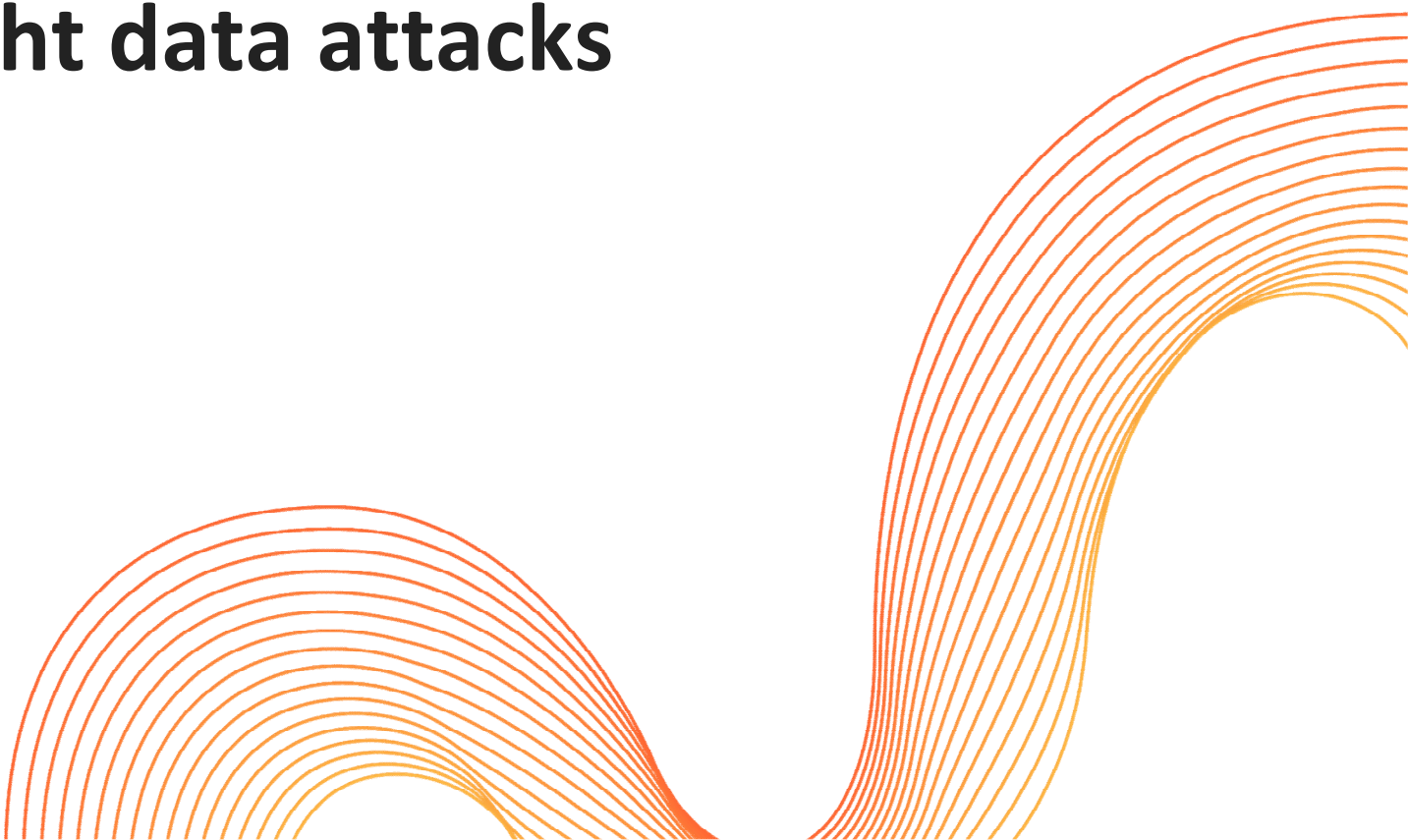
CLOUDFLARE

# How to fight data attacks

May 2021



CLOUDFLARE

# Introduction & Agenda

**Henry Heinemann**
*EMEA Head of New Product GTM*

hh@cloudflare.com
linkedin.com/in/henryheinemann

- Cloudflare blocks an average of 57 billion threats per day, including some of the largest DDoS attacks in history.
- Recently the company also started shifting its focus on securing internal networks, rather than just external.
- We will provide examples of high profile cases and give insights into how such "data attacks" can be tackled.

