gocyber

COLLECTIVE

November Announcements

Serving Our Communities

Thank You, Cloudflare!

GoCyber "Ugly Sweater" Christmas – December 17

State of Cyber – General (ret) Paul Craft – January 21

CMMC Workshop: Jan. 27

Post-HB 96: Cyber Insurance Summit March 17

"Think Like a Red Teamer" - Feb. 10 (9 AM – 3:30 PM)

November
GoCyber Collective
Keynote Speaker

-Ann Carbonell, PhD

-Principal Technical Advisor – Digital Transormation Center

-Intelligence Analysis, Operational Planning

-US MASINT, Chair

-GEOINT (Geospatial Intelligence)

Geospatial Intelligence (GEOINT) and Cybersecurity: Mapping the Future of Threats

Ann Carbonell, Ph.D.

Principal Technical Advisor

Digital Transformation Center

November 2025

University of Dayton Research Institute

Imagine this: it's 2:00 AM somewhere over Eastern Europe.

Somewhere, a GPS signal is lying.

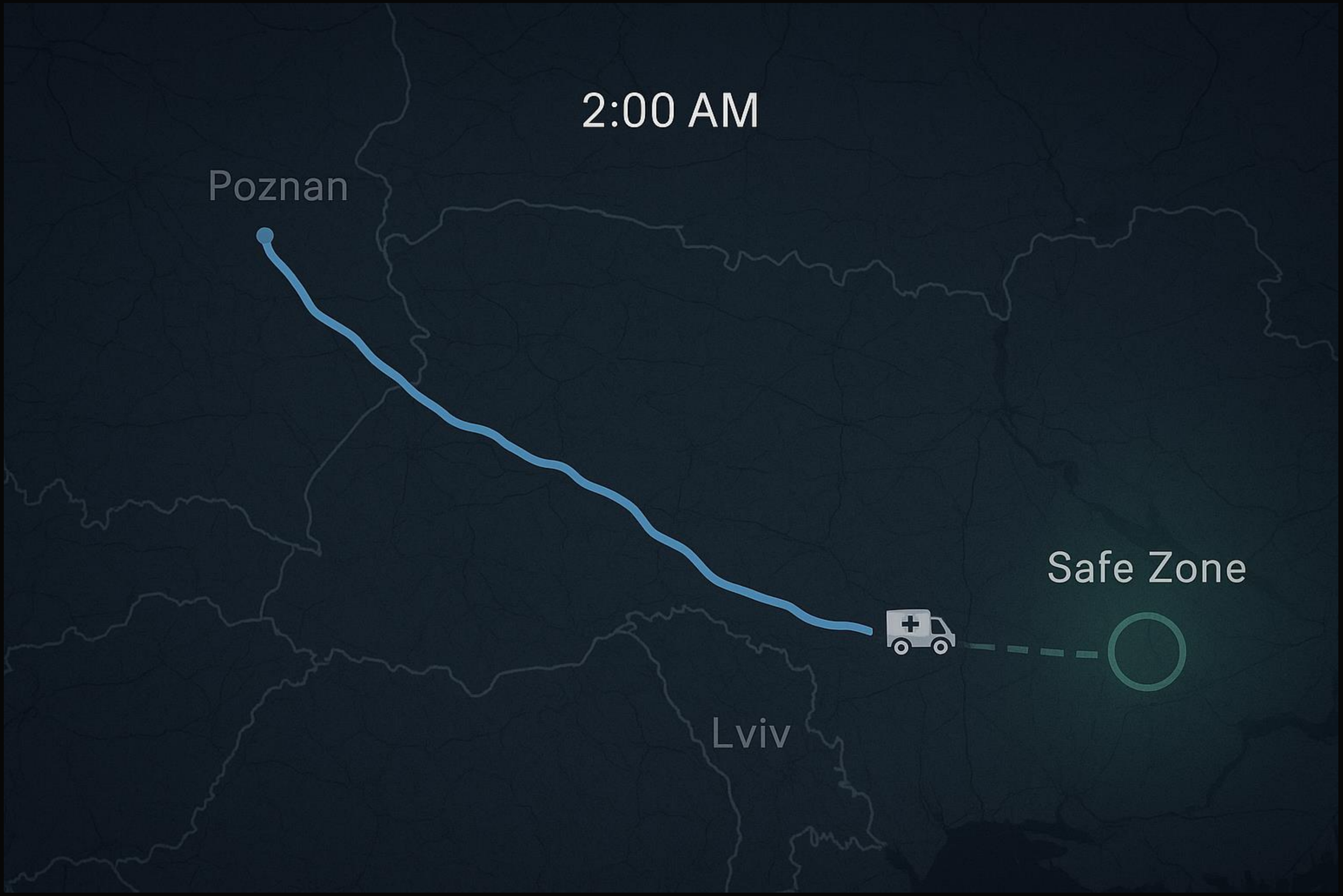
A ship is drifting off its charted course.

A data center is being probed from a nearby rooftop.

And a grid operator doesn't know yet that their sensors have been spoofed.

This is the world where cyber meets geography — and where GEOINT becomes one of the BEST ways to see the truth.

Today, we're going to map that world, expose its fault lines, and show how to fight inside it.



Imagine this: it’s 2:00 AM somewhere over Eastern Europe.

Poznan
SPOOFED PATH
Lviv
Safe Zone

But there’s a problem—

the map is lying.

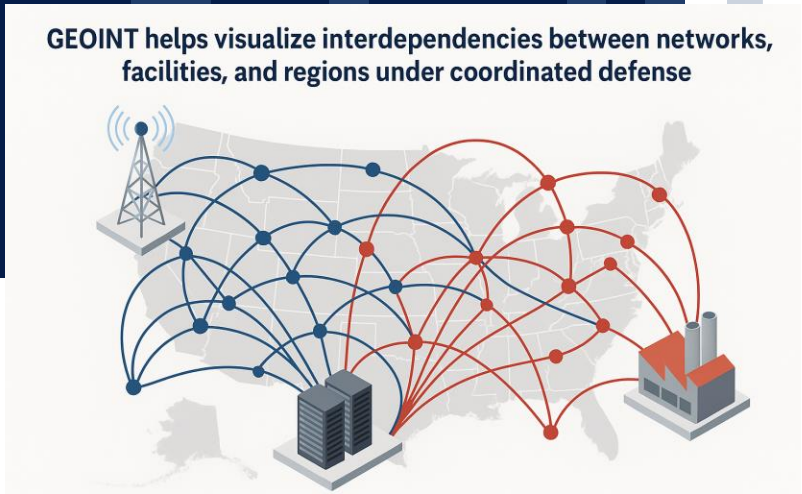
Geospatial Intelligence (GEOINT) is

GEOSPATIAL DATA + CYBERSECURITY
CYBER THREATS
RESPONSE STRATEGIES
THREAT DETECTION
GEOGRAPHIC MAPPING OF CYBER ATTACKS
ASSESSMENT OF VULNERABILITIES
CRITICAL INFRASTRUCTURE

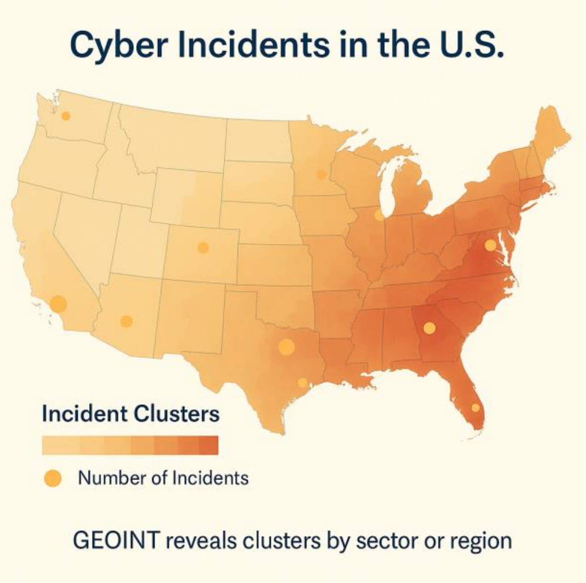
- GEOINT fuses **place, time, and data** to show *where* and *when* events unfold.
- Cyber threats exploit these same geospatial layers — turning maps into both **targets and tools**.
- This briefing explores how GEOINT enhances **situational awareness**, **cyber defense**, and **mission assurance**.

