

AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

NET207

A deep dive on the current security threat landscape with AWS

Fola Bolodeoku

AWS Security Engineer, Anti DDoS

obbolode@amazon.com

Steve Bollers

AWS Partner Solutions Architect, Security

sboller@amazon.com



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Our sources



AWS Shield, Managed DDoS Protection Service



AWS WAF, Web Application Firewall Service



Amazon GuardDuty, Intelligent Threat Detection Service



AWS Customer Incident Response Team (CIRT), 24/7 Security Event Support

Key services referenced

 **AWS CloudTrail**, Secure standardized logging of account activity

 **AWS Config**, Assesses, audits, and evaluates AWS resource configurations

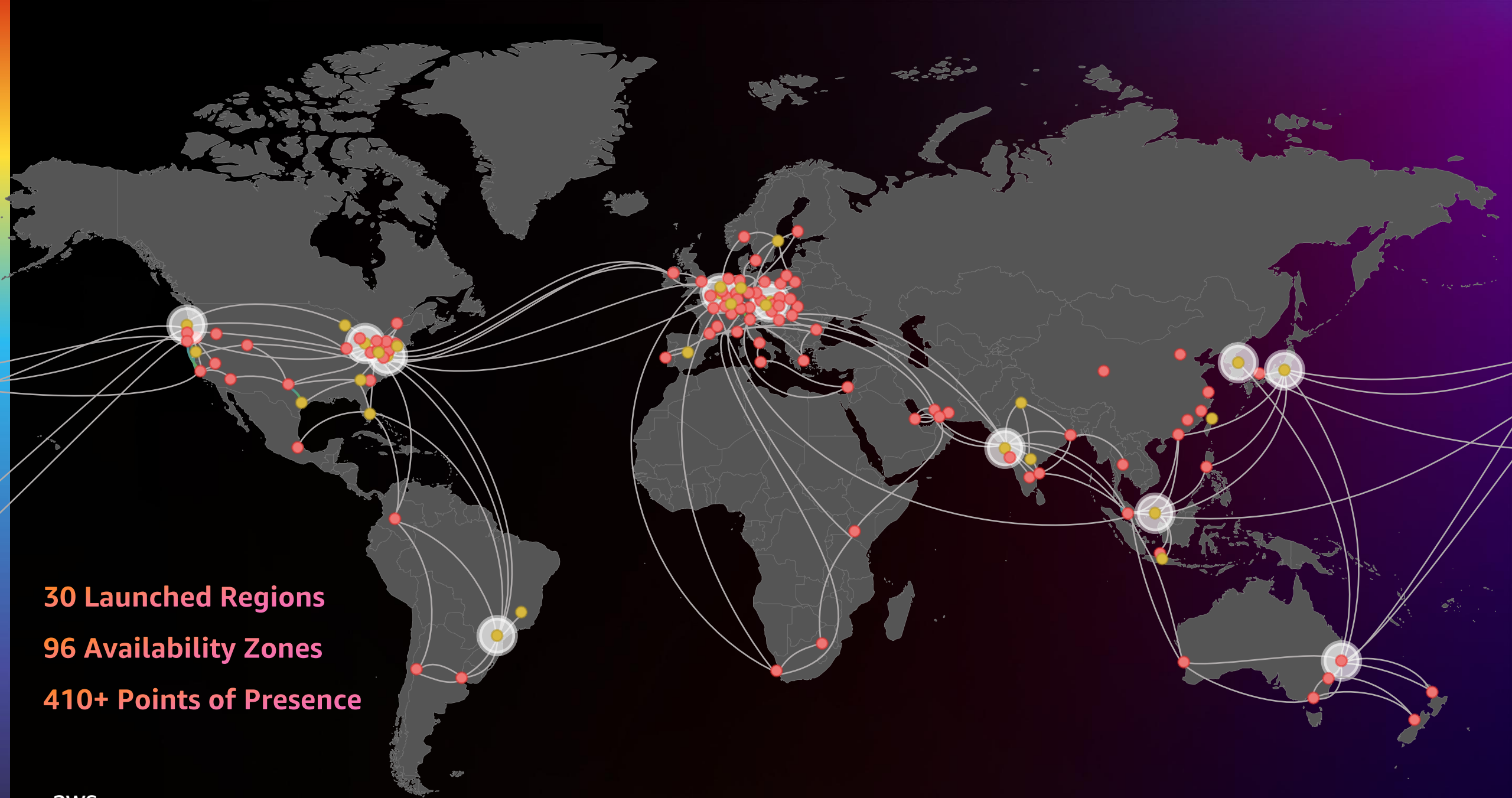
 **AWS Systems Manager**, Provides centralized management for AWS resources

