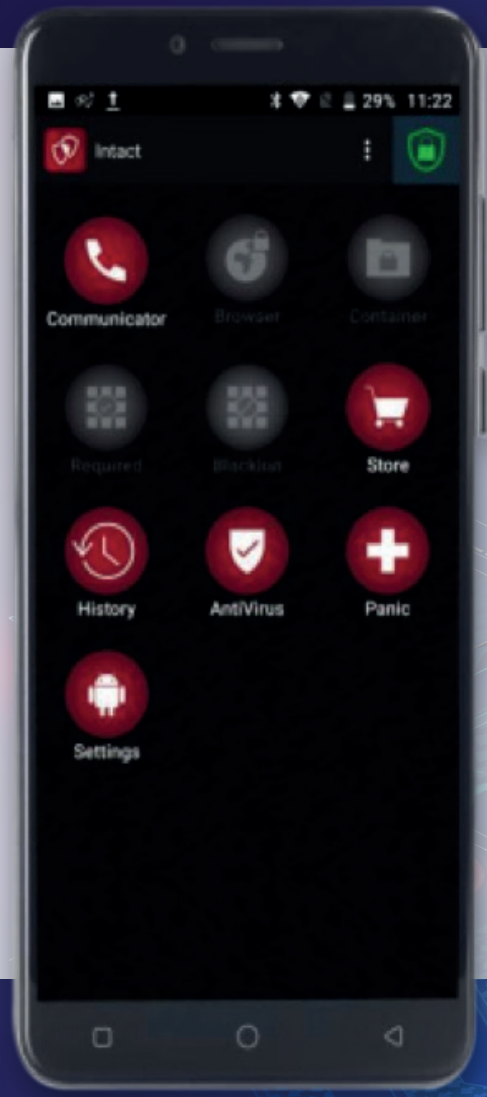
Il Cryptophone più sicuro al mondo, oggi disponibile alla tua Impresa

CREATO PER UNA MOBILE SECURITY SUPERIORE



Intactphone è il telefono cellulare più sicuro al mondo, disponibile per le organizzazioni. Questo smartphone di fascia premium è costruito da zero per fornirvi una difesa estrema contro qualsiasi tipo di cyber-crime mobile. IntactPhone racchiude un sistema operativo ricco di accorgimenti orientati alla sicurezza e appositamente sviluppato, applicazioni di gestione e controllo remoto integrati, comunicazioni criptate di livello militare, nonché molteplici utenze per garantire la protezione e la capacità operativa del dispositivo. Fuse in un unico sistema, queste componenti costituiscono la piattaforma **Intact Mobile Security**. Vi protegge da intercettazioni e ascolti non autorizzati, infezioni di malware, violazione dei Vostri dati sensibili e da ogni tentativo di hackeraggio o di manomissione delle Vostre comunicazioni e scambio di dati mobili. Vi permette di dispiegare e di implementare il più efficace ed efficiente apparato di comunicazione mobile sicura esistente, adeguato ai Vostri specifici requisiti di sicurezza mobile aziendale.

IntactPhone “Arcane”

CARATTERISTICHE ESCLUSIVE DEL DISPOSITIVO

CRITTOGRAFIA DELLE COMUNICAZIONI

Garanzia di comunicazioni sicure: comunicazioni voce e messaggistica criptata end-to-end tra utenti “DialogApp”, comunicazioni voce e messaggistica criptati verso altri sistemi Android/iOS (half-way protection), conference call protette, autodistruzione messaggi impostabile, allegati sicuri, funzione push-to-talk, impedisce l’intercettazione grazie alla rete VPN persistente, comunicazioni sicure tra ogni sistema IP

PROTEZIONE DA MALWARE, VIRUS E SITI OSTILI

Sistema antimalware/antivirus proprietario integrato: protegge ed elimina virus e malware nei file e applicazioni, monitora, blocca ed avverte da tentativi di accesso a siti dannosi, puntuali aggiornamenti Firmware-over-the-air (FOTA)

INTACTPHONE

ELIMINA OGNI TIPO DI “ATTACK SURFACE” ALLA FONTE

- Dispositivo sicuro: firmware proprietario dedicato, boot loaders e drivers esclsusivi: Previene l’installazione di sistemi operativi, boot loaders e ROM ostili o non autorizzati
- L’intero assemblaggio e le installazioni sono effettuate in un luogo protetto e affidabile, al di fuori della Cina: Esclude possibili “backdoors” nel processo produttivo
- Sistema protetto autonomo “stand-alone”: mantiene l’operatività e sicurezza anche se separato dal sistema Centrale di Comando e Controllo. Antivirus e Antimalware integrati. Funzione di self-troubleshooting del sistema
- “Granular control” avanzato sulle risorse del dispositivo: blocco dei vettori di attacco (attivazione di fotocamera, microfono, conference-call, reset di fabbrica, modifica indirizzo MAC WiFi, NFC, AppStore interno, estrazione fisica via USB)
- Utilizzo anonimo garantito: nessun servizio Google/ ibrido (nessun monitoraggio della posizione ed invio di dati a server esterni), notifiche push proprietarie, rubrica interna sicura dedicata (senza numero telefonico), bypassa la necessità di inserire dati privati nelle app, Rete VPN persistente
- Gestione e supervisione del dispositivo: previene dall’uso incauto, riducendo la vulnerabilità del dispositivo. Aggiornamenti SW, Antivirus e Malware, Gestione delle risorse, controllo degli accessi, app non affidabili (AppStore dedicato esterno), restrizioni impostabili, controllo costante browsing internet, rispetto delle policy di sicurezza, supporto da remoto per manutenzione

Elimina i rischi legati alla perdita e/o furto del dispositivo: previene l’accesso non autorizzato ai dati. Sistema completo costantemente criptato quando in “lock-screen”, da remoto localizzabile, bloccabile, cancellazione dati totale e selettiva, reset di fabbrica

INTACTPHONE

DATA PROTECTIO

IDENTIFICA MINACCE IGNOTE

Monitora, mappa e registra i funzionamenti del dispositivo segnalando comportamenti anomali: Monitora e blocca reti WiFi dubbie (attacchi MITM), monitora e blocca celle telefoniche anomale (IMSI catcher), verifica browsing internet costante, monitora le applicazioni

ASTRAZIONE DEI VETTORI D'ATTACCO

Offuscazione delle risorse interne: un livello di protezione addizionale, dedicato e proprietario, astrae le risorse interne affinchè un trojan dovesse penetrare le difese del dispositivo, non potrebbe comunque attivarle (microfono, fotocamera, WiFi, NFC, bluetooth, USB, HotKnot)

CRITTOGRAFIA DEI DATI

Sistema di crittografia stand-alone altamente resistente che protegge il disco fisso del dispositivo. Resiste ad indagine forense. "Panic Button" per azzeramento immediato del dispositivo alle condizioni di fabbrica.