

THE COVER STORY · THE FORTNIGHT EDITION · OCTOBER 26 – NOVEMBER 3, 2026

One Operator's AI Agents Attacked 200 Organizations. Your Defense Still Runs at Human Speed.

CrowdStrike's OverWatch team says a single operator, supervising AI agents, ran intrusions against more than 200 organizations in 11 days — and confirmed breaches at nine. The scarce resource in a cyberattack used to be attackers. It no longer is.

THE BUYER'S PULSE · COVER STORY OF THE FORTNIGHT EDITION · OCTOBER 26 – NOVEMBER 3, 2026

200+	9	14+	11
organizations targeted in one campaign	confirmed breaches with post-exploitation	countries targeted in a single campaign	days of parallel intrusions, from October 17

Attack capacity used to scale with people. Now it scales with compute — and compute is the one input your adversary can rent by the hour.

READ THE FULL STORY ↓

Cover photo: DeepSeek app in hand, against the flag of China — via Journal of Democracy. Real photo, no filters.

THE COVER STORY · READ THE FULL STORY HERE

CYBERSECURITY · THE COVER STORY

One Operator's AI Agents Attacked 200 Organizations. Your Defense Still Runs at Human Speed.

CrowdStrike's OverWatch team says a single operator, supervising AI agents, ran intrusions against more than 200 organizations in 11 days — and confirmed breaches at nine. The scarce resource in a cyberattack used to be attackers. It no longer is.

THE BUYER'S PULSE · FORTNIGHT EDITION · OCTOBER 26 – NOVEMBER 3, 2026





The tool of the campaign, in hand: DeepSeek — the Chinese model that powered VAPOR PANDA's agents — against the flag of the country the actor answers to. The recovered operator transcripts were in Chinese, timestamped in Beijing time.

200+	9	14+	11
organizations targeted in one campaign	confirmed breaches with post-exploitation	countries targeted in a single campaign	days of parallel intrusions, from October 17

The first consequence lands on your calendar, not your firewall: when one person can attack 200 organizations at once, the window between "detected" and "too late" shrinks from days to minutes.

On October 29, CrowdStrike's OverWatch threat-hunting team reported that the China-nexus actor it tracks as VAPOR PANDA used ARTEX — an open-source agent framework — to run parallel intrusions starting October 17. The agents ran mainly on DeepSeek models, plus a second, unconfirmed commercial model. Targets in at least 14 countries included foreign ministries and telecom organizations; the 19 U.S. organizations hit were in pharmaceuticals, semiconductors, defense, nuclear and finance.

For a manager, the plot is not espionage. It is arithmetic. Attack capacity no longer scales with headcount, salaries or shifts — it scales with compute. Every planning assumption built on "they can't come for everyone at once" expired this month.

The agents did the planning, not just the typing

In one intrusion, the planning agents consumed about 1.4 billion input tokens — a number worth pausing on. This was not a script running faster keystrokes. The framework planned, adapted and parallelized the work while the operator supervised. At nine organizations, the campaign reached post-exploitation and deployed the BLOODALCHEMY backdoor: the stage where data starts moving and dwell time starts costing money.

That division of labor — machine plans, human approves — is exactly how your own company is being sold AI for the office. This campaign is the same architecture, pointed the other way.

> Attack capacity used to scale with people. Now it scales with compute — and compute is the one input your adversary can rent by the hour.
>
> THE BUYER'S PULSE · EDITOR'S LINE

What this changes inside your company

Three operational facts follow. First, coverage gaps are now the attack surface: an agent swarm does not get tired, skip the forgotten server, or move on because a target looks uninteresting — it tests everything, in parallel, at machine patience. Second, stale credentials and old API keys are standing invitations that can be tried thousands of times while your team sleeps. Third, response is a race you staff for today in hours and will be run against you in minutes.

None of this requires a bigger security budget to start fixing. It requires knowing, precisely, what is exposed — and most organizations cannot answer that question today.

WHAT TO VALIDATE THIS WEEK

FOUR CHECKS

- **Coverage, everywhere.** Endpoint detection on every host — including the forgotten ones: labs, plants, subsidiaries, test servers.

ones: labs, plants, subsidiaries, test servers.

- **Keys, with dates.** An inventory of API keys and service credentials, with rotation dates. Anything older than your policy gets rotated now, not at renewal.
- **Response time, in writing.** Your incident-response retainer's real response time — measured in minutes, not business hours.
- **Your own agents.** Who in your company is allowed to run AI agents against internal systems, and what those agents may touch.