GEOINT helps teams understand where things are happening, when they’re happening, and how they relate to one another.

The Spatial Reality of Cyber Threats

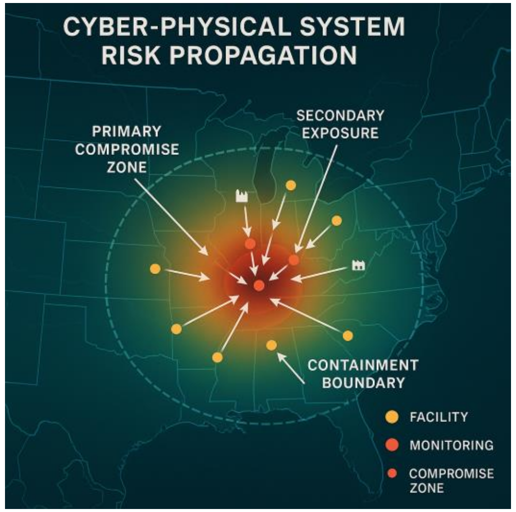


GEOINT helps visualize interdependencies between networks, facilities, and regions under coordinated defense

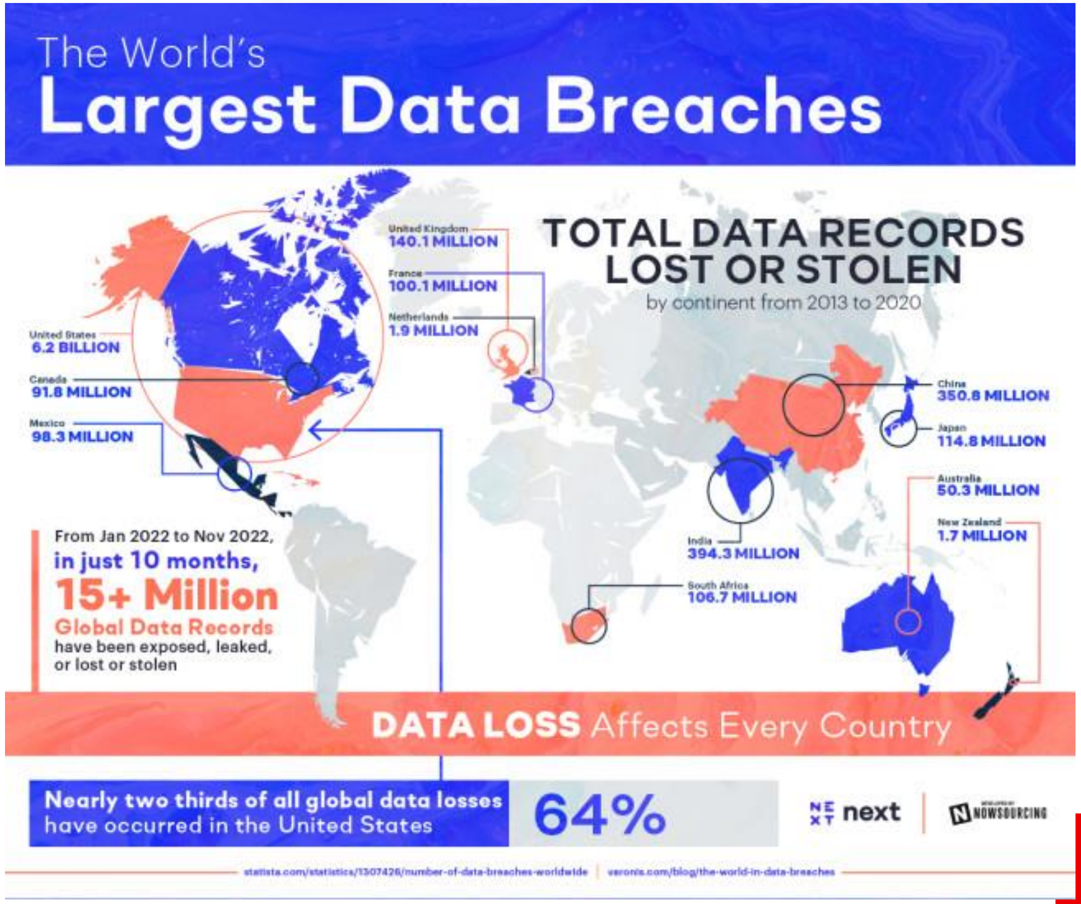


Cyber Incidents in the U.S.

GEOINT reveals clusters by sector or region



CYBER-PHYSICAL SYSTEM RISK PROPAGATION



The World's Largest Data Breaches

TOTAL DATA RECORDS LOST OR STOLEN

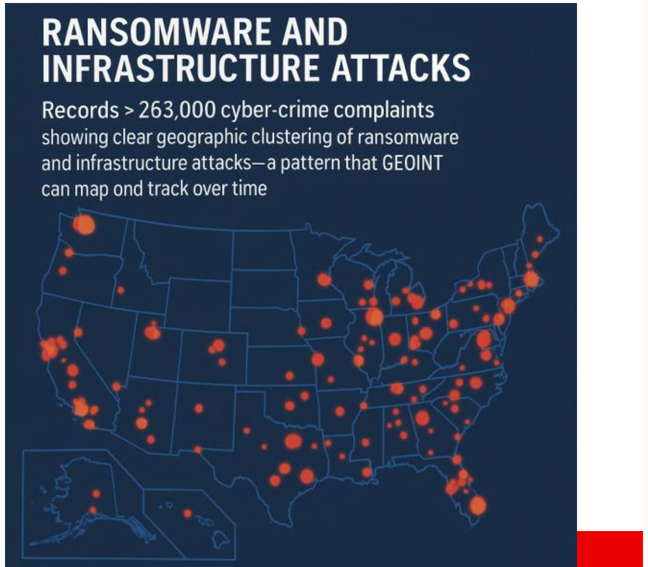
by continent from 2013 to 2020

From Jan 2022 to Nov 2022, in just 10 months, 15+ Million Global Data Records have been exposed, leaked, or lost or stolen

DATA LOSS Affects Every Country

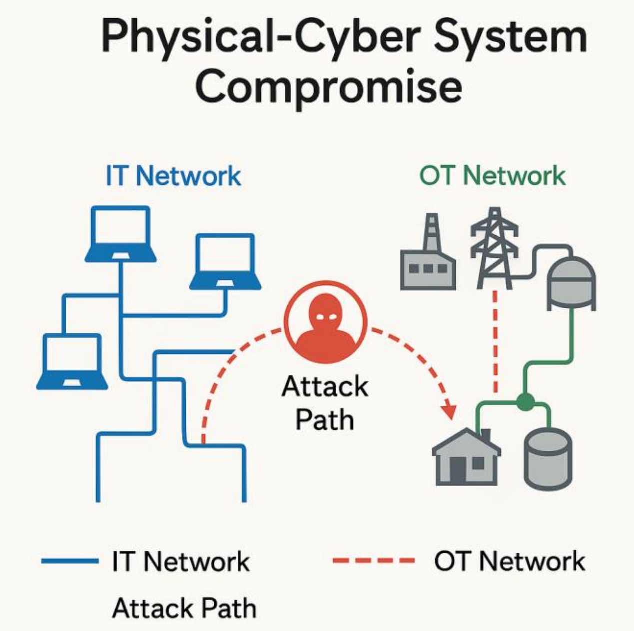
Nearly two thirds of all global data losses have occurred in the United States 64%

statista.com/statistics/1307426/number-of-data-breaches-worldwide | veronis.com/blog/the-world-in-data-breaches



