Edge Defender — A Recurring-Revenue Opportunity in Payment-Device Compliance

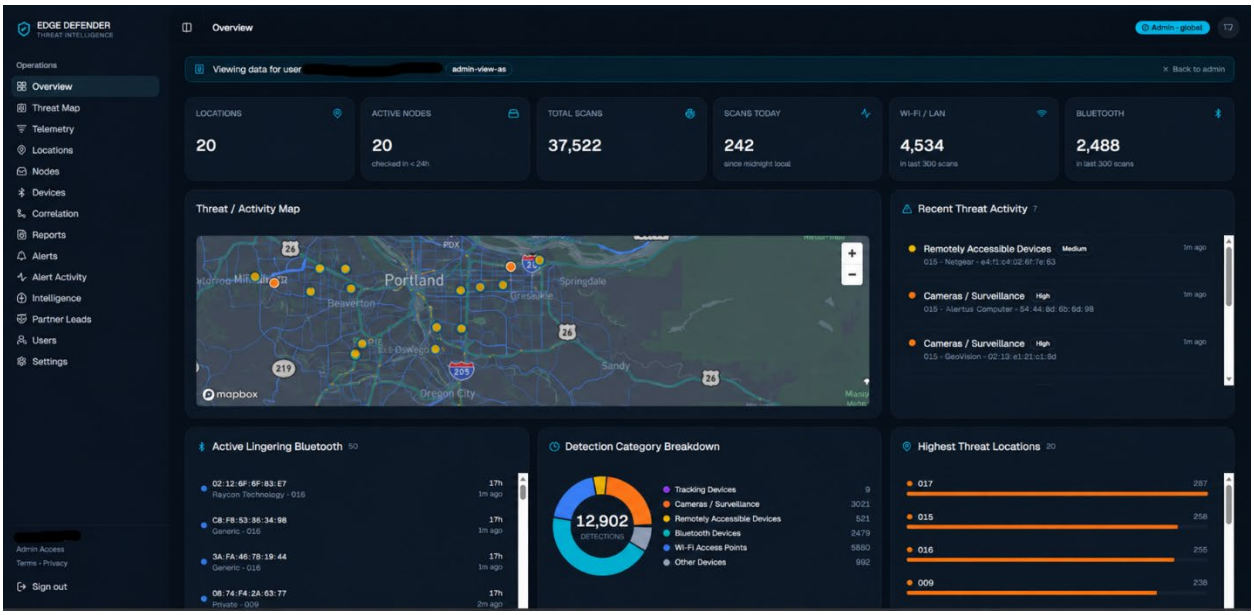
Here's the short version of what Edge Defender is, where it fits with PCI, why the timing matters, and how a distribution partnership would work.

What it is



Edge Defender is a small monitoring device you install at a site. It continuously watches the wireless airspace and network *around every payment device in range* — ATMs, fuel pumps, registers, countertop card readers, kiosks. The operator decides in the dashboard what they want to be told about and how — **an instant notification the moment something is detected, or a once-a-day summary** — and alerts go to whoever they designate. They review and act as they see fit. One box per location, one central dashboard.

Dashboard



What it does

- **Surfaces unexpected wireless devices** operating at ATMs, Gas Pumps, and POS terminals — flagging ones that are unknown, unauthorized, or match the profile of the Bluetooth modules commonly associated with skimming hardware.
- **Flags wireless devices consistent with covert cameras** near a keypad or in sensitive areas.
- **Detects rogue or unauthorized wireless and network devices** anywhere in the payment environment — not just at one machine.
- **Tunable focus** — a proximity setting and quiet-hours/risk thresholds the operator controls, so alerts stay on what matters, and a built-in **AI assistant** gives a plain-language read on any flagged device.

Because it runs continuously, it can surface suspicious activity *between* the periodic physical inspections — which is when most skimmer activity actually happens.

Where it fits with PCI DSS

Edge Defender is a detection-and-monitoring service. It doesn't make anyone "PCI certified" — no single product does. What it provides is continuous coverage and a **dated audit trail** supporting controls that are otherwise manual and periodic, across all site's card-handling devices:

- **Requirement 9.5 (protecting payment devices from tampering and substitution).** Applies to every point-of-interaction device — pumps, terminals, ATMs, kiosks — and requires periodic physical inspection for skimmers and tampering. Edge Defender adds a continuous *electronic* monitoring layer alongside those inspections, with early warning of suspicious wireless activity between them.
- **Requirement 11.2 (detecting unauthorized wireless access points).** PCI requires scanning for rogue wireless across the environment at least every three months. Edge Defender monitors *continuously* and logs it — so you're not only clearing the quarterly bar, you have standing evidence for the assessor.

In short: it adds continuous visibility and documentation to controls the operator already has to have — site-wide or across all sites. It also correlates threats or trackers appearing at multiple locations.