 **Amazon EventBridge**, Real-time access to changes in data in AWS

Agenda

- Common attacks attempted on AWS Infrastructure and applications
- How AWS protects you
- Standing up to DDoS on AWS
- Common AWS account and resource threats
- The leading cause of AWS customer security events
- Key takeaways

Common attacks attempted on AWS Infrastructure and applications



30 Launched Regions
96 Availability Zones
410+ Points of Presence



What does AWS see most?



DDoS



Web exploits



Botnet

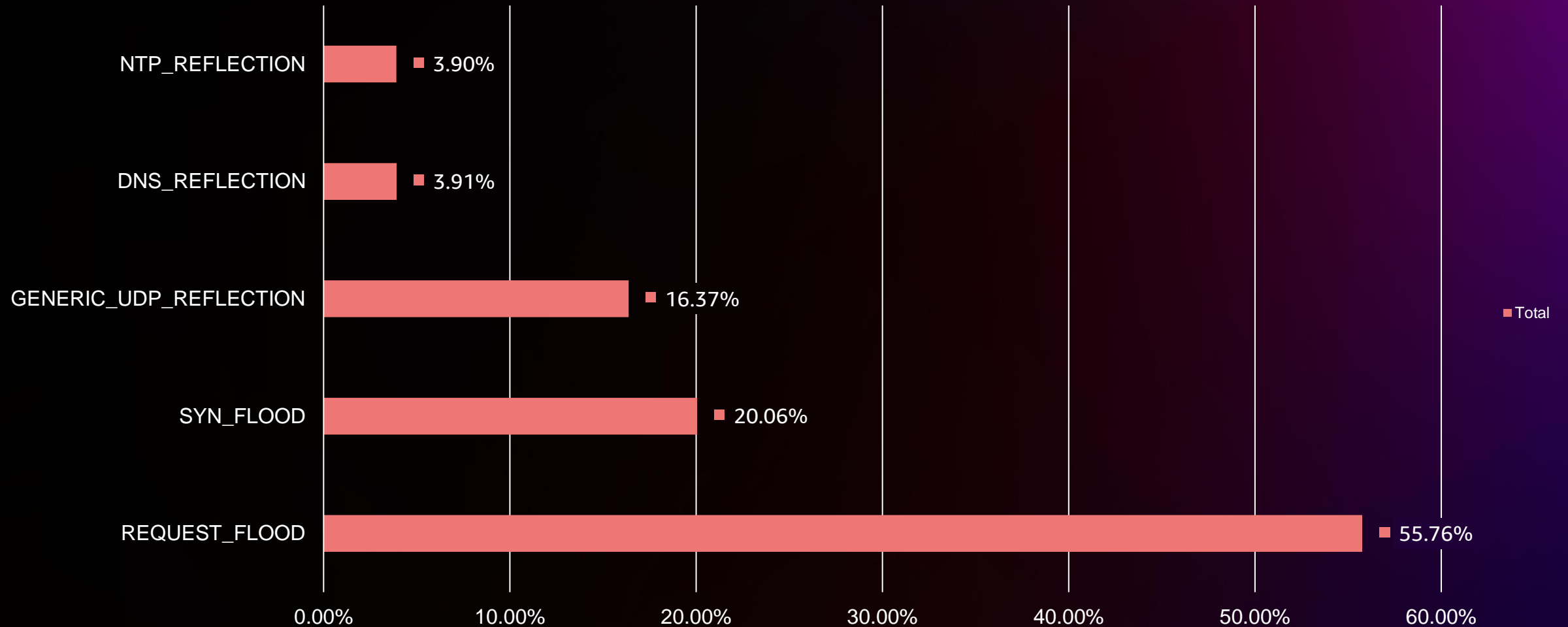
Volumetric events

673,541

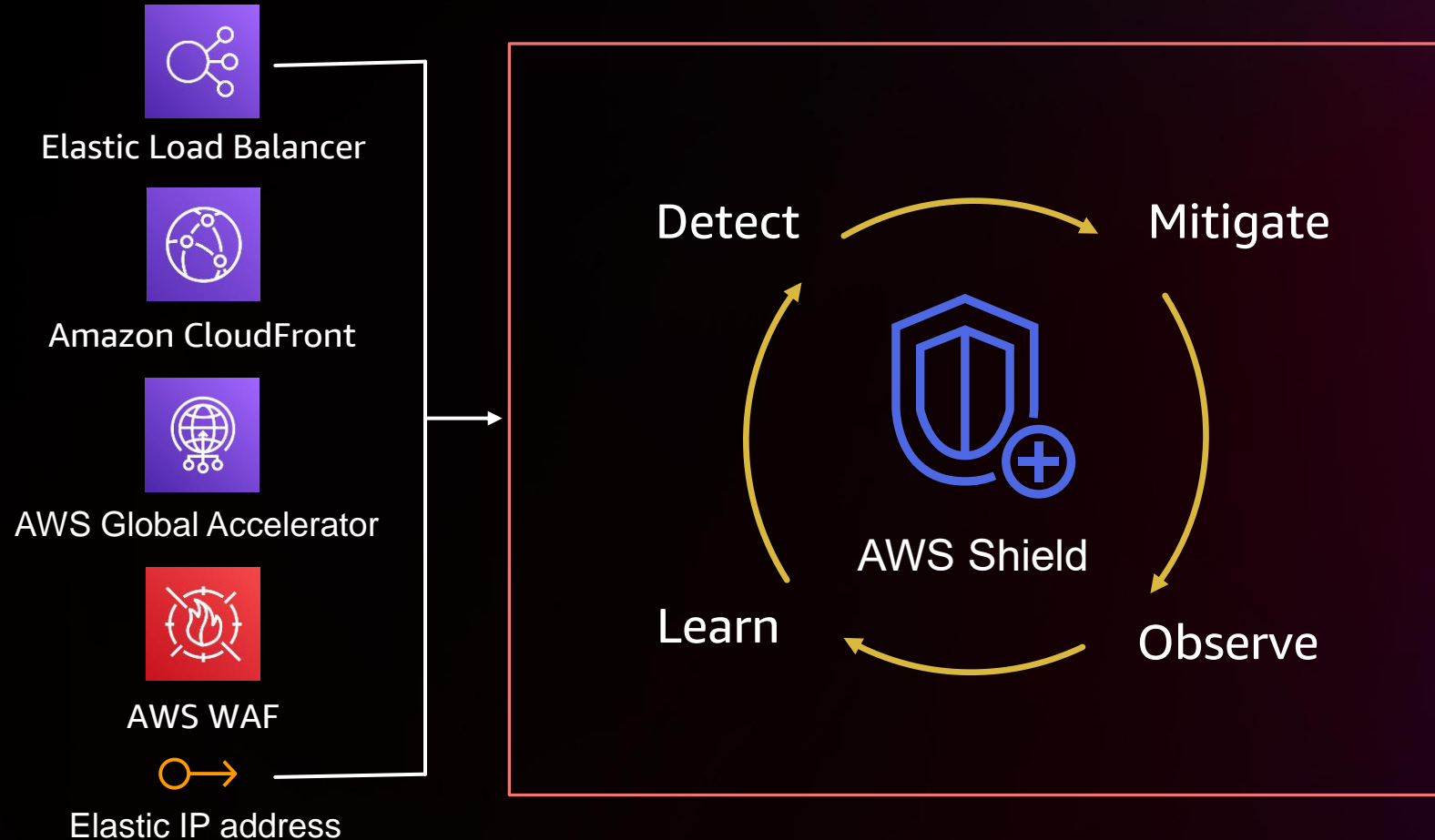
2022 Q1-Q3
DDoS events

+39% from 2021 Q1-Q3

