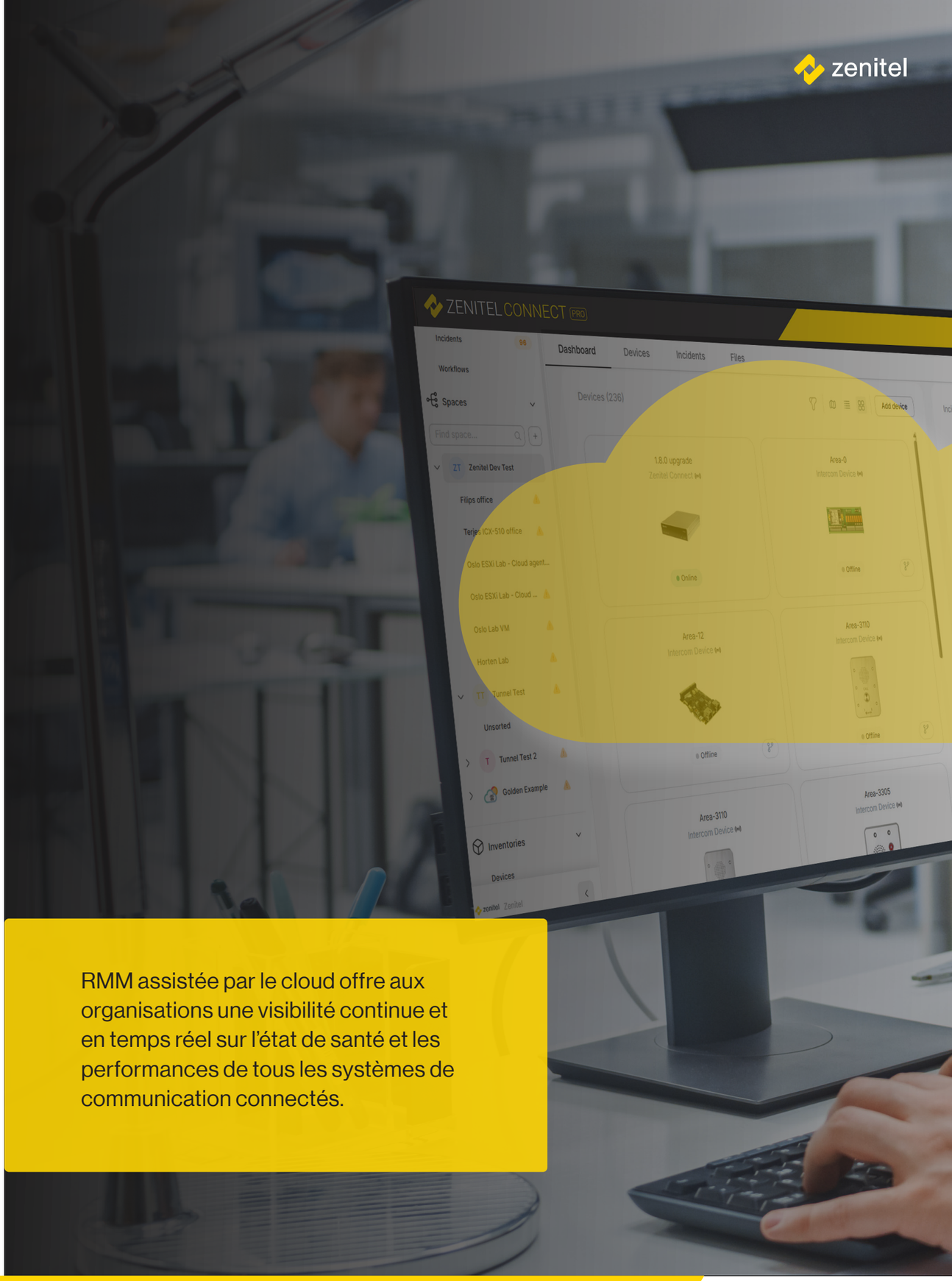
- **Surveiller l'état du système sur tous les sites**
- **Détecter les anomalies dès qu'elles se produisent**
- **Réagir rapidement avec des actions ciblées**

Les problèmes potentiels peuvent être identifiés, signalés et résolus avant qu'ils n'affectent la sécurité ou perturbent les opérations. Cette approche proactive, fondée sur les données, offre trois résultats clés :

Réduction des temps d'arrêt
Les problèmes sont traités rapidement, souvent avant même que les utilisateurs ne s'en aperçoivent.

Réduction des coûts d'exploitation
Moins de déplacements sur site, des visites plus courtes et une utilisation plus efficace des ressources.

