



GSMA Mobile Telecommunications Security Landscape 2025

Executive Summary

About this report

The classification of mobile infrastructure as critical national infrastructure in many jurisdictions, and concerns about national security have increased the focus on the security posture of mobile networks. The mobile industry has long aimed to develop and deploy robust security measures to protect its assets, customers and services. Despite the efforts of operators, we continue to see attacks¹ directly on mobile networks and services, including attacks on service delivery, denial of service, the delivery of malware and attacks seeking to exfiltrate data.

This is the GSMA's seventh annual Mobile Telecommunications Security Landscape report. Building on the previous reports², it reflects developments during 2024 and provides a look forward to emerging topics in 2025 and beyond.

Key themes

Five key themes arise from the 2025 Security Landscape report:

- Defensive force-multipliers – the industry is stronger when it acts together.
- Know the network – to defend the network, it is important to understand its infrastructure, underlying technologies, capabilities, data flows, composition, configuration and then simplify and reduce the attack surface, where possible.
- Protect the infrastructure – several key defences are essential, including patching and platform hardening, layered defences, resilience by design, log analysis, threat hunting, least privilege and multi factor authentication (MFA).
- Supply chain – as many attacks are launched through suppliers, supply chain security is a core consideration and competence now and into the future.
- Consider the future when making today's decisions – fully assess the emerging security context, core skills and capabilities to make informed decisions.

Creating a comprehensive security framework depends on an effective security strategy underpinned by a set of technical deliverables and capabilities. As 2024 has seen the continuation of many previously observed security threats, this report covers several evolving topics that were included in previous reports, such as malware, signalling, cloud security and supply chains. However, this year's report also explores some new trends, including:

- Employing the lens of strategic security to examine the landscape and improve mobile networks' security posture based on a full understanding of the attack surface, while reducing complexity and implementing resilience by design and layered defences.
- Updating the technical security landscape, including new topics, such as the need to focus on enabling services and the benefits of threat hunting.
- Describing the landscape from an emerging security context perspective that seeks to frame major enduring security areas that can inform today's security investments in the light of the longer-term operating environment.

¹ <https://www.mobileworldlive.com/att/att-discloses-data-hack-impacting-millions-of-customers/>
<https://www.bleepingcomputer.com/news/security/salt-typhoon-hackers-backdoor-telcos-with-new-ghostspider-malware/>
<https://www.scmp.com/news/world/united-states-canada/article/3281275/wall-street-journal-chinese-hackers-breach-us-court-wiretap-system>
<https://www.channelnewsasia.com/singapore/singtel-malware-chinese-hacking-group-volt-typhoon-4724931>
<https://www.t-mobile.com/news/un-carrier/update-cyberattacks-targeting-us-wireless-companies>
<https://www.sec.gov/Archives/edgar/data/20520/000119312524100764/d784189d8k.htm>
See also <https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf>

² See <https://www.gsma.com/security/publications/>

GSMA Head Office

1 Angel Lane
London
EC4R 3AB
UK

Email: info@gsma.com