Top 5 DDoS vectors in 2022

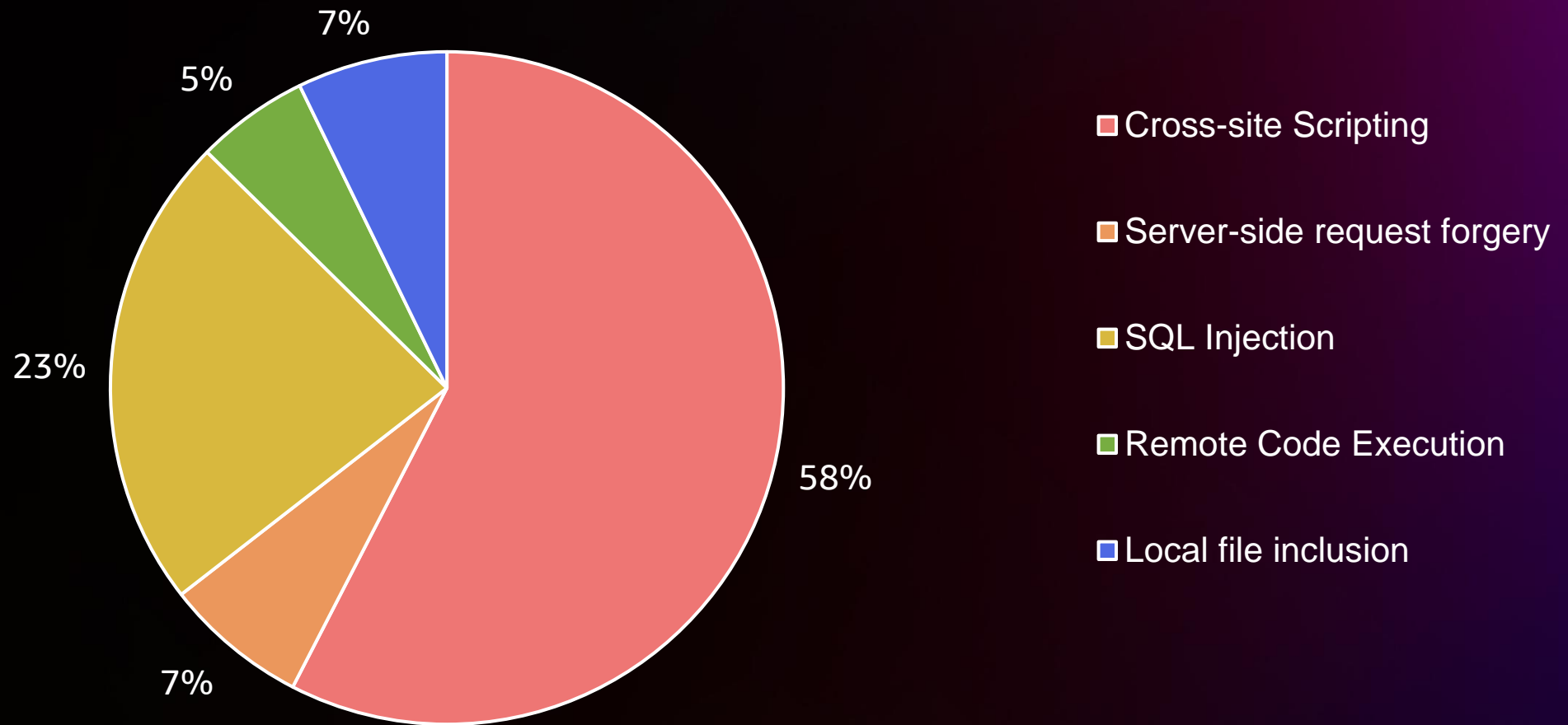


AWS Shield



Check out Breakout Session **NET314**: Building DDoS resilient applications using AWS Shield

Attempted exploits of web app vulnerabilities



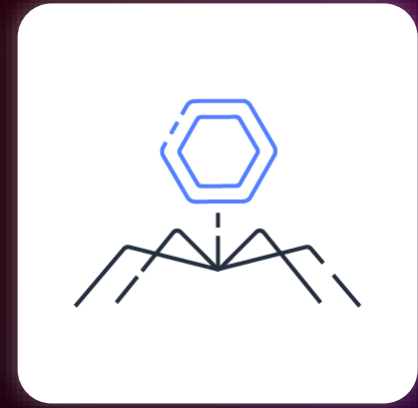
AWS Managed Rules for common web threats