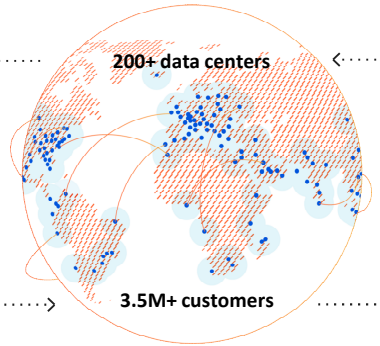
CLOUDFLARE

# We are helping build a better Internet

# Comprehensive coverage against security threats

**Threat hunting based on machine learning using our network data**

- 9100+ Network interconnects
- 738B+ DNS requests per day
- 25M+ Internet properties

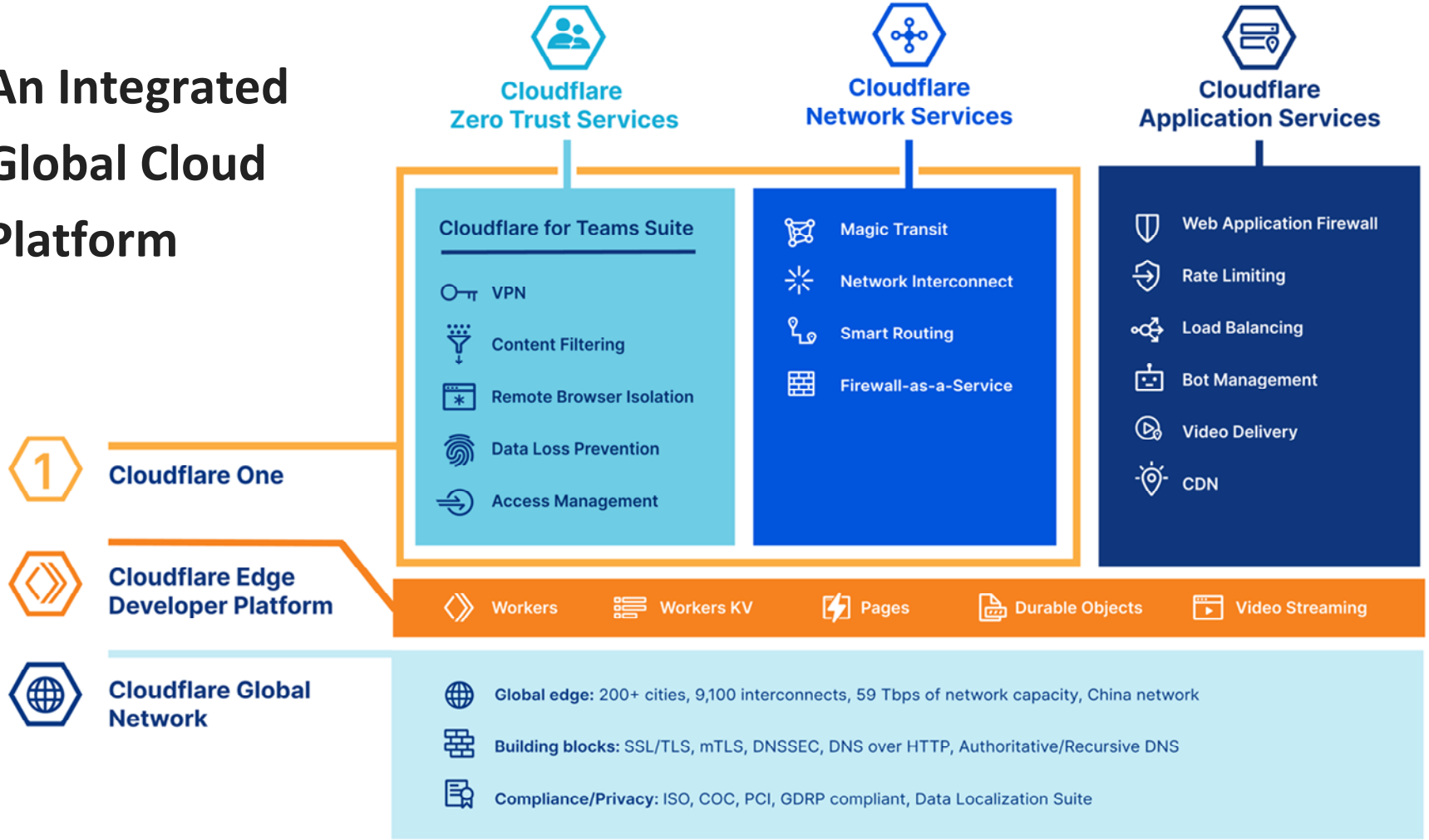



**Threat aggregation based on intelligence from our ecosystem**

- Premium third-party feeds
- OSINT and shared feeds
- Community-provided feedback

