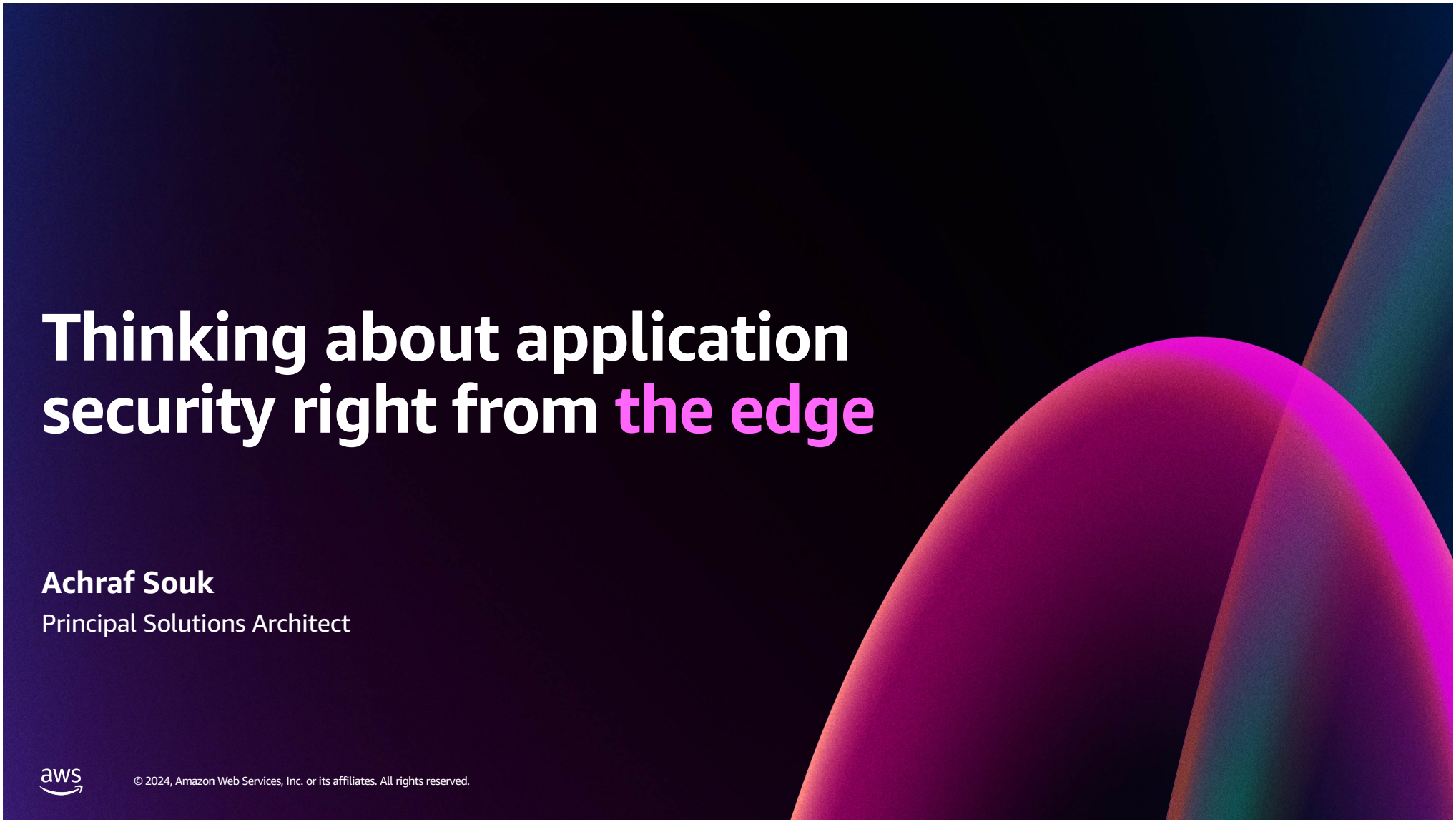
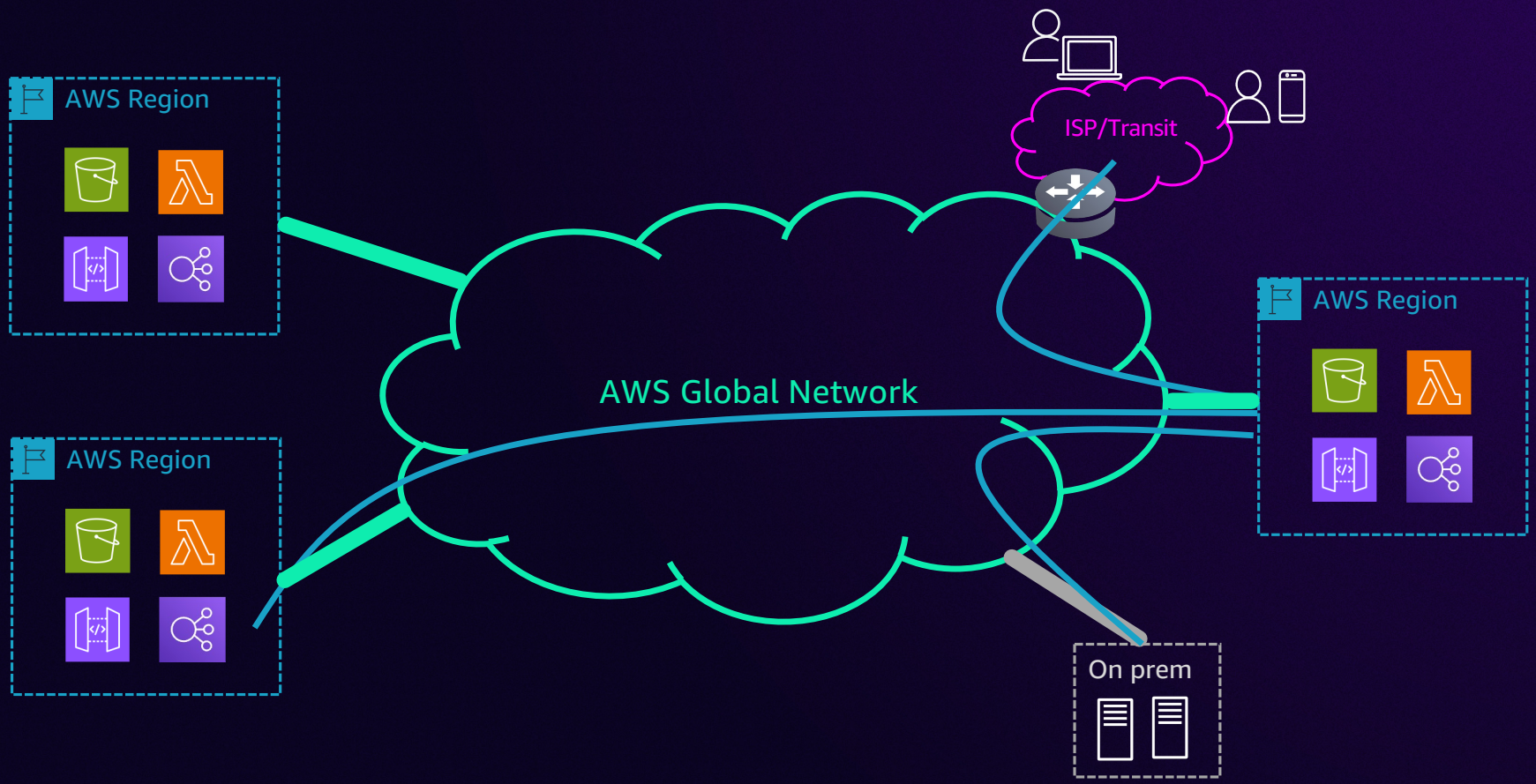
Thinking about application security right from the edge

