RDCTD-41A

AIR-GAPPED SECURITY

ISOLATE TO PROTECT

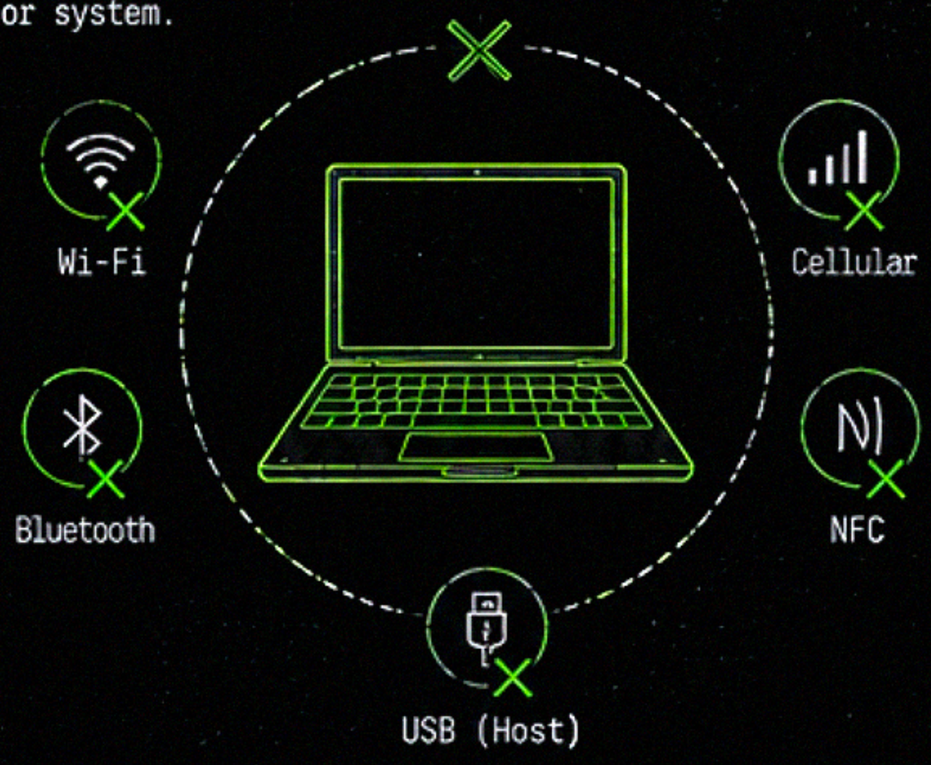
THREAT MODEL

- REMOTE EXPLOITS
- MALWARE DELIVERY
- DATA EXFILTRATION
- IMPLANT CALLBACKS
- SUPPLY CHAIN RISK

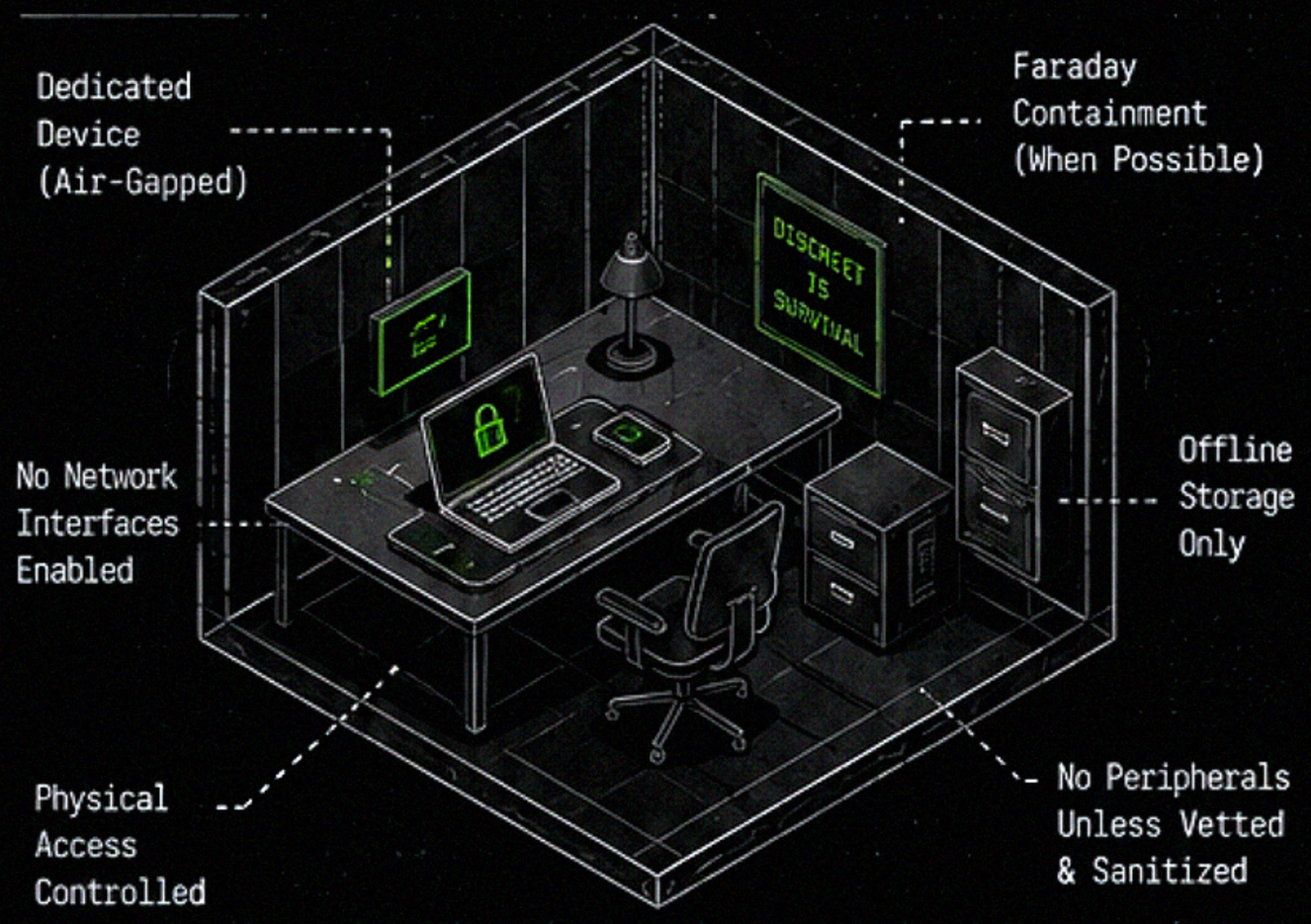
NO WI-FI. NO BLUETOOTH. NO CELLULAR. NO LINKS.
NO PATH IN. NO PATH OUT.

1. CONCEPT

Air-gapped devices have no electronic connections to any untrusted network or system.



2. HOW IT WORKS



3. DATA FLOW (ONE-WAY, CONTROLLED)

Create / edit data on air-gapped device.

Write data to sanitized removable media.

Physically move media through trusted channels.

Read data on another air-gapped device only.

Verify integrity. Wipe media after use.

MEDIA SANITIZATION

Use New or Dedicated Media

Scan on Clean System

Wipe (Full) After Use

Store in Protective Case

Label & Track Chain of Custody

4. DEVICE HARDENING

- Disable/Remove all radios (Wi-Fi, BT, Cellular, NFC)
- Remove or epoxy unnecessary ports
- Boot from trusted media (Read-Only when possible)
- Keep OS minimal & up to date (Offline)
- Use application allowlisting
- Encrypt all data at rest
- Disable auto-run & removable media execution
- Power down when not in use

5. OPERATOR TRADECRAFT

PHYSICAL SECURITY

- Control environment
- Lock devices
- No unattended access
- Use tamper seals

SUPPLY CHAIN

- Vet hardware sources
- Inspect for tampering
- Avoid pre-owned when possible

ENVIRONMENT

- Avoid RF-leaky locations
- Use Faraday when needed
- Beware of peripheral leakage (Cables, LEDs)

BEHAVIOR

- Assume observation
- Minimize pattern
- Vary routes & times
- Keep it boring

CONTINGENCY

- Assume compromise
- Wipe & rebuild
- Have backup plan
- Exfil without residue

AIR-GAPPED ISOLATION
DOESN'T MAKE YOU INVISIBLE.
IT JUST REMOVES THEIR REMOTE ACCESS.

STAY OFF THE GRID

VERSION: 1.0
CLASS: UNRESTRICTED

RDCTD