Game-Changer Watch — 2026-09-13

⍰ GAME-CHANGER: The single sentence the Outbound Wing white paper was built on — *"HoneyBook does not publish an open API"* — was already false when it was written. HoneyBook shipped an open MCP interface on Aug 19, agents can create and update projects, client records, proposals, invoices and contracts, it is live in ChatGPT as of Sept 9, and HoneyBook's own launch post says a venue-marketing agency has already used it to extend its service into the booking process.

Four net-new findings. Verified net-new by grep against the Opportunity Register before this run: MCP connector = **0**, Small Business Collection = **0**, Cysurance = **0**, SCOUTz = **0**, Magento = **0**, Adobe Commerce = **0**, 75650 = **0**. (HoneyBook returns 2 hits — both incidental, neither about an API.)

⚠ **Method note, and it is the second week running that the same failure shape has cost this board an item.** The 09-12 daily correctly diagnosed that the prior two dailies chased vendors and missed the primitive underneath. Today's finding is the mirror image: the board has been tracking *competitors'* platform moves closely while a **platform move by a system EdgePointe already integrates with, and already wrote a client-facing document about,** went unread for 25 days. The Aug 19 post is on HoneyBook's own blog under the tag "Product update." Nothing hid it. **The named-source list needs a fourth lane: the vendors already inside our own architecture diagrams.** A competitor's release changes what we sell. A partner's release changes what we have already promised.

---

1. ⍰ HoneyBook opened as a platform — and the Outbound Wing white paper's central architectural finding is now indefensible as written

What it is

HoneyBook announced the **HoneyBook MCP** on **August 19, 2026** — quoting their post verbatim where it matters:

- *"an **open interface** that lets AI agents work with a member's HoneyBook account, reading their pipeline, projects, invoices, contracts and client messages and, with the member's permission, **acting on them**."*
- *"an agent can **create and update projects and client records**, attach notes and context where they belong, **build a proposal, invoice or contract from the company's own templates, publish it for a client to open, and raise a standalone payment request**."*
- *"**any MCP-compatible client can connect**"* — Claude is where it is listed and verified, *"not the only one."*

- *"the same interface that lets an assistant work in a member's account lets **developers, agencies and technically-minded members build their own tools on HoneyBook**: a custom dashboard, an internal workflow, an automation that spans HoneyBook and the rest of a business's stack."*
- And the sentence that should be read twice: *"**One venue-marketing agency working with HoneyBook members has already used it to extend its own service into the booking process.** This is the first step in opening HoneyBook up as a platform."*

Permissioning is explicit and per-resource; requests run in an isolated environment destroyed at the end of the request; network access is restricted to HoneyBook and member credentials are never exposed to the model.

Three weeks later, **HoneyBook launched inside ChatGPT on September 9** as one of **16 tools in OpenAI's new Small Business Collection** (alongside Canva, Stripe, Gusto, Slack, Dropbox, ClickUp and **Wix**). The same release discloses adoption: **hundreds of businesses connected and 20,000+ actions in the first two weeks**, the most common use being reconciliation — delivered-but-unbilled work, stale leads, mislabeled client records.

Adjacent and in the same arc: **HoneyBook Business Phone & SMS** shipped Aug 31.

Why it matters to EdgePointe

Because we wrote the opposite down, gave it to a client, and built an architecture on it.

Vantage-Outbound-Wing-WhitePaper-2026-09-01.md § *"THE FINDING THAT RESHAPED THE WORK"* states:

> *"HoneyBook does not publish an open API or inbound webhook system. Its documented integration paths are its own embeddable contact and lead forms, or a middleware hop through Zapier."*

and in the executive summary:

> *"HoneyBook, the CRM the client's team runs on, publishes no open API."*

BUILD-PLAN-OUTBOUND-WING-2026-09-01.md carries it into the risk table as a settled premise: *"HoneyBook remains API-less | Nothing changes | Already the design assumption."*

The white paper is dated September 1. The MCP shipped August 19. The finding that "reshaped the work" was thirteen days stale on the day it was published.

Three separate consequences, and they are not the same size:

1. **Credibility — the immediate one.** This document went to Isaac. Isaac runs venues on HoneyBook. HoneyBook's own launch post names **venues** as one of the seven early-access categories and says a **venue-marketing agency** has already built on it. If Isaac, or anyone advising him, searches "HoneyBook API" this month, the first thing they find

contradicts the paragraph we called our key finding. **This is a correction to make before it is discovered, not after.**

2. **Architecture — the real but smaller one. ⚠ Do not over-read the reversal.** MCP is an agent-facing, member-authorized interface. It is *not* a server-to-server REST API with inbound webhooks, and it does **not** obviously give a Cloudflare Worker an unattended write path into a tenant's HoneyBook on lead capture. **The generic outbound webhook + Zapier design may well still be the right build.** What has changed is that it is now a *choice between two viable paths*, not the only path that exists — and the second path is the one that removes the Zapier dependency and the 15-minute cron latency the demo had to apologise for. That deserves a half-hour of reading the connector setup docs, not a rebuild.

