



UNMANAGED MOBILE DEVICES

The Hidden Threat
in Your Organization

soteradigital.com

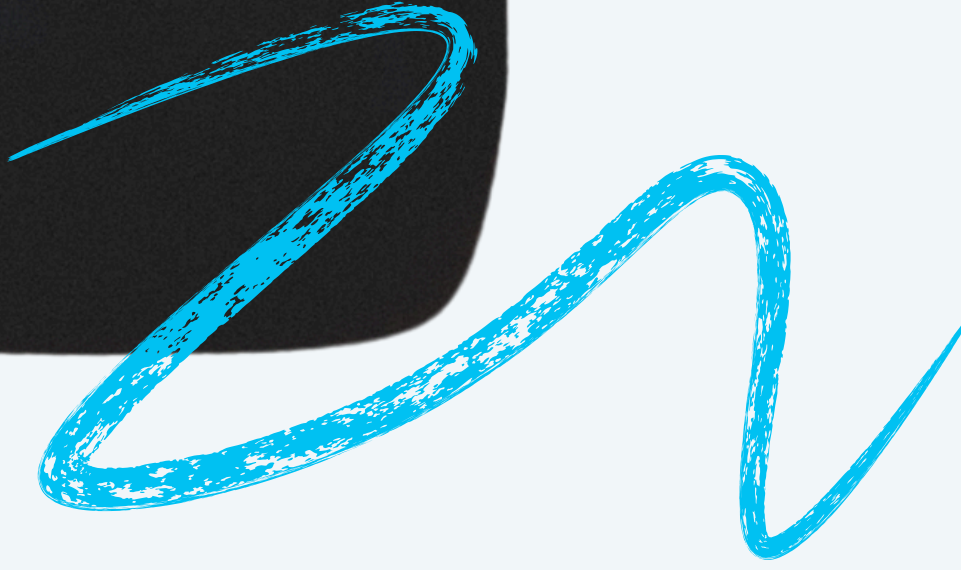




Why Unmanaged Devices Are a Risk

Personal phones used for work often fly under the radar, lacking security oversight. If these devices are compromised, so is your company's data. A single weak link is all it takes to open the door to attackers.

Microsoft reported that 92% of ransomware attacks in 2024 involved unmanaged devices.





BYOD – A Double-Edged Sword

Allowing employees to use their own devices increases flexibility and productivity, but it also introduces blind spots.

Traditional security tools like MDM weren't designed to protect personal devices, leaving security teams with little visibility and even fewer options to enforce compliance.



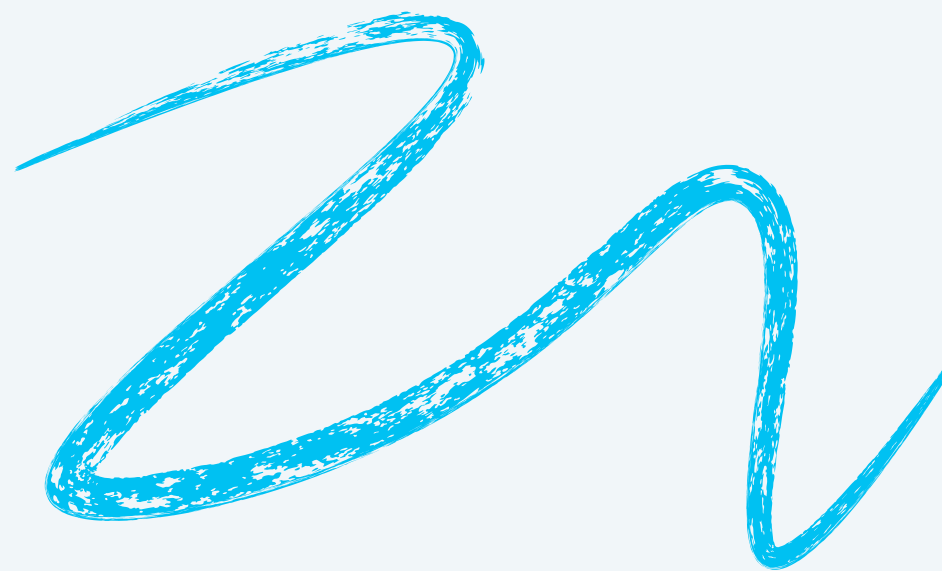


The Future of Zero Trust Includes Mobile

Security strategies must go beyond company-issued devices.

Organizations need to verify every mobile device, restrict access for unknown endpoints, and ensure sensitive communications remain private.

Without these protections, mobile remains the weakest link in your zero-trust strategy.



MOBILE SECURITY, REIMAGINED



Sotera SecurePhone is designed for professionals who can't afford to compromise on privacy.



SOTERA
DIGITAL SECURITY