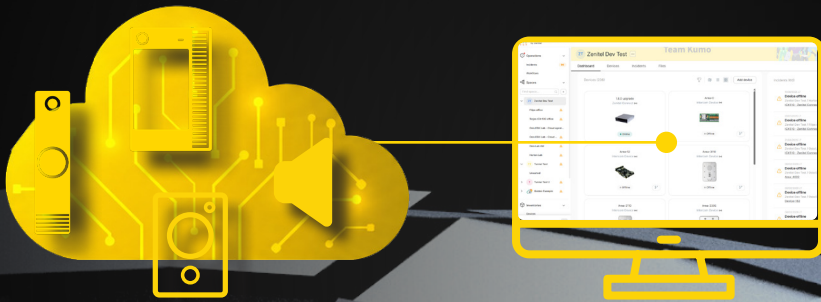


CLOUD-ASSISTED

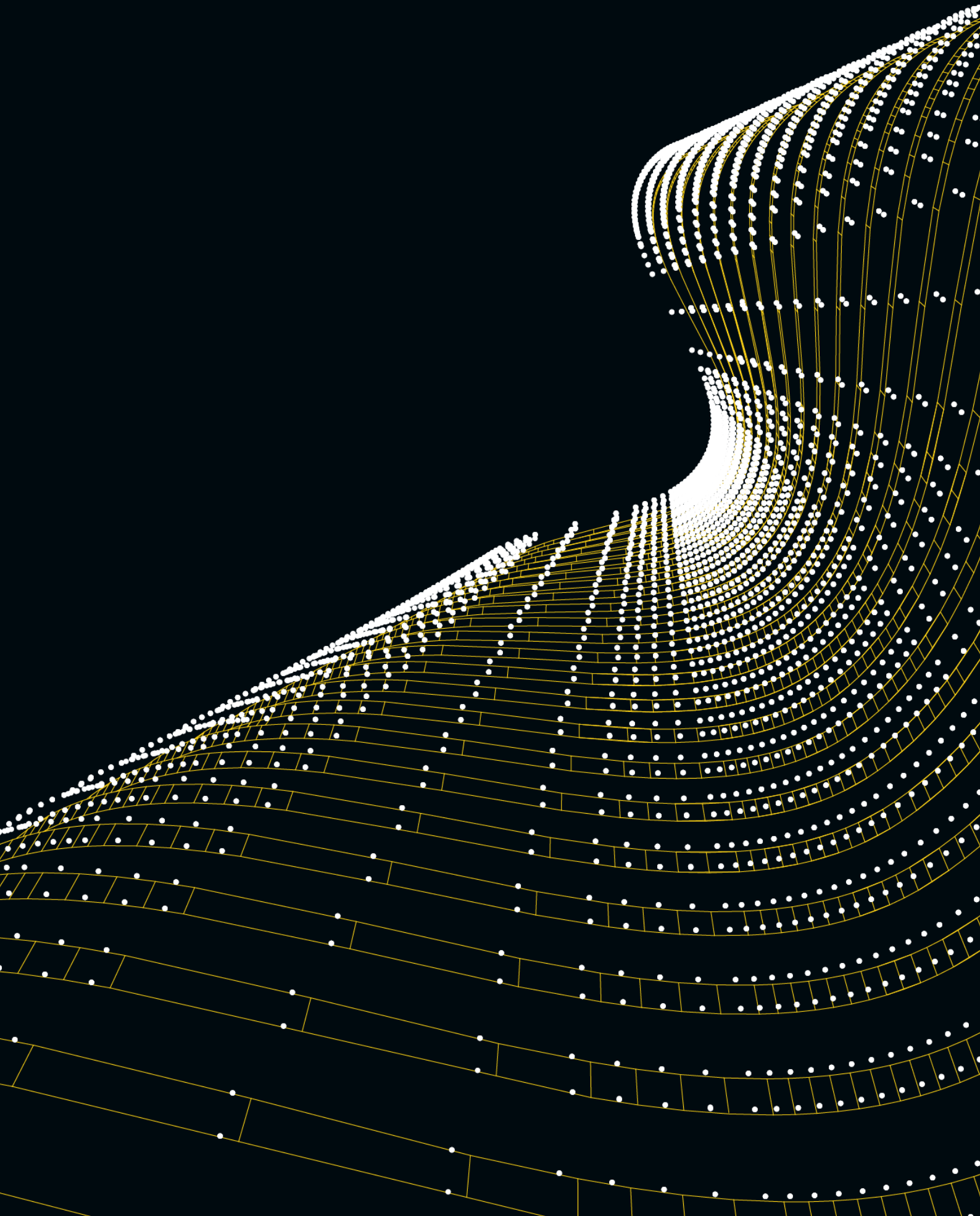
WHITEPAPER

Remote Monitoring & Management



Stay Unified
Stay Updated
Stay in Control





Content

1	Introduction	4
2	Shortfalls of Traditional Managed Services	6
3	Cloud-Assisted RMM	8
4	Why Critical Communication Systems Need It Most	10
5	Use Cases	12
6	Cloud RMM with Zenitel Connect Pro	14
7	Business Benefits	16
8	Cybersecurity	18
9	Looking Ahead	20

An Introduction

Critical communication systems – such as voice alarm systems, intercoms, help points, and public address solutions – are designed to protect people and safeguard assets. They must work flawlessly at the precise moment they are needed. Ensuring that these systems remain fully operational at all times is not just a technical responsibility – it is a safety-critical obligation.

This whitepaper explains how **cloud-assisted Remote Monitoring and Management (RMM)** is transforming the way critical communication systems are maintained, monitored, and secured. It outlines the limitations of traditional managed services, describes how a cloud-assisted approach works, and highlights the operational and business value for system integrators and end customers.





Shortfalls of Traditional Managed Services

Many organisations rely on system integrators or service partners to maintain and monitor their communication solutions under managed service contracts. Historically, this has involved:

- **Scheduled site visits**
- **Manual system checks**
- **Reactive maintenance when faults are reported**

While this approach has supported operations for many years, it has three major weaknesses.