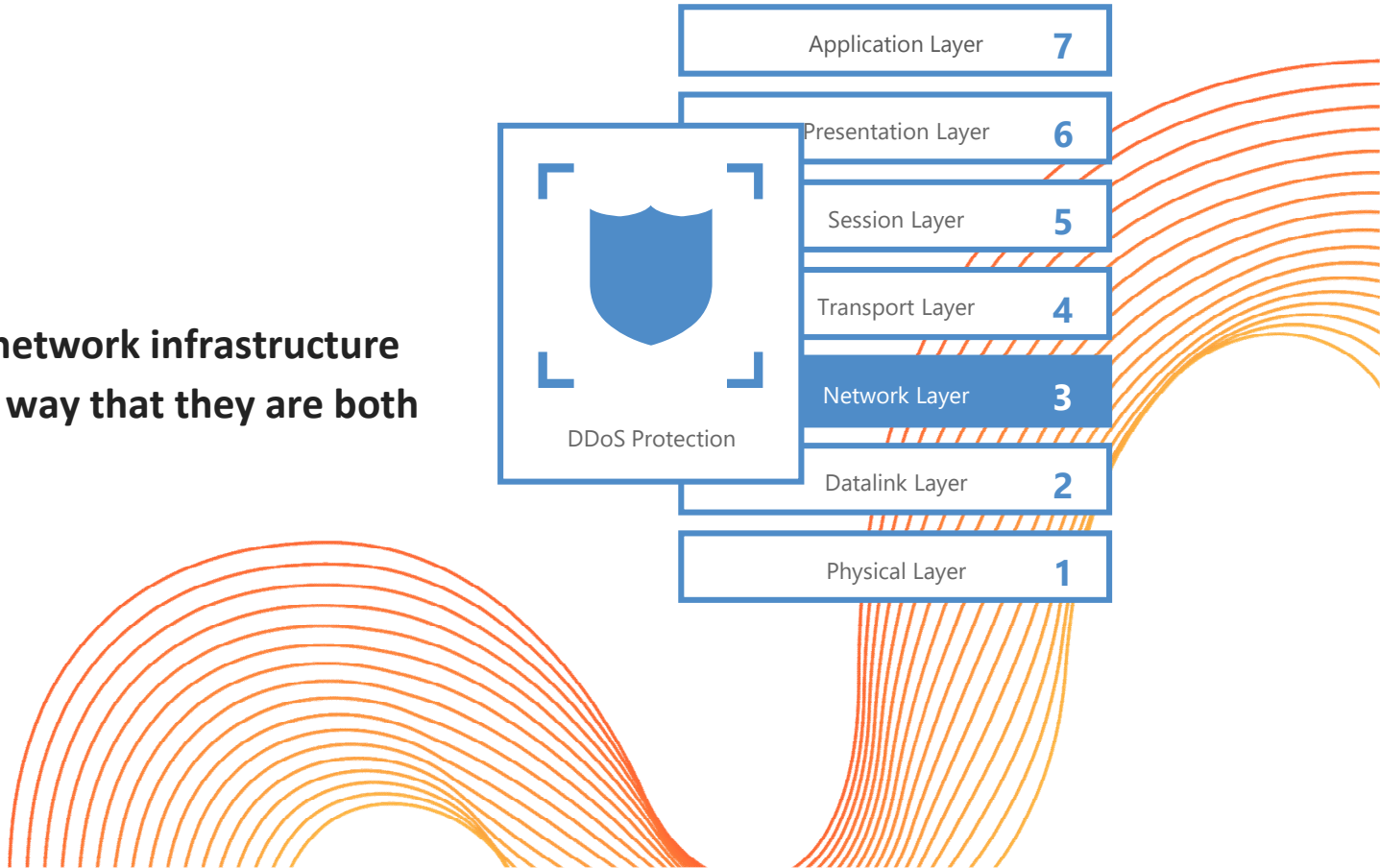
| **Security risk categories to block or isolate per policy rule** | Malware<br>Phishing<br>Cryptomining | Newly seen domains<br>New domains<br>Unreachable domains | C2 & botnet<br>DGA domains<br>DNS tunneling | Spyware<br>Spam<br>Anonymizer |
|---|---|---|---|---|

