CRYPTOITDATA

Sentinel

Autonomous security agent for Linux servers exposed to the internet. It detects, decides and alerts in under two minutes — and can stop the attack on its own.

THE PROBLEM

A server exposed to the internet is scanned continuously. Attacks are no longer run by people who get tired: they are automated, they start the minute a public vulnerability appears, and they ignore your working hours.

Small companies have nobody watching. Large products assume a person who reads alerts — and deliver thousands a month. The difference between „we were attacked" and „we had an outage" is how fast somebody decides, not how much data was collected.

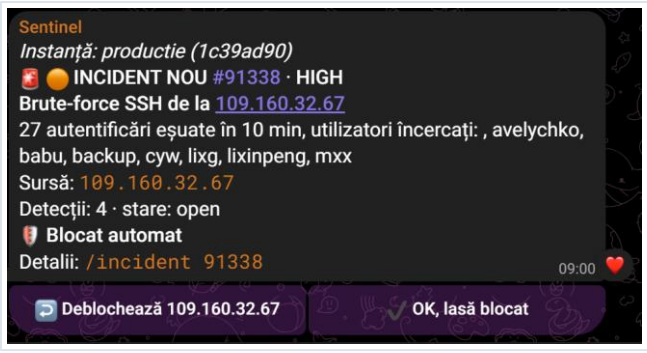
THE SOLUTION

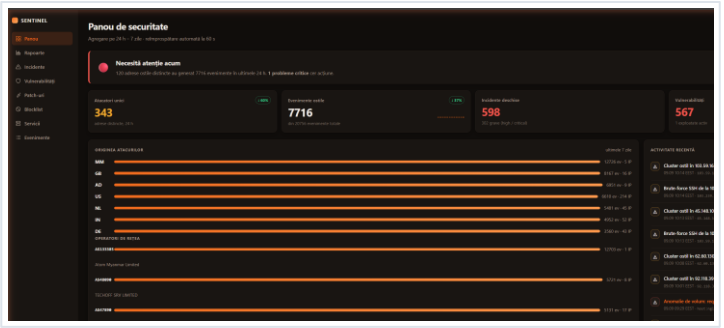
Sentinel runs on your server and closes the loop by itself: it collects, detects with deterministic rules, correlates hundreds of detections into one incident, asks the model for a verdict in plain language, notifies you on Telegram and can block the source — with an expiry and an allowlist.

HOW IT WORKS, STEP BY STEP

01 **Collection** journald (sshd, sudo, auditd), nginx, Suricata IDS, nftables. On the host, no external agent.
02 **Detection** deterministic rules, with thresholds calibrated on your own traffic. No model decides here.
03 **Correlation** detections from the same source become one incident, and related incidents become a campaign.
04 **AI triage** the model reads the incident once it is formed and writes the verdict and the procedure.
05 **Notification** Telegram, with the action buttons inside the message. Measured median: 105 seconds.
06 **Response** nftables block, with expiry and allowlist. The first 72 hours run in «observe» mode.
07 **Vulnerabilities** inventory, then an SSVC traffic light from CISA, EPSS and KEV data — not a score that gives 80 to everything.
08 **Patching** the plan is drafted by the model, checked by us, and never runs without your signature.
09 **Self-check** 79 checks every 5 minutes, because a security product fails in silence.
10 **External witness** a machine outside confirms the server is alive; if it goes quiet, the witness calls.

REAL SCREENSHOTS





Left: the alert on the phone, buttons in the message. Right: the dashboard on your machine — incidents, sources, history.

Figures and pricing

Everything below is measured on our own production server, over the last 30 days. Nothing is estimated.

WHAT MAKES IT DIFFERENT

It decides on the server

Your logs go nowhere. The analysis happens where the events are produced.

The rule decides, the model explains

No model output reaches the firewall, the shell or the package manager.

It checks itself

79 checks look for exactly how a security product dies: quietly.

It has an outside witness

An agent that dies cannot report that it died.

WHAT IT DID, IN 30 DAYS

334,752
events collected
11,158 per day

53,642
detections after rules
auth 31,473 · network 12,241

1,741
incidents after correlation
only 6 critical

100 %
with automatic action
1,741 of 1,741

105 s
from incident to phone
median

1,047
addresses blocked right now
with expiry and allowlist

7,278
vulnerabilities resolved
of 9,215 found

$2.76
cost of the AI layer
over 30 days, per server

The figure that matters most: **every incident, in every month, got an automatic action.** We are not selling „see alerts faster" — we are selling „you do not need somebody to watch".

PRICING

Launch offer: all prices halved, until 31 December 2026.

Setup

−50% €1,000

excl. VAT · one-off, per server
in Romania: €900 excl. VAT

Assessment, installation on your stack, 72-hour calibration, handover with documentation.

Managed

−50% €109

excl. VAT · per month, per server
in Romania: €88 excl. VAT

Everything in Setup, plus: we review incidents monthly, patch plans, monthly report.

Fleet

on request

project-based

Several servers or clients: per-machine configuration, own thresholds, negotiated SLA.

Volume discounts −10 % from 3 servers, −20 % from 6, −30 % from 11. **Annual payment** −8 %. Setup is included from 3 servers. Minimum 24-month term. The launch price stays locked for the whole term; from 1 January 2027 the list price applies.

— Not an antivirus and it does not cover Windows workstations. It monitors Linux servers: AlmaLinux 9, Ubuntu 22.04 and 24.04.
— It does not collect logs from inside containers — host and network events are visible.