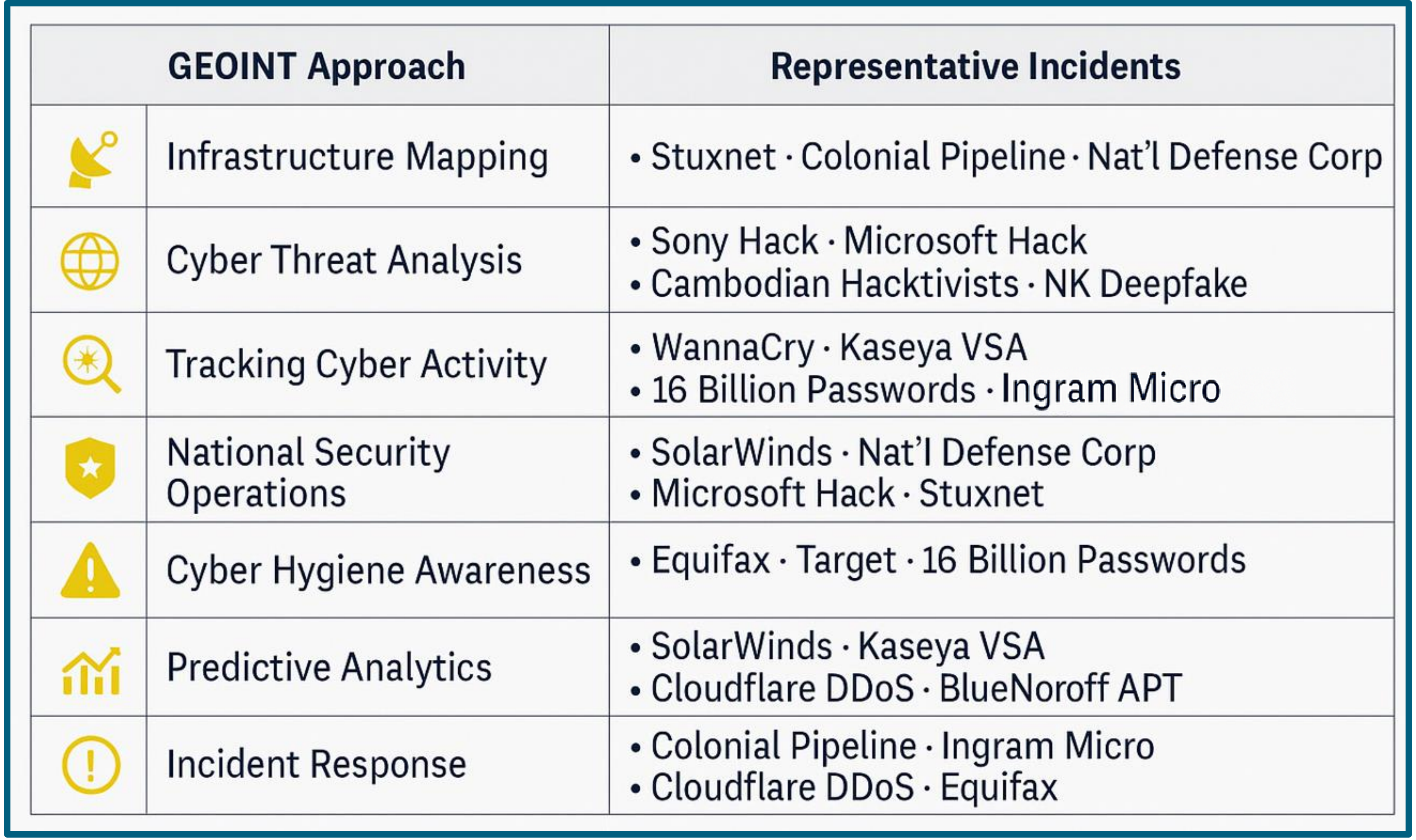
RANSOMWARE AND INFRASTRUCTURE ATTACKS

Records > 263,000 cyber-crime complaints showing clear geographic clustering of ransomware and infrastructure attacks—a pattern that GEOINT can map ond track over time



Physical-Cyber System Compromise

GEOINT Approaches and Representative Incidents



GEOINT Approach	Representative Incidents
Infrastructure Mapping	• Stuxnet · Colonial Pipeline · Nat’l Defense Corp
Cyber Threat Analysis	• Sony Hack · Microsoft Hack • Cambodian Hacktivists · NK Deepfake
Tracking Cyber Activity	• WannaCry · Kaseya VSA • 16 Billion Passwords · Ingram Micro
National Security Operations	• SolarWinds · Nat’l Defense Corp • Microsoft Hack · Stuxnet
Cyber Hygiene Awareness	• Equifax · Target · 16 Billion Passwords
Predictive Analytics	• SolarWinds · Kaseya VSA • Cloudflare DDoS · BlueNoroff APT
Incident Response	• Colonial Pipeline · Ingram Micro • Cloudflare DDoS · Equifax

GEOINT as Weapon and Shield

- **Shield – GEOINT as Protection**
  - **Detects threats early** by mapping vulnerabilities, exposure points, and risk clusters.
  - **Strengthens defense** through geospatial awareness of critical assets and mission dependencies.
  - **Improves resilience** by highlighting where defenses are weak or over-stressed.
    (Analogy: Cyber radar or armor — sees danger, protects assets.)

- **Weapon – GEOINT as Precision Intelligence**

  Reveals adversary infrastructure — their servers, supply chains, safe havens, and digital terrain.

  Enables precision response by guiding cyber teams to the right targets and priority nodes.

  Supports deterrence by showing where adversaries operate and how to counter them effectively.

  (Analogy: Precision-guided intelligence — used to neutralize threats.)

GEOINT is the bridge between digital threats and real-world infrastructure

Where the infrastructure is
Where the adversary is operating
Where the disruption will occur
Where the mission impact will be felt
Where the disruption will occur
Where the mission impact will be felt.

That's why leadership keeps saying:
A cyber incident is never just cyber, A physical impact is never just physical.
Every threat moves across both.

