// PROFULLSTACK, INC. · SEED ROUND · 2026

threatcrush.

Detect. Reduce. Respond. Strike back

Lifetime $499 · pay once

MIT-licensed core

CTEM + SIEM/EDR/SOC

MITRE · D3FEND · Sigma · OCSF

// THE PREMISE

~~Patch management~~ is no longer the bottleneck. Continuous exposure is.

2014

A SOC analyst triaged a quarterly vuln report. The hard part was prioritizing CVEs.

2026

AI agents probe your perimeter every hour — and your team finds out three weeks later from a stale dashboard.

// PROBLEM

Defense means stitching 30+ tools.

Each one has its own agent, schema, license, and quirks.
Each one can silently miss the attack that finally lands.

- Vuln scanners
- EDR agents
- SIEM
- SOAR
- XDR
- Attack-surface
- CSPM
- CWPP
- CIEM
- WAF
- IDS / IPS
- NDR
- DNS firewalls
- Honeypots
- Deception
- Threat intel
- SAST
- DAST
- Secrets scanners
- Container scanners
- Cloud audit
- Pentest tooling
- Phishing sims
- Email security
- IAM · PAM
- Compliance · SOC2
- Log shippers
- …and 20 more

→ A stack that costs a **Fortune-500 team millions** is a wall that stops **every indie ops team** from getting started at all.

// WHY NOW

Q2 · 2026

Attackers ship at *100×* human velocity. Defenders run at 1×.

AUDIENCE

28M

LINUX SERVERS RUNNING ON THE PUBLIC INTERNET

GAP

~0

SINGLE AGENTS COVERING CTEM + SIEM IN ONE BINARY

MARKET

$215B

GLOBAL CYBERSECURITY SPEND, 2026 (GARTNER)

// whoever owns the agent on the box owns the detection layer for the next ten years.

// SOLUTION

One agent. Two layers.

root@edge-01 — threatcrush v1.0

```
root@edge-01 :~# threatcrush monitor
✓ watching all ports · nginx · sshd · postgres · loaded 1,247 sigs
⚠ SQLi attempt — :443 185.43.21.8 → /api/users?id=1 OR 1=1
⚠ SSH brute force — :22 91.232.105.3 → 47 failed attempts
✓ ssh-guard banned 91.232.105.3 · tar-pit engaged

root@edge-01 :~# threatcrush scan ./src
✓ 3 secrets · 7 CVEs (2 critical) · 4 misconfigs · sigma rules emitted

root@edge-01 :~# threatcrush pentest https://api.acme.io
… fuzzing endpoints… mapping ATT&CK techniques · proposing fix #1 of 3
```

01 — DETECT

Every port. Every protocol. Live signatures.

02 — REDUCE

Code, deps, config — fix exposure before it ships.

03 — RESPOND

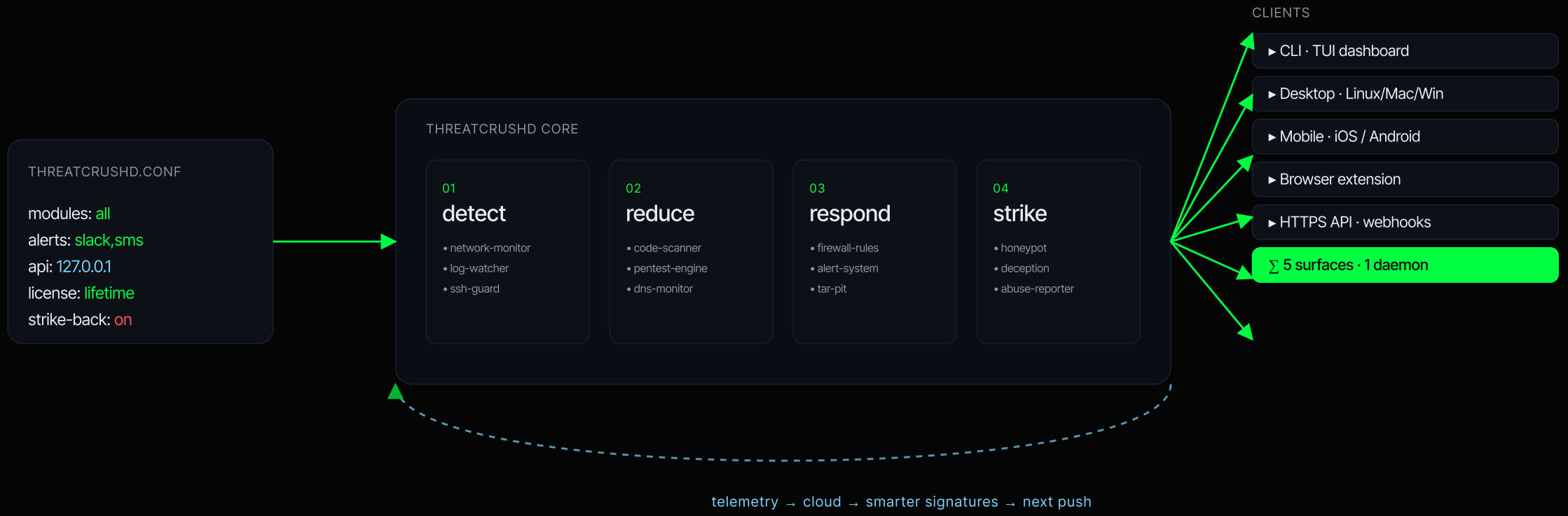
Slack · webhook · auto-ban · honeypot · tar-pit.