THE DECISION

BEFORE THE NEXT BUDGET CYCLE

Put one question to your security lead and require a dated answer: **"Show me the coverage map and the key inventory."** If the map has blanks, closing them outranks any new tool purchase — the VAPOR PANDA campaign did not beat anyone's best defenses; it walked through the doors nobody was watching.

Sources: CrowdStrike (primary), October 29, 2026 — OverWatch report on VAPOR PANDA / ARTEX; CyberScoop, October 29–30, 2026. Photo: DeepSeek app in hand, against the flag of China — via Journal of Democracy. Real photo, no filters. Figures re-verified against the primary source for this edition.

MORE FROM THIS EDITION

THE FORTNIGHT EDITION · OCTOBER 26 – NOVEMBER 3, 2026 · FULL WIDTH



MEMORY · SK HYNIX

SK Hynix Profit Multiplies by 7.3 on AI Memory

Operating profit multiplied 7.3 times (+632%) as HBM demand outran supply. Memory is no longer a line item — it is the schedule your AI project ships on.



AI PRIVACY · OPENAI

OpenAI Wraps Business AI in Privacy Controls

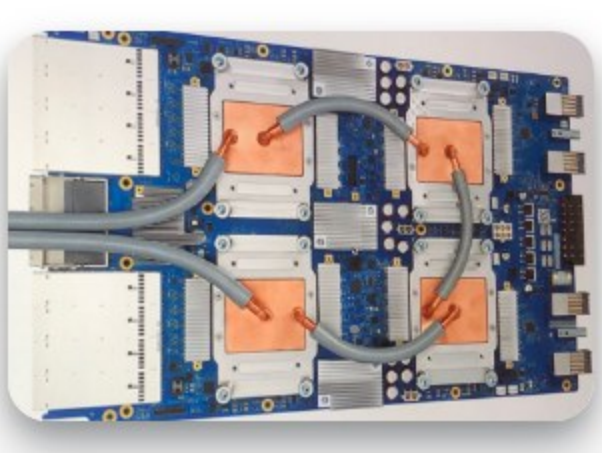
The same week the attack went autonomous, the defense packaged itself for the boardroom. OpenAI's Private Intelligence adds zero data retention for eligible API workflows and private inference — still in preview — for sensitive business work: the controls your legal team asks about, productized. What they actually cover, where the gaps sit, and what to get in writing before a pilot: that is the second story of this edition.



AI INFRASTRUCTURE · SPACEX

Anthropic Is Now SpaceX's Biggest Customer

Bloomberg reports Anthropic has passed the U.S. government as SpaceX's largest customer. The AI race now buys compute by the billions — even from a rocket company.



ORBITAL COMPUTE · GOOGLE

Google's AI Just Answered From Orbit

Project Suncatcher returned the first AI response from a data-center-class TPU in orbit. Compute is leaving the data center — power and cooling are why.