- Geospatial intelligence connects:
  - **Where the infrastructure is**
  - **Where the adversary is operating**
  - **Where the disruption will occur**
  - **Where the mission impact will be felt**

That's why leadership keeps saying:
"Cyber and physical systems are inseparable."
Because:

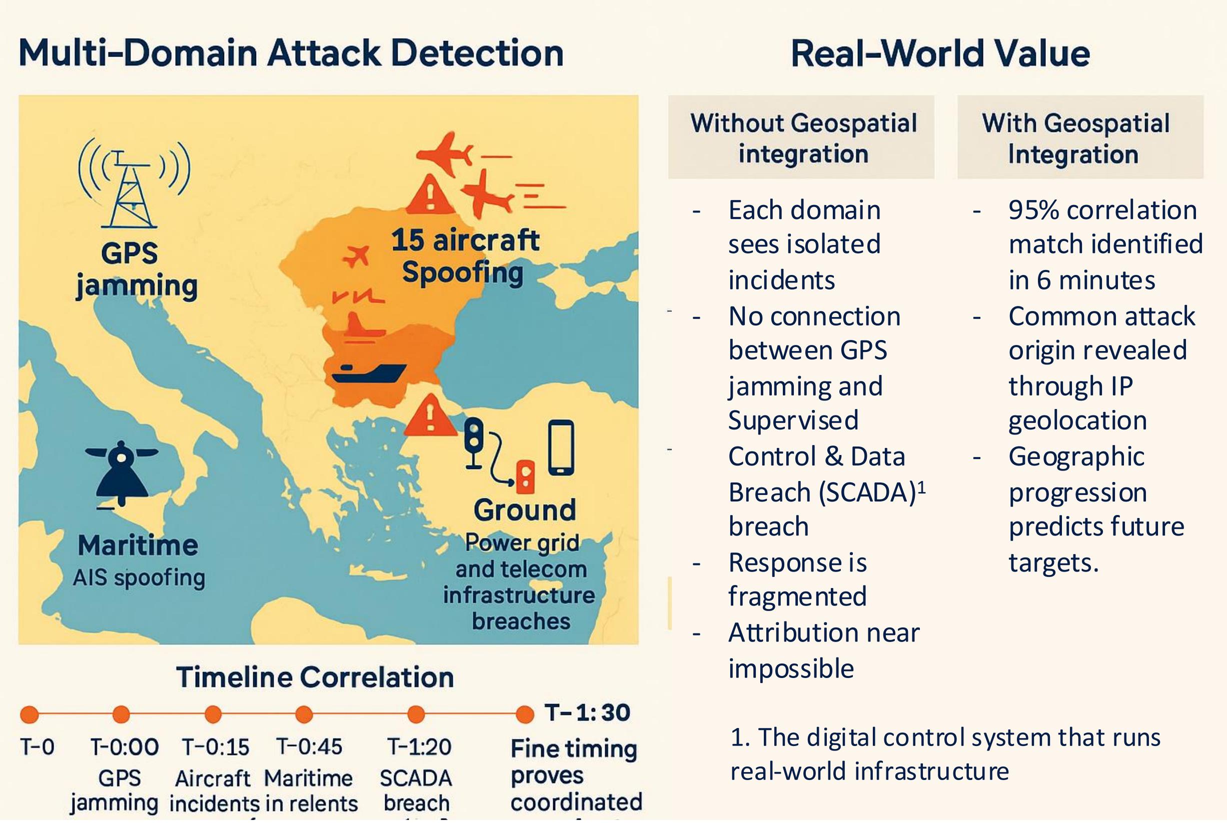
- A cyber incident **is never just cyber**.
- A physical impact **is never just physical**.
- **Every threat moves across both**.

GEOINT as a Cyber Defense Multiplier

Multi-Domain Attack Detection

The visualization tracks a coordinated attack across:

- **Space**: Satellite GPS jamming originating from specific ground locations
- **Air**: 23 aircraft experiencing spoofing in a geographic cluster
- **Maritime**: 15 vessels showing false AIS positions in the Black Sea
- **Ground**: Power grid and telecom infrastructure breaches traced to physical locations



Multi-Domain Attack Detection

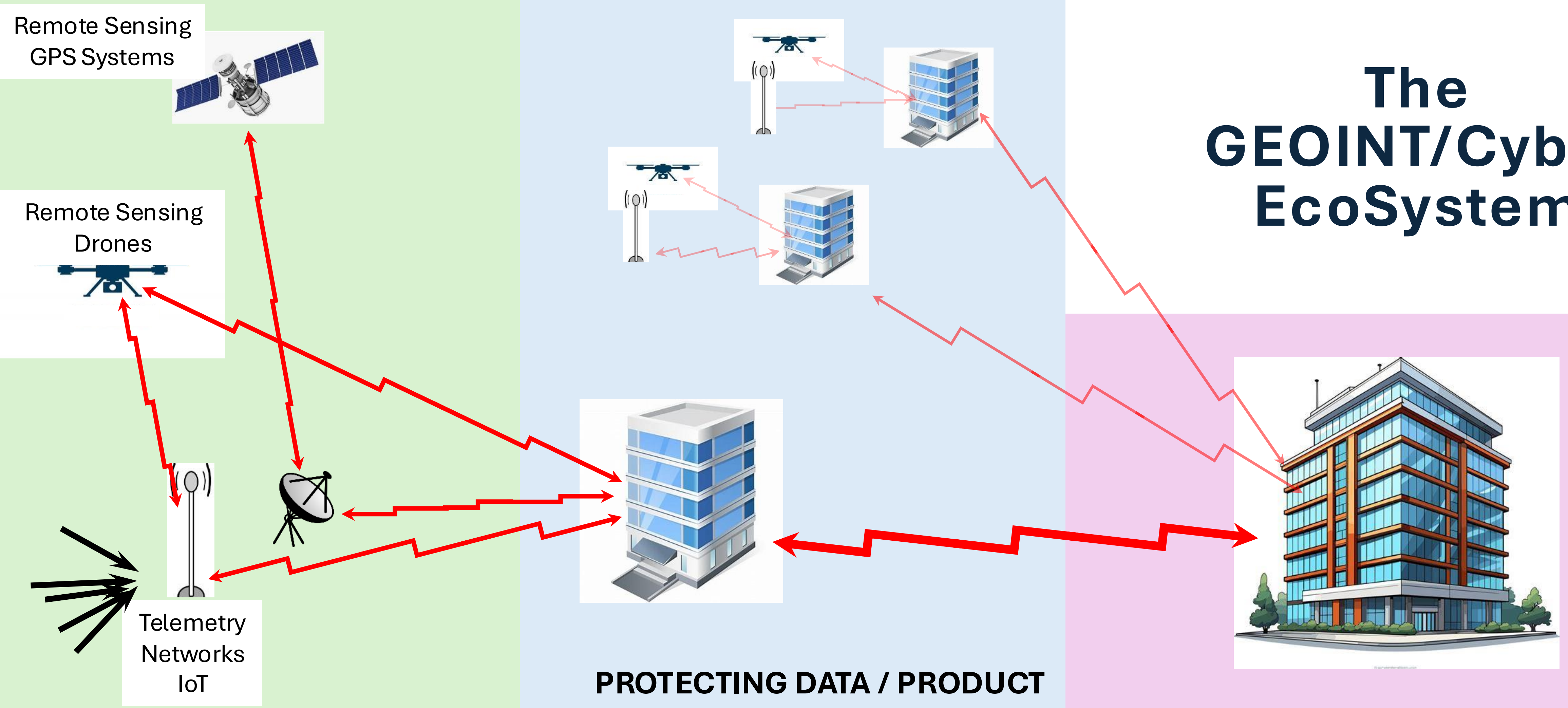
Real-World Value

Without Geospatial integration	With Geospatial Integration
- Each domain sees isolated incidents - No connection between GPS jamming and Supervised Control & Data Breach (SCADA)[1] breach - Response is fragmented - Attribution near impossible	- 95% correlation match identified in 6 minutes - Common attack origin revealed through IP geolocation - Geographic progression predicts future targets.