Failures Often Go Undetected Between Inspections

Issues can arise shortly after a scheduled visit and remain unnoticed until the next inspection – or until the system fails during an emergency. For critical communication, that gap in visibility is unacceptable.



Maintenance Is Reactive, Not Proactive

Service actions are typically triggered by visible problems or manual reports, not by early warnings from the system itself. Thus, organisations often react to incidents rather than prevent them.



Scaling Across Multiple Sites Is Inefficient

As organisations grow and add more locations, maintaining the same service level demands more travel, more time, and more manpower.

Traditional reactive and labour-intensive models can create unnecessary strain for organisations that rely on their communication systems for safety and operational continuity.

Cloud-Assisted RMM: From Reactive to Proactive

Cloud-assisted Remote Monitoring and Management (RMM) fundamentally changes the limitations of traditional managed services models.

Instead of depending on periodic manual checks, organisations gain continuous, real-time visibility into the health and performance of all connected communication systems. Devices and subsystems report their status to a secure, cloud-based platform, where integrators and operators can:

- **Monitor system health across sites**
- **Detect anomalies as they occur**
- **Respond quickly with targeted actions**

Potential issues can be identified, reported, and resolved before they affect safety or disrupt operations. This proactive, data-driven approach delivers three key outcomes:



Reduced downtime

Problems are addressed early, often before users notice.



