HUMAN

Trust under attack

How agencies detect and defeat malicious bots

Introduction

Bots aren't just supporting human activity online anymore. They're outpacing it. Bots move at machine speed, hide in plain sight, and slip past simple defenses without a trace. What started as a tool for simple automation has become a weaponized threat.

If you've ever tried to buy event tickets and lost out on the chance in a matter of seconds, you've seen how fast and effective bots can be. That same automation **flooded vaccine appointment portals during the pandemic**, blocking real patients and allowing scalpers to profit.

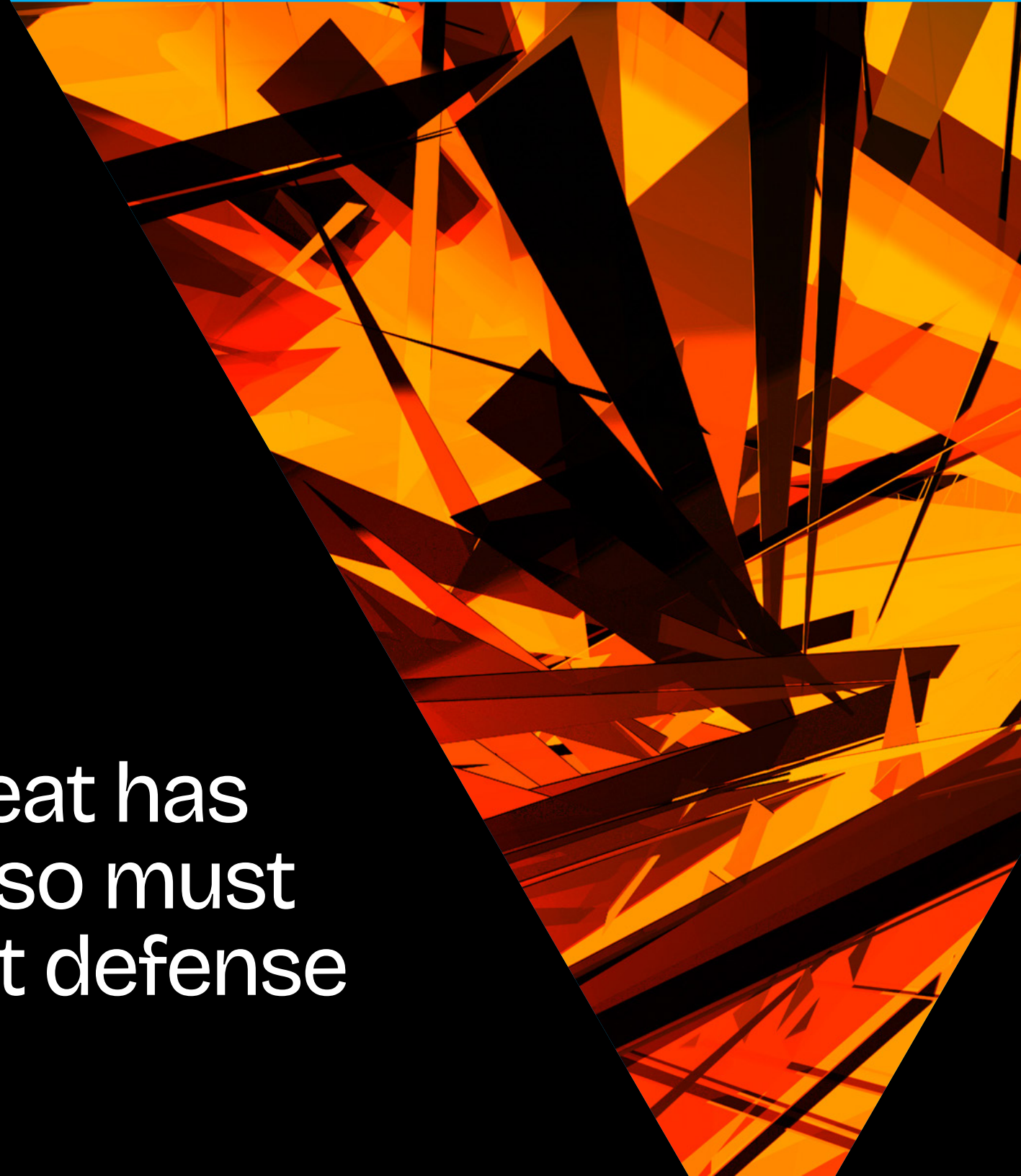
Now imagine that power turned on core government systems: infrastructure, services, and public trust.