Achraf Souk
Principal Solutions Architect

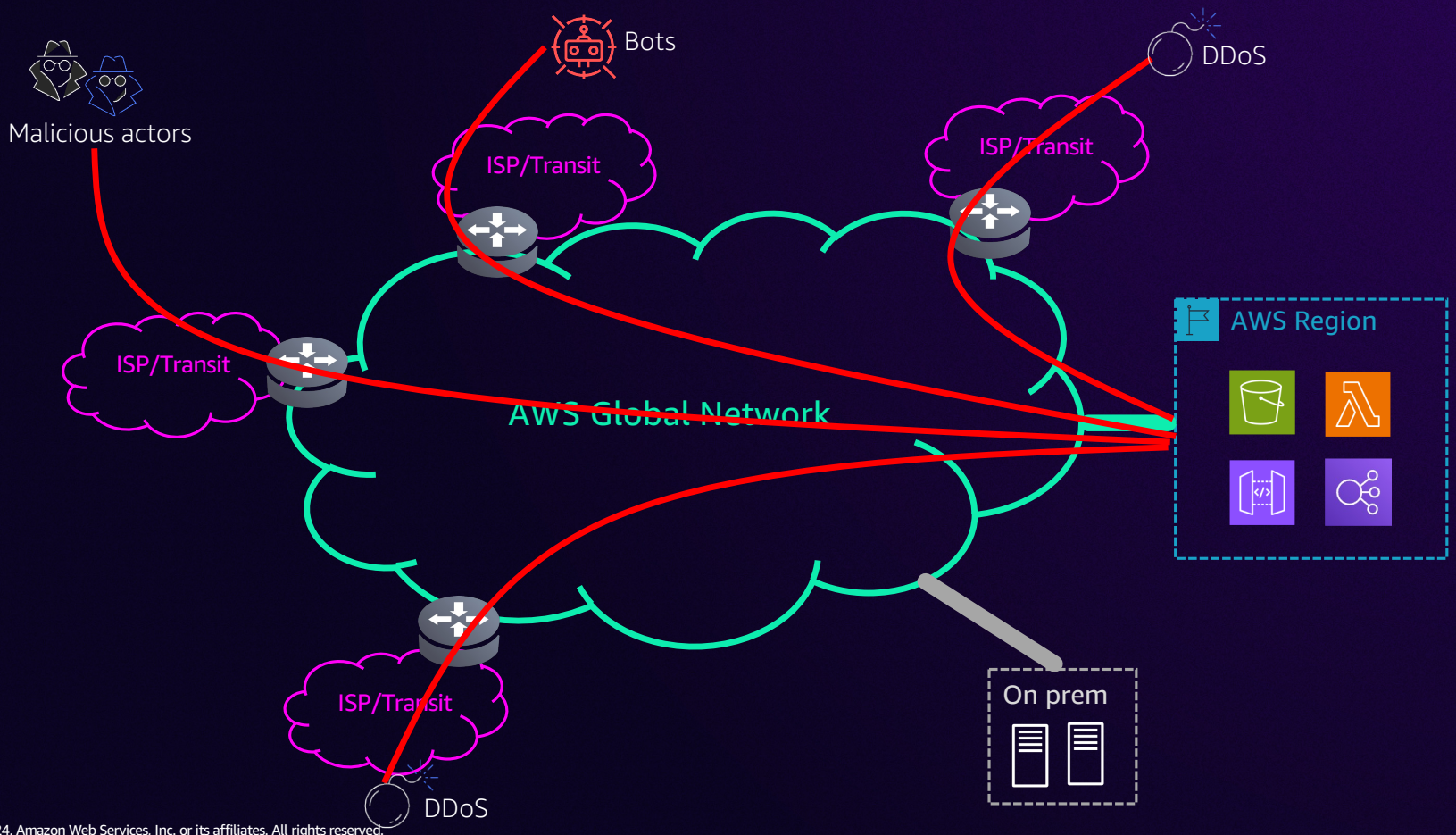



The edge?

