



















# Cyber Incident Communication: Sentinel vs WhatsApp / Signal

Feature		WhatsApp / Signal	Sentinel
	<b>Cost</b>	Free to use	Annual license; justified by advanced compliance, security & audit features
	<b>Immediacy</b>	Immediate comms if contact is pre-known; requires app installation	Instant Video Crisis Rooms (VCRs); no app or registration needed
	<b>Familiarity</b>	Widely used; familiar UI	Simple interface; intuitive, minimal training needed for advanced use
	<b>Security</b>	End-to-end encrypted, but data readable by group members; unencrypted backups possible	Full encryption in transit and at rest; real-time malware scanning; secure VCR recordings
	<b>Compliance &amp; Auditing</b>	No central logging; deletions possible; not audit-friendly	Centralised, admin-only access to logs; supports legal & regulatory audits
	<b>Group Control</b>	No identity checks; anyone can join if link shared	Verified users only; synced with HR/AD databases; instant external expert invites
	<b>Privacy</b>	Requires sharing mobile numbers; contacts visible to others	No need to reveal phone/email to join; privacy controls in user profiles
	<b>File Sharing</b>	Basic sharing; limited/no malware checking; no audit trail	All files malware-scanned; full audit logs; admin can delete inappropriate content
	<b>Backup Encryption</b>	User-controlled; often unencrypted; backup may leak	Centralised, fully encrypted backups; no local device backups
	<b>Video Recording</b>	No native call recording; no audit trail	VCRs recorded by default; secure, encrypted, admin-access only
	<b>Call Transcription</b>	Not available; external apps can record, increasing leakage risk	Transcribed, encrypted and stored securely; available for audit, compliance, training
	<b>Mass Notification</b>	Group-based only; no external contact capability	Mass alerts via SMS, email, voice to full org or defined groups
	<b>Phishing Risks</b>	Open group access; users often exposed to phishing	Closed, verified environment; ISO 27001 certified; pen-tested
	<b>Analytics &amp; Logs</b>	No central logs or analytics	Logs all comms and actions (chat, email, SMS, VCR); key for post-incident reviews
	<b>Branding &amp; Customisation</b>	Generic apps with no branding	Fully brandable apps; SSO; white-labeled SMS/email alerts
	<b>Metadata Handling</b>	Extensive data & metadata collected; some shared with Meta (for WhatsApp)	Minimal metadata; all data stays on client-owned servers; never shared externally
	<b>Data Residency</b>	Data location controlled by providers; no jurisdictional choice	Client can select AWS data centre/jurisdiction for compliance
	<b>User Data Control</b>	Users' PII visible to group; no profile visibility control	Admin-verifiable profiles; users control visibility of PII

**Talk To Us About Improving Your Cyber Incident Communications**

 [enquiries@sentinelresilience.com](mailto:enquiries@sentinelresilience.com)  
 +44 (0) 808 169 7218