ZERO-TRUST
vs. A WALLED GARDEN

Consumer Apps

When a product is Free, You are the product

- Uncertified encryption often with fundamental security flaws, e.g., using telephone numbers as User IDs
- Requires trust in both the service provider and their infrastructure
- Call and messaging metadata is owned by the service provider; this includes:
  - Your phone number, profile name, photo, online status and status message, and last seen status
  - Information on who, when, and how often you are messaging, calling, etc., and which groups you belong to
  - Location data
  - Information on your online status, such as when you were last seen online, when you updated your status message, etc.
  - Device data, such as hardware model, operating system information, browser information, IP address, mobile network information including phone number, and device identifiers

Cellcrypt FEDERAL

Why is Cellcrypt different?

- Cellcrypt is certified (NIST, NIAP, and NSA) to protect information up to US Classified Top Secret and is used by organizations and governments worldwide
- With Cellcrypt, organizations manage the apps, users, and policies with full ownership and control of the communication stack **and** metadata
- Cellcrypt is designed to be secure, even when the network has been proactively compromised


FORRESTER®

The Rise Of Anti-Surveillance Capitalism

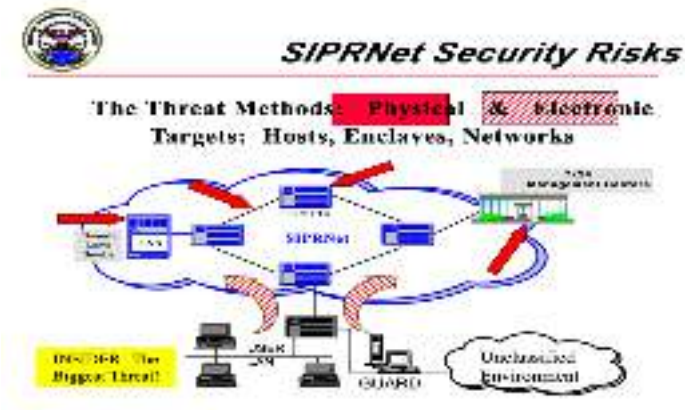
The Apparel, Cosmetics, And Technology Shaping Surveillance Resistance And Why It's Time For CISOs To Adopt Them

"Secure messaging technology: Signal and WhatsApp entered the enterprise world through consumerization of IT, but they lack enterprise control features. The successful adoption of the software does demonstrate a desire for encrypted communications by end users, and vendors like Cellcrypt, KnoiSpac, and Salt0ft4 exist to offer an IT-managed solution to facilitate the need for secure messaging."

Walled Garden

Many solutions rely on ‘trust’ in a “Walled Garden” i.e., companies that provide the solution, individuals that run the system and security of the network

- Weak points can often be overlooked/discounted as apps reside in the walled garden
- Encryption in
- Walled Gardens do not tackle the greatest problem – the INSIDER – the biggest threat as acknowledged by DISA.



Cellcrypt FEDERAL

Why is Cellcrypt different?

- Cellcrypt was designed to provide **Zero-Trust** security of communications across networks that are assumed to have been ‘proactively compromised’
- Cellcrypt delivers this through real-time, end-to-end encryption of all data – voice, video, messaging, and files, so that only the end user parties in calling, messaging and file transfers can encrypt/decrypt communications
- With Cellcrypt, NIAP Certified encryption (the US Top Secret standard) is the base level through which CNSA/Quantum-Safe Cryptography is tunneled, removing reliance on a “Walled Garden”

“The foundational tenet of a Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted.”

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET - JAN 26,2022

CNSA Suite Comparison	Cellcrypt Crypto Core
Advanced Encryption Standard (AES), per FIPS 197, using 256-bit keys to protect up to TOP SECRET.	AES-256 **Fully Compliant**
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange, per FIPS SP 800-56A, using Curve P-384 to protect up to TOP SECRET.	ECC-521 **Exceeds Guideline**
Elliptic Curve Digital Signature Algorithm (ECDSA), per FIPS 186-4, using ECDSA-384 to protect up to TOP SECRET.	ECDSA-521 **Exceeds Guideline**
Secure Hash Algorithm (SHA), per FIPS 180-4, using SHA-384 to protect up to TOP SECRET.	SHA-512 **Exceeds Guideline**

Cellcrypt FEDERAL

Cellcrypt Encryption

Multi-Layer Cryptographic Approach

1. Data is Obfuscated

All data - voice, video, messages, and file attachments - are first obfuscated using the ChaCha20-256 algorithm to mitigate any future potential AES vulnerabilities. This occurs before the data is encrypted through the Cellcrypt Crypto Core.