Fiabilité accrue
Les systèmes sont vérifiés en continu, et non pas simplement contrôlés selon un calendrier.



RMM assistée par le cloud offre aux organisations une visibilité continue et en temps réel sur l'état de santé et les performances de tous les systèmes de communication connectés.

4

Pourquoi les systèmes de communication en ont le plus besoin

Le RMM assisté par le cloud peut être appliqué à de nombreuses technologies, mais son impact sur les systèmes de communication cruciale est particulièrement significatif. Fondamentalement, ces systèmes ont un seul et unique objectif vital :

Garantir une communication vocale claire et fiable lorsque cela compte le plus.

Si les messages ne peuvent pas être transmis, entendus ou clairement compris, le système a failli à son rôle fondamental.

ZONES À HAUT RISQUE ET ZONES PUBLIQUES

Le défi est encore plus grand dans les environnements à haut risque ou publics tels que :

Cellules de prison et centres de détention

Gares et quais

Parkings et zones d'accès public

Dans ces lieux, le vandalisme et les utilisations abusives délibérées sont fréquents. Un exemple simple est celui des prisonniers qui bloquent les microphones des interphones avec du chewing-gum pour éviter la surveillance ou perturber la communication.

Sans surveillance continue, de telles altérations ne seraient détectées qu'au cours de la prochaine intervention de maintenance programmée ou lors d'un incident critique. Grâce à la gestion à distance des équipements (RMM) basée sur le cloud, les anomalies de niveaux audio ou du comportement des appareils peuvent être détectées rapidement, ce qui permet aux opérateurs d'intervenir avant que l'intégrité du système ne soit compromise.

SYSTÈMES PEU UTILISÉS

Certains points de communication, tels que les interphones d'accès ou les points d'aide fréquemment utilisés, sont naturellement « auto-testés » par leur utilisation quotidienne. En cas de défaillance, les utilisateurs s'en aperçoivent.
D'autres, en revanche, ne sont utilisés qu'en cas d'urgence :

Systèmes d'alarme vocale

Systèmes de notification de masse

Solutions de diffusion des alertes d'évacuation et des incidents

Ces systèmes peuvent rester inactifs pendant de longues périodes. Une défaillance peut passer inaperçue pendant des semaines, voire des mois, si personne n'interagit avec ces systèmes.

Dans le pire des cas, un incendie ou un incident de sécurité se produit, révélant que le système d'alarme vocale est hors service depuis longtemps. L'incapacité à informer, guider ou avertir les personnes à temps peut avoir des conséquences catastrophiques.

Le RMM assisté par le cloud permet de remédier à ce risque en assurant une surveillance continue et des tests automatisés réguliers afin que les problèmes soient détectés et résolus bien avant qu'une situation d'urgence ne survienne.

zenitel

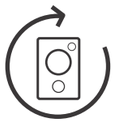
Cas d'utilisation du **RMM basé sur le cloud**

Une plateforme RMM basée sur le cloud offre aux intégrateurs et aux opérateurs un accès distant sécurisé aux systèmes et appareils distribués. Les interventions qui nécessitaient autrefois une présence sur site peuvent désormais être effectuées depuis un poste centralisé.

Test des tonalités
Des tests de tonalité automatiques ou à la demande peuvent être effectués à distance pour vérifier que :

- Les haut-parleurs et les amplificateurs fonctionnent
- Le son est diffusé au volume attendu
- Les zones sont correctement adressées et accessibles

Ceci est particulièrement utile pour les systèmes d'alarme vocale et de notification de masse, qui doivent être opérationnels 24 heures sur 24, 7 jours sur 7, mais qui sont rarement utilisés dans des conditions normales.



Redémarrage des appareils
Les appareils doivent parfois être redémarrés pour récupérer après des pannes mineures ou des anomalies logicielles. Au lieu d'envoyer un technicien :

- Les appareils peuvent être redémarrés à distance
- Le service est souvent rétabli immédiatement
- Les perturbations en dehors des heures de bureau peuvent être résolues sans intervention sur site

Cela minimise les temps d'arrêt et améliore l'expérience utilisateur.

Configuration des appareils
Configurez et gérez les appareils à distance pendant le déploiement et tout au long du cycle de vie du système afin de garantir des performances optimales et de simplifier l'administration du système.

- Configurez les paramètres des appareils sans avoir besoin d'un accès sur site
- Ajustez les paramètres et mettez à jour les configurations à distance
- Accélérez les opérations de déploiement et de mise en service
- Assurez la cohérence entre les appareils et les sites

Cela s'avère particulièrement utile pour les installations décentralisées et les déploiements à grande échelle, où la réduction des interventions sur site peut considérablement améliorer l'efficacité tout en réduisant les coûts d'exploitation.