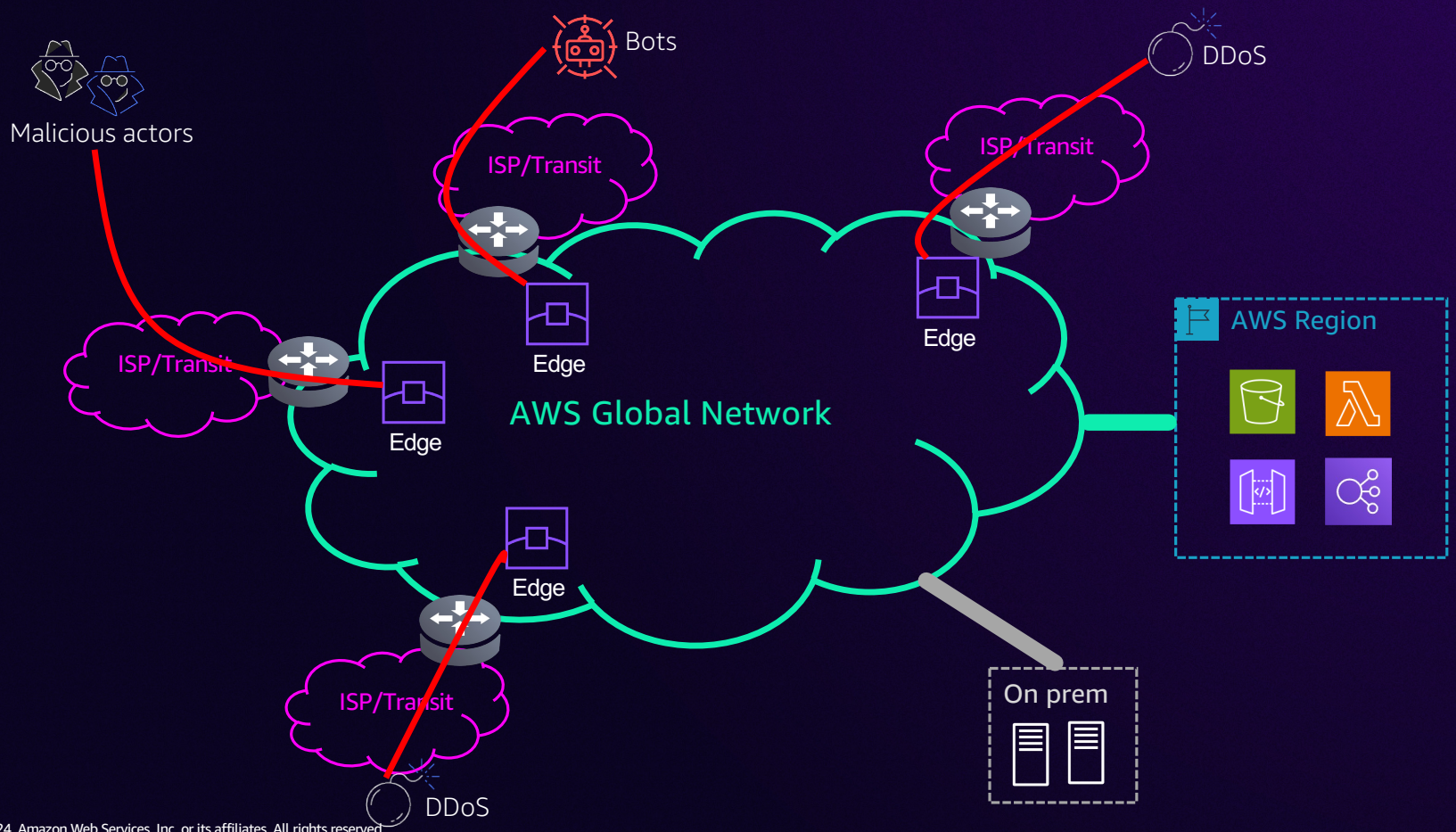
Primer on AWS Global Network



Primer on AWS Global Network



Primer on AWS Global Network



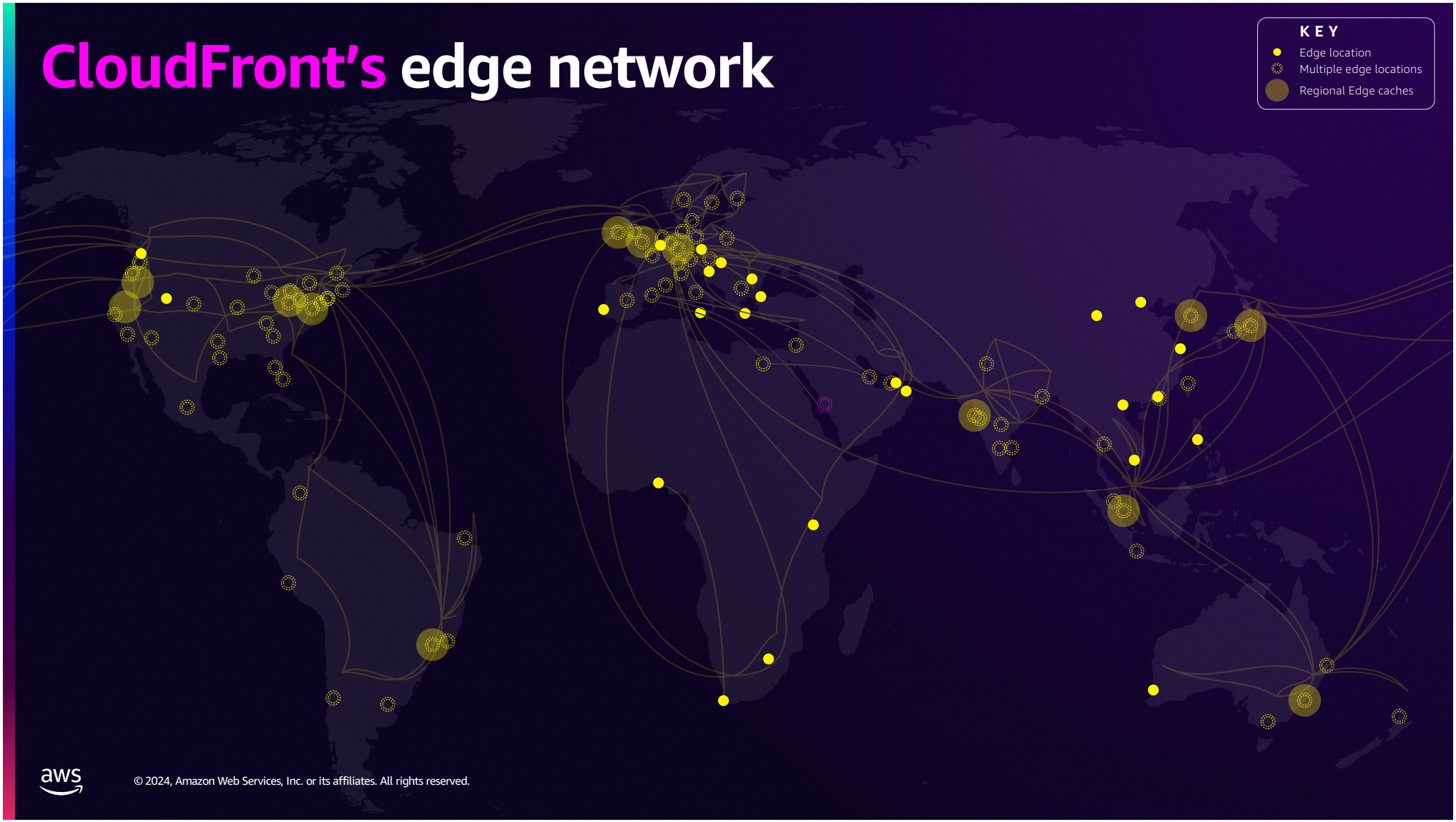
AWS Edge services

Amazon
Route 53

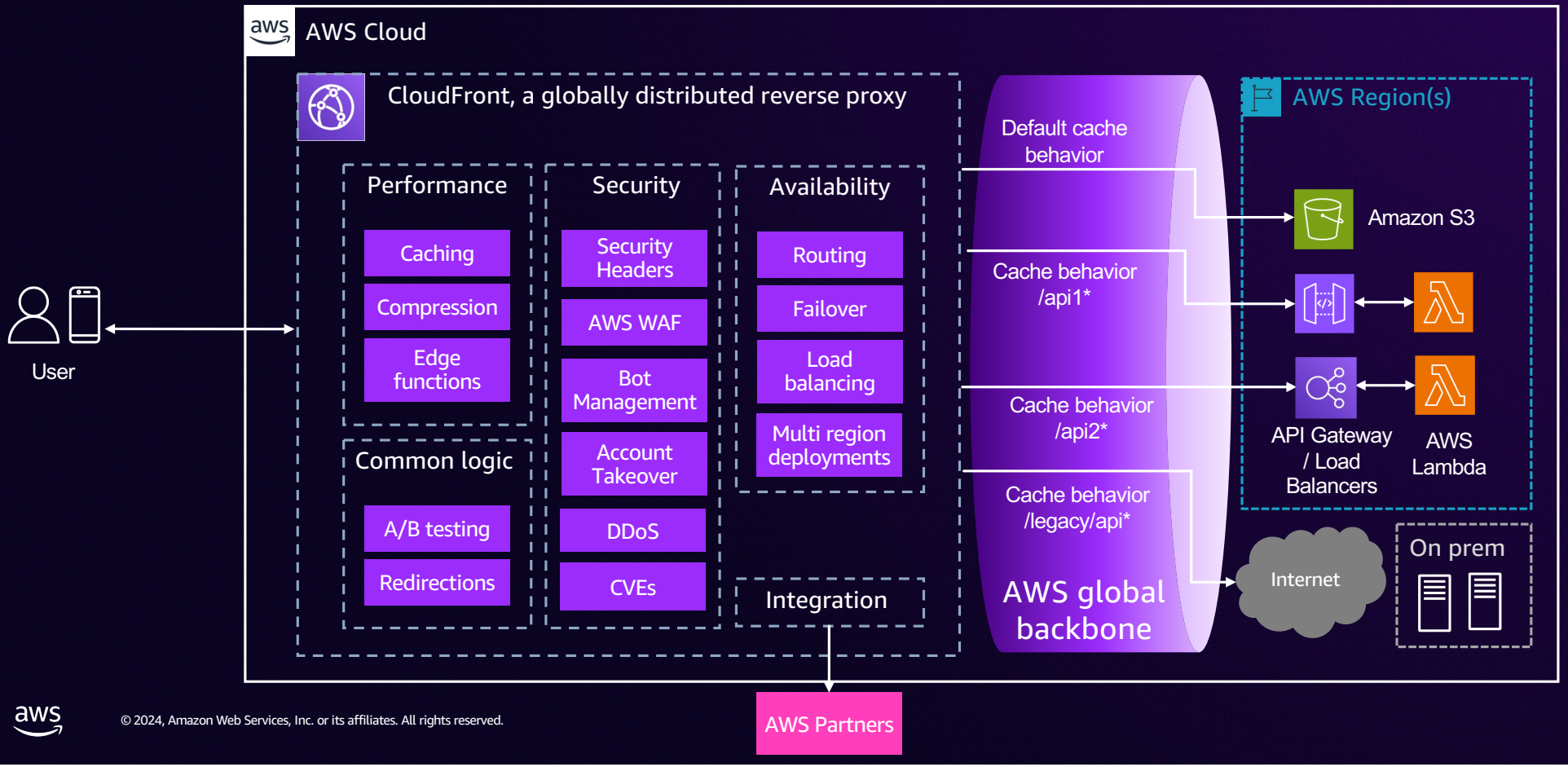
Amazon
CloudFront

AWS Global
Accelerator

CloudFront's edge network



Mental model for CloudFront



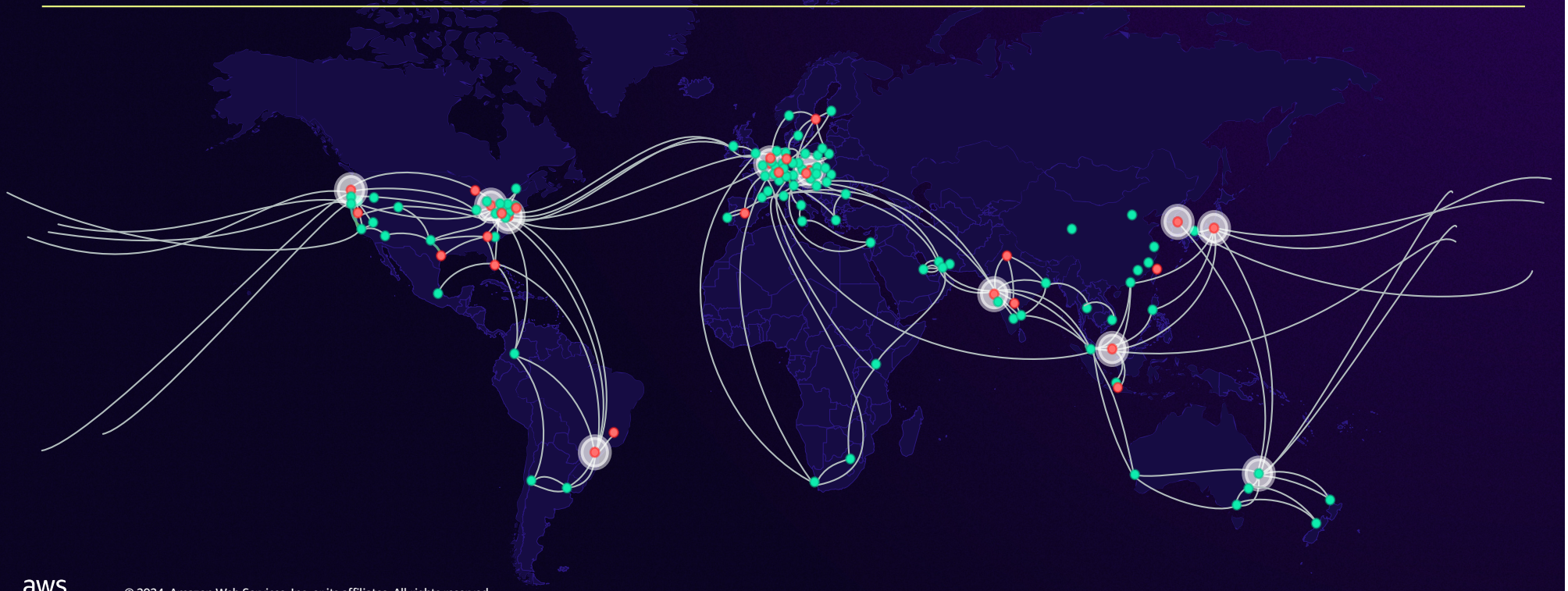
Security at the edge

Scale of AWS threat intelligence

Thousands of DDoS attacks mitigated every day

100+ billion AWS managed rules requests processed per day

Exabytes of data are analyzed every 60 sec



How AWS uses active defense to protect you

MadPot	Sonaris	Mithra
Globally-distributed **network of honeypot** threat sensors with automated response capabilities	An **active defense tool** that analyzes potentially harmful network traffic	An internal **neural network graph model** that uses algorithms for threat intelligence
Observe and react to threat actors' evolving tactics, techniques, and procedures (TTPS)	Deny attempts to find unintentionally public S3 buckets and vulnerable services	Ranks domain trustworthiness to help protect customers from threats