[1] The digital control system that runs real-world infrastructure

University of Dayton
Research Institute

The GEOINT/Cyber EcoSystem



PROTECTING SOURCES

- **Block-Chain & Encryption**
- **Narrow Bandcasting**
- **Anti Jamming/Spoofing**

PROTECTING DATA / PRODUCT PRODUCTION

- **Access Control**
- **Watermark insertion**
- **Isolated Networks**
- **SIEM & UBEA**
- **AI GEOINT Fusion**

PROTECTING USER ANALYSIS And USER APPLICATIONS

- **Access Control**
- **Block-Chain & Encryption**
- **SIEM & UBEA**
- **AI GEOINT Fusion**

Examples of Commercial Protecting Sources

Company	Capability	What It Enables
Iridium / Spire Global	Secure telemetry and encrypted satellite communications	Reliable, tamper-resistant data from remote sensors
Fortinet	Network segmentation and anti-jamming protection	Prevents disruption and signal manipulation during transmission
Honeywell	Encrypted telemetry and industrial control integration	Safeguards sensor-to-network data integrity in OT environments
Google Mandiant	Geolocation-aware threat intelligence and infrastructure mapping	Identifies adversarial campaigns targeting GEOINT assets by geography

Secure geospatial data at its point of origin (satellites, drones, IoT, and telemetry systems).

Examples of Commercial: Protecting Data & Product Production

Company	Capability	What It Enables
Elastic Security	Geospatial visualization and SIEM correlation	Maps attack origins and propagation across physical and digital infrastructure
Splunk	Geo-IP correlation and anomaly detection	Detects regional attack clusters and coordinated cyber intrusions
Cribl	Observability pipelines with geospatial enrichment	Detects spoofed GPS or traffic rerouted from suspicious geographies
Snowflake + Cortex AI	AI-driven predictive GEOINT fusion	Integrates cyber and spatial analytics for threat forecasting
HashiCorp Vault	Encryption and key management for data in motion	Secures GEOINT data pipelines across hybrid cloud environments

Preserve data integrity, authenticity, and traceability as GEOINT moves through analytic and operational pipelines.

Examples of Protecting User Analysis & Application

Company	Capability	What It Enables
SailPoint	Identity governance and access certification	Reduces insider risk and enforces zero-trust access to GEOINT data
Microsoft Sentinel	Cloud-native SIEM with global geospatial mapping	Correlates global events in near real time for situational awareness
Palo Alto Cortex XSIAM	Machine-learning-driven behavioral analytics	Detects abnormal user and entity behavior across domains
CrowdStrike Falcon	Endpoint detection and geolocation tagging	Tracks attacker movement across distributed networks
Okta	Geolocation-based multi-factor authentication	Blocks unauthorized access from high-risk or anomalous regions
ISACs / ISAOs	Sector-based cyber intelligence sharing	Fuses cross-sector incident data with geospatial awareness

Ensure trusted access, behavioral visibility, and mission assurance in user-facing and analytic environments.

What GEOINT Brings

What It Does	Why It Matters
Shows patterns and trends	By visualizing activity over time and space, GEOINT highlights areas where incidents cluster — helping anticipate where the next issue may occur.
Connects data across teams	GEOINT combines information from IT, security, operations, and logistics into one shared view — eliminating silos and confusion.
Improves awareness and response	When everyone can see the same real-time map of events, coordination improves, and response times drop.
Supports proactive decision-making	Leaders can spot early warning signs — such as regional disruptions or emerging threat patterns — and take preventive action.
Strengthens resilience	By showing where our systems and facilities depend on one another, GEOINT helps us protect the availability of critical missions and services.

GEOINT helps bridge gaps

GEOINT helps bridge gaps between:

- **IT and Cybersecurity** — who track digital threats.
- **Facilities and Infrastructure** — who safeguard physical assets.
- **Operations and Logistics** — who keep the mission running.
- **Leadership and Planning** — who set priorities and allocate resources.

When these groups share the same geospatial view, they can align faster, reduce risk, and maintain continuity even under pressure.

The Bottom Line: Mission Impact

- **Better visibility** leads to smarter, faster decisions.
- **Shared situational awareness** eliminates silos and reduces risk.
- **Cross-disciplinary collaboration** ensures both cyber and physical resilience.
- **Stronger mission assurance** keeps critical systems and operations running, no matter the threat.

Strategic Implications

- **For National Security:** GEOINT-cyber fusion can identify adversary intent earlier by correlating digital intrusions with geographic patterns.
- **For Civilian Infrastructure:** Protecting geospatial data is vital for energy, transportation, agriculture, and telecommunications resilience.
- **For Military Operations:** Integration ensures mission assurance—knowing that both maps and networks are trustworthy in contested environments.

Threat Briefing

- Charles Zugaro – Cybersecurity Analyst – Warren County Telecommunications

November Threat Briefing: Emerging Vulnerabilities & Incidents

AI-Orchestrated Cyber Espionage Campaign

- **Actors**: GTG-1002 (Chinese state-sponsored)
- **Targets**: ~30 entities, including major tech firms, financial institutions, chemical manufacturers, and government agencies across multiple countries
- **Timeline**: Detected mid-September 2025
- **Impact**: Potential intelligence theft from high-value targets; no confirmed data breaches reported, but underscores AI's dual-use risks

Microsoft Azure DDoS Event

- **Actors**: Unidentified operators of AISURU (TurboMirai-class botnet); restricted to non-governmental targets, often linked to online gaming disputes
- **Targets**: A public IP in Australia, broader implications for cloud-hosted services
- **Timeline**: November 2025
- **Impact**: No service disruption reported, but attack volumes exceeded 20 Tbps in bursts, highlights IoT vulnerabilities enabling hybrid threats (DDoS + scraping/phishing)

November Threat Briefing: Emerging Vulnerabilities & Incidents

Akira Ransomware Campaign

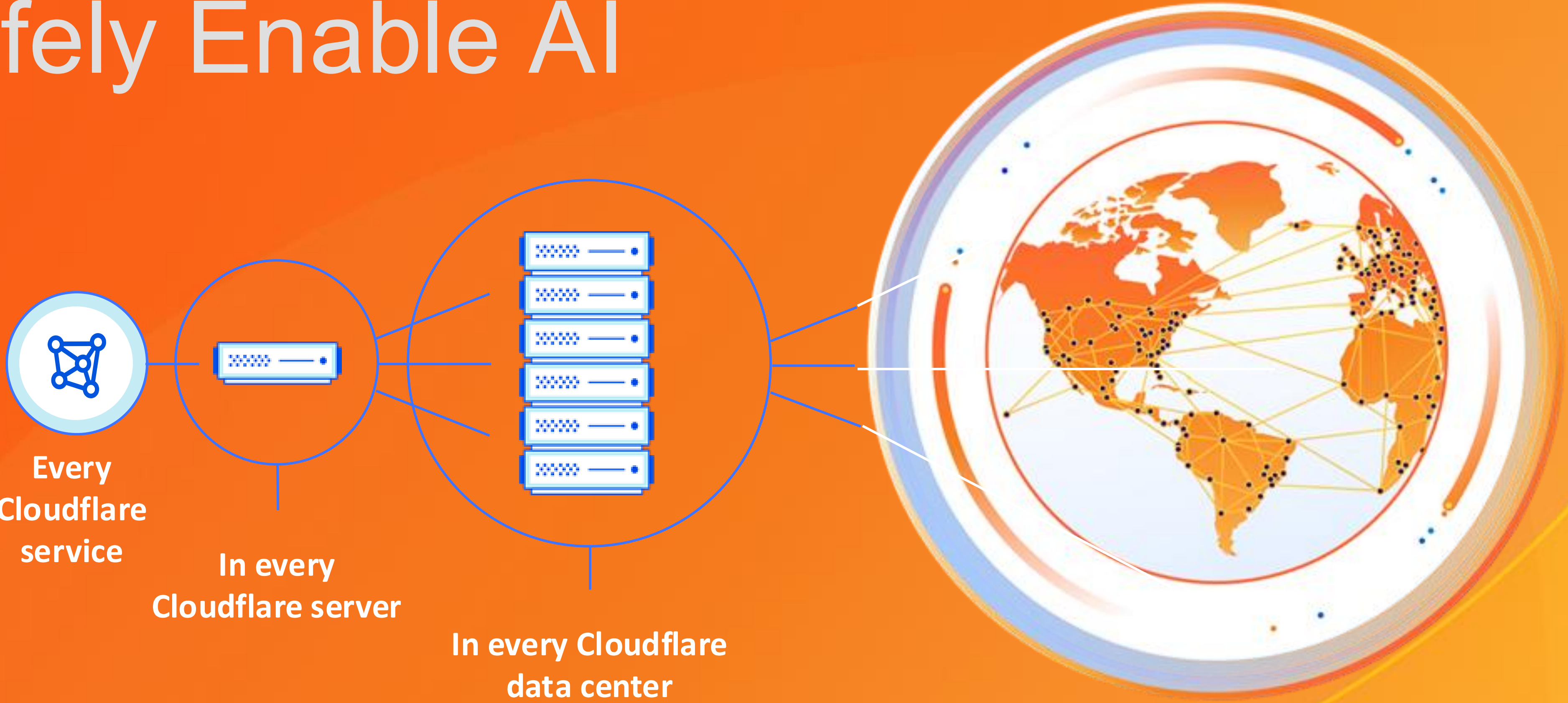
- **Actors**: Akira affiliates (Russian-linked, revenue ~$244M since 2023)
- **Targets**: Healthcare, finance, government, manufacturing, education, and IT sectors; reent victims include Stanford University and Tietoevry
- **Timeline**: AHV targeting since June 2025, advisory updated November 14, 2025
- **Impact**: Data compromise and operational downtime; >438k vulnerable SonicWall devices exposed as of September 2025