Bots create both risk and efficiency. Artificial intelligence-powered automation can improve service delivery but also fuels credential stuffing, data theft and disinformation campaigns. That's why government defenses can't just be technically sound. They have to be transparent, compliant and built for accountability.

This eBook breaks down the full bot defense process: from fraud risk management to AI operations to real-time mitigation. It shows how agencies can combine detection tools, human oversight and clear communication to secure systems and earn trust.

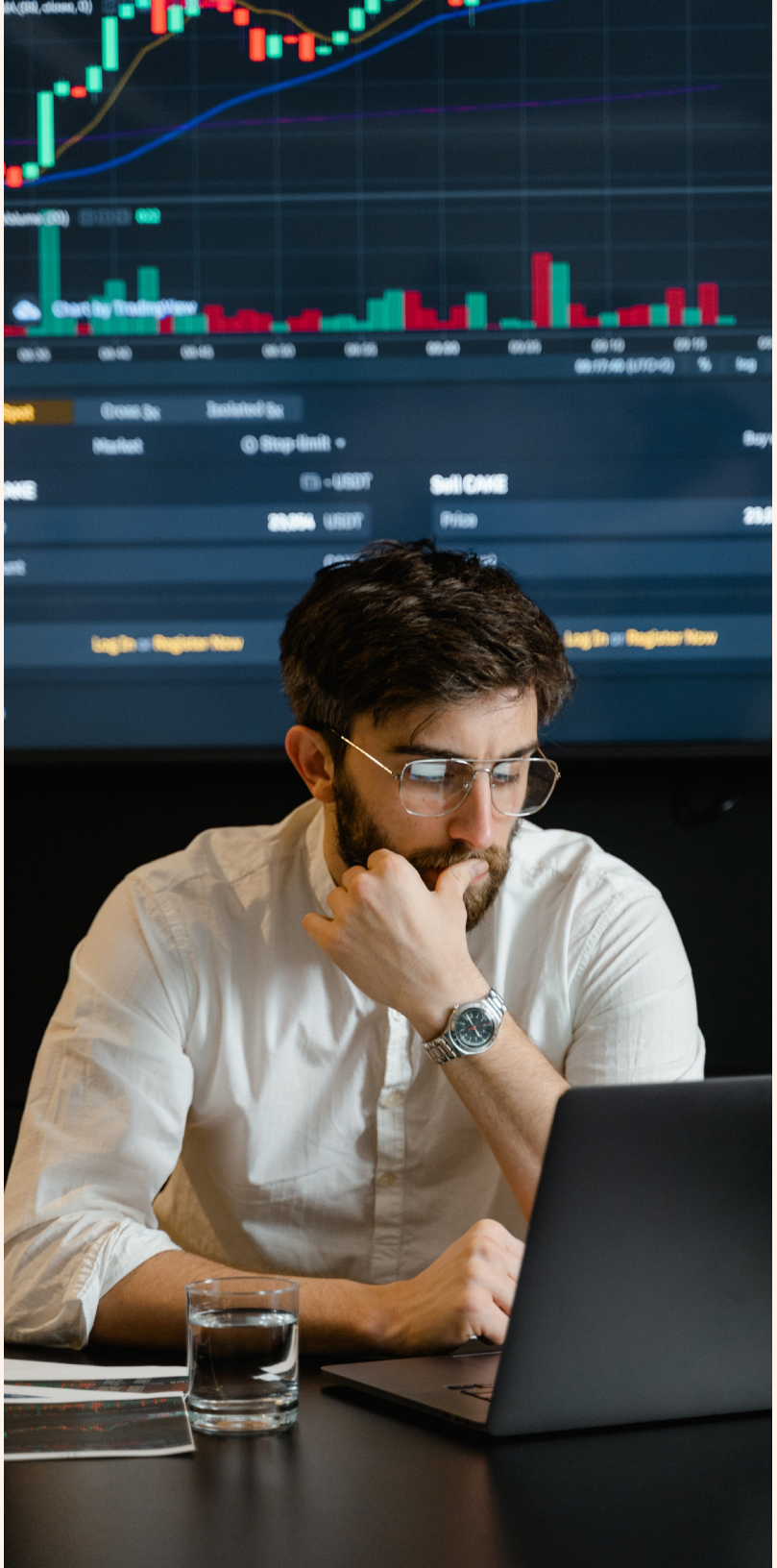
Table of Contents

HUMAN



01.

