Risks of not having an efficient dedicated MDM solution

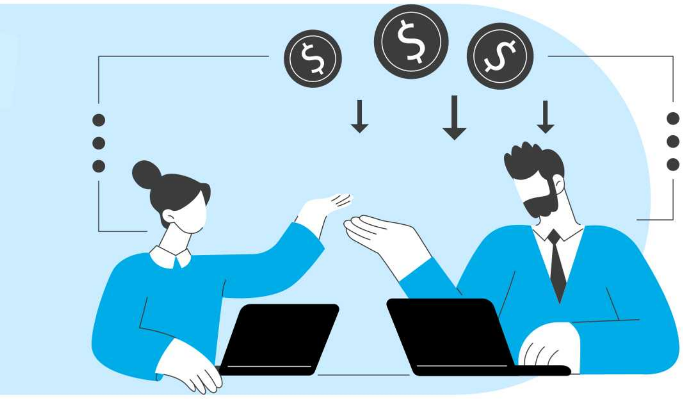
Mobile Device Management (MDM) is a software application that allows IT admins to secure, control, and manage mobile devices remotely. Using an MDM solution, admins can provision devices with required settings and applications, configure various policies, implement kiosk functionalities, and monitor devices' performance and health. Without Mobile Device Management (MDM), organizations struggle to manage and secure their mobile devices. This lack of control can affect productivity, security, and compliance with industry regulations.

Let's take a detailed look at the risks involved when IT Teams are not employing a dedicated MDM solution:

Increased MDM Complexity

Are you using multiple MDM solutions to manage different types of devices?

Provisioning different types of devices into different solutions is tedious and time-consuming for IT teams. Training and maintaining multiple systems can be expensive.

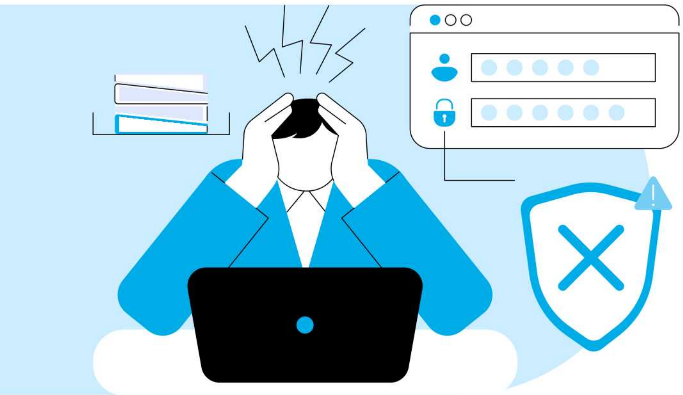


Distracted Employees: Costing Billions

Disengagement among employees leads to a yearly loss of $8.8 trillion in productivity, most of it attributed to device misuse and unmonitored internet usage.

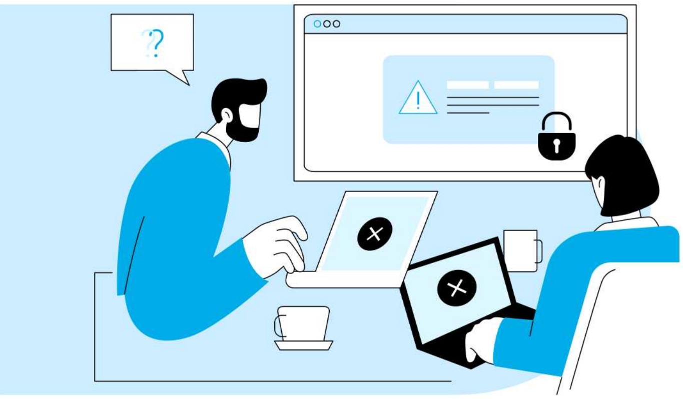
Cyberthreats (Malicious Apps and Phishing Attacks)

CloudSEK found that 193 apps on the Google Play Store were infected with malware. Without an MTD integrated MDM solution, businesses are vulnerable to cyber security threats and data leaks.



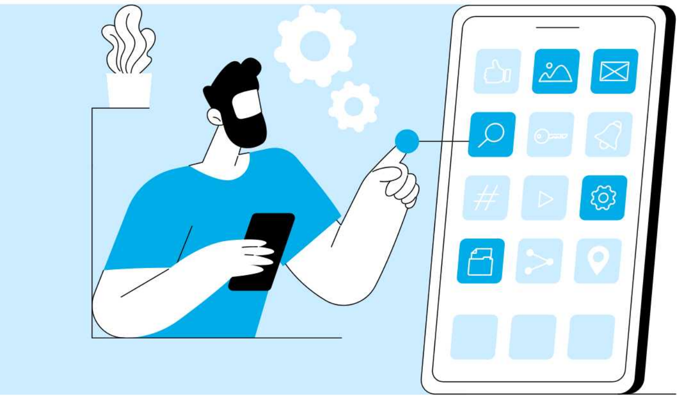
Unsecured Access and Network Attacks

Over 50% of businesses are vulnerable to unsecured WiFi threats. Unsecured remote access and outdated defenses leave your company vulnerable to network based attacks.



