



daisy.

COMMUNICATIONS




# Mobile Device Management

and how it contributes to a  
secure remote workforce

# Contents

- 03 Remote work, works
- 04 Mobile devices are here to stay
- 05 Levels of Risk
- 06 What is UEM?
- 07 Working from home with MDM
- 08 Containing Corporate Data
- 09 Ensure Authorised Access
- 10 Wandera Mobile
- 11 Threat Defence
- 12 MDM and Wandera
- 13 Conditional Access  
Mangement
- 14 Remote Desktop Management
- 15 Building trust among home  
workers
- 16 Simple Support
- 17 Contact Us





# Remote work, works

In March 2020, most businesses were forced to adopt a working from home policy. More than a year on, some businesses and employees have seen benefits with 85% of surveyed businesses reporting increased productivity after adopting working from home policies.

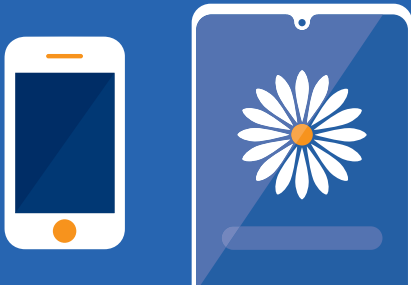
In a study of 500 employees, Stanford University Researchers found a 50% decrease in employee attrition, emphasising the positive impact of the 'new normal' on people's lives.

In a survey by Frost & Sullivan it was found that employees gain nearly an hour (58 minutes) of work time each day and see an estimated productivity increase of a whopping 34 percent when using smartphones to get work done.

Cisco also found that implementing BYOD (Bring Your Own Device) saved an average of \$350 per employee, per year.

# Mobile devices are here to stay

Make the most of your business' devices with Mobile Device Management.



# Diverse apps for any use case



# Easy access to email & content



# Work from any device type





# Levels of Risk



Device Risk



Content Risk



App Risk



Network Risk

# What is UEM?



MDM is the more traditional software used by businesses. However, UEM combines MSM and Enterprise Mobility Management (EMM) to give you a solution that encompasses management, security and identity across mobile devices as well as other devices. It's an evolution of MDM and with Daisy Comms you'll get the best software for your mobile devices.

## Unified applications

Data protection, device configuration and usage policies.



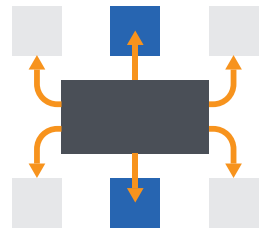
## Single view of users

Enhance end-user support and gather workplace analytics.



## Single console

Configure and manage IoT, smartphones, tablets and laptops.



## Coordination points

Orchestrate activity of related technologies (SIEM, IAM, CMT).

# Working from home with MDM

and its benefits



## Automated Set-Up

With Daisy Comms, you'll get a solution that has your emails, apps and policies configured out-of-the-box. What's more, we'll ensure your VPN can be deployed and configured to your fleet of mobile devices.

## Remote Actions

Ensure your devices are safe no matter where your employees are with our MDM solution.

- Remote lock function
- Real-time location available
- Factory wipe
- Selective wipe
- Self-service user portal

## Data Management

Keep your devices safe and manage your data by implementing a usage cap. You'll also be able to ensure apps can only be used when employees are using WiFi.

## Advanced Policy

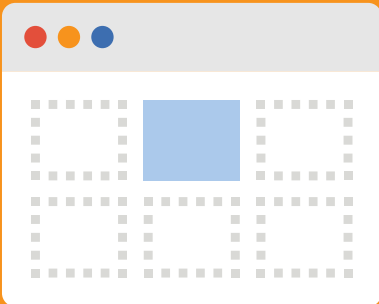
Make sure your mobile fleet is configured with our granular policy configuration. What's more, we can align with best practices through the AI policy recommendation.