# An Integrated Global Cloud Platform

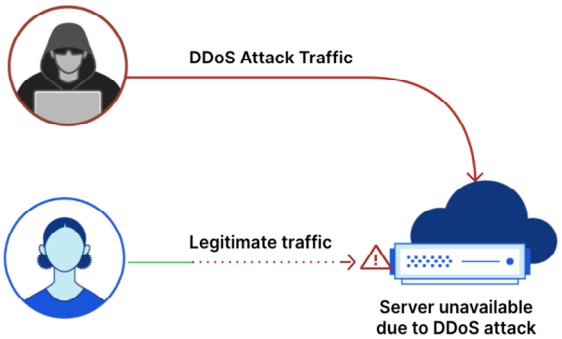


# Networks

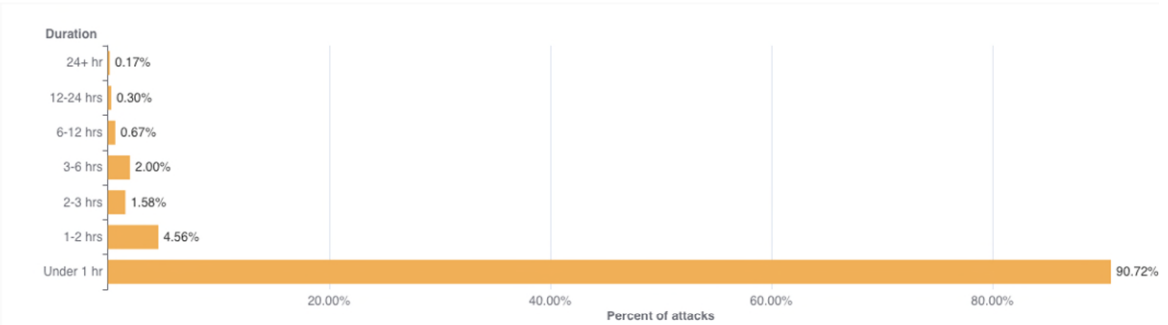
**Secure the underlying network infrastructure from DDoS attacks in a way that they are both fast and secure.**



# DDoS attack trends

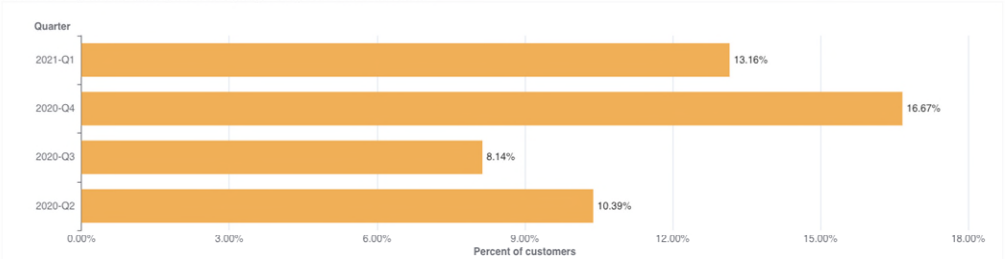



**Network-layer DDoS attacks: Distribution by duration**

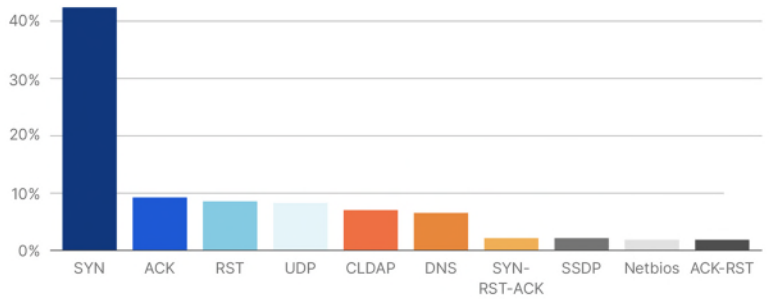



**Ransom DDOS Attacks & Threats**

Percent of respondents that reported being targeted by a ransom DDoS attack




**Network-Layer DDoS Attacks - Top attack vectors**



# Cloudflare helps Wikimedia restore service following a massive DDoS attack

## Challenges

- Target of a massive coordinated DDoS attack campaign of **~300Gbps** of bandwidth, **105MPPS** of TCP ACK traffic, and **340MPPS** of UDP floods
- Significant increase in HTTP response times from servers that were still reachable
- Site accessibility impacted in various regions around the world

## Cloudflare Solution

- Magic Transit protects their on-premise data centers from volumetric attacks
- Even as the attack changed patterns, Magic Transit was a resilient shield protecting Wikimedia's network infrastructure

## Key Results

- Improved resilience and availability
- **Zero performance degradation** due to filtering traffic at the edge
- Valuable partnership with Cloudflare and influence on product roadmap

WIKIMEDIA FOUNDATION

North American non-profit organization that hosts Wikipedia, one of the world's most renowned open collaboration projects.