2. Encrypted with CNSA Cryptography

The obfuscated data is secured end-to-end using a package of Elliptic Curve Cryptography (ECC) and Symmetric-Key Cryptography that meets or exceeds the key length standards of the CNSA Suite for Top Secret communications.

Cellcrypt FEDERAL

Cellcrypt Encryption

Multi-Layer Cryptographic Approach

3. With Post-Quantum Protection

Cellcrypt's Crypto Core is then cryptographically overlaid with Post-Quantum Cryptography. The quantum-safe envelope allows for algorithms to be layered and changed as standards in this area emerge without affecting the strength of the underlying ‘classical’ CNSA encryption.

4. Running through a NIAP Architecture

All data and cryptography detailed is run through a NIAP validated MA CP 2.5 compliant architecture where the outermost layer and all server links are secured with TLS using NIST validated algorithms (ECC-384 and AES-256).

Cellcrypt FEDERAL

FIPS Certification

National Institute of Standards and Technology

- The current CAVP validations for Cellcrypt can be found at: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=34608
- CAVP certification is a pre-requisite for the NIST Cryptographic Module Validation Program (CMVP), the purpose of which is to validate cryptographic modules and provide assurance to US Federal agencies in procuring equipment containing validated cryptographic modules.
- CMVP Cert. #4178 has been issued for the Cellcrypt Core V4 FIPS 140-2 Module at the following link:: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4178

Cellcrypt FEDERAL

NIAP CCEVS Certification

Validated / In Evaluation

- **Cellcrypt Server**

  NIAP Certified

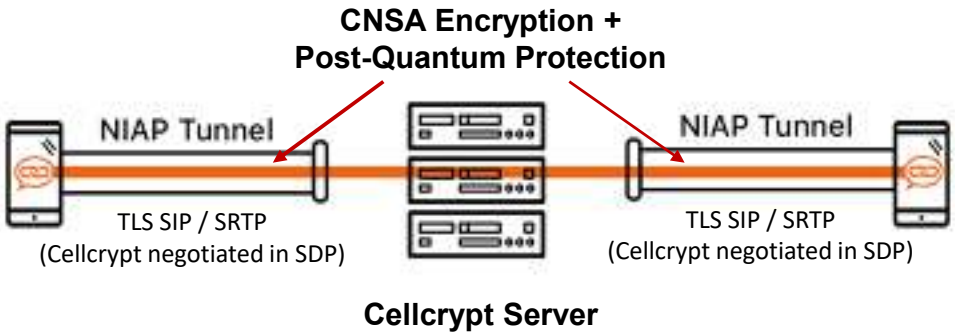
  - U.S. Government Approved Protection Profile – Collaborative Protection Profile for Network Devices - Version 2.2e cpp_nd_v2.2e
  - U.S. Government Approved Protection Profile – PP-Module for Enterprise Session Controller (ESC) - Version 1.0 mod_esc_v1

- **Clients**

  NIAP Certified - Android

  Windows (in Eval Oct 2022), iOS (TBD)

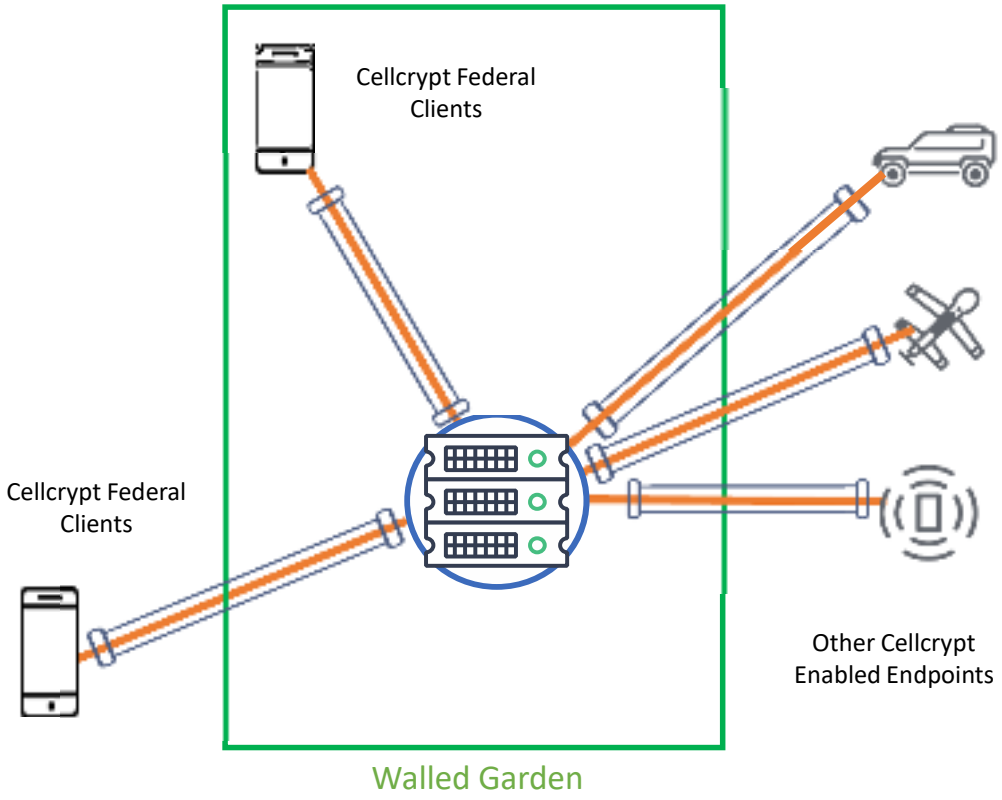
  - U.S. Government Approved Protection Profile - Protection Profile for Application Software - Version 1.3, 2019-03-01 AppPP
  - U.S. Government Approved Protection Profile - PP Module for Voice and Video over IP (VVoIP) - Version 1.0, 2016-09-28 mod_vvoip_v1
  - U.S. Government Approved Protection Profile - Functional Package for Transport Layer Security (TLS) Version 1.1, 2018-12-17 TLS-PKG