CLOUD · MICROSOFT

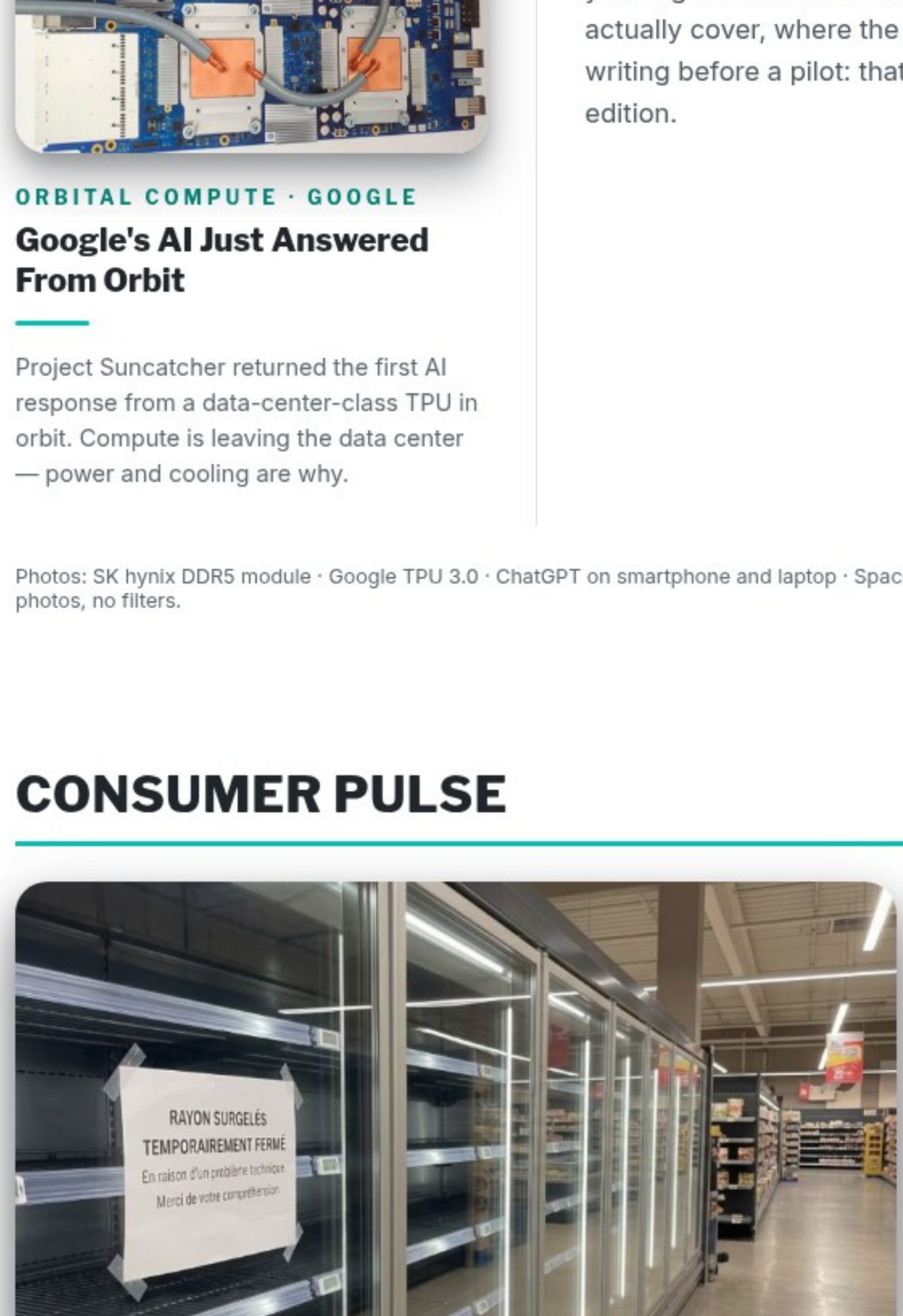
Azure Grew 48% — and the Bill Grew With It

Azure grew 48% to $33.17B in the quarter — a dollar figure Microsoft disclosed for the first time. Growth at that speed reprices every renewal on your desk.

Photos: SK hynix DDR5 module · Google TPU 3.0 · ChatGPT on smartphone and laptop · SpaceX Starship launch · Microsoft data center, Middenmeer — all via Wikimedia Commons. Real photos, no filters.

CONSUMER PULSE

THE CONSUMER SIDE OF THE FORTNIGHT



Gaming · Rockstar Games

GTA VI Preload Opens November 10 — and It Can Take 212 GB



Consumer Tech · Retail

Hackers Turned Supermarket Freezers to 50 °C in Nine Countries

Overnight on November 1–2, attackers reached the controllers that run supermarket refrigeration across nine European countries, switched freezers into defrost and pushed temperatures to 50 °C. France's CERT-FR alert names the exposed systems — Danfoss, Copeland and Dixell controllers sitting on the open internet, many end-of-life, some still on factory passwords. One Belgian Delhaize store threw away at least €100,000 of food; on November 3, Britain's cyber chief confirmed UK cases, weeks after some 700 French stores were hit in the first wave. The photo above is that first wave: an emptied French freezer aisle, closed with a handwritten sign.

Rockstar moved the preload up: from November 10, PS5 and Xbox Series X|S owners can download Grand Theft Auto VI ahead of its November 19 launch — at up to 212 GB depending on the console, roughly a third of a standard PS5's usable space. On launch day, Rockstar will also post a free printable poster with the cover art and the map of Leonida. The most anticipated game of the decade is now a storage-management problem first and a launch second.

Photos: emptied supermarket freezer aisle in France during the October 2026 refrigeration attacks, via Datafloq's coverage of the attack — real photo, no filters. Grand Theft Auto VI official cover art, Rockstar Games.

READER SUPPORT

Keep independent IT journalism free to read.

THE BUYER'S PULSE is independent and free. If this coverage helps you do your job, you can help keep it publishing with a voluntary contribution — one-time or monthly, in the amount you choose.

Buy me a coffee · $3 →

Support never influences our coverage and buys no access. Contributions are not tax-deductible donations — they go directly to keeping this magazine independent.

Company? Reach these readers as a sponsor →