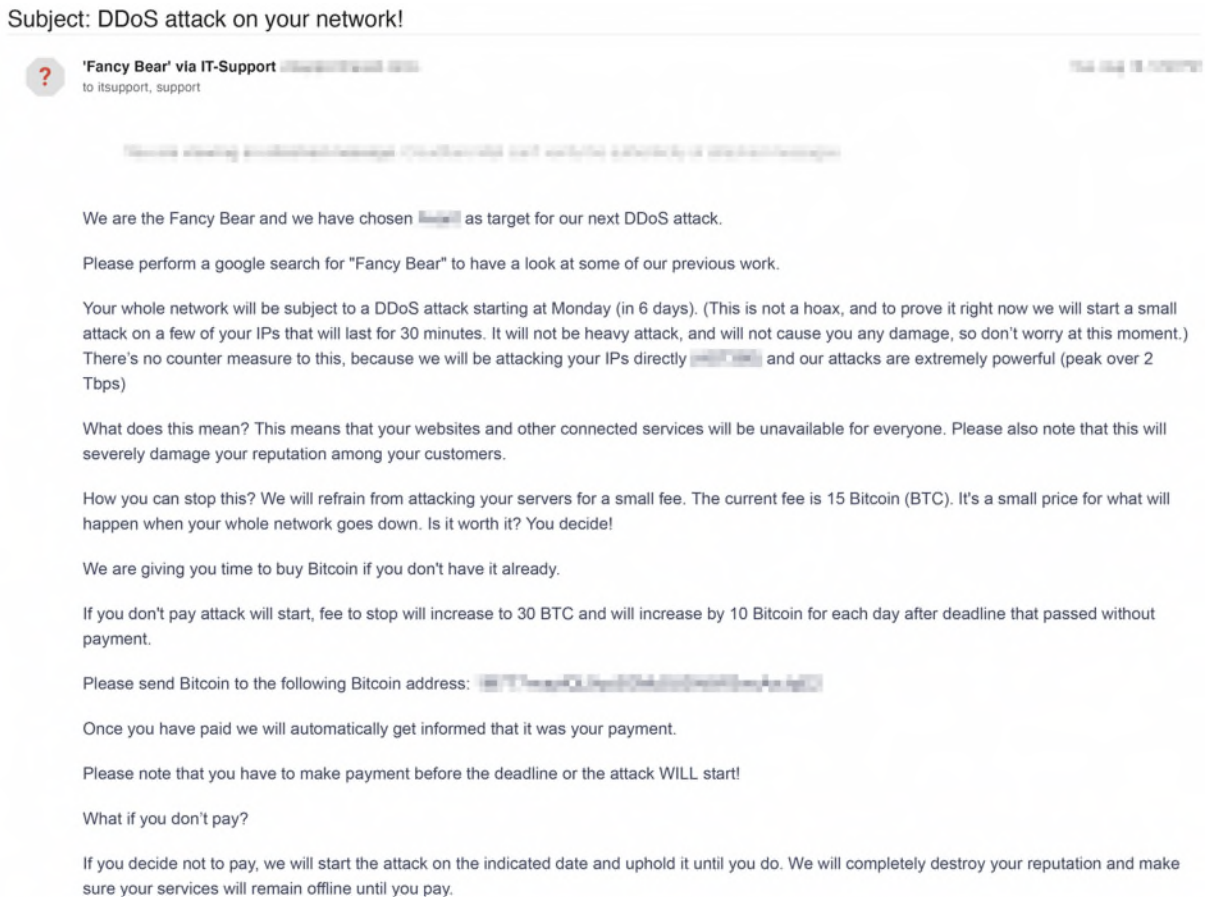
- Founded in 2003
- One of the most visited websites in the world
- Over 25 billion page views monthly
- Hosts 13 collaborative knowledge projects including Wikipedia

Read more: https://www.cloudflare.com/case-studies/wikimedia-foundation/

# Ransom notes

Ransom-DDoS (RDDoS) attacks are on the rise.

- Organizations of all sizes, geos being targeted
- Groups claiming to be Fancy Bear, Cozy Bear, Lazarus
- Launching a test DDoS attack as demonstration
- Demanding ransom (in bitcoin)



Subject: DDoS attack on your network!

**'Fancy Bear' via IT-Support**
to itsupport, support

We are the Fancy Bear and we have chosen as target for our next DDoS attack.

Please perform a google search for "Fancy Bear" to have a look at some of our previous work.

Your whole network will be subject to a DDoS attack starting at Monday (in 6 days). (This is not a hoax, and to prove it right now we will start a small attack on a few of your IPs that will last for 30 minutes. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.) There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

What does this mean? This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers.

