TechSafe Defend

Threat Protection that keeps every mobile device secure.



Who it's for

- CISO
- Security Operations Manager
- Endpoint Manager

What it does

Enhances mobile security by detecting and managing threats across your device fleet, wherever your people work.

Key features

- Mobile malware detection
- Advanced jailbreak and root detection
- Phishing detection
- Insecure Wi-Fi blocking
- Enforceable security compliance policies

Business outcomes

- **Reduced breach risk**
- **Earlier threat detection**
- **Protected business data**
- **Consistent policy enforcement**

ISO 27001 CERTIFIED

How TechSafe Defend protects your mobile fleet

Four layers of protection that stop mobile threats before they become incidents.

1

Detect

Spot mobile malware and jailbroken or rooted devices early.

2

Block

Stop phishing attempts and connections to insecure Wi-Fi.

3

Enforce

Set and enforce security policies against known vulnerabilities.

4

Respond

Act quickly on risky devices to contain threats and protect business data.

Result: fewer incidents, safer mobile users and stronger security.

Use Case 1: Mobile Malware & Jailbreak Detection



Business Challenge

Mobile devices hold sensitive data but often go unmonitored, so malware and compromised devices go unnoticed. This results in:

- Data theft risk
- Unseen compromised devices
- Slow incident response
- Compliance breaches

Who Cares?

- CISO
- Security Operations Manager
- Endpoint Manager
- CIO
- Head of Technology

How TechSafe Helps

- Mobile malware detection
- Jailbreak and root detection
- Continuous threat monitoring
- Clear device risk alerts

Business Outcomes

- Reduced breach risk
- Earlier threat detection
- Protected business data
- Stronger security posture

ISO 27001 CERTIFIED

Use Case 2: Phishing & Insecure Wi-Fi Protection



Business Challenge

Mobile users face phishing links and unsafe public Wi-Fi whenever they work away from the office. This results in:

- Credential theft
- Data interception
- Account compromise
- Reputational damage

Who Cares?

- CISO
- Security Manager
- IT Operations Manager
- Field Operations Manager
- End User Computing Manager

How TechSafe Helps

- Phishing detection
- Insecure Wi-Fi blocking
- Safer connectivity for field staff
- Protection without extra user effort

Business Outcomes

- Fewer successful attacks
- Safer remote working
- Protected credentials
- Greater user confidence

ISO 27001 CERTIFIED

Use Case 3: Security Policy Enforcement



Business Challenge

Device vulnerabilities go unaddressed because security policies are hard to apply consistently. This results in:

- Inconsistent policies
- Vulnerable devices in use
- Audit findings
- Manual follow-up

Who Cares?

- Compliance Manager
- CISO
- Endpoint Manager
- Infrastructure Manager
- CIO

How TechSafe Helps

- Set security compliance policies
- Enforce on detected vulnerabilities
- Device risk reporting
- Works with leading MDM platforms

Business Outcomes

- **Consistent enforcement**
- **Lower vulnerability exposure**
- **Audit-ready reporting**
- **Less manual effort**

ISO 27001 CERTIFIED

Who Buys TechSafe Defend?

Executive Buyer

- CIO
- CISO
- Director ICT
- Head of Technology

Operational Buyer

- Security Operations Manager
- IT Operations Manager
- Service Delivery Manager
- Compliance Manager

Technical Buyer

- Endpoint Manager
- Security Engineer
- Infrastructure Manager
- Desktop Support Lead

Key message: TechSafe Defend protects mobile devices and the data on them, giving executive, operational and technical stakeholders confidence in their security posture.

Industries We Help



Healthcare

Protect clinical and mobile workforce devices handling sensitive data.



Aged Care

Keep frontline carers' devices safe from phishing and malware.



Government

Defend distributed workforces against mobile threats and meet security requirements.



Utilities

Secure field worker devices on public and untrusted networks.



Telco

Protect large mobile fleets and customer-facing devices.



Enterprise

Deliver consistent mobile threat protection at scale.

Why TechSafe Defend

Proactive Protection

Detect mobile malware before it spreads.

Identify jailbroken and rooted devices that put business data at risk.

Safer Connectivity

Detect phishing attempts and block unsafe links.

Block insecure Wi-Fi so staff stay protected on the move.

Policy Enforcement

Set security compliance policies for your fleet.

Enforce them automatically when vulnerabilities are found.

TechSafe Defend delivers mobile threat protection that keeps every device secure, wherever your people work.

Next Steps

Three steps to protect your mobile fleet from day one.

1

Book a security review

Review your device fleet, current risks and security requirements with our team.

2

Agree protection policies

Define the threat, phishing and compliance policies that suit your business.

3

Monitor and respond

Track threats and device risk, with expert support when you need it.

Talk to the TechSafe team to start protecting your devices.