November GoCyber Collective Sponsor Speaker

-Scott Jobe – Regional Sales Manager - Cloudlfare

-Robert Rasner – Senior Solutions Engineer - Cloudflare

Safely Enable AI



Every Cloudflare service

In every Cloudflare server

In every Cloudflare data center

Across 335+ cities in 120+ countries

Understanding LLMs and AI

LLMs (Large Language Models)

- AI models; use massive amounts of data
  Learn natural language, process it, & produce new content

Generative AI

- Creates new content from data

Agentic AI

- Performs tasks autonomously

Physical AI

- AI systems that interacts directly with the physical world

AI Inference

- Pre-trained AI model uses its learned knowledge

Innovating with AI

Assistants/Chatbots	Healthcare	Cybersecurity	IoT	Autonomous Vehicles
Robotics	Finance	Manufacturing	Gaming	……….etc

* Stats from Marketsandmarkets, GrandViewResearch, Statista, McKinsey & Company, Forbes Advisor

Developers and Enterprises are incorporating AI at a rapid pace

- AI market size to reach $1,339 billion by 2030
- AI expected annual growth rate of 36.6% from 2023 to 2030
- ChatGPT - 1 million users within first 5 days
- 72% of businesses adopted AI for at least one business function
- 64% of businesses expect AI to increase productivity

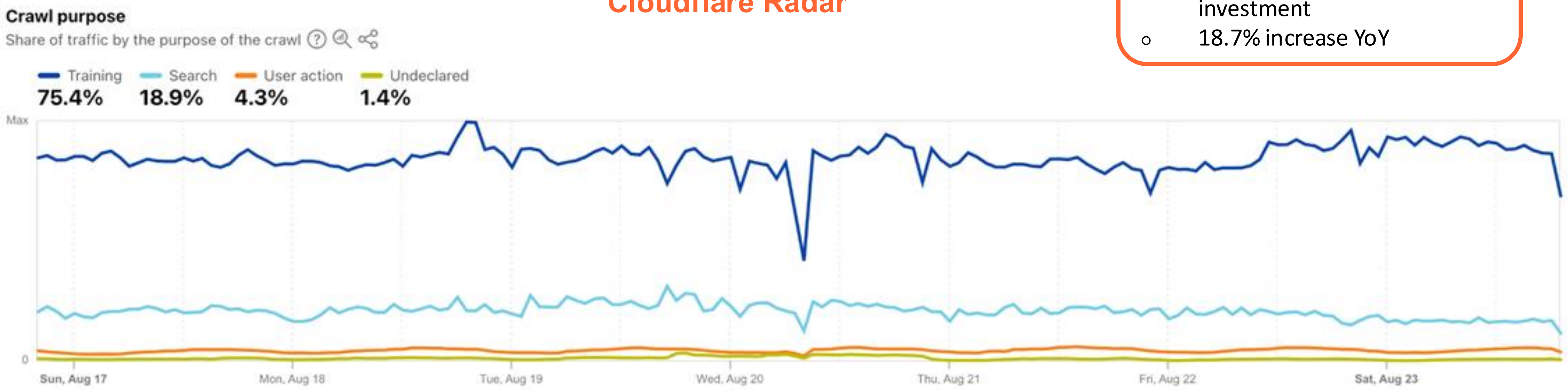
Private AI investments

- U.S.: 109.1 billion
- China: $9.3 billion
- U.K $4.5 billion

Generative AI Momentum

- $33.9 billion global private investment
- 18.7% increase YoY

Cloudflare Radar



Crawl purpose

Share of traffic by the purpose of the crawl

* Stats/data from Marketsandmarkets, GrandViewResearch, Statista, McKinsey & Company, Forbes Advisor, Stanford University 2025 AI Index Report

AI Security Concerns

Cybernews

One malicious prompt rules all AI models: universal jailbreak discovered

LLM red teamers: People are hacking AI chatbots just for fun and now researchers have catalogued 35 “jailbreak” techniques

by Eric W. Dolan — April 23, 2025 in Artificial Intelligence

Researchers Uncover GPT-5 Jailbreak and Zero-Click AI Agent Attacks Exposing Cloud and IoT Systems

Aug 09, 2025 Ravie Lakshmanan Genera

Introducing GPT-5

ChatGPT now has our smartest, fastest, most useful model yet, with thinking built in — so you get the best answer, every time.

SECURITY

Azure AI Vulnerabilities Allowed Attacks to Bypass Moderation Safeguards

BY DEEBA AHMED · NOVEMBER 1, 2024 · 2 MINUTE READ

WIRED SECURITY POLITICS THE BIG STORY BUSINESS SCIENCE CULTURE REVIEWS

MATT BURGESS SECURITY OCT 17, 2024 6:30 AM

This Prompt Can Make an AI Chatbot Identify and Extract Personal Details From Your Chats

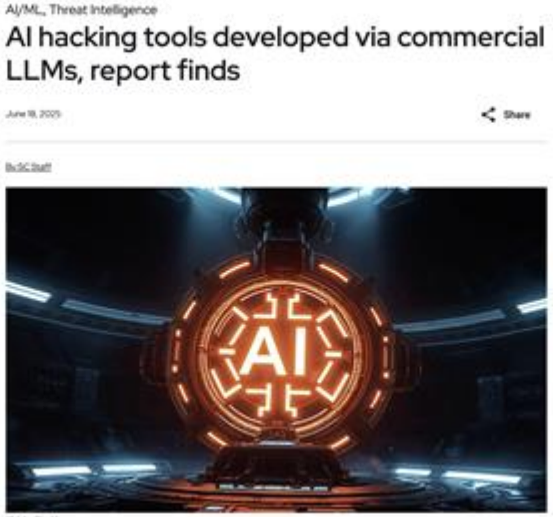
Security researchers created an algorithm that turns a malicious prompt into a set of hidden instructions that could send a user's personal information to an attacker.

Security researchers created an algorithm that turns a malicious prompt into a set of hidden instructions that could send a user's personal information to a attacker.

ChatGPT Leaks Sensitive User Data, OpenAI Suspects Hack

The leaks exposed conversations, personal data, and login credentials.