How you can stop this? We will refrain from attacking your servers for a small fee. The current fee is 15 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay attack will start, fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day after deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address:

Once you have paid we will automatically get informed that it was your payment.

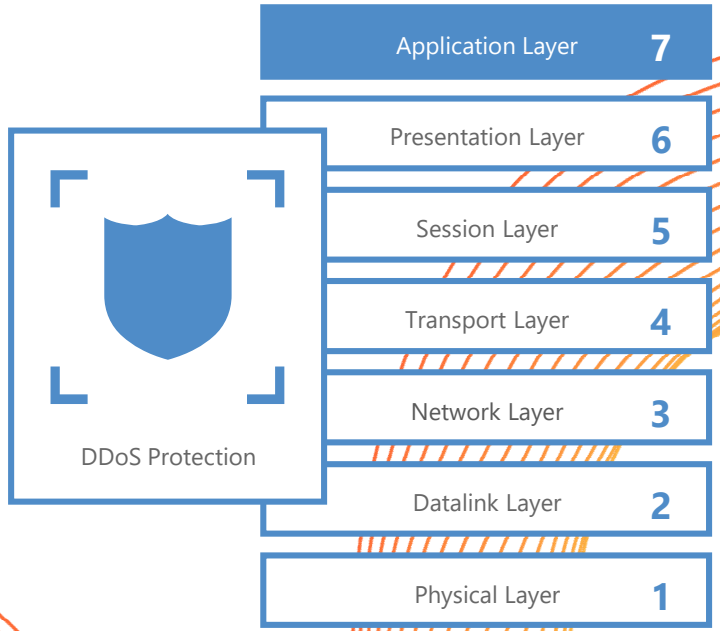
Please note that you have to make payment before the deadline or the attack WILL start!

What if you don't pay?

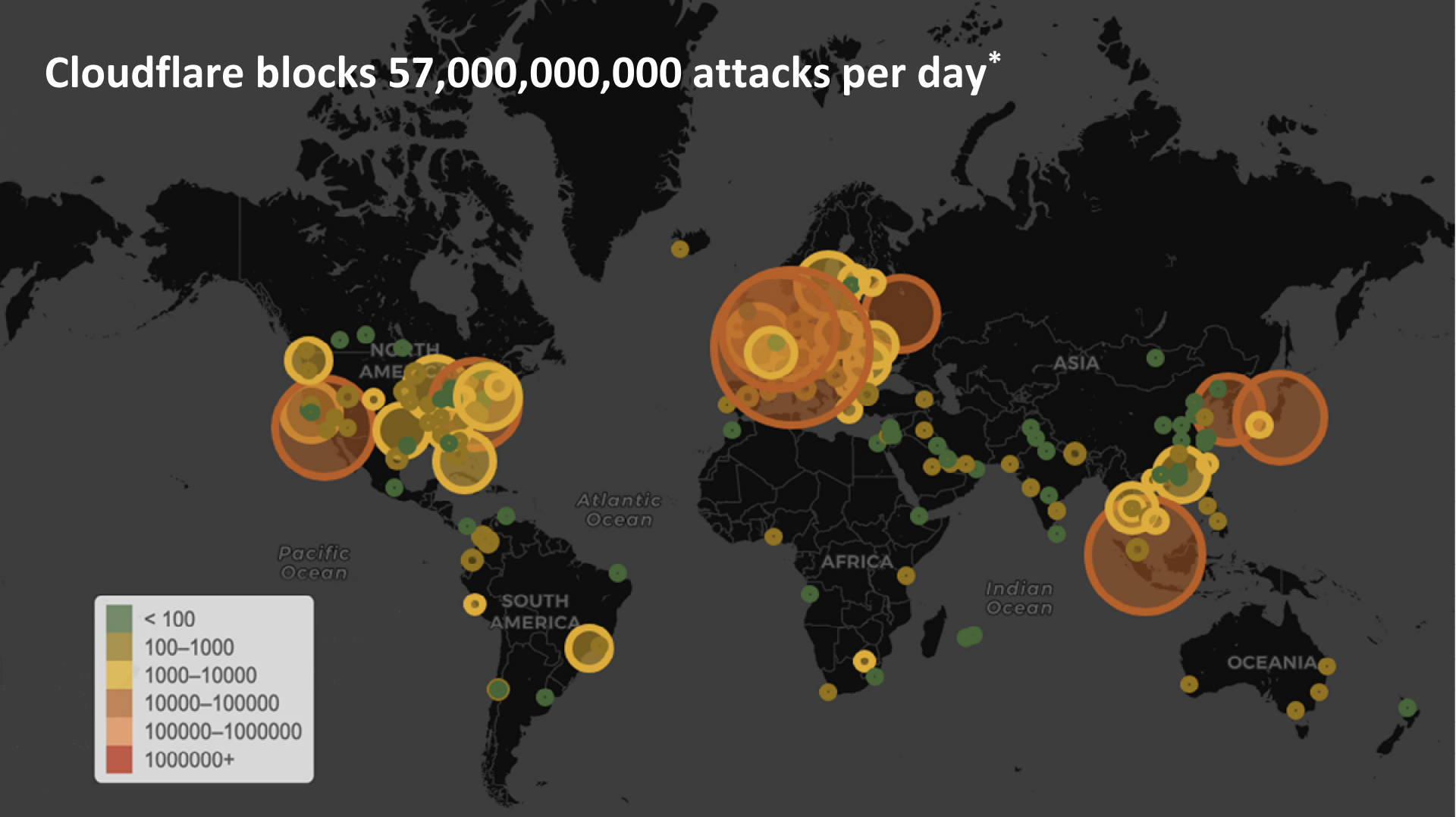
If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

