

# JEOPARDY!



**How many cyber attacks is the caribbean facing per week?**

**A. Less that 100?**

**B. More than 1000?**

**C. More than 2000?**

# JEOPARDY!



Which verticals in the Bahamas experienced the most attacks in 2025?



Real state?



Finance?



Government?



Retail?



Hospitality?

alivbusiness  
**CYBER  
SECURITY  
SUMMIT**  
— 2026

**CYBER RESILIENCE**  
DEFENDING THE DIGITAL FRONTIER

EMPOWER, PROTECT, EVOLVE

## Cyber Risk by Numbers:

What Cloudflare's Data Reveals About Business Exposure  
in the Caribbean

**Jorge Vendries**  
Territory Account manager Cloudflare



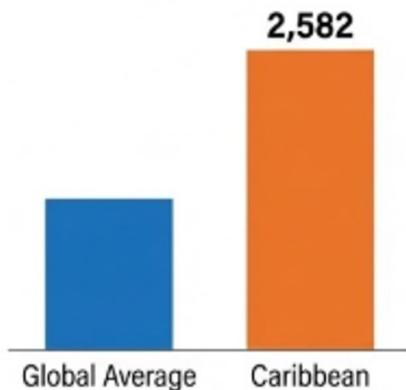
# Caribbean Threat Landscape (Regional Exposure)

## Attack Volume

**2,582**

Average Weekly Cyberattacks  
(Late 2024/Early 2025)

40% higher than the global average



## BOT ATTACKS & API TARGETING



**44%**

of Advanced Bots Target APIs

44% of all advanced bot traffic now targets APIs (used for mobile banking apps), attempting "Credential Stuffing" to take over user accounts.