The bot threat has changed — so must government defense



ACCORDING TO THE QUADRILLION REPORT: 2025 Cyber Threat Benchmarks, the number of attempted account takeover (ATO) attacks **more than doubled** from 2023 to 2024. And the number of fake accounts created by bots rose by **360%** from one year to the next.

"Bots adapt in real time," said Joe Rogers, vice president of public sector at HUMAN Security, a cybersecurity provider that protects organizations by disrupting bot attacks, digital fraud, and abuse. "If your security model isn't bot-aware, it's already outdated."

Bots aren't new. But what's changed is that today, they're deployed by nation-states and hacking groups to take down systems, spread disinformation and mimic real users to bypass defenses.

These aren't simple scripts anymore. With agentic AI, bots can plan, evolve, and change tactics mid-attack. They don't just break in; they log in. That means traditional defenses like multifactor authentication and traffic filters can't keep up.

Public sector platforms, which manage taxpayer services, infrastructure, and national security systems, are high-value targets. Yet many agencies still rely on outdated tools and alerts that operate on 30-day-old threat definitions.

"Agencies are using basic platforms that they used in the past, and sometimes, they're using alerts that come out from CISA, but those things are dated," Rogers said. "Bots adapt in real time."

HUMAN sees this shift firsthand. The company analyzes signals from over 500 commercial sites, giving it real-time visibility into bot behavior. That insight helps distinguish humans from bots and respond before attacks escalate.

Zero trust frameworks weren't built with bots in mind. They were designed to verify humans. Bots now exploit that gap by hijacking sessions, using stolen credentials, exploiting device trust, and quietly moving through networks. That's the Zero Trust Bot Gap, and it leaves agencies exposed.

The March 2020 distributed denial-of-service attack on the Department of Health and Human Services is a prime example. While the agency was coordinating the national pandemic response, attackers targeted its digital infrastructure in an attempt to disrupt services and shake public confidence. The incident exposed cybersecurity weaknesses in a system built to serve the country during a crisis.

More recently, in late 2023, the U.S. government took down a Chinese state-sponsored botnet called Volt Typhoon. The group infected hundreds of routers across the country to hide its origin while targeting critical infrastructure. Known as KV Botnet, the malware was serious enough that the Justice Department stepped in to remove it and block future attacks. The operation showed just how far malicious bots can go when they aren't caught early.

To stay ahead, agencies need bot-aware defenses that evolve as fast as the threats. Legacy tools and static frameworks aren't enough, not when bots are already inside the perimeter.

The most expensive breaches cost agencies nearly $5 million, a 10% jump from the year before, highlighting just how costly these gaps in defense can be. ▼

HUMAN

02.

AI + automation ≠ protection without oversight

BOTS ARE EVOLVING WITH AI. Agencies are also turning to AI-driven automation to deliver services more efficiently. But like bots, automation plays a dual role. It brings speed and scale, but without proper oversight, it creates serious risk.

AI is now fueling cybercrime. Bots powered by AI steal identities and apply for government benefits at scale. Deepfake scams generate fake officials to authorize fraudulent activity. And in addition to impersonating humans, bots are now hunting for vulnerabilities.

Hybrid attacks are also becoming more common. In these cases, bots team up with human hackers, scanning for vulnerabilities, suggesting attack strategies, and even powering chatbots that impersonate officials. These bot-assisted intrusions are faster, smarter, and harder to detect.

One of the biggest threats, according to Rogers, is AI-powered reconnaissance. These bots scan networks for weak points faster than human defenders can react. Traditional cybersecurity tools aren't designed for this. They don't account for real-time adaptation, which means bots can slip through undetected while posing as legitimate users.

The issue isn't automation itself. It's unprotected automation. Agencies need to stop assuming AI-driven threats won't exploit AI-driven systems. Every automated process should include real-time bot detection. Anything less leaves systems exposed.

Zero trust frameworks have to evolve, too. Authentication alone isn't enough when bots are hijacking legitimate sessions, Rogers said. That means verifying credentials isn't the finish line; it's the starting point.

"Automation should improve government services, not create attack surfaces," he said.

"The key is behavior-based AI defenses that detect intent, not just credentials."

Agentic AI adds another layer to the threat. In the right hands, it has major benefits: proactive service delivery, personalized assistance, and fewer manual errors. It can even act on behalf of citizens, anticipating needs and reducing friction.

But agentic AI also empowers attackers. These bots evolve mid-attack, constantly adjusting to bypass defenses. Some use deepfake technology to impersonate officials and push through fraudulent transactions.

And now, anyone can deploy them, not just experienced programmers, Rogers said. Even nation-states can simply give a directive and let the AI handle the rest.