Mises à jour logicielles et correctifs de sécurité
La sécurité et la mise à jour des systèmes sont un processus continu. Une approche gérée dans le cloud permet aux intégrateurs de :

- Déployer les mises à jour du micrologiciel de manière centralisée
- Déployer des correctifs de sécurité sur un ou plusieurs sites
- Garantir la cohérence des versions et des configurations

Cela améliore la cybersécurité et aide à respecter les exigences de conformité sans avoir à effectuer de mises à jour manuelles sur chaque site.

Interface unique, contrôle centralisé
Les intégrateurs de systèmes servent souvent plusieurs clients, chacun disposant de plusieurs sites et types d'appareils. Sans centralisation, la gestion de ces environnements devient complexe et mobilise d'importantes ressources. Une solution RMM basée sur le cloud répond à ce besoin en fournissant :

- Un tableau de bord unique et centralisé pour superviser tous les systèmes gérés
- Un accès utilisateur à plusieurs niveaux, permettant aux intégrateurs et aux utilisateurs finaux d'avoir des rôles et des privilèges clairement définis
- Une séparation sécurisée des projets et des utilisateurs, garantissant que l'environnement de chaque client reste isolé et protégé

Grâce à ce « tableau de bord unique », les intégrateurs bénéficient d'une vue d'ensemble complète de l'état de santé des systèmes chez tous leurs clients et sur tous leurs sites, ce qui leur permet d'allouer plus efficacement les ressources là où elles sont nécessaires et d'offrir une meilleure qualité de service.

6

Zenitel Cloud RMM avec **Zenitel Connect Pro**

Zenitel apporte plusieurs décennies d'expérience dans le domaine de la communication cruciale à l'ère du cloud. Avec Zenitel Connect Pro, les organisations disposent d'une plateforme de communication cruciale unifiée pouvant être étendue à des fonctionnalités RMM assistées par le cloud pour prendre en charge des opérations proactives et des services gérés.

En s'appuyant sur Zenitel Connect Pro, Zenitel Cloud RMM offre les avantages suivants :

Une visibilité unifiée sur les interphones, les haut-parleurs IP, les systèmes d'alarme vocale et les points d'aide

Une surveillance de l'état de santé, des alarmes et des diagnostics assistés par le cloud pour tous les appareils connectés

Des actions de gestion à distance telles que des tests de tonalité, le redémarrage des appareils et les mises à jour du micrologiciel

Contrôle d'accès basé sur les rôles, garantissant que seul le personnel autorisé puisse effectuer des opérations critiques

Connectivité sécurisée entre les systèmes sur site et les services cloud, conforme aux meilleures pratiques modernes en matière de cybersécurité

Pour les intégrateurs de systèmes, cela signifie une plateforme robuste permettant de créer des services gérés en plus des solutions Zenitel. Pour les clients finaux, cela se traduit par une disponibilité accrue, une sécurité renforcée et des opérations plus prévisibles.

Zenitel apporte des décennies de fiabilité au cloud grâce à Zenitel Connect Pro et Zenitel Cloud RMM.

7

Avantages commerciaux clairs

L'ajout de Zenitel Cloud RMM est bien plus qu'une simple mise à niveau du système : cela transforme la manière dont les organisations exploitent, entretiennent et sécurisent leur infrastructure de communication.

De réactif à proactif
Les organisations passent d'une attitude réactive face aux pannes à une attitude préventive. La surveillance et les tests continus fournissent des alertes précoces, et les commandes à distance permettent de corriger les problèmes avant qu'ils n'affectent les utilisateurs.

Efficacité opérationnelle

- Moins de visites imprévues sur site
- Temps de résolution plus courts
- Planification plus efficace des interventions sur site lorsque celles-ci sont réellement nécessaires

Cela se traduit directement par une réduction des coûts opérationnels tant pour les intégrateurs que pour les clients finaux.

Sécurité renforcée
En centralisant les mises à jour logicielles et les correctifs de sécurité, les services gérés assistés par le cloud prennent en charge :

- Une protection renforcée contre les cybermenaces
- Un meilleur contrôle des configurations et des accès utilisateurs
- Une meilleure conformité aux normes de sécurité internes et externes

Réduction des coûts de maintenance du système
Avertissements précoces, contrôles à distance, moins de visites sur site, résolutions plus rapides, et des mises à jour de sécurité centralisées — le tout contribuant à réduire les coûts d'exploitation et à améliorer la disponibilité du système.