# Applications

**Protect external facing applications from DDoS attacks, bots, zero day exploits and other security incidents.**



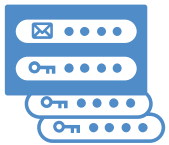
# Cloudflare blocks 57,000,000,000 attacks per day*



CLOUDFLARE

# 40%

of web traffic is bots



Credential Stuffing


Content Scraping

Content Spam

Inventory Holding

Credit Card Stuffing

CLOUDFLARE

lastminute.com

**Worldwide travel company**

**40 countries**

**60MM unique visitors/month**

**Situation:**

- Overwhelmed by bot traffic and scraper bots.
- Ruined analytics and led to mining of site for pricing and availability data.
- Existing provider created an unnecessary layer of complexity and obfuscation.

CLOUDFLARE

lastminute.com

**200,000**

Attacks blocked each month

**20%**

Performance gain

**“By consolidating our security and performance providers into a single service we’ve lowered our total cost of ownership — and Cloudflare’s solution is much easier to use than our previous setup.”**

**— Mirco Patroncini**

Director of Platform Engineering, lastminute.com

# Account Takeovers

the majority of account takeover attacks start from one of three initial attack vectors:

- An attacker compromised Remote Desktop Protocol (RDP) or Virtual Private Network (VPN) servers
- An attacker exploited an unpatched vulnerability in a web application or server
- An attacker spear-phished key individuals to gain a foothold in the target environment


**61 %**
of breaches were caused by outsiders.

**74 %**
of breaches were financially motivated.

**37 %**
of breaches were attacks on web applications, more than double the results from last year.

**24 %**
of malware incidents can be attributed to ransomware.

CLOUDFLARE

# Teams

**Protects enterprises, their devices, and their data by securing every connection without compromising user performance.**

CLOUDFLARE

## Zero trust & Data Loss Prevention

**Do not automatically trust** anything inside or outside perimeters.

**Verify everything** trying to connect to systems before granting access.

1. **Audit Trail**
2. **RBAC**
3. **Safety Net**
4. **Filter**

# Cloudflare Access: Our origin story

**Challenges**

- ‘On call’ engineers were fed up with clunky VPN login experience to access internal apps like Grafana during time-sensitive assignments
- Setting access control policies on the VPN was onerous for the IT team
- Our standalone VPN was becoming a performance bottleneck and a single point of failure for a rapidly expanding global workforce

**Solution**

Our engineers first built Access in 2015 to speed up their logins, and we have progressively shifted authentication for the majority of our internal applications onto our global network edge. Today, all employees onboard onto Access (not our VPN) and benefit from a fast and consistent login experience to every application.

**Value**

- Get employees access to the resources they need without friction
- Modernize our security posture with Zero Trust best practices
- Improved employee productivity:
    - $100K+ savings in IT support staff productivity
    - ~80% reduced time spent servicing VPN related tickets
    - ~70% reduction in ticket volume
    - 300+ annual hours of unlocked productivity during onboarding

“As a CIO, I'm proud that I don't have to worry about our colleagues getting frustrated with reaching the basic tools they need to stay productive. With Access, Cloudflare does not have to make any trade-offs between improving security and creating an amazing user experience.”