"You can basically say, 'I want to attack the IRS,' and agentic AI isn't just following instructions; they're thinking, they're planning, and adapting in real time," Rogers said.

These capabilities make bots harder to detect and stop. They scan for vulnerabilities around the clock, refining their tactics instantly. They study failed attacks, modify their approach, and quietly sidestep static defenses. Some scrape sensitive data faster than traditional systems can detect, using evasion techniques that constantly shift their behavior.

Three key threats agencies face include:

- **CREDENTIAL STUFFING:** Bots hijack accounts using pilfered passwords to access benefits and sensitive data
- **AI-POWERED FRAUD:** Fake users apply for unemployment, tax refunds and government subsidies
- **DISINFORMATION ATTACKS:** Bots flood social media and forums to manipulate public trust in agencies and systems

"If your defenses aren't evolving at machine speed, you're already behind," Rogers said.

To keep up, agencies need tools built for these advanced threats. HUMAN's bot detection platform uses behavioral signals and adaptive machine learning to separate legitimate activity from malicious automation. It prevents attackers from exploiting public websites without disrupting vital services.

"There are good bots out there, whether they're aggregating content for search rankings or acting as virtual assistants, and we're able to distinguish between what a good bot is and what a bad bot is," Rogers said.

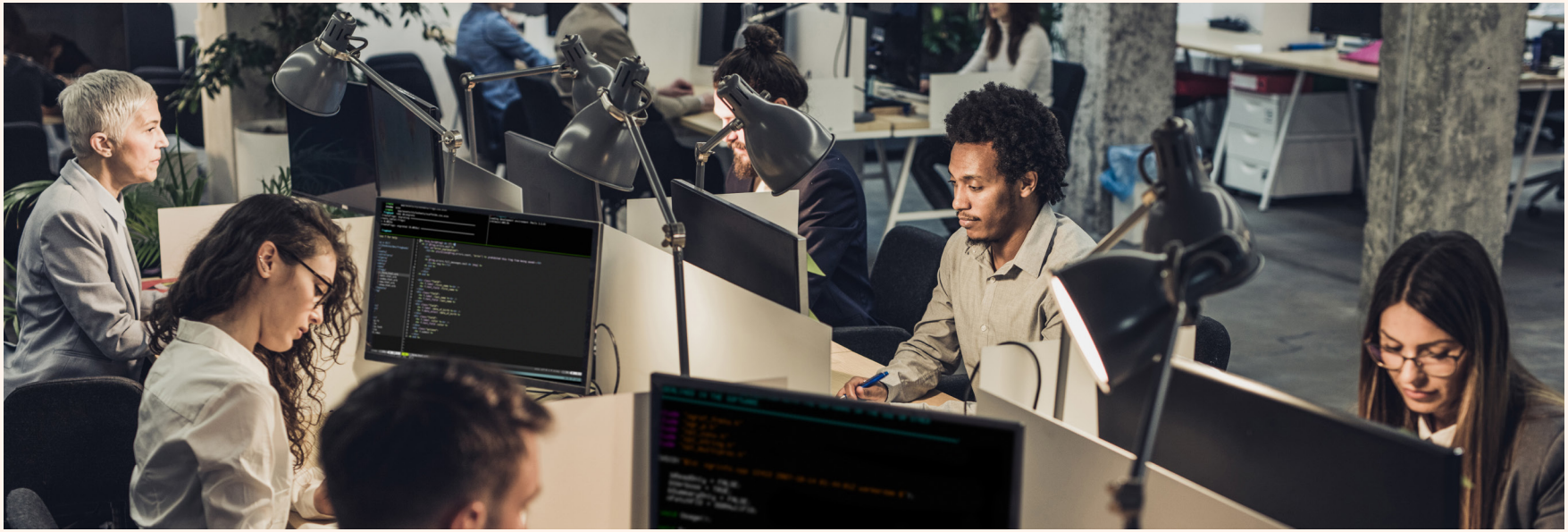
HUMAN customizes detection rules based on an agency's unique needs, maintaining essential automation while helping each agency block malicious activity.

"Everyone has different rules or different configs that they need," Rogers added. "We have our own custom rules engine that we work with customers on — what might be a good bot in their world." ▼

HUMAN

03.

Trust demands transparency and explainability



WHEN AGENCIES EXPERIENCE A BREACH, public trust takes a hit, especially when citizens don't understand how—or if—their data was protected or why the defenses failed.