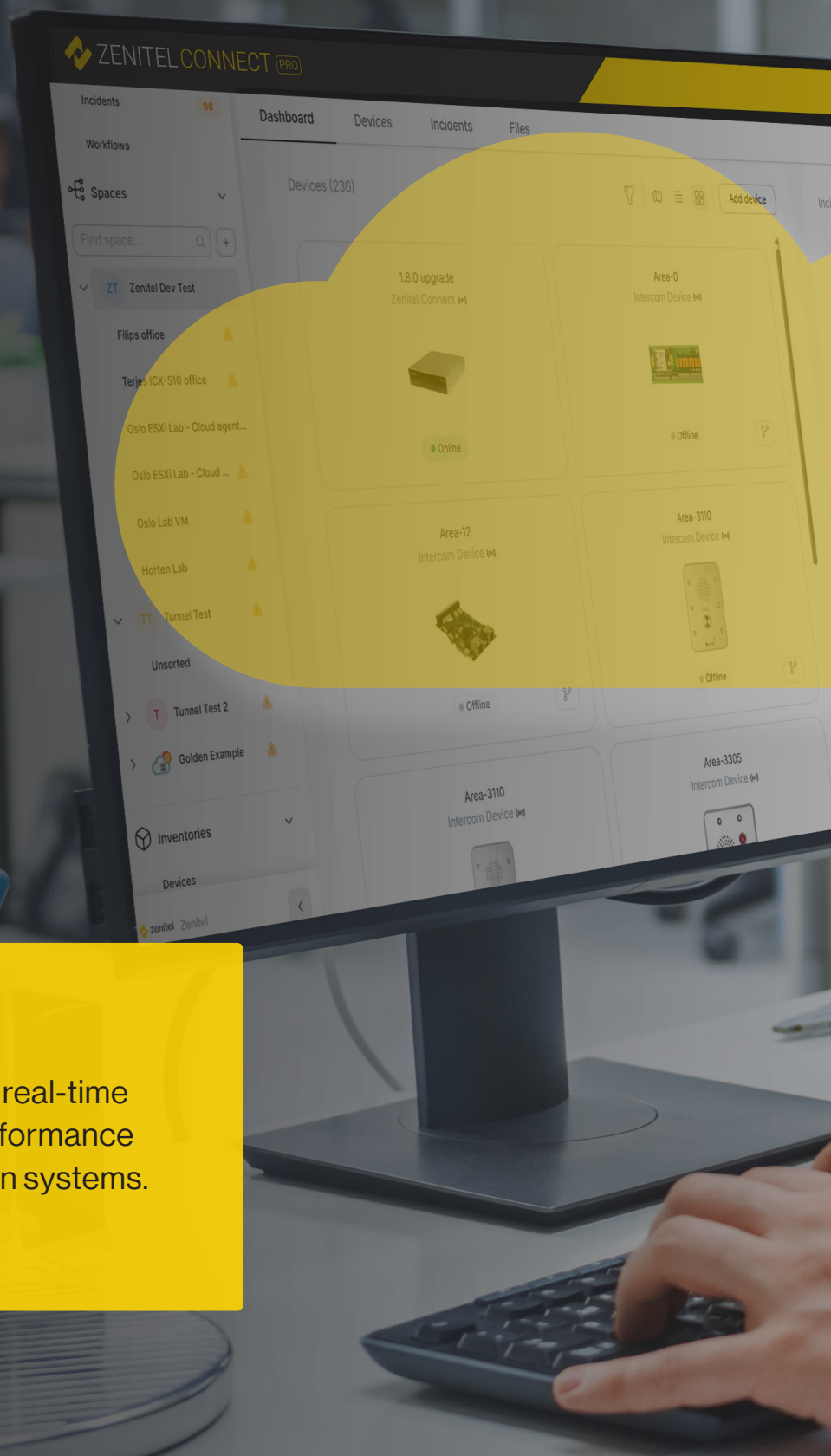
Lower operational cost

Fewer truck rolls, shorter sites visits, and more efficient resource utilization.



Higher reliability

Systems are continuously verified, not just checked according to a calendar.



Cloud-assisted RMM provides organisations with continuous, real-time visibility into the health and performance of all connected communication systems.

Why Critical Communication Systems Need It Most

Cloud-assisted RMM can be used across a wide range of technologies, but its impact is particularly pronounced in critical communication systems. At their core, these systems serve a single, vital purpose:

Ensure clear and reliable voice communication when it matters most.

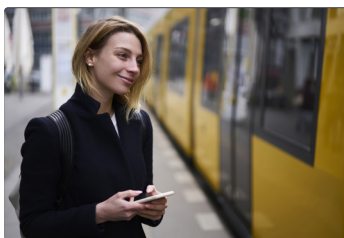
If messages cannot be transmitted, heard, or clearly understood, the system has failed in fulfilling its fundamental role.

HIGH-RISK AND PUBLIC AREAS

The challenge increases in high-risk or public environments such as:



Prison cells and detention facilities



Transportation hubs and platforms



Parking structures and public access areas

In these locations, vandalism and deliberate misuse are common. A simple example is prisoners blocking intercom microphones with chewing gum to avoid surveillance or to disrupt communication.