8

La cybersécurité – Reste une préoccupation majeure pour l'adoption du cloud

Bien qu'il existe un large consensus sur les avantages opérationnels et commerciaux de la technologie basée sur le cloud, la cybersécurité reste l'un des principaux obstacles à son adoption dans les environnements où la sûreté et la sécurité sont essentielles.

Pour de nombreuses organisations, en particulier celles opérant dans des secteurs réglementés tels que les transports, la santé, l'énergie et les administrations publiques, la question n'est pas seulement « Que peut nous apporter le cloud ? », mais aussi « Pouvons-nous lui faire confiance pour protéger nos systèmes et nos données ? »

Les principales préoccupations en matière de cybersécurité sont les suivantes :

Confidentialité et intégrité des données
Quelles informations sont envoyées vers le cloud ? Sont-elles cryptées ? Peuvent-elles être modifiées ou interceptées ?

Exposition des réseaux sur site
La connexion d'un système au cloud ouvre-t-elle de nouvelles voies d'attaque vers les réseaux internes ?

La conformité aux normes et réglementations
La solution prend-elle en charge les cadres de cybersécurité pertinents et les meilleures pratiques du secteur, et peut-elle être alignée sur les politiques de sécurité existantes du client ?

La cybersécurité ne devrait pas dépendre de la présence d'une grande équipe interne dédiée à la cybersécurité. Les services cloud de Zenitel sont « **Secure by Design** » (sécurisés dès la conception) et **« Private by Default**» (privés par défaut), ce qui aide les clients à respecter des réglementations strictes tout en se concentrant sur leur cœur de métier. Notre plateforme est conforme à la norme SOC 2 Type 2, prend en charge les exigences **du RGPD et du CCPA** en matière de confidentialité des données en Europe et aux États-Unis, et est conçue conformément aux principes de sécurité de la norme ISO 27001.

Toutes les communications vers et depuis Zenitel Cloud RMM sont authentifiées et chiffrées. Avec Zenitel, vous bénéficiez d'un cadre fiable pour protéger les données, les systèmes et les personnes.

Pour les opérations cruciales en matière de sécurité, les préoccupations liées à la cybersécurité freinent souvent l'adoption du cloud. Zenitel élimine cet obstacle en proposant des services RMM conçus dès le départ pour garantir la sécurité et la confidentialité par défaut.

9

Perspectives d'avenir : **Communication cruciale gérée dans le cloud**

La demande d'environnements opérationnels multisites et toujours actifs est en hausse dans tous les secteurs :

- **Transport et mobilité**
- **Santé et hôpitaux**
- **Installations industrielles et énergie**
- **Prisons et environnements de haute sécurité**
- **Bâtiments commerciaux et campus**

À mesure que ces environnements deviennent plus dispersés et complexes, les organisations ne peuvent plus se contenter d'une maintenance manuelle sur site. Les services gérés assistés par le cloud passent du statut d'« option intéressante » à celui de nécessité.

En adoptant la RMM basée sur le cloud pour les systèmes de communication cruciale, alimentée par des plateformes telles que Zenitel Connect Pro, les organisations peuvent :

- **Rester connectées** – grâce à une visibilité continue sur l'état du système
- **Rester en sécurité** – grâce à des mises à jour et un accès contrôlés et centralisés
- **Rester efficaces** – grâce à des opérations optimisées et à une réduction des coûts

Et surtout, ils peuvent être sûrs que leurs systèmes de communication fonctionneront lorsque cela compte le plus.

À mesure que les environnements multisites gagnent en ampleur et en complexité, la maintenance manuelle ne suffit plus. Le RMM basé sur le cloud permet aux organisations de rester connectées, sécurisées et efficaces, en garantissant le bon fonctionnement des systèmes de communication cruciale lorsque cela est le plus important.

zenitel

À propos de Zenitel

Zenitel propose des solutions de communication intelligentes qui accordent une grande importance à la cybersécurité, à l'évolutivité et l'interopérabilité. Les solutions de Zenitel offrent un son d'une clarté cristalline et s'intègrent de manière transparente aux systèmes de contrôle d'accès, de gestion vidéo et aux systèmes de sécurité plus larges afin de protéger les personnes, les biens et les opérations.

Grâce à l'interopérabilité à tous les niveaux, nous nous intégrons de manière intuitive aux plateformes de contrôle d'accès, de gestion vidéo et de sécurité.

2026.06

info.france@zenitel.fr

zenitel.fr