Honeypots of Madpot

100M

Volume of potential threat interactions observed daily, WW

500K

of observed activities that are classified as malicious

90secs

Time taken for workload to be discovered by probes

From threat data to actionable intelligence

Case Study - Anonymous Sudan

United States Attorney's Office
Central District of California

About CDCA | Find Help | Contact Us

Search

About | Meet the U.S. Attorney | News | Divisions | Programs | Community Engagement | Employment | Contact Us

Justice.gov > U.S. Attorneys > Central District of California > Press Releases > Two Sudanese Nationals Indicted For Alleged Role In Anonymous Sudan Cyberattacks On Hospitals, Government Facilities, and Other Critical Infrastructure In Los Angeles and Around The World

PRESS RELEASE

Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks on Hospitals, Government Facilities, and Other Critical Infrastructure in Los Angeles and Around the World

Wednesday, October 16, 2024

Share

For Immediate Release
U.S. Attorney's Office, Central District of California

LOS ANGELES–A federal grand jury indictment unsealed today charges two Sudanese nationals with operating and controlling Anonymous Sudan, an online cybercriminal group responsible for tens of thousands of Distributed Denial of Service (DDoS) attacks against critical infrastructure, corporate networks, and government agencies in the United States and around the world.

In March 2024, pursuant to court-authorized seizure warrants, the U.S. Attorney's Office and FBI seized and disabled Anonymous Sudan's powerful DDoS tool, which the group allegedly used to perform DDoS attacks, and sold as a service to other criminal actors.

Ahmed Salah Yousif Omer, 22, and Alaa Salah Yusuuf Omer, 27, were both charged with one count of conspiracy to damage protected computers. Ahmed Salah was also charged with three counts of damaging protected computers.

"Anonymous Sudan sought to maximize havoc and destruction against governments and businesses around the world by perpetrating tens of thousands of cyberattacks," said United States Attorney Martin Estrada. "This group's attacks were callous and brazen—the defendants went so far as to attack hospitals providing emergency and urgent care to patients. My office is committed to safeguarding our nation's infrastructure and the people who use it, and we will hold cyber criminals accountable for the grave harm they cause."

"The FBI's seizure of this powerful DDoS tool successfully disabled the attack platform that caused widespread damage and disruptions to critical infrastructure and networks around the world," said Special Agent in Charge Rebecca Day of the FBI Anchorage Field Office. "With the FBI's mix of unique authorities, capabilities, and partnerships, there is no limit to our reach when it comes to combating all forms of cybercrime and defending global cybersecurity."

"These charges and the results of this investigation, made possible through law enforcement and private sector partnerships, have an immeasurable impact on the security of networks in the U.S. and of its allies, and demonstrates the resolve of the Defense Criminal Investigative Service (DCIS) to safeguard the Department of Defense from evolving cyber threats," said Kenneth A. DeChellis, DCIS Cyber Field Office, Special Agent in Charge. "Cybercriminals need to understand that if they target America's warfighters, they will face consequences."

amazon

Who We Are | What We Do | Our Workplace | Our Impact | Our Planet | Follow Us | Subscribe | EN

News / AWS

5 min

October 16, 2024

Amazon helps the US Department of Justice thwart international cybercriminal group Anonymous Sudan

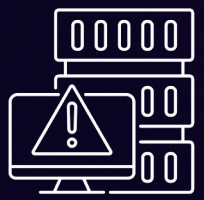
Written by Amazon Staff

5 min

Reading:
Amazon helps the US Department of Justice thwart international

Two individuals behind the Anonymous Sudan cybercriminal group were indicted by the U.S. Department of Justice, which acknowledged AWS for its contributions.

