PRODUCT & BUSINESS PLAN // v1.0 // CONFIDENTIAL

SENTINEL

Track-Back Defense Platform

A lawful cyber-deception, forensics, and vault platform that lures attackers into decoys, records everything, analyzes captured threats, and hands a court-ready evidence package to law enforcement — protecting everyone from a single family to a national government.

TRACK-BACK, NEVER HACK-BACK

CFAA-COMPLIANT BY DESIGN

PERSON → GOVERNMENT

Prepared for the founder · Brandon, Florida · Confidential

The problem we refuse to accept

Executive Summary

Cybercrime is a multi-trillion-dollar industry and the individual, the small business, and even the government are usually on defense — reacting after the breach, after the ransom, after the theft. SENTINEL flips the posture without ever breaking the law. Instead of striking back at attackers (which is a federal crime), SENTINEL builds a landscape of irresistible decoys, watches criminals walk into them, and quietly documents every move for the authorities who are legally empowered to act.

The founder's principle is simple and non-negotiable: we hate what hackers do, and we will never become one. SENTINEL is a track-back platform, not a hack-back platform. Every capability is designed to observe, preserve, and report — never to reach into, damage, or steal from anyone else's systems.

4
CORE MODULES
Honeypot · Forensics · Vault · Filter

3
MARKET TIERS
Family · Business · Government

$0
HACK-BACK RISK
100% CFAA-safe architecture

What SENTINEL is, in one line

A self-contained "digital crime lab in a box": decoy systems that catch attackers, a forensic microscope that analyzes what they leave behind, an evidence engine that reports them to the FBI/CISA, and an air-gapped vault that keeps the things you actually care about untouchable.

The Legal Bedrock: Track-Back vs. Hack-Back

The single most important design decision in SENTINEL is legal. "Hacking back" — reaching into an attacker's computer to delete stolen files, corrupt their data center, or claw back a ransom — is a federal crime under the Computer Fraud and Abuse Act (CFAA, 18 U.S.C. §1030), even when you are the victim.[1] The Department of Justice warns that such actions "may be illegal, regardless of motive," and note that most attacks are routed through the compromised machines of innocent third parties — so hacking back usually harms another victim.[2]

HACK-BACK (illegal — we never do this)	TRACK-BACK (legal — what SENTINEL does)
Access the attacker's computer without authorization	Attacker voluntarily opens our bait file on their machine; it reports home
Delete or corrupt the attacker's data	Preserve evidence of what the attacker did to us
Drain or reverse the ransom payment	Tokenize and log the ransom demand; forward to law enforcement
Identify a suspect and pursue them yourself	Hand a chain-of-custody package to FBI IC3 / CISA who pursue lawfully

Bills to legalize a narrow form of hack-back (the Active Cyber Defense Certainty Act of 2017 and 2019) never even received a vote.[3] Honeypots, beacons, and canary tokens, by contrast, are explicitly recognized as legal active-defense tactics because they operate only on your own infrastructure.[4] SENTINEL lives entirely on the legal side of that line — which is exactly what makes it sellable to businesses and government.

1. Congressional Research Service, "Cybercrime and the Law: Primer on the CFAA." congress.gov/crs-product/R47557
2. Bloomberg Law, summarizing the DOJ computer-crime manual. news.bloomberglaw.com
3. GovTrack, Active Cyber Defense Certainty Act (H.R. 3270, 2019) — no vote. govtrack.us/congress/bills/116/hr3270
4. Security Today, "Hacking Back: Revenge is Sweet, But is it Legal?" — honeypots & beacons are lawful. securitytoday.com

What we actually build and sell

The Four Modules

01 Honeypot & Deception Grid

THE TRAP · "looks vulnerable, is a trap"

A network of decoy servers, fake admin logins, and phony "data center" file portals that appear vulnerable but are pure bait. Every click, credential attempt, and download is logged.

» Fake vulnerable systems that catch intruders
» Full logging of every action (IP, time, payload)
» Watermarked canary/bait files for lawful track-back

02 Forensics Lab & Malware Microscope

THE MICROSCOPE · analyze what they leave

An isolated lab that fingerprints captured samples — hashes, file type, extracted strings, threat classification — and builds a growing database ("virus zoo") of everything analyzed. Nothing is ever executed outside containment.

» Hash + classify captured malware
» Growing searchable threat database
» Attribution hints flagged for law-enforcement follow-up

03 Air-Gapped Encrypted Vault

THE SAFE · tokenized, offline, untouchable

A personal-to-government vault that stores your sensitive files, notes, and credentials fully encrypted and offline. Every item is referenced by an opaque token, so even the listing reveals nothing. Scales from one person to nuclear-grade physical air-gap.

» Strong encryption at rest, works fully offline
» Tokenized references — real content never exposed
» Tiered: Family → Business → Government

04 Filter & Track-Back Gateway

THE SHIELD · catch it before it hits you

A protective layer — like a virtual card number that absorbs fraud before it touches your real account — that detonates suspicious links and attachments in a safe sandbox before anything reaches your phone, inbox, or business files.

» Threats hit the filter, not your real systems
» Suspicious links swapped for safe tokenized ones
» Includes a phishing-simulation trainer for staff

The signature capability, explained simply

How Lawful Track-Back Works

This is the heart of the founder's vision — following a criminal back to the authorities without ever touching the criminal's machine. Here is the chain, step by step, all of it legal:

01

Bait is planted

SENTINEL seeds decoy files (fake "passwords.xlsx", fake "network_diagram.pdf") inside the honeypot. Each carries a hidden, unique token and a callback address.