Without continuous monitoring, such tampering might only be discovered during the next scheduled maintenance visit or a critical incident.. With cloud-based RMM, anomalies in audio levels or device behaviour can be detected quickly, allowing operators to intervene before system integrity is compromised.

INFREQUENTLY USED SYSTEMS

Some communication points – such as door intercoms or frequently used help points – are naturally “self-tested” through everyday usage. If they fail, users notice.

Others, however, are only used during emergencies:



Voice alarm systems



Mass notification systems



Evacuation and incident broadcast solutions

These systems may remain idle for long periods of time. A fault can go unnoticed for weeks or months if no one interacts with them.

In the worst-case scenario, a fire or security incident occurs, only to reveal that the voice alarm system has been out of operation for a long time. The inability to inform, guide, or warn people in time can have catastrophic consequences.

Cloud-assisted RMM addresses this risk by enabling continuous monitoring and regular automated tests so that issues are detected and resolved long before an emergency arises.

Use Cases of Cloud-Based RMM

A cloud-based RMM platform gives integrators and operators secure, remote access to distributed systems and devices. Actions that once required an on-site presence can now be executed from a centralised location.

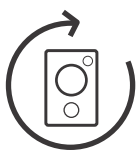


Tone Testing

Automatic or on-demand tone tests can be executed remotely to verify that:

- Speakers and amplifiers are functioning
- Audio is delivered at the expected volume
- Zones are correctly addressed and reachable

This is especially valuable for voice alarm and mass notification systems, which must be ready 24/7 but are seldom used under normal conditions.



Device Reboot

Devices occasionally require a reboot to recover from minor faults or software anomalies. Instead of dispatching a technician:

- Devices can be rebooted remotely
- Service restoration is often immediate
- Out-of-hours disruptions can be resolved without site visits

This minimises downtime and improves the user experience.



Device Configuration

Configure and manage devices remotely during deployment and throughout the system lifecycle to ensure optimal performance and simplify system administration.

- Configure device settings without requiring on-site access
- Adjust parameters and update configurations remotely
- Accelerate deployment and commissioning activities
- Maintain consistency across devices and sites

This is especially valuable for distributed installations and large-scale deployments, where reducing on-site visits can significantly improve efficiency while lowering operational costs.



Software Updates and Security Patches

Keeping systems secure and up-to-date is a continuous process. A cloud-managed approach allows integrators to:

- Deploy firmware updates centrally
- Roll out security patches across one or many sites
- Ensure consistent versions and configurations

This improves cybersecurity posture and helps meet compliance requirements without manual updates at each location.



Single Interface, Centralised Control

System integrators often serve multiple customers, each with multiple sites and device types. Without centralisation, managing these environments becomes complex and resource-intensive. A cloud-based RMM solution addresses this by providing:

- A single, centralised dashboard to oversee all managed systems
- Multi-tier user access, allowing integrators and end users to have clearly defined roles and privileges
- Secure segregation of projects and tenants, ensuring each customer environment remains isolated and protected

With this “single pane of glass,” integrators gain a full system health overview across customers and sites, allowing them to allocate resources more efficiently to where they are needed, and deliver a higher service quality.

Zenitel Cloud RMM with **Zenitel Connect Pro**

Zenitel brings decades of experience in critical communication to the cloud era. With Zenitel Connect Pro, organisations gain a unified critical communication platform that can be extended with cloud-assisted RMM capabilities to support proactive operations and managed services.

Using Zenitel Connect Pro as the foundation, Zenitel Cloud RMM enables:



Unified visibility across intercoms, IP speakers, voice alarm systems, and help points



Cloud-assisted health monitoring, alarms, and diagnostics for all connected devices



Remote management actions such as tone testing, device reboot, and firmware updates



Role-based access control, ensuring only authorised personnel can perform critical operations



Secure connectivity between on-premises systems and cloud services, aligned with modern cybersecurity best practices

For system integrators, this means a robust platform to build managed services on top of Zenitel's solutions. For end customers, it means higher availability, better security, and more predictable operations.

An abstract background graphic featuring a dense field of vertical, slightly curved lines in shades of yellow and white. These lines are topped with numerous small, semi-transparent circles in various sizes and colors, including yellow, orange, and white, creating a bokeh-like effect against a dark grey background.

Zenitel brings decades of reliability
to the cloud with Zenitel Connect
Pro and Zenitel Cloud RMM.

