INDUSTRY RESEARCH
&
WHY THIS MATTERS

The Internet Is No Longer Human

New industry research finds that for the first time in measurable history, more than half of the traffic on the open internet is no longer driven by people. We unpack what it means — and why it changes the question your feed is asking you.

DeepFake DEFENDER Editorial · Canberra, Australia · 6 May 2026

If you've been scrolling through your social feed lately and felt as though something was off — that the conversation feels less like people, that the replies feel templated, that the wonder has slowly drained out of the videos — there is now research that says the feeling is not in your head.

Imperva, the security research division of Thales, has published its 12th annual Bad Bot Report, and the headline finding is the kind of structural inflection point that gets buried in cybersecurity press releases but probably belongs on the front page of every newspaper. For the first time since the company began monitoring web traffic in 2013, machines now make up the majority of activity on the open internet.

More than 53% of all web traffic in 2025 was automated, up from 51% in 2024. Human activity has fallen to 47% — and according to the report's authors, it continues to fall.

53%	47%	27%
AUTOMATED TRAFFIC	HUMAN TRAFFIC	API ATTACKS
of all web traffic in 2025	*and continuing to decline*	*of bot attacks target APIs*

Source: Imperva 2026 Bad Bot Report (Tim Chang, 29 April 2026).

> *"This is not a short-term spike driven by a specific attack cycle or technology trend. It reflects a structural change in how the internet operates."*
>
> — TIM CHANG, IMPERVA

Why this matters for what you're scrolling

Imperva's report is framed for cybersecurity professionals. Its concerns are about API abuse, account takeover, financial-services fraud, and the difficulty of distinguishing legitimate AI-agent traffic from malicious automation. Those are real and important problems — but they are also a partial picture.

The same structural shift that creates Imperva's concerns also reshapes the consumer's everyday experience of the internet. If most of the activity on the platforms you use is no longer human, that is not just a security problem for the platforms. It is a sense-making problem for you.

Consider the asymmetry. The traffic you generate — opening apps, scrolling, tapping, watching — is human. The traffic you receive, increasingly, is not. The video that surfaces in your feed may have been generated by a model. The reply under your post may have been written by an agent. The account that follows you, the comment that praises a product, the news headline that matches your political priors a little too neatly — each of these now arrives with an open question attached. Was a person involved in producing this, and if so, what part?

This is the question DeepFake DEFENDER was built to answer in the moment of consumption, while you scroll, without breaking your flow. The Imperva research provides the macro context for why a tool like this is now necessary at the consumer level rather than only at the enterprise level.

The numbers behind the headline

Beyond the headline shift, the report identifies several specific patterns worth flagging.

AI agents are a new category of internet participant. The report describes them as systems that "don't just scan websites; they interact with them, retrieve data, execute workflows, and increasingly act on behalf of users." In practice, this means that what appears to be a customer interaction may not be a customer at all — and the line between legitimate AI-driven traffic and malicious automation is becoming difficult to draw.

Financial services bear the brunt. The sector accounts for 24% of all bot attacks and 46% of account-takeover incidents documented in the report. Attackers increasingly bypass the user-facing interface entirely and operate directly against APIs at machine speed.

The shift is structural, not episodic. The report explicitly frames the inflection as a permanent change in how the internet operates rather than a temporary spike. "Increasingly," Chang writes, "businesses are not serving customers alone. They are serving machines."

> *"Companies that continue to operate under the assumption that users are human risk misreading their own systems."*
>
> — TIM CHANG, IMPERVA

What this means for the rest of us

The Imperva report is written for people responsible for defending corporate infrastructure. But it points at something that affects every social-media user with a phone in their pocket. If automated traffic now exceeds human traffic at the infrastructure level, the content that infrastructure delivers is increasingly produced by, amplified by, and replied to by systems that are not human. Some of that automation is benign. Some is search-engine indexing and the kind of background agents that make modern services work. Some is not.

DeepFake DEFENDER does not solve the broader problem the Imperva report describes. No consumer tool can. What it does is operate at the only point in the chain where an individual person retains agency: the moment of consumption. When a video, post, image, or claim crosses the user's screen, the application surfaces an integrity signal in the corner — a probabilistic indicator, not a verdict — that gives the user a moment to ask whether what they are seeing belongs to the human side of that 47% or the other side.

That is not a technical claim. It is a quality-of-life one. The pattern is documented. It is not your imagination.

SOURCES & FURTHER READING

Tim Chang, *"Bad Bot Report 2026: The Internet Is No Longer Human and It's Changing How Business Works,"* Imperva (Thales), 29 April 2026.

Read the original article on imperva.com →

Download the full 2026 Bad Bot Report from Imperva →

E D I T O R ' S N O T E · *DeepFake DEFENDER summarises and contextualises industry research from third-party sources. All findings, statistics, and direct quotes in this article are attributed to the Imperva 2026 Bad Bot Report by Tim Chang. The editorial framing connecting these findings to consumer social-media experience is the work of the DeepFake DEFENDER editorial team and does not represent the views of Imperva or Thales. We encourage readers to consult the original report directly.*

D E E P F A K E D E F E N D E R
Eagle Corporation (Australasia) Pty Limited · ABN 67 089 764 358 · ASIC Key 1-74110561520
deepfakedefender.com.au