Tunneling End-to-End Encryption
Solves the Problem

- Cellcrypt Federal tunnels end-to-end encryption through NIAP-approved tunnels
  - Cellcrypt Federal encryption tunnels through RTP for end-to-end CNSA+QSE voice encryption.
  - Cellcrypt Federal protocol negotiated via Session Description Protocol (SDP).
- E2E Encryption delivers robust communication security for every message, voice, and video call.

Assume Zero-Trust
The Safe Play



- Mutually Authenticated CNSA + Quantum-Safe Encryption tunneled end-to-end negates reliance on a fully trusted network
- Cellcrypt Federal provides the same degree of protection even when the network has been proactively compromised
- Network / Carrier Agnostic
- **Eliminates the Risk**

Cellcrypt FEDERAL

ZERO-TRUST
SECURE COMMUNICATIONS

Cellcrypt FEDERAL

Trust in a Zero-Trust World

- The Cellcrypt Trusted Communications Network is a FIPS/NIAP validated, end-to-end encrypted, Security-as-a-Service (SECaaS) solution.
- Full assurance for communications and data-in-transit in austere, proactively compromised, ‘Zero-Trust’ environments.
- A multi-layered cryptographic approach, streaming end-to-end CNSA (Commercial National Security Algorithm Suite) with Post-Quantum Cryptography (PQC).
- Cellcrypt’s Ephemeral Key Exchange negates the need for COMSEC Key Management, and for every call, message, or file transfer, a new keyset is generated.

Cellcrypt Features

Authenticated, E2E Encrypted Messaging, Voice, Video

- Messaging, voice/video, and large file transfers are fully-encrypted end-to-end (E2EE).
- Mutual Authentication for all parties eliminates spoofing and eavesdropping (MiTM) risks.
- Secure groups for messaging, calling, and file sharing.
- Device (iOS, Android, Windows) agnostic with enhanced “Data at Rest” Protection.
- Advanced codes for HD quality and low bandwidth mode for any network, e.g., 5G, 4G/LTE, 3G/HSDPA, 2G/EDGE, Wi-Fi, satellite.
- Interoperability with 3rd Party NIAP devices and PBX desk phones.

Native Cellcrypt Clients

Cross-Platform Client Apps

- Native Cellcrypt client apps are available for Android, iOS and Windows smartphones, tablets, and desktops.
- Clients can be obtained/updated through:
  - Consumer App Stores
  - MDM Distribution (MobileIron/App Config)
  - A white-label ‘Get Store’ from Cellcrypt

Cellcrypt FEDERAL

Cellcrypt Server

PRIVATE STACK

- The Cellcrypt Server is NIAP and CSFC validated and controls users, policies, and permissions and safeguards meta-data and confidential information.
- The self-contained, secure communications infrastructure provides signaling services and facilitates secure messaging, voice and video, file transfer, and storage.
- The Cellcrypt Private Stack can be deployed on-premises, multi-Cloud (Azure or AWS), or field-deployed on a NUC or notebook.
- Flexible hardware/network requirements
  - Servers can be installed on-premises, cloud, or even on notebook computers.
  - Seamless integration with Azure Active Directory