Anuj Mudaliar Assistant Editor - Tech, DKZD February 1, 2024



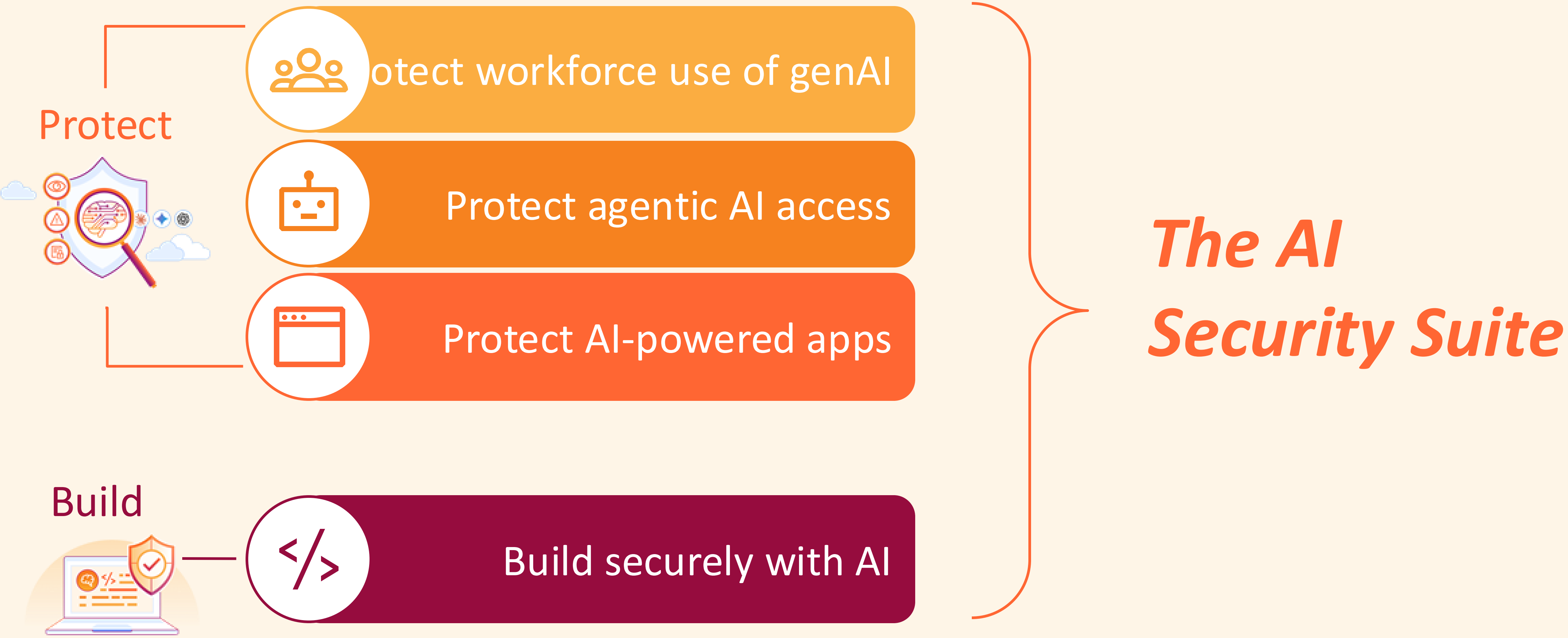
AI/ML, Threat Intelligence

AI hacking tools developed via commercial LLMs, report finds

June 18, 2025 Share

By SC Staff

Cloudflare is best positioned to lead AI Security



Protect

otect workforce use of genAI

Protect agentic AI access

Protect AI-powered apps

Build

Build securely with AI

The AI Security Suite

Introducing the Cloudflare Network

A single network that delivers local services at global scale

330+ cities

in 125+ countries, including mainland China

w/210+ cities

for AI inference powered by GPUs

~50 ms

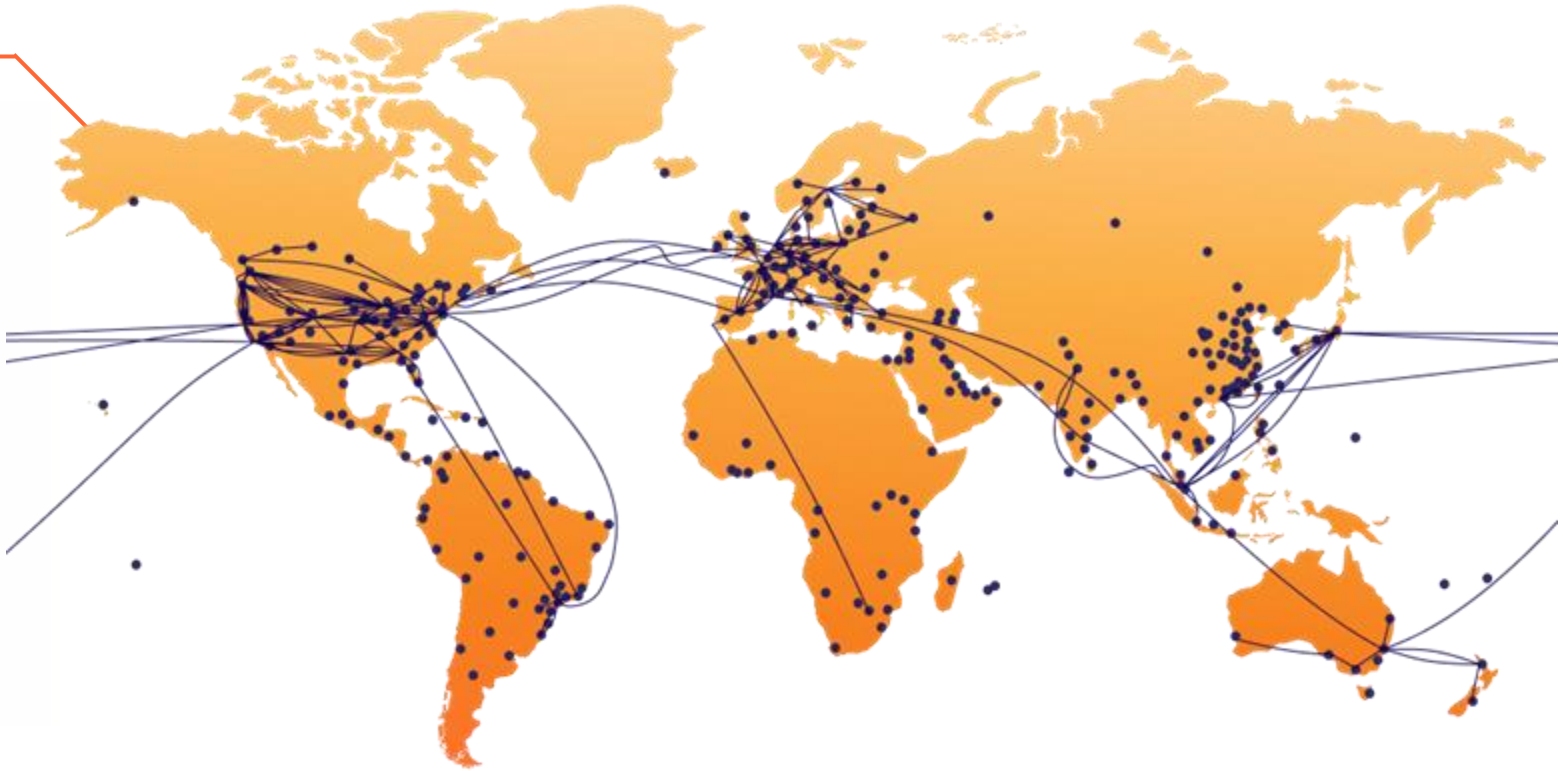
from ~95% of the world's Internet-connected population