# Containing Corporate Data

Businesses have used device management software for almost a decade but the trusted containers are still going strong. In a remote working scenario, using the container is one of the quickest and most secure ways to grant access to sensitive data.

## The reason it works:

- Data separation on personal devices
- Flexible, secure and encrypted



# Ensure authorised access

Out of the box!



User launches application





## Device Authentication

Authenticate the device using your native single user sign on.

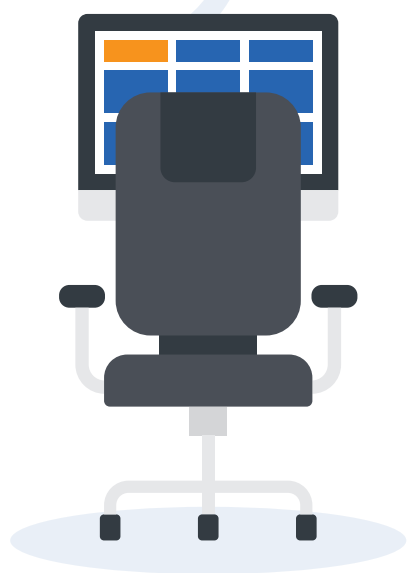


## Access Granted

Once our security system has established the identity of the user and the device, app access is provided.



## Daisy Comms Security Cloud Identity



# Wandera Mobile Threat Defence

Get multi-level protection against cyber threats and usage risks



On your mobile devices, Wandera will be a lightweight mobile application.



From your management console Wandera will give you real-time threat intelligence, cellular data monitoring and in-depth reporting



In your network Wandera will provide a secure access layer to your network and, ultimately, your business data.



With our one click deployment you'll be able to integrate changes and updates across your mobile fleet.



# MDM & Wandera

Get continuous and informed conditional access management

Real-time risk assessment



## Wandera

- Continuous risk assessment
- Multi-level security context (device, apps, networks, content)