Evolution of threat landscape



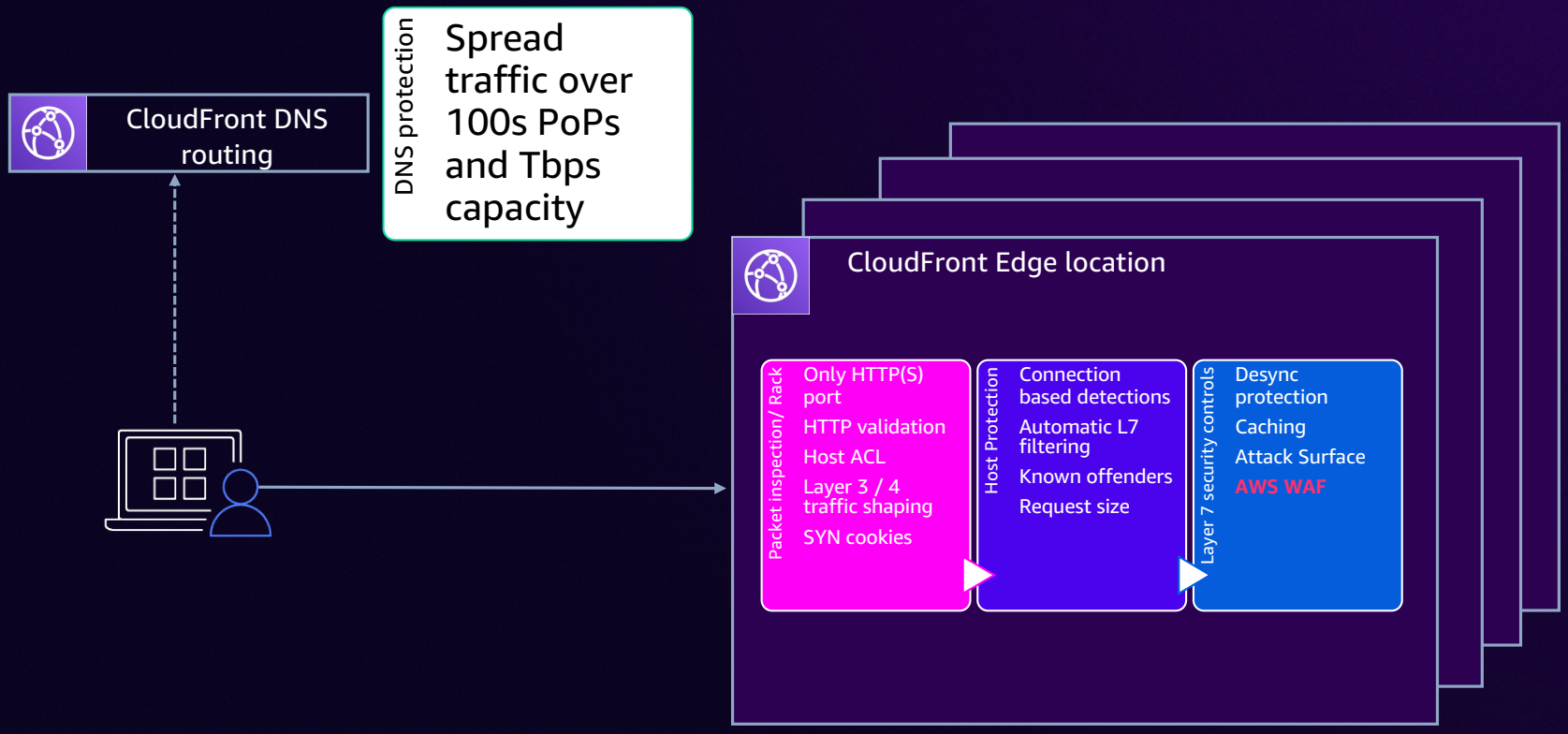
56%

of DDoS attacks observed target applications

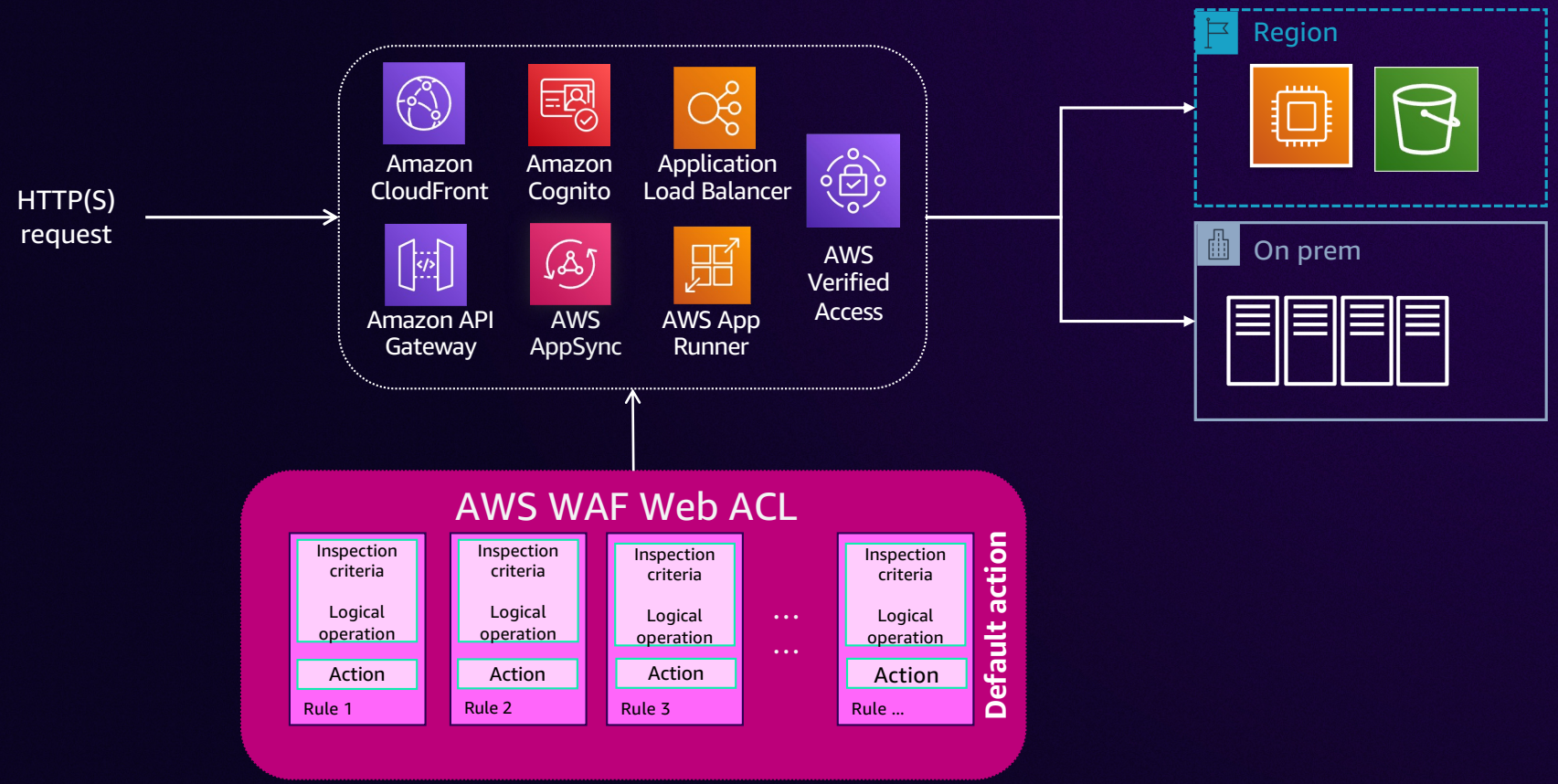
42%

of overall web traffic is composed of bots, and **65%** are malicious.

CloudFront's native security

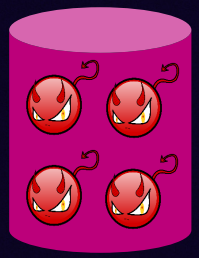


How does AWS WAF work?



