Frequently Asked Questions

What Is Enterprise Mobile Protect?

Enterprise Mobile Protect is a network-level security solution that leverages on 5G network slicing technology and next-generation firewall to secure your mobile fleet. With mobile devices becoming prime targets for cybercriminals due to the rise in remote work settings, this service is essential for safeguarding against device viruses, phishing attacks, and malicious websites. It also enhances your email security by blocking harmful website links and preventing malware from connecting to command-and-control servers.

The following features are included:

1. **Anti-Virus** – Safeguards against malware, worms, trojans, and spyware downloads.

2. **Anti-Spyware** – Prevents spyware on compromised hosts from communicating with external command-and-control (C2) servers, helping you detect malicious traffic leaving the network from infected clients.

3. **Wildfire Analysis** – Utilises machine learning and crowdsourced intelligence to block unknown threats in real-time.

4. **Vulnerability Protection** – Prevents attempts to exploit system vulnerabilities or gain unauthorised access.

5. **URL Filtering** – Monitors and controls web access over HTTP and HTTPS by managing traffic to specific URL categories based on your configuration.

6. **Whitelist/Blacklist** – Manages access to websites, email, software, and IP addresses based on your configuration.

What malicious software does Enterprise Mobile Protect block detect and protect against?

Enterprise Mobile Protect safeguards you against various types of malicious threats and viruses including:

1. **Zero-day threats** – which are new viruses that do not match any existing malware signatures, making them undetectable by traditional signature-based solutions.

2. **Malware & spyware attacks** – which gain unauthorised control on devices, resulting in unpermitted access to personal data stored.

3. **Phishing scams** – which steal one's sensitive information.

4. **Botnet attacks** – which use hijacked networks to spread viruses and other malicious software to devices.

How to be eligible for Enterprise Mobile Protect?

Customers need to be on 5G Standalone (5GSA) – have a 5G SIM card, a 5G plan, and a 5G-enabled mobile device to be eligible to use Enterprise Mobile Protect. Find out if your device is 5GSA compatible here.

To switch on 5G SA on your device, here's how:
- On Apple devices: Settings > Mobile Service > Mobile Data Options > Voice & Data > Select "5G On" and turn on "5G Standalone".
- On Android devices: Settings > Connections > Mobile Networks > Select Network Mode > Select "5G/LTE" > Turn on "Use 5G standalone networks".
- For Android devices, do also ensure "Turn off 5G" under Power Savings is turned off. To check: pull down notification panels > tap & hold "Power Savings" > Toggle off "Turn off 5G".

Singapore Telecommunications Limited
Company registration number: 199201624D
31 Exeter Road, Comcentre Singapore 239732
Tel: +65 6838 3388 Fax: +65 6732 8428
www.singtel.com

I am already subscribed to another mobile security product. Can I sign up for Enterprise Mobile Protect?

Certainly. It is advisable to enhance Enterprise Mobile Protect by incorporating a mobile threat defense application to provide an additional layer of security. This ensures protection even when you are not connected to the Singtel 5G network, such as while traveling abroad.

I have switched on 5G Standalone on my device. However, I am in an area where I am logged on to 4G instead. Am I still protected?

If you have enabled 5G Standalone in your device settings and previously connected to the Singtel 5G network before switching to the Singtel 4G network, you will continue to be protected by Enterprise Mobile Protect.

What is the agreement term for sign up?

Enterprise Mobile Protect is available at $5/month ($5.45/month with GST) and it comes with a minimum contract term of 12 months upon subscription. Any termination before the 12 months contract term will be subject to early termination charge based on cessation date. The service can only be used for one mobile line per subscription.

I am changing my mobile number to another Singtel number. Can I keep my Enterprise Mobile Protect?

Yes.

I have signed up for Enterprise Mobile Protect. How do I set it up?

No setup or client installation is required. To confirm your protection status, please allow up to 3 hours, then reach out to your mobile administrator, who can verify it on Singtel's Empower portal.

Does Enterprise Mobile Protect scan encrypted message content and attachments?

No, it does not. However, if you have clicked on a malicious link, Enterprise Mobile Protect will block you from proceeding with the page.

If I am connected to Wi-Fi at home, will I still be protected by Enterprise Mobile Protect?

No, it does not.

Does Enterprise Mobile Protect work for roaming?

No, it does not support roaming.

Singapore Telecommunications Limited
Company registration number: 199201624D
31 Exeter Road, Comcentre Singapore 239732
Tel: +65 6838 3388 Fax: +65 6732 8428
www.singtel.com