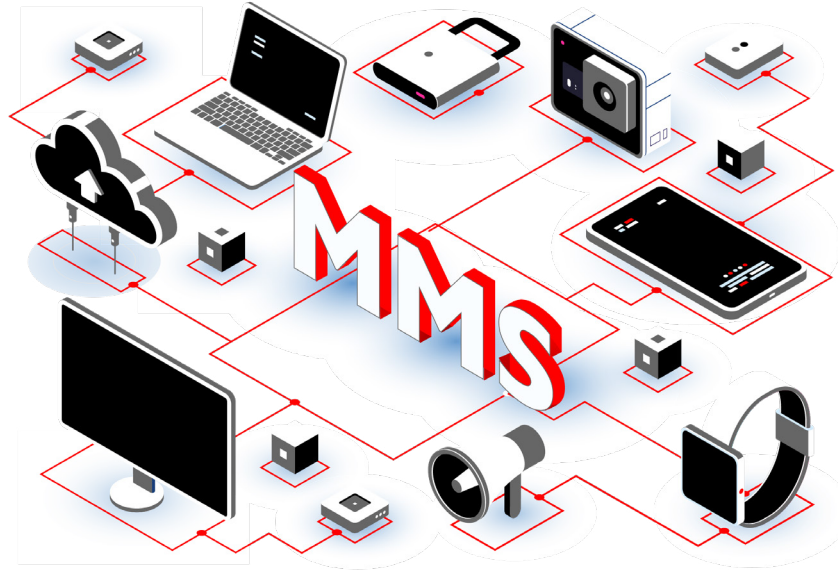


# Mobility Managed Services Trends to Watch in 2021

Technology moves at breakneck speed and the mobility revolution is no exception! In today's workforce, every new piece of technology that can enhance personal and professional lives is considered an opportunity to boost productivity. For organizations, the influx of new technology into the workforce places increasing pressure on effective Mobility Managed Services (MMS) to maintain and support these diverse devices, both in terms of productivity and security.

Be on the lookout for these six trends that are reshaping the 2021 MMS landscape.





## Internet of Things (IoT)

The term IoT refers to any device that is connected to the Internet. Each IoT device has a unique identification number, and when connected to a network, communicates and transfers data seamlessly. With an estimated [31 billion IoT devices](#) installed worldwide in 2020, IoT is sure to take the business world by storm! However, few enterprises are prepared for the mobility challenges associated with this transformative trend.

As businesses consider integrating IoT in their day-to-day processes, two priorities should come to mind: **Visibility and Security.**

- As IoT becomes commonplace, usage visibility is critical to allowing organizations to pool data based on department, determine data trends, and optimize carrier relationships.
- The more IoT connections that exist, the greater the risk to your security. Each connected device creates the opportunity for malware and the breach of sensitive company data. It is critical to work with an MMS provider that ensures real-time access into all devices to detect early signs of malicious activity, remotely wipe data, and enforce security protocols.

# 2

## BYOD & Work-from-Anywhere Environments

The Bring Your Own Device (BYOD) model is quickly becoming an industry staple. According to Microsoft, regardless of the office's official "bring your own device" policy, [two out of three employees use their own devices at work](#).

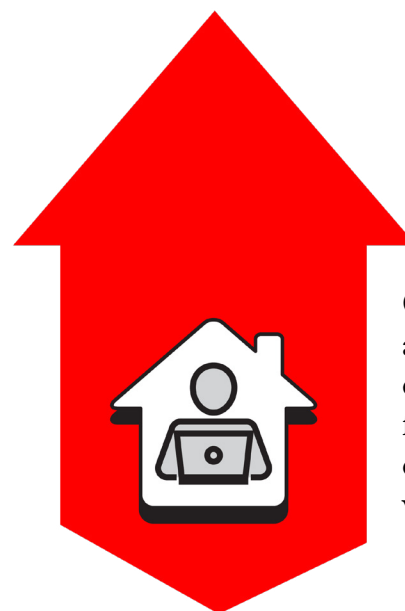
**In 2020, 59% of companies implemented a BYOD model** within their organization, and this number is projected to increase significantly in 2021, largely as a result of the ongoing pandemic. Even as the vaccine is disseminated globally, the reality is that the work-from-home trend isn't going away. Employees' lifestyles have changed dramatically, and it is essential for organizations to adapt accordingly.

As BYOD reshapes the MMS landscape and employees continue to work from anywhere, make sure your organization takes these steps to prepare:

- Support employee well-being and productivity (regardless of their home office situation)
- Quickly identify devices that are not compliant with security protocols
- Process complex reimbursement requests and other customer service issues
- Integrate and synchronize data across devices and departments
- Eliminate erroneous payments and alert administration when data exceeds thresholds



67% of employees use personal devices at work.



Companies gain an extra 240 hours of work per year from employees due to mobile working.

## The 5G Network Takeover

One of the fastest growing enterprise mobility trends of 2021 is 5G. **“Worldwide 5G network infrastructure market revenue nearly doubled in 2020 to reach \$8.1 billion”**, according to [Gartner, Inc.](#) Key benefits of 5G technology include ultra-fast speed, decreased latency, improved connectivity, and highly stable connections.

According to [research](#) by the Society for Human Resource Management (SHRM), productivity among employees is expected to increase by 90%. This increase creates numerous challenges for enterprises. The dynamism and density of the networks will require stricter security protocols and complex data analysis capabilities. Organizations should start evaluating their mobility ecosystem now to determine gaps or weaknesses that could become exploited in the 5G paradigm.