## Economic Impact

### Card Fraud:

**BSD \$21 million** in losses annually to card fraud, with a shift toward "card-not-present" (online) attacks



<https://radar.cloudflare.com/year-in-review/2025/bs#most-attacked-industries>

**February 2, 2025**

**Phones, email, classes disrupted in University of The Bahamas ransomware attack**

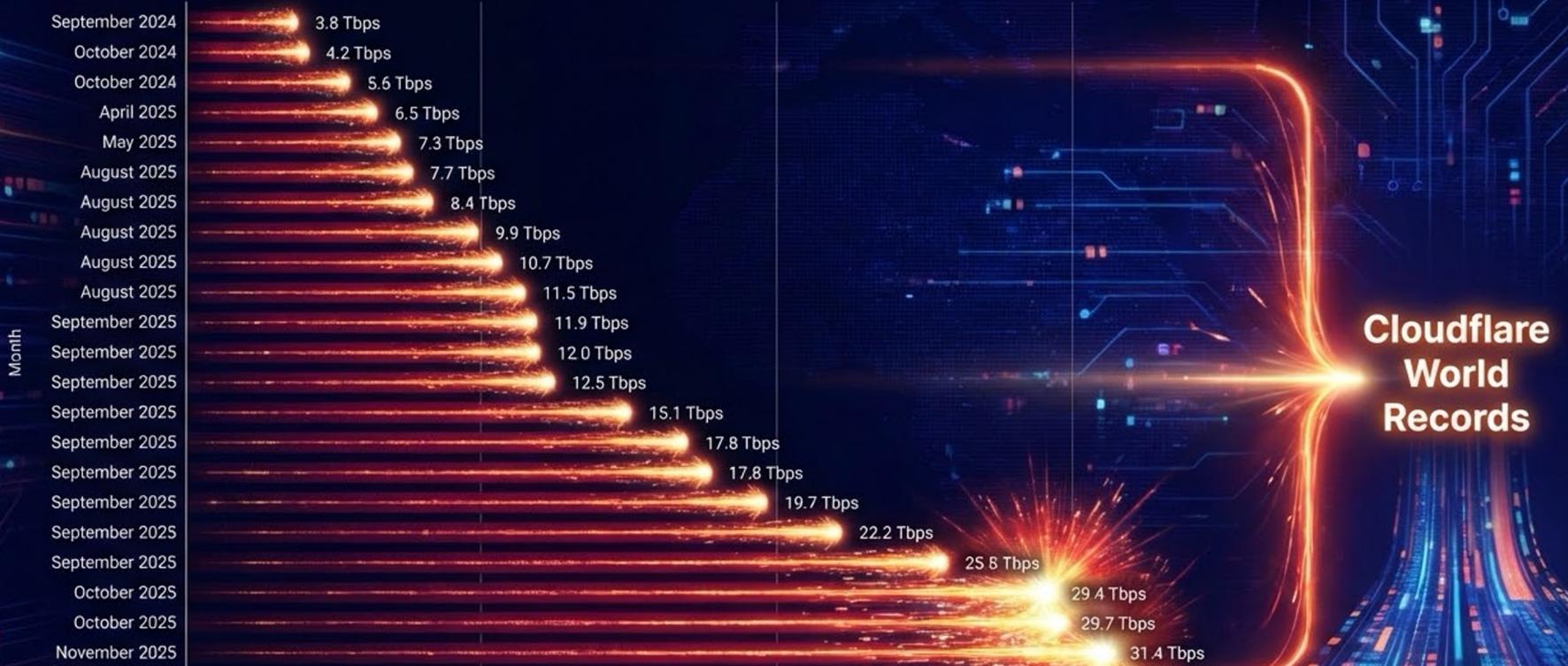


**March, 2025**

**Cyber attack at Water and Sewerage Corporation**



# A handful of the largest DDoS attacks mitigated by Cloudflare



Cloudflare  
World  
Records

## Global Network that delivers local capabilities at scale



**335+** 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



<https://sasecloudmap.com/#loc=3.55/14.1/-63.71>

# Every service built to run on every server in every data center



Every  
Cloudflare  
service



Built to run over  
every  
Cloudflare  
server



In every  
Cloudflare data  
center



Across 335+ cities  
in 125+ countries

# How Cloudflare works?



Every service we offer runs on every server in every datacenter around the world

 DNS	 DDoS	 TLS	 Firewall	 Rate Limiting	 CDN	 WAF	 Argo
--	--	--	---	--	--	--	---