- **Juan Rodriguez**, Chief Information Officer

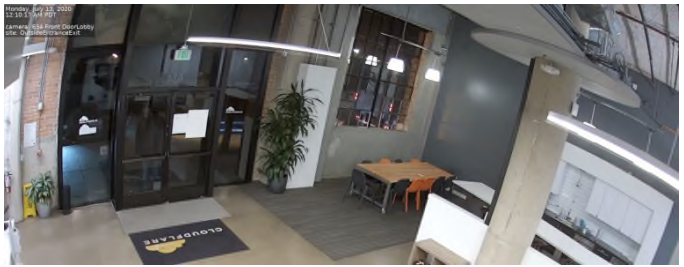
Link to Public Case Study

# Verkada Hack

tillie crimew (APT-69420 Arson Cats 🔥) @nyancrim...

let me just clarify again, we (APT-69420 Arson Cats) had root shells inside the corporate networks of both CloudFlare and Okta.

if we wanted to we could have probably owned half the internet in like a week.



tillie crimew (APT-69420 Arson Cats 🔥) 18h

we will not elaborate whether it would have been possible to pivot into @eastdakota's laptop, whether we did it or if we even considered doing it.

APT-69420 wishes all companies affected a very have fun doing incident response.

Bloomberg

Cybersecurity

## Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals

By William Turton

9 March 2021, 22:32 CET *Updated on 10 March 2021, 17:35 CET*

- Hacker group says it wanted to show prevalence of surveillance
- Video footage was captured from Sequoia-backed startup Verkada

CLOUDFLARE

# “I want to protect my user identities from being phished and my data from being accessed by phishers.”

Remote worker clicks Workday email link to workdayy.cm

Gateway policy isolates uncategorized site and **disables keyboard input** for newly seen domain

Browser isolated; **user cannot enter credentials**

Remote worker clicks link on unmanaged device and is phished

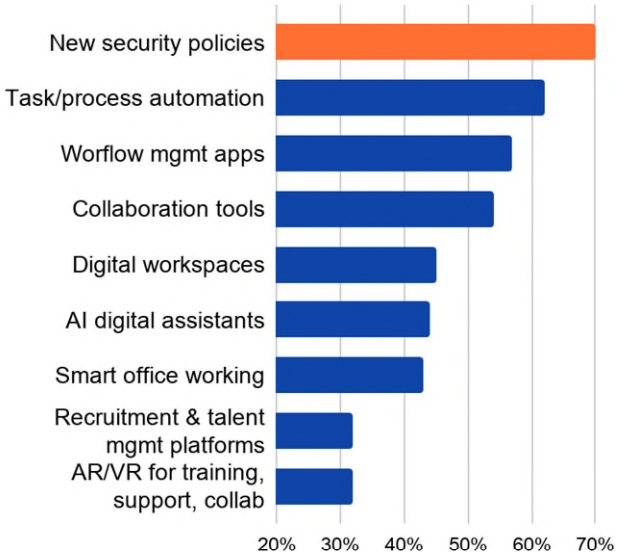
Access prevents phisher due to **incomplete MFA requirement**

workday
workdayy.cm

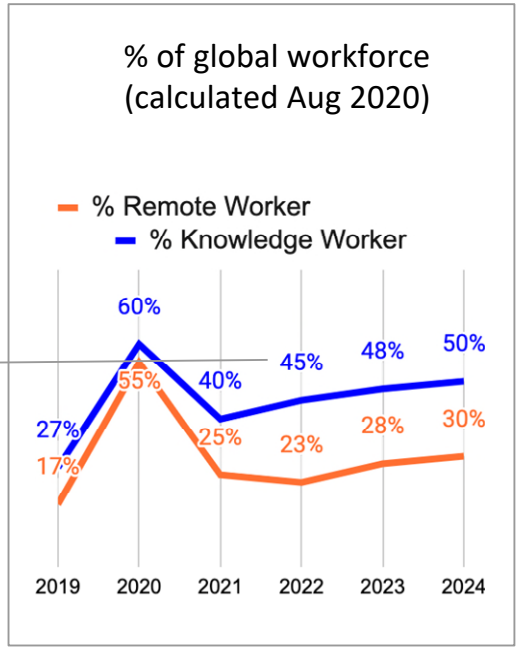
Logs user, device, location, request details

# Remote work surged in 2020. What's next?

Digital initiatives you expect to see a significant change in your org's 2021 investments




- By 2022, **budgets for modern secure access solutions will quadruple** as flaws in legacy VPN solutions are illuminated by the massive WFH migration.
- Permanently remote knowledge workers will increase to **45% in 2022**. And by 2023, 60% will work remotely at least part time.



CLOUDFLARE

# Thank You!

hh@cloudflare.com
linkedin.com/in/henryheinemann/