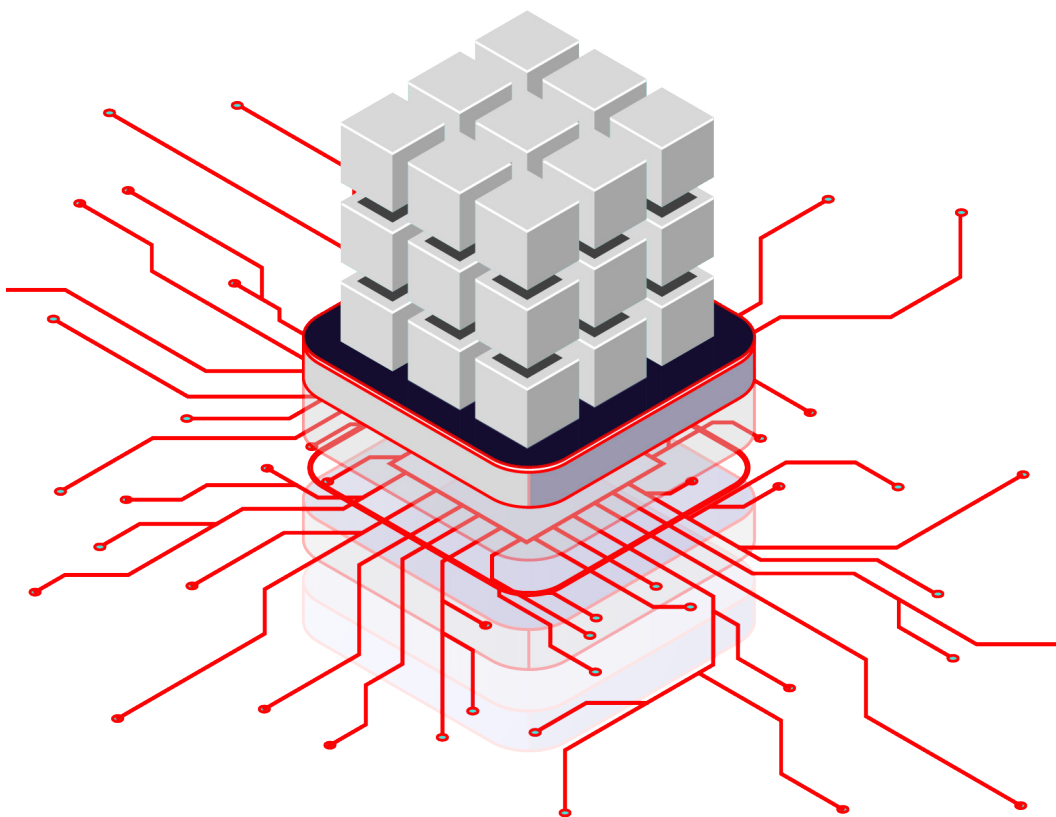
## Artificial Intelligence

Artificial Intelligence (AI) continues to be one of the hottest trends in the business world. A recent [Gartner poll](#) concluded that 47% of AI investments were unchanged since the start of the pandemic, and 30% of organizations actually planned to increase such investments in the immediate future. The intersection between MMS and AI allows for automation and machine learning to increase the overall productivity of your business units.

AI benefits include:

- Chatbots with increased natural language processing capabilities that can simulate flawless conversations with customers (providing faster response times and increased employee productivity)
- Enhanced employee well-being through self-service support
- The ability to identify and address security risks before they occur

Don't miss out on the opportunities presented by AI, as there's a strong likelihood that your competitors are already benefiting or plan on leveraging this technology. In fact, between 2020 and 2027, the global AI market will surge from \$62.4 billion to [\\$733.7 billion](#).





## Augmented Reality vs. Virtual Reality

Augmented and virtual reality are becoming enterprise actualities and will have a big impact on mobility in the years to come. Augmented reality shows a user's digital information overlaid on the real world, while virtual reality creates a completely new, digital environment. Enterprises are just now beginning to explore the business use cases for these technologies (including virtual meetings, immersive design, hands-free workflows, and streamlined employee onboarding).

It's critical to work with an MMS provider that understands this technology and is prepared to integrate it within your mobility ecosystem.



# 6

## Zero-Trust Security

Zero-Trust Security is gaining steam among organizations attempting to minimize the many threats impacting their telecom operations. **Gartner defines a Zero-Trust Access Network (ZTNA) as a network that establishes access boundaries around application(s) that hide or restrict public access to these apps.** This security approach enables businesses to verify “the identity, context and policy adherence of the specified participants before allowing access and prohibits lateral movement elsewhere in the network.”

To achieve this Zero-Trust Security model, businesses can protect their telecom environments by implementing these various safeguards:

- Multi-factor authentication
- Data encryption
- Blocking infected devices from accessing corporate data
- Enforcing privileged access policies

Expect zero-trust security to become the norm, as the global demand for such solutions will increase 17% annually between 2018 and 2025, [reaching almost \\$38 billion.](#)



Verify



Contextualize &  
Secure Systems



Control Privileges

While many of these trends appear futuristic, they will soon become workplace realities. Your organization needs to be ready for all productivity opportunities and security vulnerabilities these trends bring to your telecom environment.

WidePoint is a trusted MMS provider that addresses all aspects of mobility deployment, management, and security. [Request a consultation today](#) to learn how WidePoint can help your organization prepare for the future of mobility.

**Brad Hall** [bhall@widepoint.com](mailto:bhall@widepoint.com) 916.390.2615