Why now

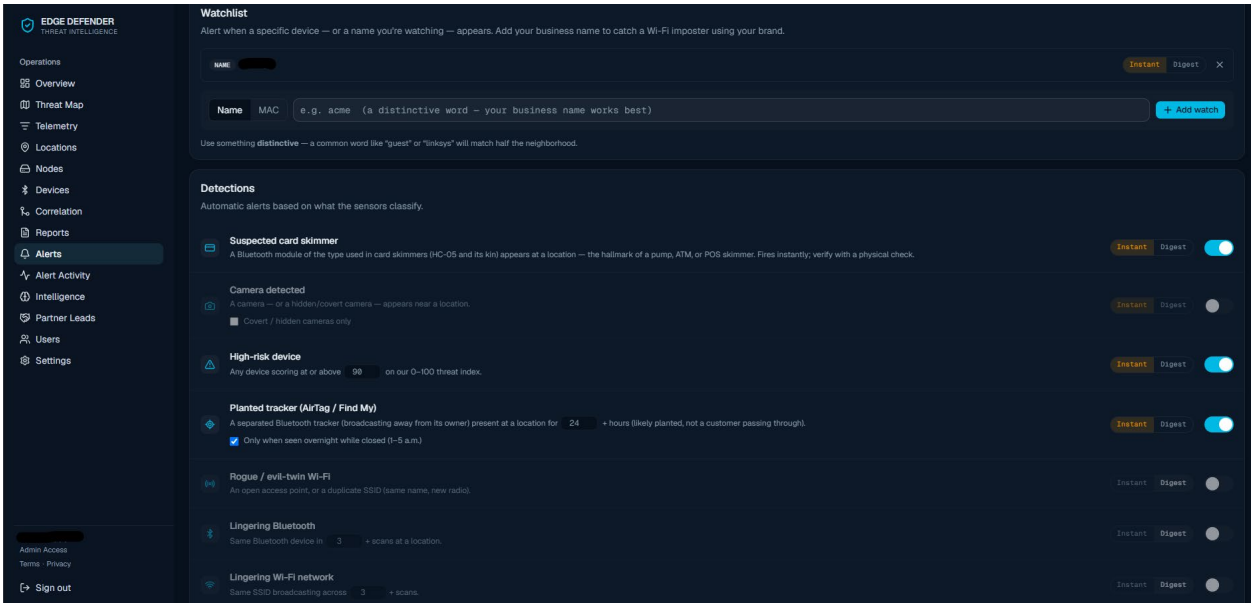
PCI DSS v4.0.1 is now fully in force and many operators are getting ahead of the expectation toward continuous monitoring rather than occasional checks. Meanwhile skimming has shifted to Bluetooth and future deep-insert devices that defeat a glance-and-go inspection, and fuel pumps and unattended terminals remain prime targets. The operators often carry the fraud liability and the brand damage. A continuous, documented, whole-site layer is exactly what the moment calls for — and almost nobody is offering it as a managed service yet.

The partnership

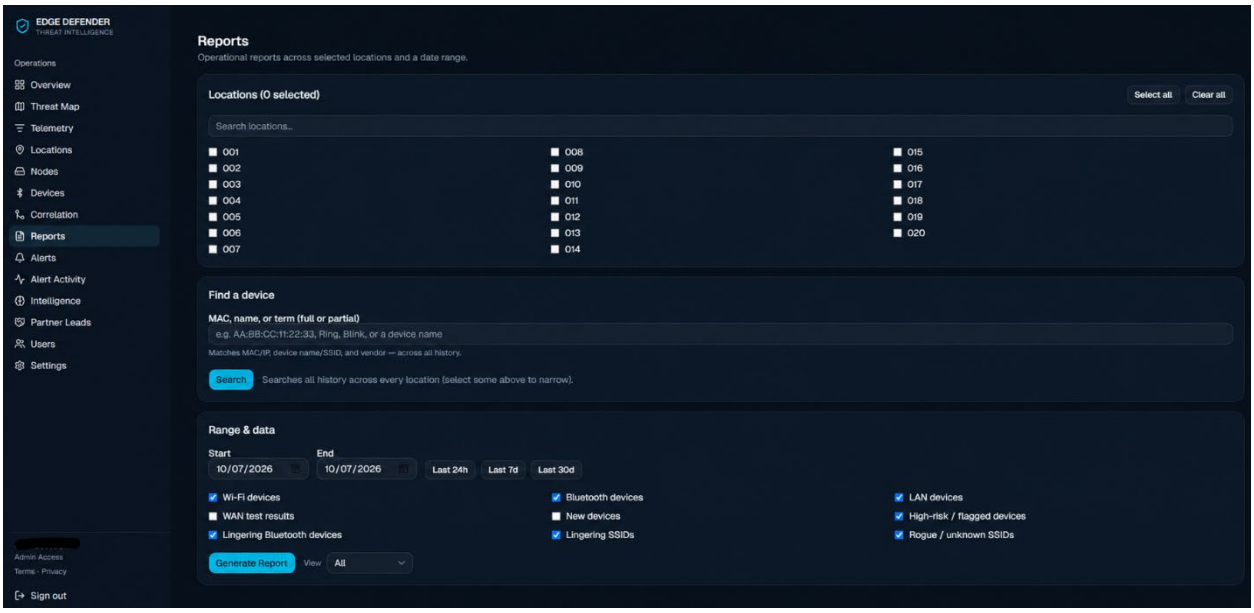
This is a natural recurring-revenue line — the same monitored-subscription model as alarm monitoring — and it isn't limited to ATMs. Your market is every site with card-present payments: gas stations, c-stores, retail, gaming, hospitality:

- **It runs itself.** Detection and alerting are automated — nobody has to sit and watch a screen. The operator sets their alerts once and the system notifies them; you don't staff a monitoring desk to deliver the service.
- You buy at **wholesale** and set your own retail / monthly price — **you keep the margin and the recurring revenue. Billing can be generated by us or you.**
- One device covers multiple machines and lanes, so the value per site is high and the install/maintenance rides on calls you're already making.
- Revenue scales with every site, and it's sticky once it's in.
- Co-branding is available if you want it under your own name.

Alerts Panel



Full Reports Engine



Next step: a short call and a live demo so you can see the dashboard and the alerts in action.

Randy Andrews
503.260.9077
Edgedefenderai.com

Edge Defender PCI Compliance and Introduction 2026