KOOLSPAN

CASE STUDY:
GOVERNMENT AGENCY – SOUTH ASIAN MINISTRY

Ministry
CHALLENGES

A South Asian Ministry operates across multiple countries with officers exchanging highly confidential government information. China-borne cyber-espionage necessitates secure communications for all open internet and mobile communications. Foreign governments routinely exploit the network vulnerabilities of local carriers to intercept mobile communications. Even though some consumer messaging platforms provide a degree of security, the South Asian Ministry cannot risk the reputational damage resulting from intercepted messages or exposure of their usage metadata.

HOW KOOLSPAN TRUSTCALL ADDRESSES MINISTRY CHALLENGES:

The TrustCall Dome environment is wholly disconnected from the public Web and installed behind the Ministry's firewall. Ministry personnel connect to the TrustCall Dome environment via a secure VPN tunnel.

1. When connected to the secure, private TrustCall Dome, users may share sensitive documents, chat in real-time, and place audio/video calls without exposure to prying eyes.
2. TrustCall administrators have granular control of user authorizations and groupings. Ministry personnel may communicate freely with members of their groups and may not communicate with anyone outside their groups.
3. When a device is lost or stolen, the TrustCall administrator remotely wipes the device, preventing the theft or loss of sensitive data.
4. When officials work remotely, they may schedule secure TrustCall audio and video conference calls with the members of their groups.