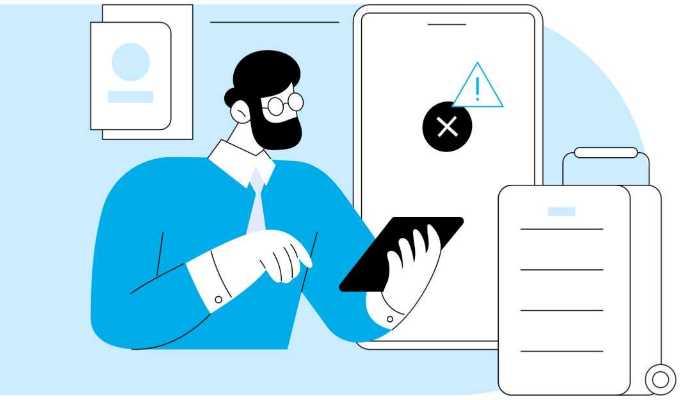
Stalled Work and Overhead costs

Disruptions in operations or downtime caused by device malfunctions lead to decreased business productivity and higher overhead costs. Additionally, shipping devices and providing on-site support incur both financial and time expenses.



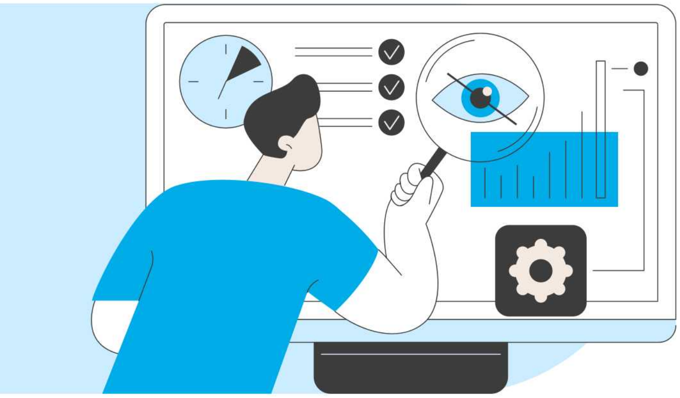
Time-Consuming App Management

Manually installing and updating all business applications on multiple enterprise devices consumes a significant amount of time and negatively impacts the productivity of IT teams.



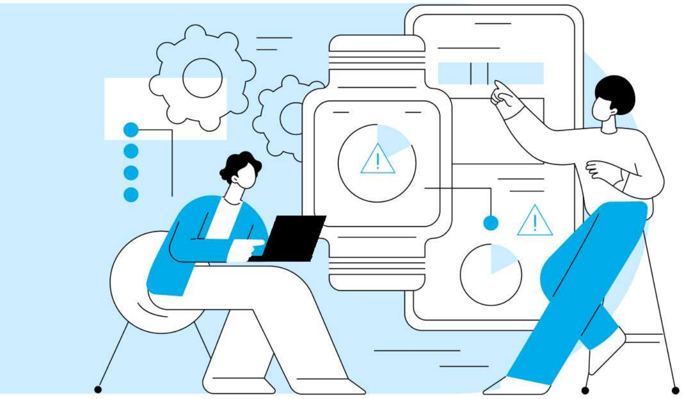
Lost Assets, Last-Mile Delivery Delays

27% of supply chain companies have reported misplacing 10% of their devices each year. Loss of devices both outdoors and indoors leading to financial loss and data breaches. Last mile deliveries result in wasted time and excess fuel costs.



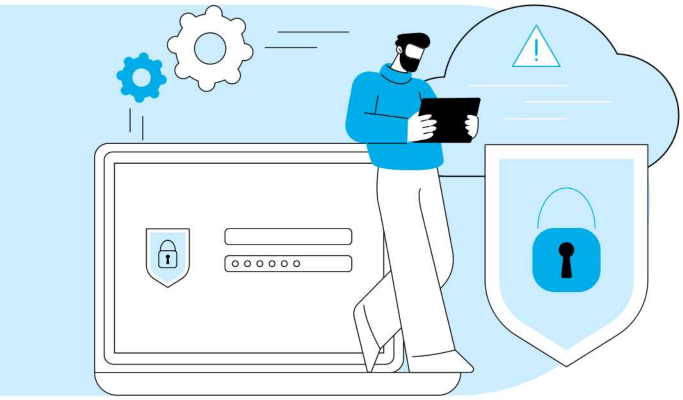
Limited Visibility on Device Health

Blind spots in monitoring the devices' health and performance can lead to potential device issues.



Inefficient BYOD Implementation

According to a report, 63% of the cybersecurity professionals are worried about data leakage as their primary security concern in BYOD (Bring Your Own Device). BYOD offers convenience, but raises serious data privacy and security concerns.



Security Risks, Hidden Costs

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years. Your organization could face potential security risks if devices have weak passwords, data on lost devices, and lack of control over firewall policy and peripheral settings can lead to potential security risks.