3. **Strategy — the one that compounds.** HoneyBook now holds the venue's client lifecycle *and* an agent interface onto it *and* phone/SMS *and* a slot inside ChatGPT. That is the same absorption pattern the 09-10 and 09-11 dailies logged for SkySwitch (#98) and Intermedia (#102), arriving from the CRM side instead of the telephony side. **Third vendor in twelve days to absorb a piece of the Vantage bundle.** And the answer is the same one the board has now written nine weeks running: the half nobody can absorb is **#10** — an AI layer trained on a venue's own leads, calls and tours. HoneyBook can read the venue's pipeline. It cannot read the venue's *website* traffic, its call recordings, its tour outcomes, or tie any of it to ad spend.

How we'd apply it

---

a

b

c

d

2. ⍰ Emergency WAF release — actively exploited unauthenticated RCE in Adobe Commerce / Magento (Sept 10)

Cloudflare shipped an **emergency WAF release on Sept 10** for **CVE-2026-75650 ("StyleSmuggler")** — unauthenticated remote code execution in Adobe Commerce and Magento Open Source storefronts, *"caused by improper neutralization of special elements in*

the platform's template engine," letting attackers *"inject arbitrary PHP payloads through style properties to execute system commands and deploy persistent malware."* New rule …440f5c55, action **Block**.

Cloudflare's own guidance goes further than patching: apply Adobe's hotfix APSB26-146 **and immediately rotate all potentially exposed encryption keys, integration tokens and system credentials, as patching alone does not remediate an existing compromise.**

Why it matters: structurally identical to **#76** (Next.js RCE), which this board correctly ranked act-now. **Vantage platform exposure is NIL — we run no Magento.** The exposure, if any, is a client storefront. **Run the inventory, record the zero.** Edge mitigation buys time; it is not immunity, and if a client *is* on Magento the credential-rotation instruction makes this a billable incident-response engagement, not a patch ticket. → **#107**, routes to Managed IT / edge-pointe-cybersecurity.

⚠ Also note, unchanged from the 09-12 daily: the **scheduled WAF release lands Sept 15** (SSRF-Cloud-3, Command Injection Generic 10, Version Control Information Disclosure — all Log). Same day as **#32**, which is now **2 DAYS OUT AND STILL NEVER RUN — sixth consecutive stack.**

---

3. ▯ Cysurance names ESET preferred MDR vendor — security-plus-warranty is now bundled one tier above us

ESET announced (wire, Sept 3; ChannelPro roundup, Sept 11) that ESET PROTECT MDR and MDR Ultimate buyers automatically receive a **cyber warranty of $500,000 or $1M by tier**, plus **same-day cyber insurance without underwriting at a reported 60–80% off standard market premiums.**

Why it matters: EdgePointe's compliance and cyber-insurance motion (**#48**, edge-pointe-compliance) currently assembles MDR and insurance attach as separate conversations. A vendor bundling a warranty into the MDR SKU changes what "included" means in a security proposal, and a prospect who has seen this will ask what *our* stack warrants. ⚠ **The 60–80% discount figure is vendor-supplied — do not repeat it to a client as a market fact.** Action is a positioning paragraph, not a stack change. → **#108**.

---

4. ▯ SCOUTz out of stealth — the manual security-audit pitch is now a product in open beta

SCOUTz launched Sept 10 — security sales intelligence for MSPs, **30-day open beta**, from RYTHMz founder Steve Copeland; closed beta ran with 50 MSPs. It runs **156 check types** against a prospect's external footprint plus public growth signals (new locations, IT hiring), and — after read-only consent — reviews a prospect's **Microsoft 365 tenant agentless** across identity, apps, consent, security and managed devices.

Why it matters: that is precisely the job of EdgePointe's hand-built Security Audit tool and the pre-first-meeting evidence pack. Not a threat — **a benchmark and possibly a shortcut.** The honest question for the weekly: does our audit produce anything a prospect would notice that 156 automated checks plus an M365 read do not? If the answer is "the interpretation and the roadmap," say so and stop investing in the *collection* half. **Free 30-day beta makes this cheap to answer empirically.** → **#109**.

Quiet scan log — sources checked BY NAME, with the URL read

Lane
Anthropic
Cloudflare
Cloudflare — voice
Major labs
Website builders
MSP channel
AI voice / receptionist
Venue software

Act-now stack after today

Unchanged at the top. One insertion at position 2.

0
1
2
3
4
5

#10 is unbuilt for the tenth consecutive week. Today is the third straight daily whose finding ends at the same sentence: every layer of the bundle is being commoditised by a

vendor except the one trained on the venue's own data. That is either the moat or it is nothing, and it has now been "the moat" for seventy days without a line of code.

Sources are linked inline. Vendor-reported figures — the 97% venue-booking statistic, the 60–80% insurance discount, SCOUTz's 156 checks — are flagged as such at the point of use and should not be repeated to a client as independent findings.