Bots are also fueling a more insidious threat: AI-powered "**thoughtnets**." These combine cyberattacks with disinformation campaigns to infiltrate digital spaces, manipulate narratives, disrupt services and undermine confidence in government. They target elections, emergency communications, and policymaking processes with fake content that looks and sounds real, including audio, video, and text.

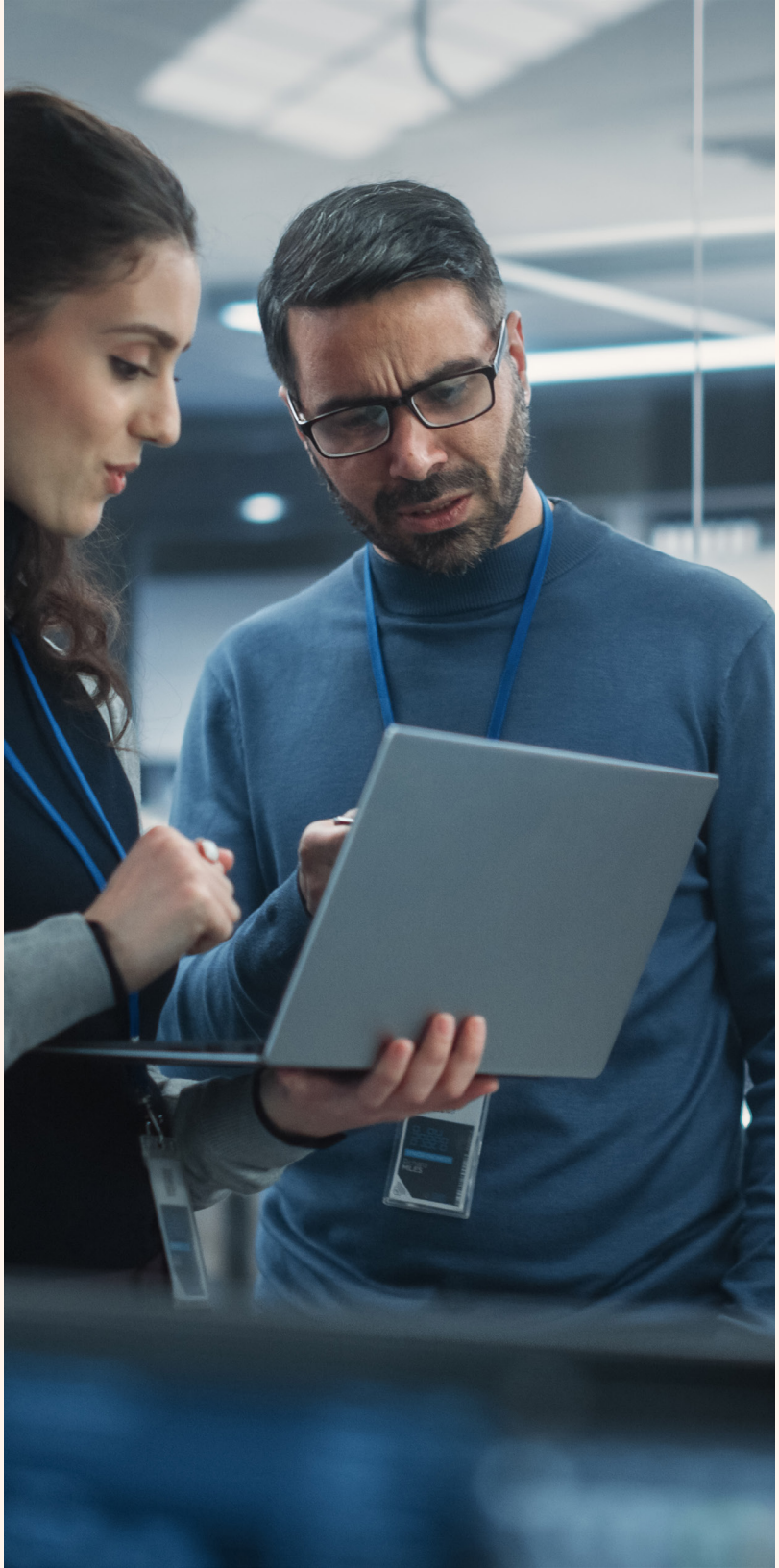
As thoughtnets grow more advanced, it becomes harder for citizens to separate fact from fiction. That raises the stakes for agencies to build a cybersecurity approach that protects both systems and trust.

Trust starts with transparency. In bot defense, that means real-time auditing, alerting, and explainable decisions.