02

Attacker steals the bait

The intruder breaches the decoy (not your real system) and exfiltrates the bait file, believing it is valuable.

03

Their machine reports home

When the attacker OPENS the file on THEIR OWN computer, the embedded token quietly beacons back to SENTINEL. We never reached into their system — theirs contacted us. This is the legal line.

04

Evidence is preserved

SENTINEL records the beacon (time, reporting network, token) and packages it with the honeypot logs under a tamper-evident chain of custody.

05

Authorities are notified

A complete forensic report is forwarded to the FBI's IC3 and CISA. The tokenized ransom trail goes to the cyber-forensics lab — never to the consumer.

06

Law enforcement acts

Because a real crime (unauthorized access + theft) has already occurred, investigators can lawfully obtain warrants and pursue the suspect. SENTINEL's role ends at reporting.

Who buys it, and for how much

Market Tiers & Pricing Model

SENTINEL is one architecture sold in three sizes. The same core scales down to a single person and up to a national government — the higher the stakes, the higher the value and the price.

TIER	WHO	WHAT THEY GET	MODEL
1 · Family	Individuals & families	Personal air-gapped vault + filter gateway that stops phishing/malware before it reaches phone & email. Track-back reports go to authorities, never to the user.	**Low monthly subscription**
2 · Business	SMBs & enterprises	Everything in Tier 1 + honeypot deception grid, forensics lab, staff phishing trainer, SIEM/SOC integration, team dashboards, tokenized track-back.	**Per-seat + platform fee**
3 · Government	Agencies & critical infra	Full platform + nuclear-grade physical air-gap, formal chain-of-custody, direct evidence hand-off to federal cyber-forensics, and (only under explicit government authorization) advanced attribution support.	**Enterprise / gov contract**

Revenue streams

» Subscriptions — recurring SaaS revenue across all three tiers.

» Government & enterprise contracts — high-value, multi-year deployments.

» Threat-intelligence data — anonymized, aggregated findings from the malware microscope, sold to researchers and defenders.

» Training & certification — the phishing-simulation trainer as a standalone security-awareness product.

Turning the vision into traction

Go-To-Market Strategy

A strong product still needs a path to real users. SENTINEL's go-to-market plan rests on four grounded pillars — build a credible pilot, fund it through non-dilutive grants, prove it with partners, and earn trust through public education. Everything below is achievable from a Brandon/Tampa Bay home base.

01 Prototype & Pilot

Start with the working prototypes shipped here. Harden the honeypot + forensics pair first — it is the most differentiated — with a simple interface non-technical users can trust.

» Run a controlled pilot with 2–3 friendly local businesses
» Use only synthetic attacks and opted-in testers
» Capture testimonials and before/after metrics

02 Funding via Grants

Pursue non-dilutive funding before giving up any equity. Federal SBIR/STTR programs and critical-infrastructure security grants are a natural fit for a lawful track-back-and-report platform.

» Draft an SBIR/STTR proposal (DHS/CISA cyber topics)
» Explore Florida small-business & innovation grants
» Frame impact: prevent loss, protect infrastructure, aid law enforcement

03 Partnerships

Credibility comes from partners. Team with a local university cyber program for testing and validation, and with regional cybersecurity firms for real-world scenarios and referrals.

» Partner with a Florida university cyber center (e.g., USF)
» Offer student research / internship collaboration
» Co-develop with a regional MSP or security firm

04 Awareness & Trust

Because this touches privacy and law enforcement, transparency is a feature. Lead with education so customers understand exactly where the legal line is and why SENTINEL never crosses it.

» Publish plain-language 'track-back, not hack-back' explainers
» Host a local workshop for small businesses
» Turn anonymized findings into public case studies

From prototype to trusted vendor

Roadmap, Ethics & Next Steps

Phased roadmap

PHASE 1 — Prototype (now)

Working demos of all four modules (delivered with this plan). Validate the track-back flow end to end in a lab.

PHASE 2 — Pilot

Deploy the honeypot + forensics + vault with 2–3 friendly local businesses in the Tampa/Brandon area. Gather real (synthetic-attack) telemetry and testimonials.

PHASE 3 — Certify & comply

Independent security audit and penetration test. Formalize the chain-of-custody process with a cyber-law attorney and establish the reporting pipeline to IC3/CISA.

PHASE 4 — Government track

Pursue FedRAMP / relevant authorizations and partner with a federal cyber-forensics program for the Tier 3 offering.

Ethics & compliance guardrails

Non-negotiable operating principles

- » We never access, damage, or exfiltrate from any system we do not own.
- » All malware analysis is contained; nothing is detonated in the wild.
- » All demo/prototype data is synthetic — no real personal data.
- » We collect and report evidence; only law enforcement pursues suspects.
- » Phishing simulations are sent only to opted-in internal users.
- » GDPR / CCPA-aware handling of any user-like data.

Immediate next steps

- » Review the four working prototypes shipped alongside this plan.
- » Pick a lead module to harden first (recommend: Honeypot + Forensics — it is the most differentiated).
- » Engage a cybersecurity attorney to review the track-back-and-report workflow.
- » Line up 2–3 pilot customers for Phase 2.