Use Case: National Security

Permitting smartphones within secure spaces

OVERVIEW

Information warfare has moved to a new battlefield: the smartphone. In recent years, threat actors have gained the ability to remotely hijack the cameras and microphones of a target's mobile device, creating a whole new paradigm of surveillance. Some high-value government buildings, responding to a valid fear of foreign intelligence services observing and listening to key intel, have banned personal mobile devices from the secure spaces in which classified information is being processed, handled or discussed. In the case of the Pentagon, policies have been crafted that require personnel to power down and store their smartphones in daily-use cabinets before entering their workspaces.

CHALLENGE

Restrictive smartphone policies within national security organizations damage both productivity and morale. Without mobile devices at the ready, communication within and between teams is slower and less versatile, resulting in diminished efficiency through delays in making critical decisions, reduced mission flexibility and missed chances for collaboration. In addition, employees have less time to conduct personal business, whether it's keeping in touch with spouses or making doctor's appointments. In the long run, such policies breed disillusionment among personnel and put a damper on recruiting, especially for the younger cohort of workers who grew up in the age of smartphones.

SOLUTION

A government entity dealing with classified information can adopt Privoro Anti-Surveillance – with approval from the proper authorities – to enable workers to use their personal smartphones within secure spaces. Each person working within a secure space is provided a SafeCase, a high-security smartphone case that neutralizes potentially compromised cameras and microphones through integrated camera covers and intelligent audio masking. Anti-Surveillance, which can integrate with an organization's existing mobile device management (MDM) solution, enables administrators to verify protections, set geofences and enforce policies tied to camera/microphone exposure. In essence, Anti-Surveillance gives organizations the ability to leverage workers' smartphones without needing to trust them.

PRIVORO®