"Public sector cybersecurity only works if the public trusts it," Rogers said. "AI-driven defenses can't be black-box security models."

True transparency means agencies can explain how security decisions are made. Defenses should leave an auditable trail showing why a bot was blocked. Controls must stop threats without creating friction for real users.

Transparency isn't just about deploying security; it's about proving it works. HUMAN advocates for visible controls, including PCI-style JavaScript audits on critical sites, so agencies can show protections are active and effective.



> **Public sector cybersecurity only works if the public trusts it. AI-driven defenses can't be black-box security models."**

JOE ROGERS
Vice president of public sector, HUMAN Security

But transparency has limits. If bot defenses feel like surveillance, the public won't trust them. AI-powered security should be invisible to humans but impenetrable to bots, Rogers said. While transparency helps make decisions understandable to the average person, it also gives botmasters insight into how to adapt and outmaneuver defenses. Bot mitigation, in that sense, becomes a high-stakes game of chess.

Compliance also plays a key role. More than a checklist, it's an opportunity to build trust. As regulations evolve to keep pace with technology, agencies can use compliance to demonstrate responsible security practices.

Rogers recommends going beyond the minimum. Treat regulations as a starting point, not the goal. Communicate clearly how AI-powered defenses protect citizen data. Show the security without exposing vulnerabilities.

"Regulatory compliance isn't just about checking boxes; it's about demonstrating responsible AI security in a way that builds public confidence," he said.

HUMAN

04.

The human role in defending against bots

AT THE END OF THE DAY, AI isn't a "set it and forget it" tool. Human oversight is indispensable.

"AI fights bots. Humans build trust. Both are essential," Rogers said. Humans make the rules and configurations that automation runs on, after all. It's up to humans to continue making sure those rules are relevant, evolving, and accurate.

AI can detect, block, and respond to threats in milliseconds. But it can't explain itself — and that's a critical part of public trust. Just because the technology is automatic doesn't mean the trust is. That must be earned through clear communication and visible security, and that's something only humans can provide.

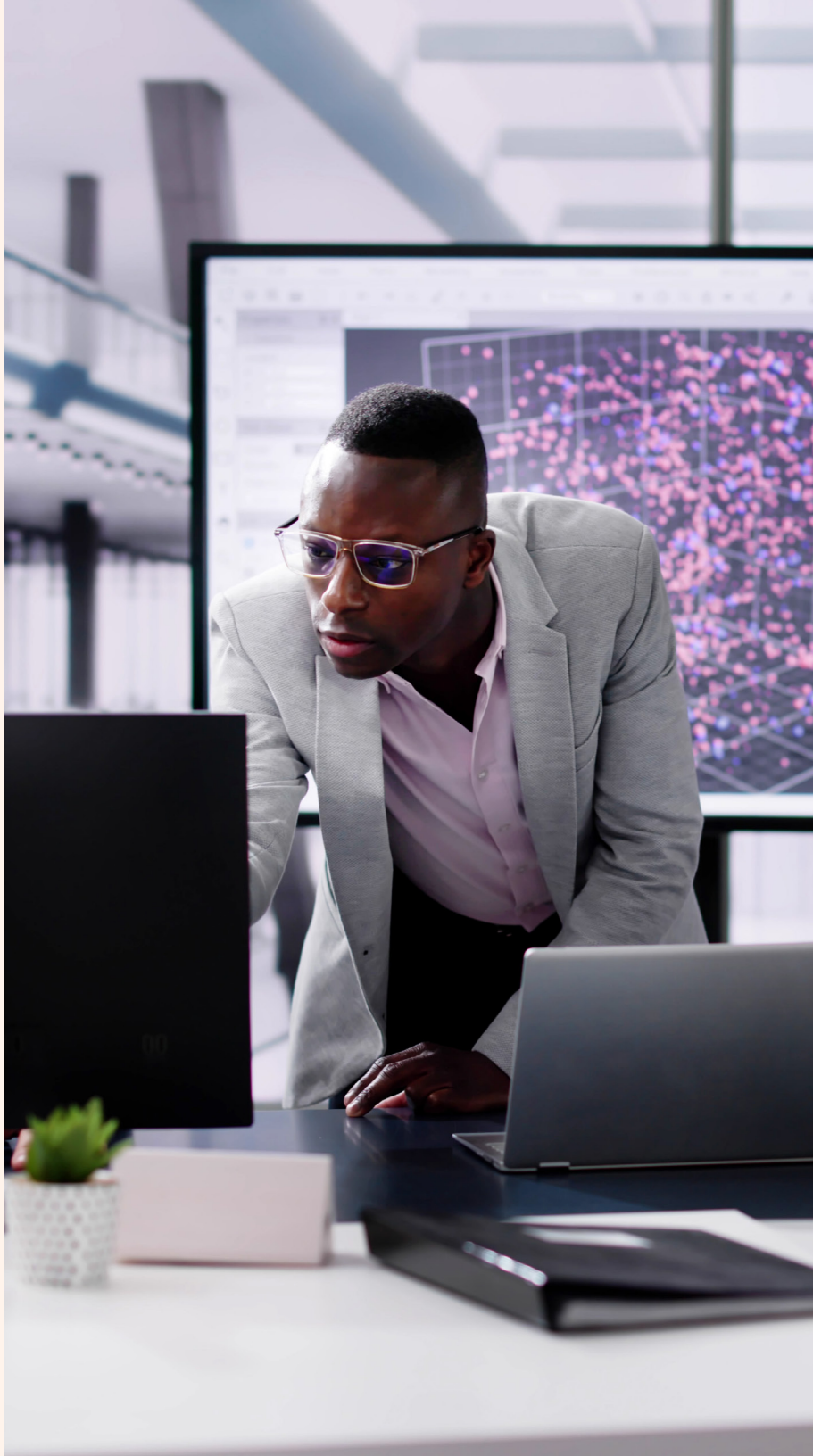
Humans also play the most important role in how agencies communicate these defenses. Show the impact. Highlight real-world success stories of stopping fraud. Citizens need proof that it works, and case studies deliver that proof best.