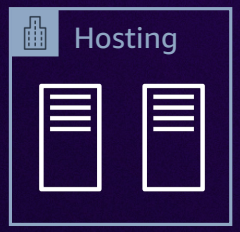
Defense in depth using WAF
Example of DDoS Protection

1. Based on signature – IP reputation



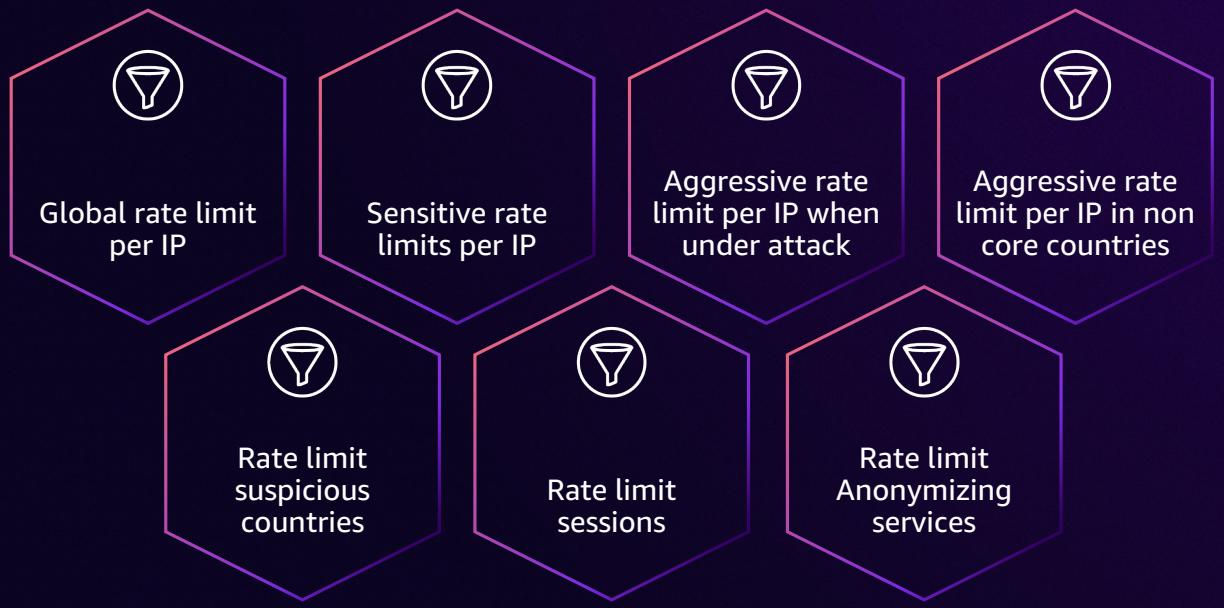
Amazon IP reputation based on AWS threat intelligence