Clear Business Benefits

Adding Zenitel Cloud RMM is more than a system upgrade — it changes the way organisations run, maintain, and secure their communication infrastructure.



From Reactive to Proactive

Organisations shift from reacting to failures to preventing them. Continuous monitoring and testing provide early warnings, and remote controls make it possible to correct issues before they affect users.



Operational Efficiency

- Fewer unplanned site visits
- Shorter resolution times
- More efficient scheduling of on-site work when it is really needed

This directly translates into lower operational costs for both integrators and end customers.



Enhanced Security

By centralising software updates and security patches, cloud-assisted managed services support:

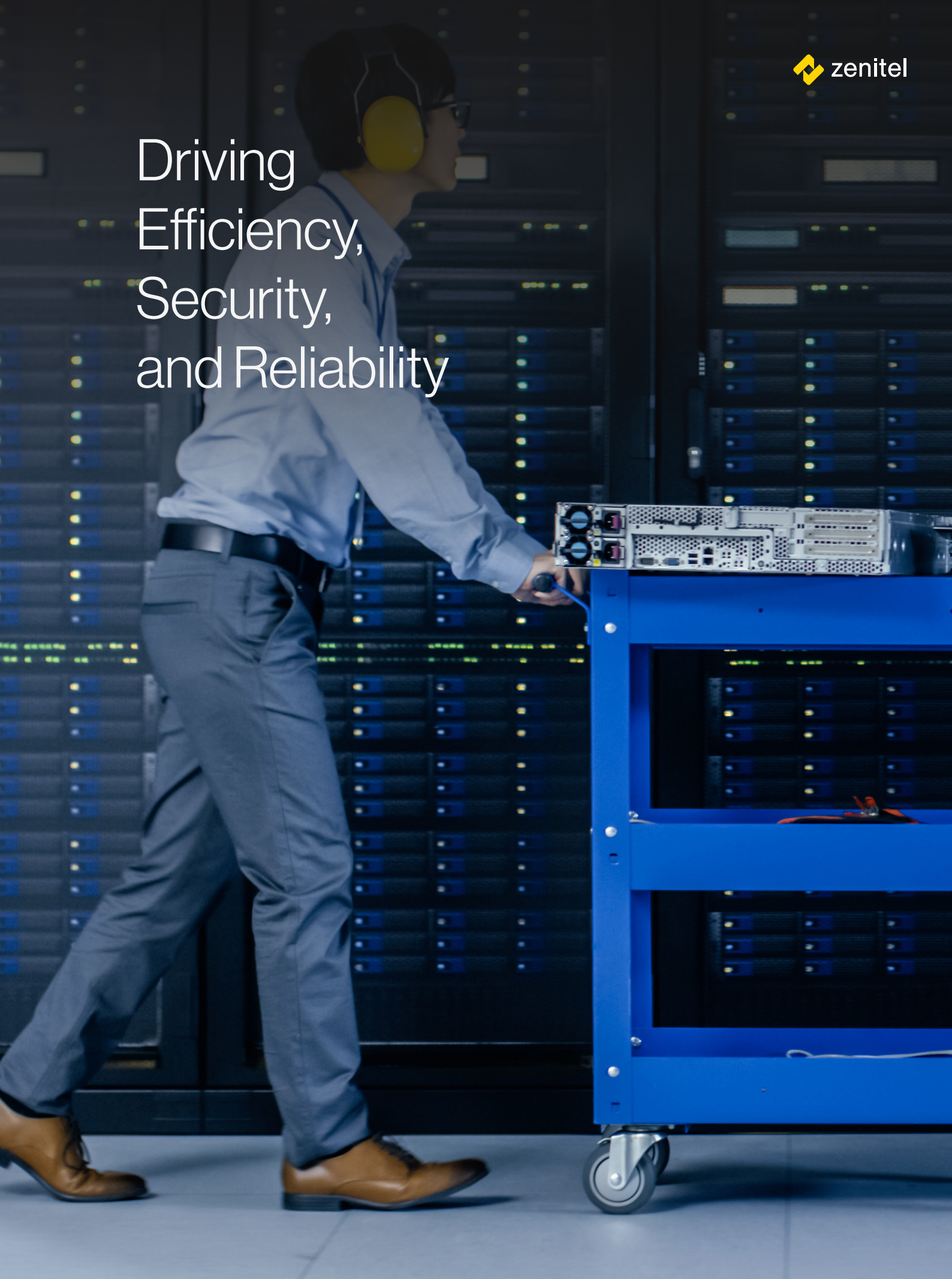
- Stronger protection against cyber threats
- Better control over configurations and user access
- Improved compliance with internal and external security standards



Lower system maintenance cost

Early warnings, remote controls, fewer site visits, faster resolutions, and centralised security updates - all contributing to lower operational costs and higher system availability.