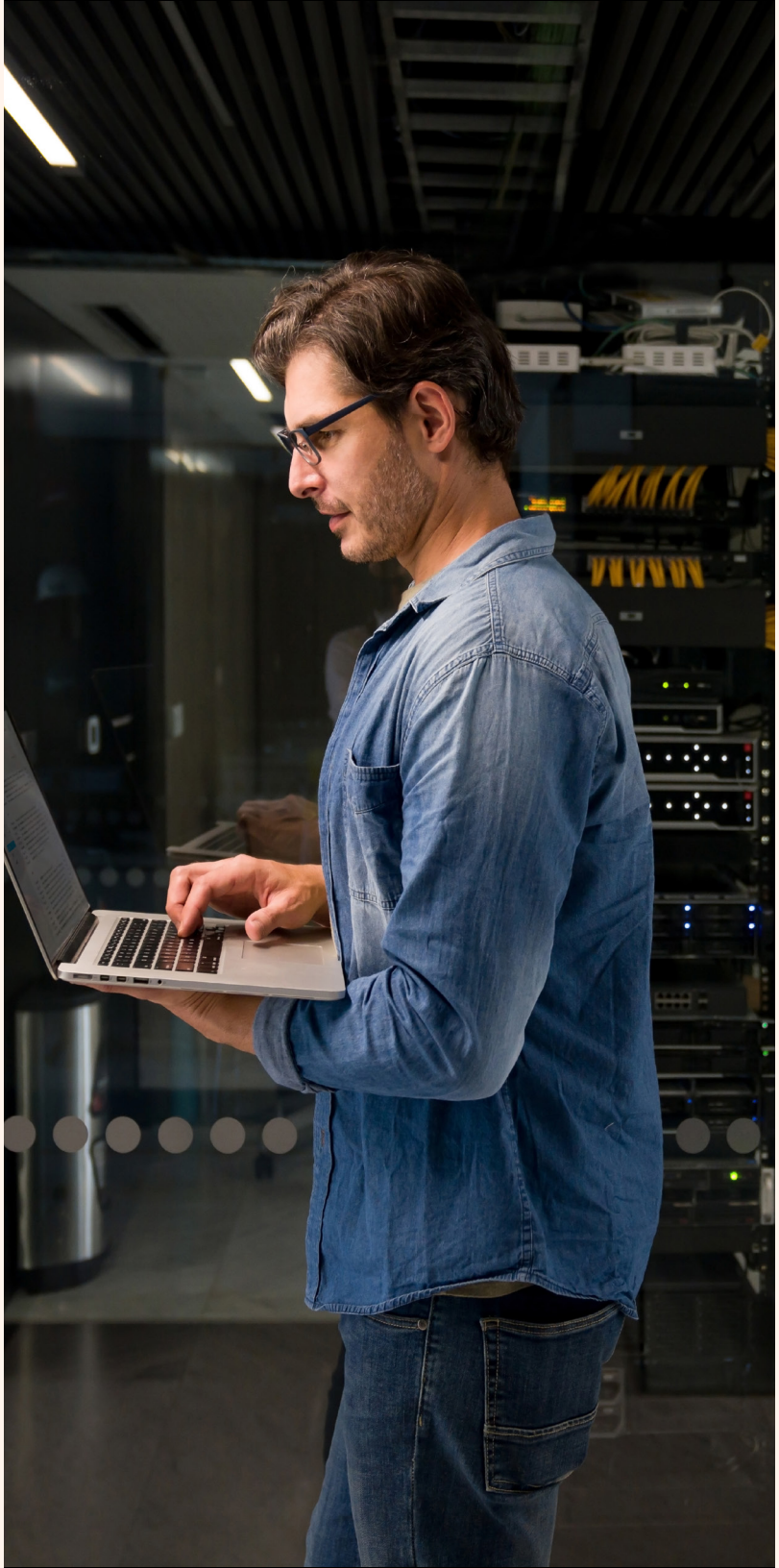
Rogers recommends explaining AI in plain language. Security teams should demystify how AI-driven bot detection works so citizens understand it. Then, reinforce the message: AI is defending and protecting, not watching or threatening.