04 — STRIKE BACK

Deception, abuse reports, attacker-cost economics.

// ARCHITECTURE

One daemon. Pluggable modules.



// COVERAGE

12 core modules. 5 clients. One license unlocks all.

12
CORE MODULES

DETECT	REDUCE	RESPOND · STRIKE	CLIENTS · CHANNELS
network-monitor	code-scanner	alert-system	CLI
log-watcher	secrets-scanner	tar-pit	TUI dashboard
ssh-guard	pentest-engine	honeypot	Desktop app
dns-monitor	dependency-cves	deception	Mobile · iOS / Android
firewall-rules	compliance-reporter	abuse-reporter	Browser extension
k8s-watcher	cloud-audit	rate-limiter	HTTPS API · webhooks
docker-monitor	wordpress-scanner	geo-blocker	Slack · Discord · email · SMS

shipping beta roadmap Q3

// OUR WEDGE

One curl, zero dashboards.

`curl -fsSL threatcrush.com/install.sh | sh` drops a full SOC on a Linux box in under 60 seconds — daemon, modules, alerts, dashboard. Indie-friendly. Enterprise-ready.

MINUTE 0
curl install
$ threatcrush init

→

MINUTE 1
Daemon live
systemd · all ports · all sigs

→

HOUR 1
First attack caught
SSH brute force · auto-ban · alert

→

DAY 7
Replaces the stack.
cancels Snyk, Datadog, CrowdStrike trials

// we ran this on ourselves — every threatcrush.com server runs threatcrush.

// BUSINESS MODEL

Lifetime license. Open-core forever.

OPEN-CORE

$0

MIT license · top-of-funnel · trust w/ ops devs

- → daemon + core modules
- → self-host forever
- → upgrade path to lifetime

LIFETIME · INDIE + SMB

$499 / once

$399 with referral · pay once · all updates

- → all core modules + future
- → priority support
- → private module store

ENTERPRISE · GOV

$$$

contract · air-gap · FedRAMP · ITAR · GSA

- → on-prem appliances
- → FIPS 140-2 build
- → custom modules · SLAs

RECURRING REVENUE

AI-enhanced modules are usage-metered — anomaly detection, classification, smart alerting. Module marketplace pays a 70/30 split to authors.

EXPANSION

Per-host metering, team plans, gov / defense contracts — no per-seat tax that punishes growth, no per-event fee that punishes visibility.

// WHY WE WIN

Why the moat compounds.

Open-core distribution. Every install on a public server is a passive telemetry node — signatures sharpen as the deployed base grows. Closed competitors can't replicate this without buying it.

Standards-native.MITRE ATT&CK, D3FEND, Sigma, OCSF, NIST CSF speak directly into the same SOC pipelines incumbents already buy. We integrate where they refuse to.

Modules marketplace. Anyone can ship a paid module — WordPress scanners, K8s admission, cloud-audit, compliance reports. We collect 30% on every sale and own the standard interface.

Linux-first. 28M public Linux servers, no Windows EDR vendor really wants them. We do. As the default agent on indie+SMB Linux fleets, we earn the right to expand into containers, k8s, and cloud.

// ROADMAP

The next 12 months.

Phase 1	**MVP — shipping.** CLI + daemon, log-watcher, ssh-guard, alert system, systemd, waitlist + referral live at threatcrush.com.
Phase 2	**Beta — Q3 2026.** network-monitor (pcap), code-scanner, pentest-engine, module store + publish, license activation. First 100 paying lifetime customers.
Phase 3	**Launch — Q4 2026.** dns-monitor, firewall-rules, dashboard web UI, cloud sync, AI-enhanced modules generally available.
Phase 4	**Enterprise + gov — 2027.** air-gap appliances, FedRAMP, FIPS 140-2, GSA Schedule pricing — the security stack the SLED + DoD market keeps asking for.

// THE ASK

Raising $100k seed.

Live crowd-fund at threatcrush.com/investors — credit card or crypto via CoinPay. 12 months of runway to lock the default detection agent on Linux before incumbents notice.

USE OF FUNDS

55%	Engineering — module SDK, pcap stack, pentest engine, dashboard
20%	AI R&D — anomaly detection, smart alerting, threat classification
15%	Compliance — FedRAMP / FIPS / SOC2 prep, security audits
10%	GTM — devrel, content, launch, community modules program

TRACTION · IN-FLIGHT

Live
CROWD-FUND @ THREATCRUSH.COM/INVESTORS

Open
WAITLIST + REFERRAL PROGRAM

12
CORE MODULES SCAFFOLDED

MIT
CORE OPEN AT PROFULLSTACK/THREATCRUSH

```
$ threatcrush metrics — live
— CC + crypto rails open · backers live · we will not fabricate numbers.
```

invest@threatcrush.com →

// PROFULLSTACK, INC. · 2026

Crush every threat before it crushes you.

CONTACT	SOURCE	BACK US	TRY IT
invest@threatcrush.com	github.com/profullstack/threatcrush	threatcrush.com/investors	$ curl threatcrush.com/install.sh | sh