# Application layer attack activity

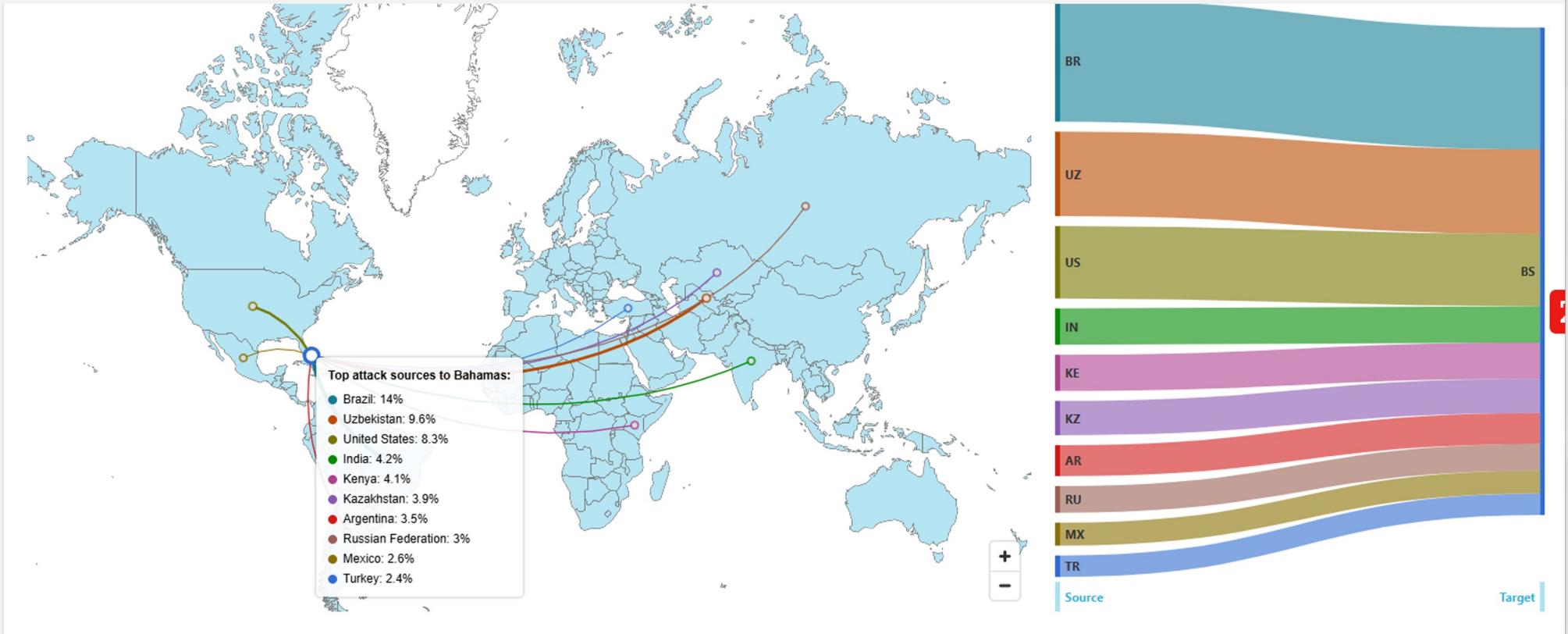
Top attacks by target location

Application Layer Security for

Bahamas



Last 7 days



<https://radar.cloudflare.com/security/application-layer/bs>

# Product portfolio

## Application Services

CDN and DNS

Web App and API Protection

Load Balancing and Routing

DDoS Mitigation

SSL for Software as a Service

Client Side Security

## Cloudflare One

*(Zero Trust & Network Services)*

Zero Trust Network Access

Secure Web Gateway

Data Loss Prevention

Cloud Access Security Broker

Firewall as a Service

Network as a Service

Email Security

## Developer Platform

Workers

Pages

R2 Object Storage

AI

Media

Database

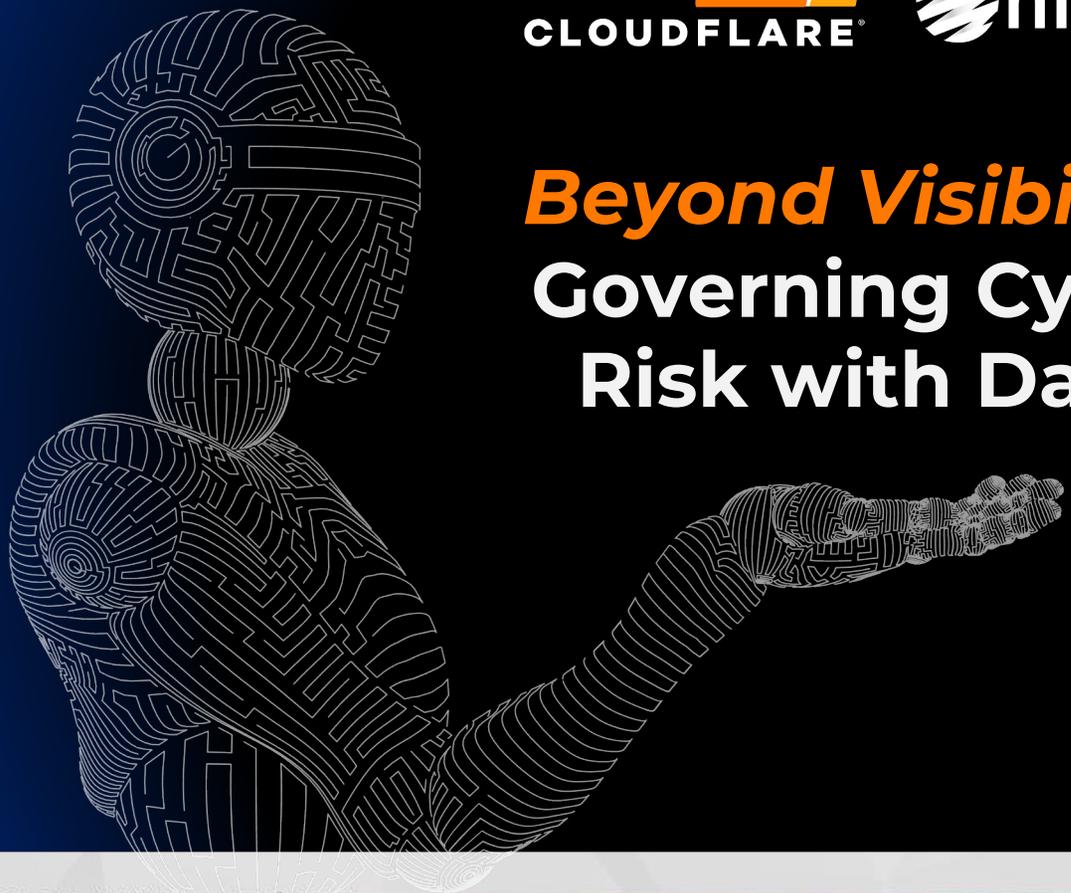
One unified platform



One network



***Beyond Visibility:***  
**Governing Cyber  
Risk with Data**





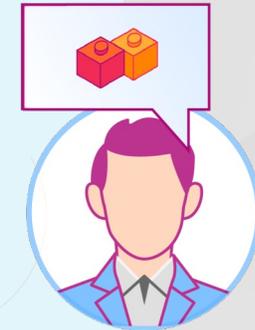
## From Threat Visibility to Executive Accountability

### What we just saw proves two things:

- *The threat landscape is real.*
- *Visibility is no longer the problem.*

### The real challenge for CISOs and CIOs is:

- *Turning visibility into defensible decisions.*





# The CISO / CIO Dilemma

## You are navigating:

- *Increasing attack surface*
- *Tool fragmentation*
- *Budget constraints*
- *Board expectations*
- *Regulatory scrutiny*

**You are not *lacking data*.**

**You are lacking alignment  
between data, architecture,  
and governance.**



# When Data Exists, Accountability Changes

Because Cloudflare Radar and global intelligence exist:

- *“We didn’t know” is no longer a defense.*
- *Boards expect oversight.*
- *Regulators expect evidence.*
- *Customers expect continuity.*

Cybersecurity  
becomes:

- *A governance issue*
- *A capital allocation decision*
- *A resilience strategy*



## From Noise to Risk Clarity

### ***Operational mode:***

- *Respond to incidents*
- *Chase alerts*
- *Add tools*



### ***Strategic mode:***

- *Measure exposure*
- *Prioritize architectural risk*
- *Simplify control planes*
- *Align investments with threat reality*



## Three Questions Every CISO and CIO Must Answer

Is our architecture aligned to the threats we actually face?

Are we measuring the risks that matter to our business?



Can we defend our decisions to the board and regulators?



# Cybersecurity with Data



Cybersecurity  
with data means:

Translating threat intelligence into  
architectural decisions

Using exposure trends  
to guide budget allocation

Turning telemetry into  
board-ready narratives

Designing for continuity under attack

## What Mature Organizations Do Differently



*Consolidate to reduce blind spots*



*Align controls to real exposure*



*Report cyber risk in business language*



*Design for resilience, not just protection*





# Visibility Creates Responsibility

*Cybersecurity data only creates value when it changes how leaders decide.*

**Learn how:**

**Visit Cloudflare's booth**



**MORE INFO:**  
[info@onistec.com](mailto:info@onistec.com)



# Thank you



CYBER SUMMIT 2026