Conditional access



## Daisy Comms MDM

- Compliance rules driven by Wandera mobile risk



## Daisy Comms Cloud Identity

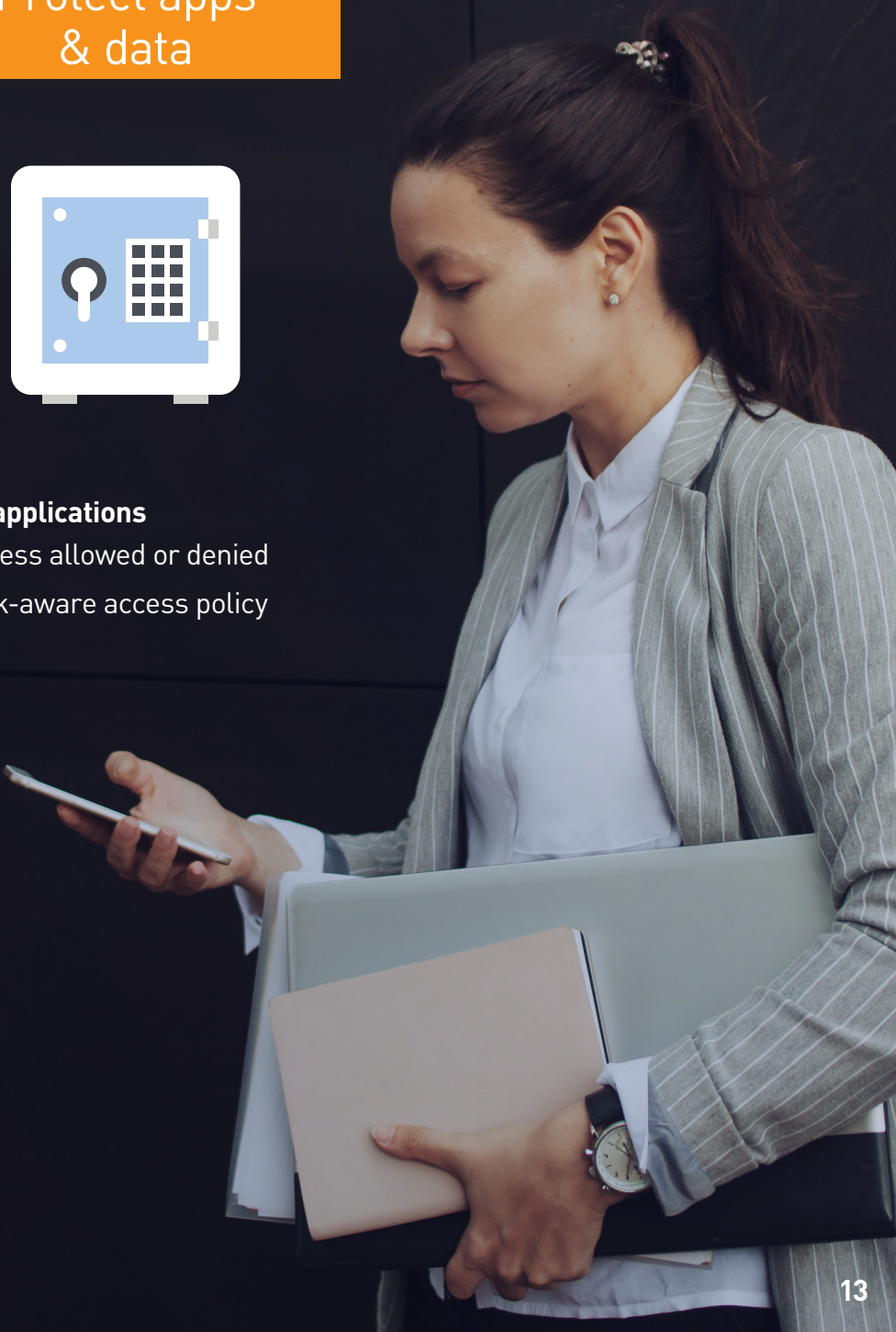
- Access rights determined by mobile risk and compliance state

# Protect apps & data



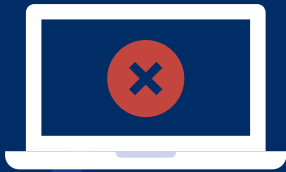
## Cloud applications

- Access allowed or denied
- Risk-aware access policy



# Remote Desktop Management

With Remote Desktop Management you can give administrators control over devices both in and outside of the office and allow them to remotely troubleshoot and configure endpoints.



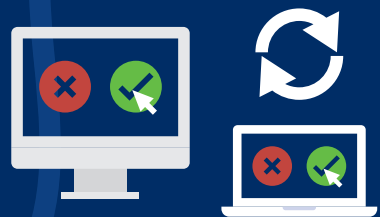
End User has a high-impact device issue.



Administrator requests control via the desktop management portal through MDM console.



Issue is resolved. Control returns to end user.



Administrator is given remote access to end user device for troubleshooting.

# Building trust among home workers



Users working from home need to work from any device. Unified endpoint management (UEM) defines device usage.



Identity and access management verifies user access.



Mobile threat defense keeps the session secure.



Remote support puts the help desk everywhere, avoiding disruption.

# Simple Support

Enable your employees to handle simple support issues with our self-service online portal.

Safely put control back in your employees hands and allow them to manage their own content, apps and devices.

- Sync content across devices
- Add and share content, files and folders
- Take remote action on devices including location, lock, wipe and passcode reset
- View device information including action history, hardware and network information as well as its security and compliance state.





# Contact Us



For more information about our MDM solution either contact your account manager or give us a call on **0808 2749 016.**



Alternatively, head to our website **[www.daisycorps.com](http://www.daisycorps.com)** and take a look at all of our mobile offerings and how we can help you and your business.



daisy.

COMMUNICATIONS