"If the public doesn't understand how AI security works, they'll assume the worst," he said.

Humans are needed to keep building public trust, and communicating both the risk and the response is key to doing that.

Beyond communication, human oversight remains essential to actual security operations. Security decisions require





> **AI fights bots. Humans build trust. Both are essential."**
>
> **JOE ROGERS**
> Vice president of public sector, HUMAN Security

accountability, interpretation, and judgment. That's how agencies ensure AI outcomes are accurate and explainable.

When internal teams understand how AI makes decisions, they can explain those choices to the public. And the more the public understands, the more confidence they'll have in those defenses.

HUMAN keeps humans in the loop. Its team works with agencies to apply customized detection rules based on each organization's unique needs. Automation has to know what it's automating — and humans are responsible for defining that.

As bots are getting smarter, AI security is getting faster. But humans are still the final layer of defense.

That includes staying vigilant, reviewing protections, and working with the right partner to keep systems secure. ▼

HUMAN

05.

Using collective threat intelligence to fortify government platforms

BOTS WERE ONCE SEEN AS A NUISANCE — hoarding PS5s or generating fake ad clicks to siphon off billions in marketing spend — but that's changed.

"They've now adapted, and now they have different targets in mind," Rogers said. "They are being used by nation-states and hacking groups as modern-day weapon systems."

In 2023, bots overtook humans as the dominant force online. Malicious automation now targets government systems nonstop, adapting its tactics with AI. Yet most defenses remain siloed.

Working with cybersecurity experts and private-sector leaders helps agencies dismantle silos, strengthen defenses and respond faster to evolving threats. HUMAN's defense platform identifies malicious behavior early and delivers actionable insights agencies can use, even if they aren't direct customers.

With visibility into 20 trillion interactions every week and insights from over 2,500 behavioral signals, HUMAN spots emerging bot patterns before they reach government systems. This broad telemetry powers predictive protection, allowing agencies to stay ahead of attacks and better secure citizen data.

But insight alone isn't enough. Agencies also need real-time defense that keeps up with the pace of bot-driven threats.

HUMAN's platform delivers real-time, intent-based defense at internet scale — analyzing behavior instead of relying on static rules. It verifies 20 trillion digital interactions weekly and flags malicious activity before it reaches public-sector systems.

"Our network sees bot behavior across every industry, meaning we detect attacks before they spread," Rogers said.

Fighting bots alone doesn't work. Security needs to be networked, proactive and real-time — just like the threats."

JOE ROGERS
Vice president of public sector, HUMAN Security

While most security tools react after the fact, HUMAN enables agencies to act first. That speed and visibility are critical, especially as bots scan constantly and adapt faster than traditional defenses can keep up.

Bots ignore boundaries. Agencies must break down silos to defend against them. Sharing intelligence and aligning defense strategies strengthens individual systems and raises the bar across government. HUMAN gives agencies the scale, speed, and decision precision needed to block sophisticated bots.

But success still depends on more than technology.

Ethical automation, guided by human oversight and backed by trusted partnerships, is how agencies build security both resilient and accountable. That's how they protect infrastructure and the public's trust.

"Fighting bots alone doesn't work," Rogers said. "Security needs to be networked, proactive and real-time — just like the threats."

Learn more about how HUMAN is protecting the government from digital threats.