Driving Efficiency, Security, and Reliability



Cybersecurity – Still a Major Concern for Cloud Adoption

While there is broad agreement on the operational and business benefits of cloud-based technology, cybersecurity remains one of the biggest barriers to its cloud adoption in safety- and security-critical environments.

For many organisations, especially those operating in regulated sectors such as transportation, healthcare, energy, and government, the question is not only “What can the cloud do for us?” but also “Can we trust it to protect our systems and data?”

Primary cybersecurity concerns include:

Data confidentiality and integrity

What information is sent to the cloud? Is it encrypted? Can it be altered or intercepted?

Exposure of on-premises networks

Does connecting a system to the cloud open up new attack paths into internal networks?

Compliance with standards and regulations

Does the solution support relevant cybersecurity frameworks and industry best practices, and can it be aligned with the customer’s existing security policies?

Cybersecurity shouldn’t depend on having a large in-house cybersecurity team. Zenitel’s cloud services are **Secure by Design and Private by Default**, helping customers meet demanding regulations while focusing on their core business. Our platform is **SOC 2 Type 2 compliant**, supports **GDPR and CCPA** requirements for data privacy in Europe and the US, and is designed in accordance with ISO 27001 security principles.

All communication from and to Zenitel Cloud RMM is authenticated and encrypted. With Zenitel, you gain a trusted framework for protecting data, systems, and people.



For safety-critical operations, cybersecurity concerns frequently stall cloud adoption. Zenitel removes this barrier by delivering RMM services built with security-by-design and privacy-by-default at their core.

Looking Ahead: Cloud-Managed Critical Communications

The demand for multi-site, always-on operational environments is growing across industries:



■ **Transportation and mobility**



■ **Healthcare and hospitals**



■ **Industrial facilities and energy**



■ **Corrections and high-security environments**



■ **Commercial buildings and campuses**

As these environments become more distributed and complex, organisations can no longer rely on manual, site-based maintenance alone. Cloud-assisted managed services are moving from a “nice-to-have” to a necessity.

By adopting cloud-based RMM for critical communication systems, powered by platforms such as Zenitel Connect Pro, organisations can:

- **Stay connected** – with continuous insight into system status
- **Stay secure** – with controlled, centralised updates and access
- **Stay efficient** – with optimised operations and reduced costs

And above all, they can be confident that their communication systems will perform when it matters most.

A close-up portrait of a young man with dark hair and glasses, looking slightly off-camera. The background is blurred, showing what appears to be a computer screen with some colorful light patterns. A large, semi-transparent yellow circle is overlaid on the right side of the image, partially covering the man's face and the text box.

As multi-site environments grow in scale and complexity, manual maintenance is no longer enough. Cloud-based RMM keeps organizations connected, secure, and efficient - ensuring critical communication systems perform when it matters most.



About Zenitel

Zenitel delivers intelligent communication solutions with a strong focus on cybersecurity, scalability, and interoperability. Zenitel's solutions provide crystal-clear audio and seamlessly integrate with access control, video management, and broader security systems to protect people, assets, and operations.

With interoperability at all levels, we seamlessly integrate with access control, video management and security platforms.

Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Zenitel, Vingtor-Stentofon and Phontech products are developed and marketed by Zenitel. The company's Quality Assurance System is certified to meet the requirements in NS-EN ISO 9001. Zenitel reserves the right to modify designs and alter specifications without notice. ZENITEL PROPRIETARY. This document and its supplementing elements, contain Zenitel or third party information which is proprietary. Any copying is prohibited, if not otherwise explicitly agreed in writing with Zenitel. Any authorized reproduction, in part or in whole, must include this legend. Zenitel © All rights reserved.