Singtel

Next-gen security for the remote workplace

The traditional office, previously marked by physical boundaries and in-house security, has evolved into a borderless environment due to the rise of remote and hybrid work models. Today, employees are not confined to a single location; they work from various places, including their homes, co-working spaces, or while travelling.

Enterprise threat landscape

The shift to remote work has elevated network-level security from an IT issue to a C-suite priority. As mobile attacks surge and sophisticated phishing campaigns bypass traditional defences, the threat landscape has expanded dramatically, putting sensitive data at risk across all remote devices.

Remote workers are **3x more likely** to be targeted by malware attacks.[1]

47% **of remote workers** have clicked on a phishing link while working remotely.[1]

33.8 million mobile device attacks occurred, a **50% increase** from the previous year.[2]

70% **of remote workers** report using personal devices for work purposes.[1]

Adware accounts for **40.8%** of all mobile threats detected.[2]

Underlying challenges of the remote workspace

Increased attack surface

Remote work and personal devices expand potential entry points for cyber threats.

Home network security

Many home networks lack robust security, making them vulnerable to breaches.

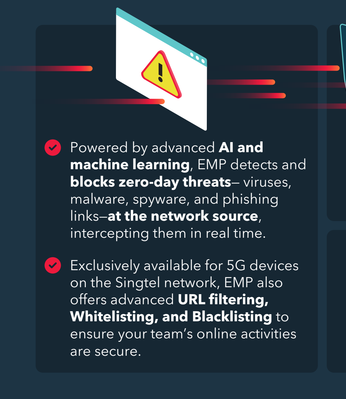
Use of personal devices

Employees' personal devices often lack essential security measures like antivirus and firewalls.

What is Singtel Enterprise Mobile Protect (EMP)

Singtel partnered with Palo Alto Networks to pioneer one of the **world's first Security-as-a-Slice cyber security solutions. Enterprise Mobile Protect leverages 5G Network Slicing technology to integrate a Next-Generation Firewall (NGFW)** into Singtel's 5G network to provide a layer of protection at the network level.

Why Enterprise Mobile Protect (EMP)



- Powered by advanced **AI and machine learning**, EMP detects and **blocks zero-day threats**— viruses, malware, spyware, and phishing links—**at the network source**, intercepting them in real time.
- Exclusively available for 5G devices on the Singtel network, EMP also offers advanced **URL filtering, Whitelisting, and Blacklisting** to ensure your team's online activities are secure.

- EMP offers **zero-touch** deployment, eliminating the need for manual onboarding or installation by end users. With automatic cloud updates, it reduces vulnerability windows by patching the latest threat detection and blocking data without requiring user intervention.
- Additionally, EMP provides exceptional **flexibility and customisation** of policies and profiles, delivering tailored and adaptive security solutions to meet unique organisational needs.

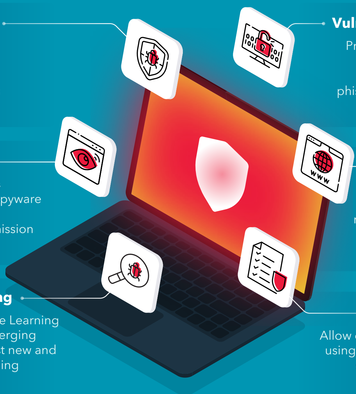
From vulnerability to security with Enterprise Mobile Protect

Antivirus protection

Safeguard your business from disruptive cyber threats, ensuring uninterrupted operations and data integrity.

Vulnerability protection

Protect your business from system vulnerabilities, authorised access, and phishing attempts to reduce data breach risks.



Anti-spyware

Protect sensitive business information by blocking spyware and botnets, preventing unauthorised data transmission to third parties.

URL filtering

Control online activity by blocking harmful or non-productive websites, enhancing security and productivity.

AI & Machine Learning

Leverages AI and Machine Learning to detect and analyse emerging threats, protecting against new and unknown malware, including zero-day attacks.

Whitelist/Blacklist

Allow or deny specific websites using IP addresses to enhance security and compliance.

Block threats at the network level with Singtel

Secure your business now

Learn about Singtel Enterprise Mobile Protect

References

[1] Remote work cybersecurity statistics: alarming trends revealed by recent data, WiFi talents, 2024

[2] Attacks on mobile devices significantly increase in 2023, Kapersky, 2024