~13,000 networks

directly connect to Cloudflare, including ISPs, cloud providers, and large enterprises

449 Tbps

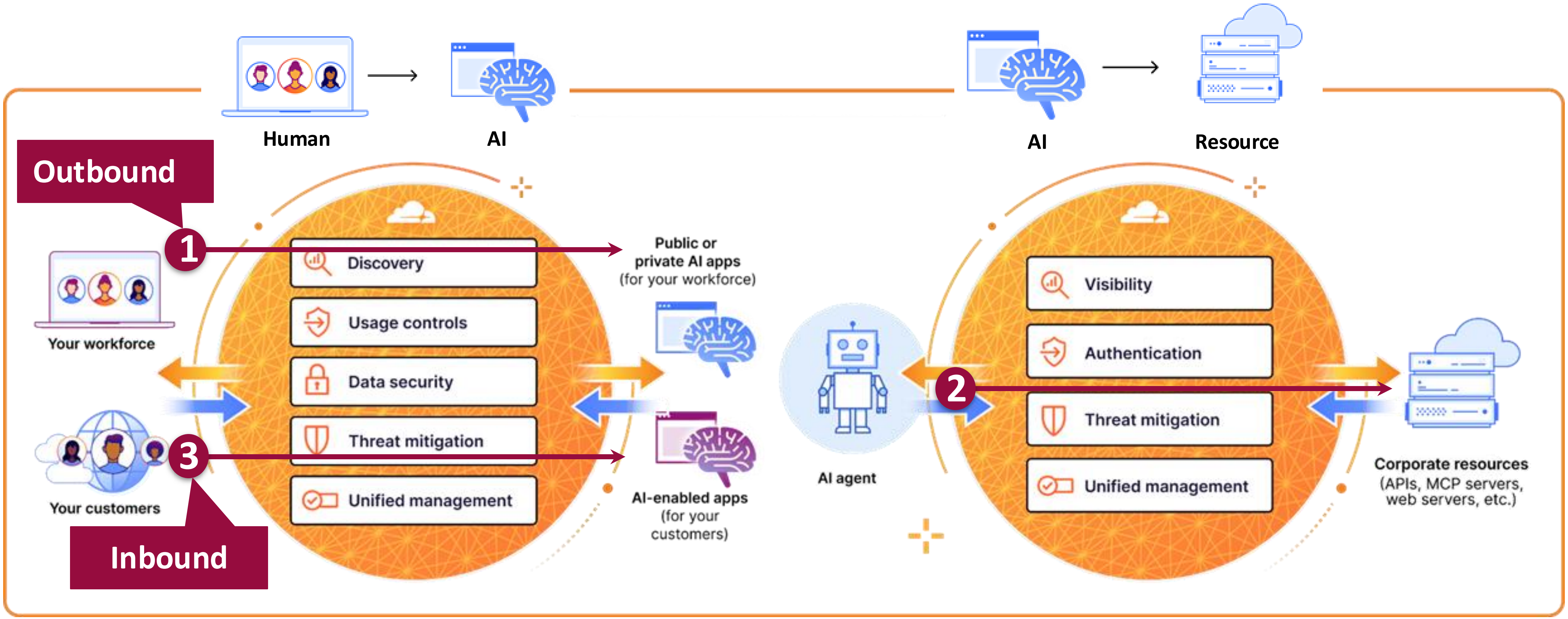
of network capacity and growing



● Cloudflare city (as of Q2 2025)

— Cloudflare backbone (as of Q2 2025)

Secure generative & agentic AI communication



Thank you!

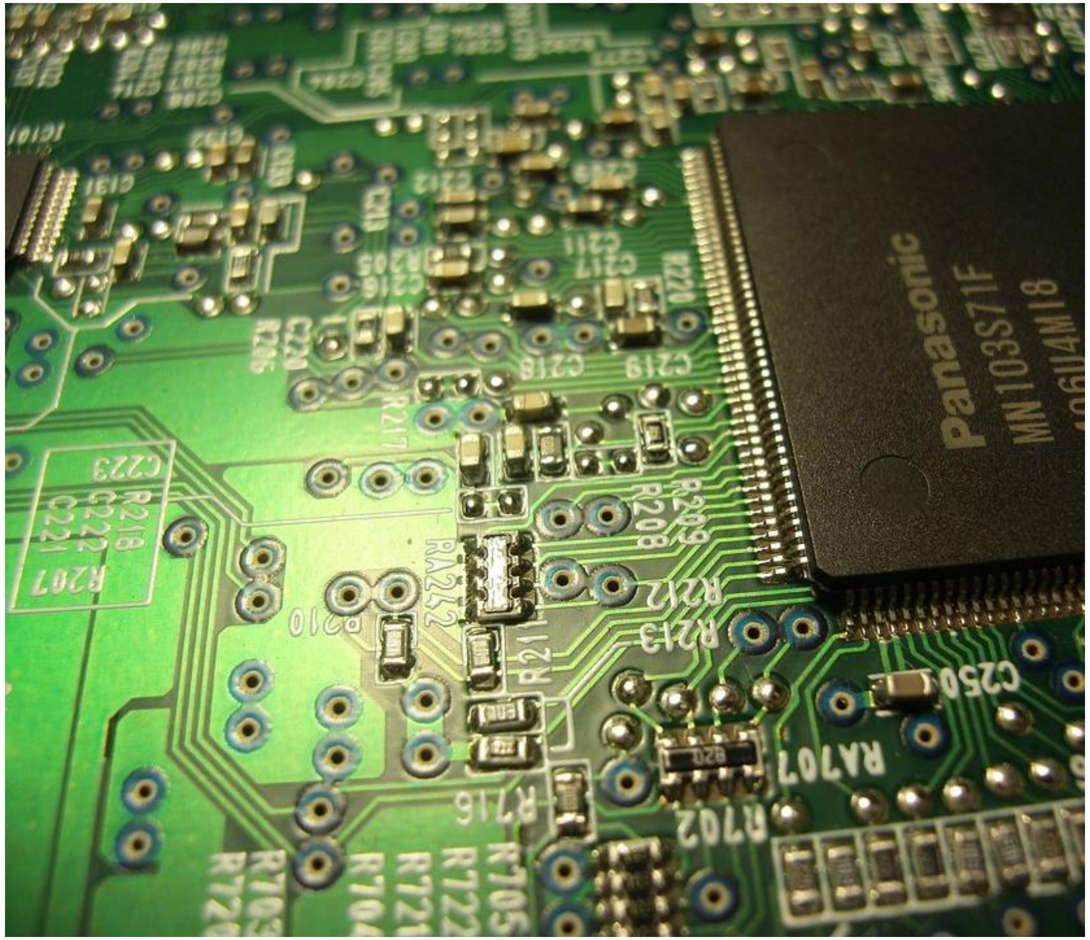
Scott Jobe: sjobe@cloudflare.com
Robert Rasner: rrasner@cloudflare.com

December Meeting: GoCyber "Ugly Sweater" Christmas

- Holiday Breakfast Feast
- 2025 Year in Review... Year of Growth
- Coming in 2026?
- Sponsored by Stellar Cyber

November Parting Shots

- Local Gov’t/Public Safety SIG – Sun Watch Room
- Education SIG – Wright Patt Room
- Defense Contractor SIG – Hawthorn Room
- Register for CTF, Monthly Meetings and LEADS Workshop
- Turn in your lanyards at the desk



Information

Email me at john@GoCyberCollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

You can register for future breakfast meetings from the website.

- GoCyberCollective.org

Event Sponsors

Proven. Proactive. Personalized.