Anonymous IPs from AWS or from Marketplace



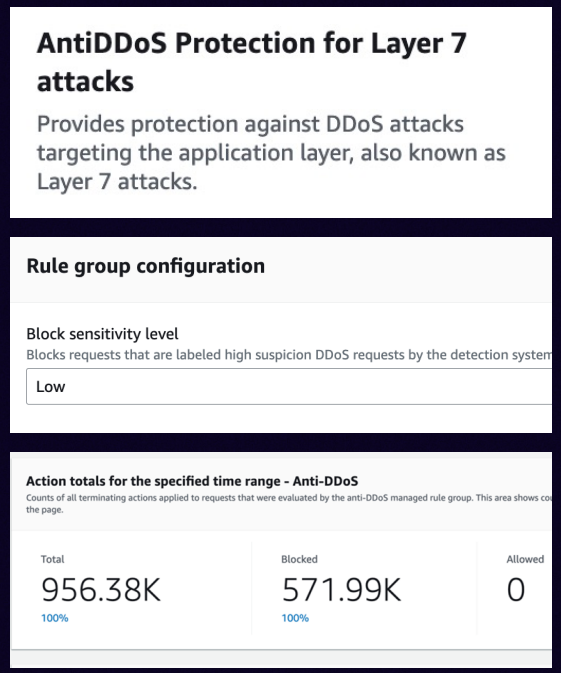
IPs from Hosting Providers

3. Based on signature – Rate limits



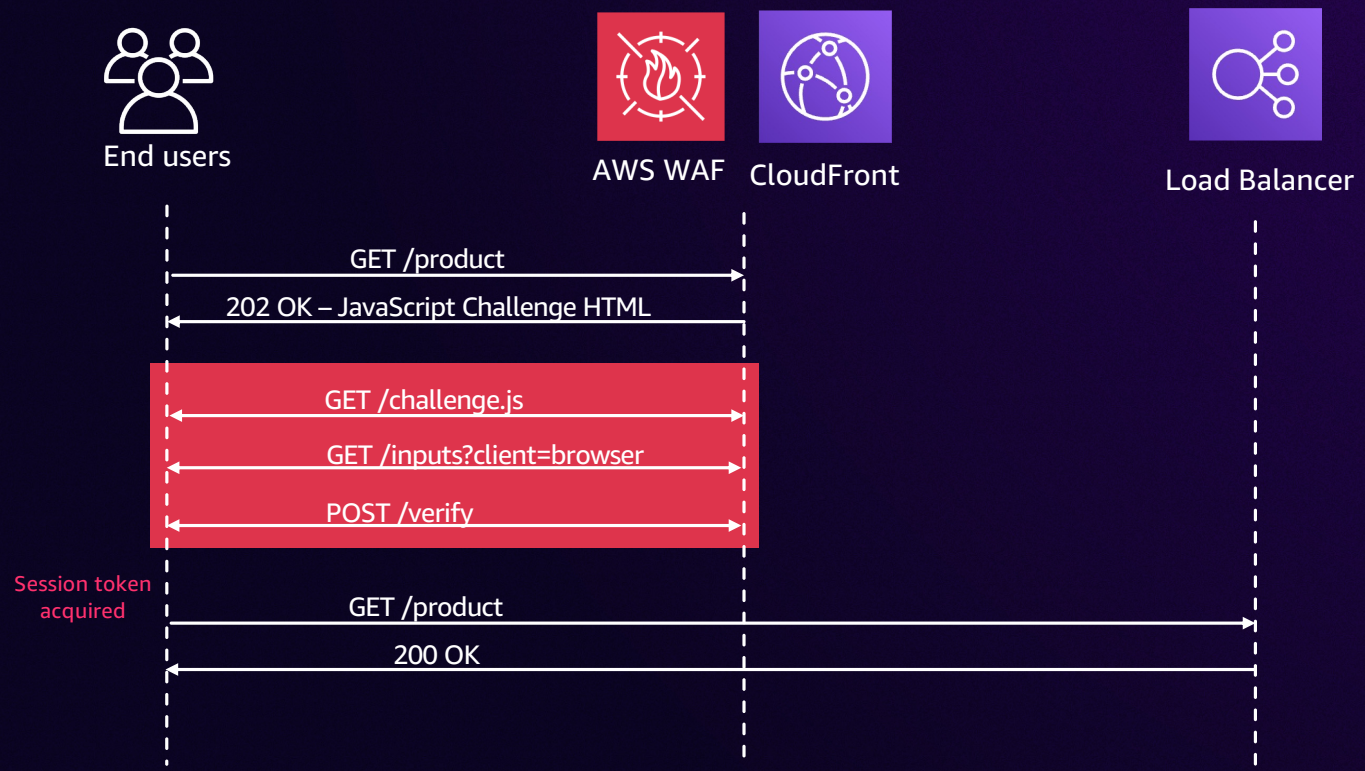
4. Based on client side interrogation

🚀 Announcing AWS WAF Anti-DDoS Managed rule in preview 🚀



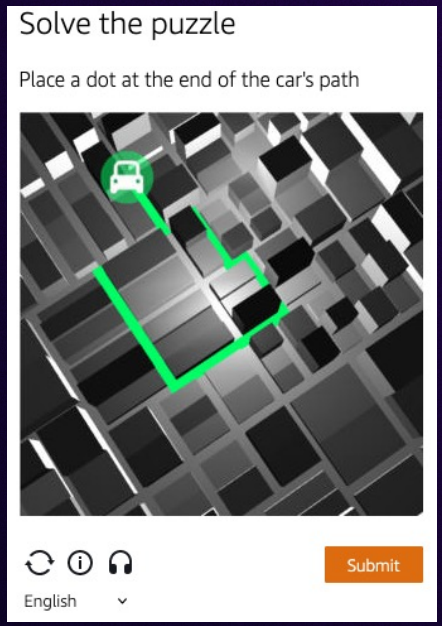
- Mitigation in seconds
- High accuracy
- Granular control
- Native dashboards

JavaScript Challenge – Token acquisition

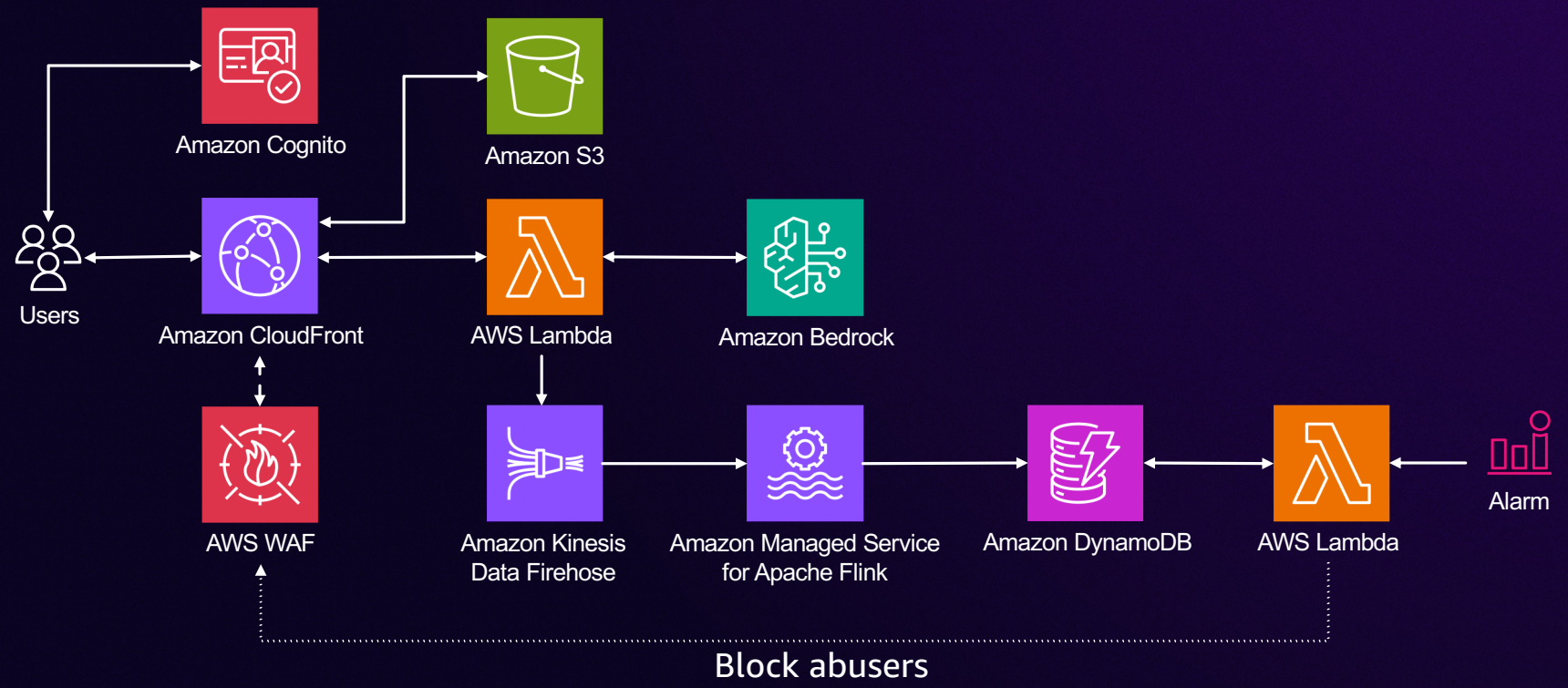


5. Based on behavioral analysis – Bot Control

- Client-side fingerprinting to detect automation frameworks
- Behavioral analysis using session token
- Machine Learning based detection of coordinated activities
- CAPTCHA challenge

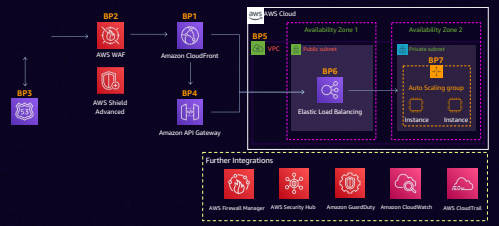


6. Based on behavioral analysis – App signals

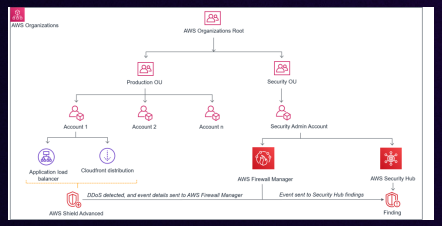


More resiliency against DDoS attacks

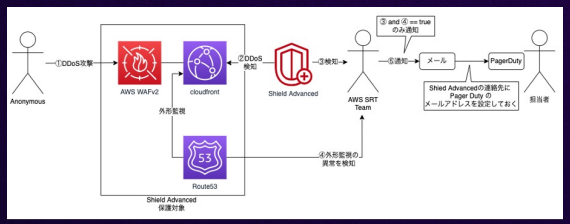
Architecture



Governance



Incident Response



Resource – Application Security & Performance

Thank you!

Achraf Souk

/in/achrafsouk

Your feedback is important!