Baseline



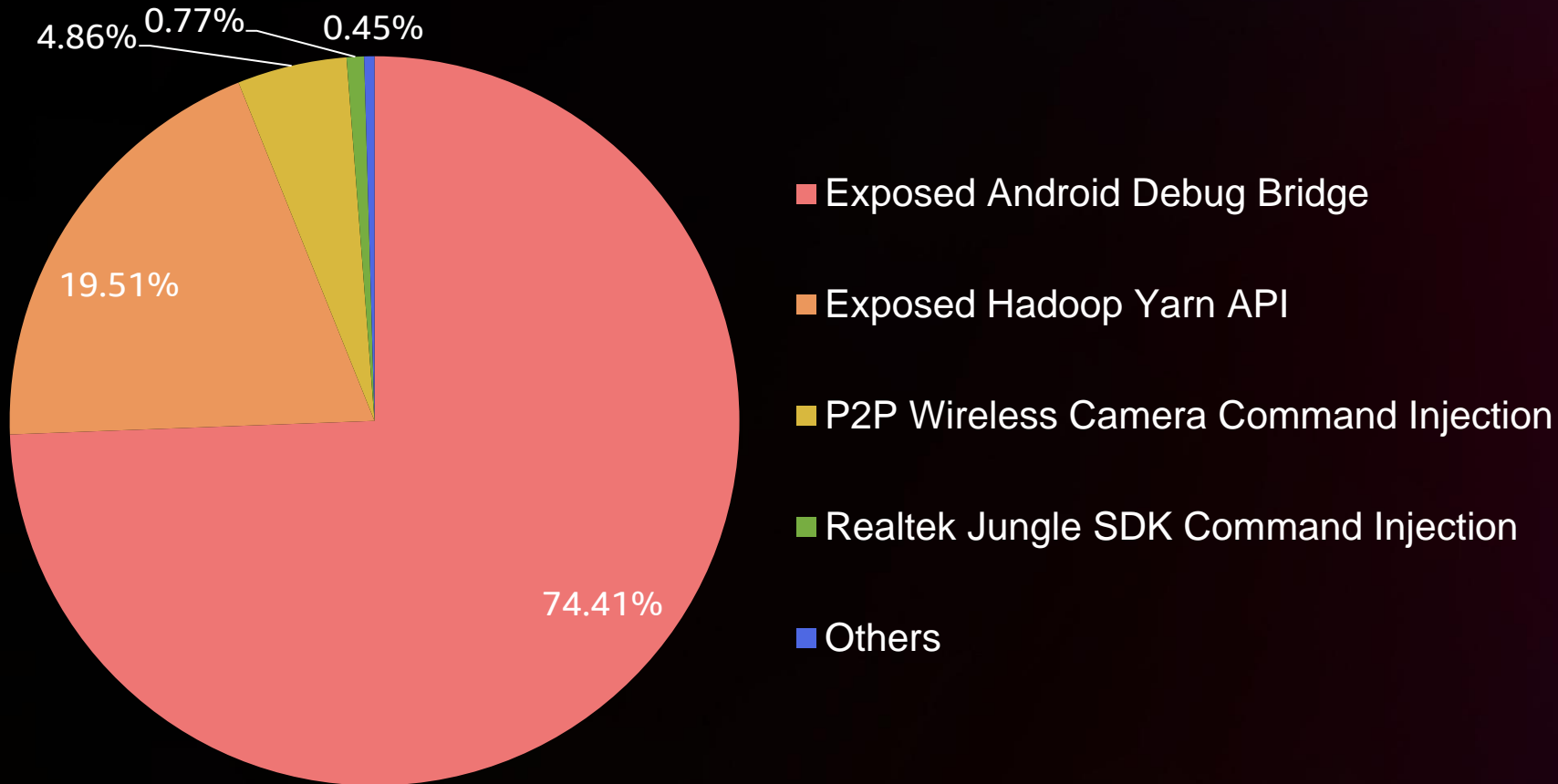
Use-case
Specific



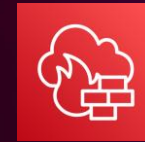
IP Reputation
List

Learn more about WAF in our Builder Session NET318-R:
Protect your application security perimeter with AWS WAF

Top 5 attack vectors for botnet malware



**Update managed
firewall rules**



AWS
Network
Firewall



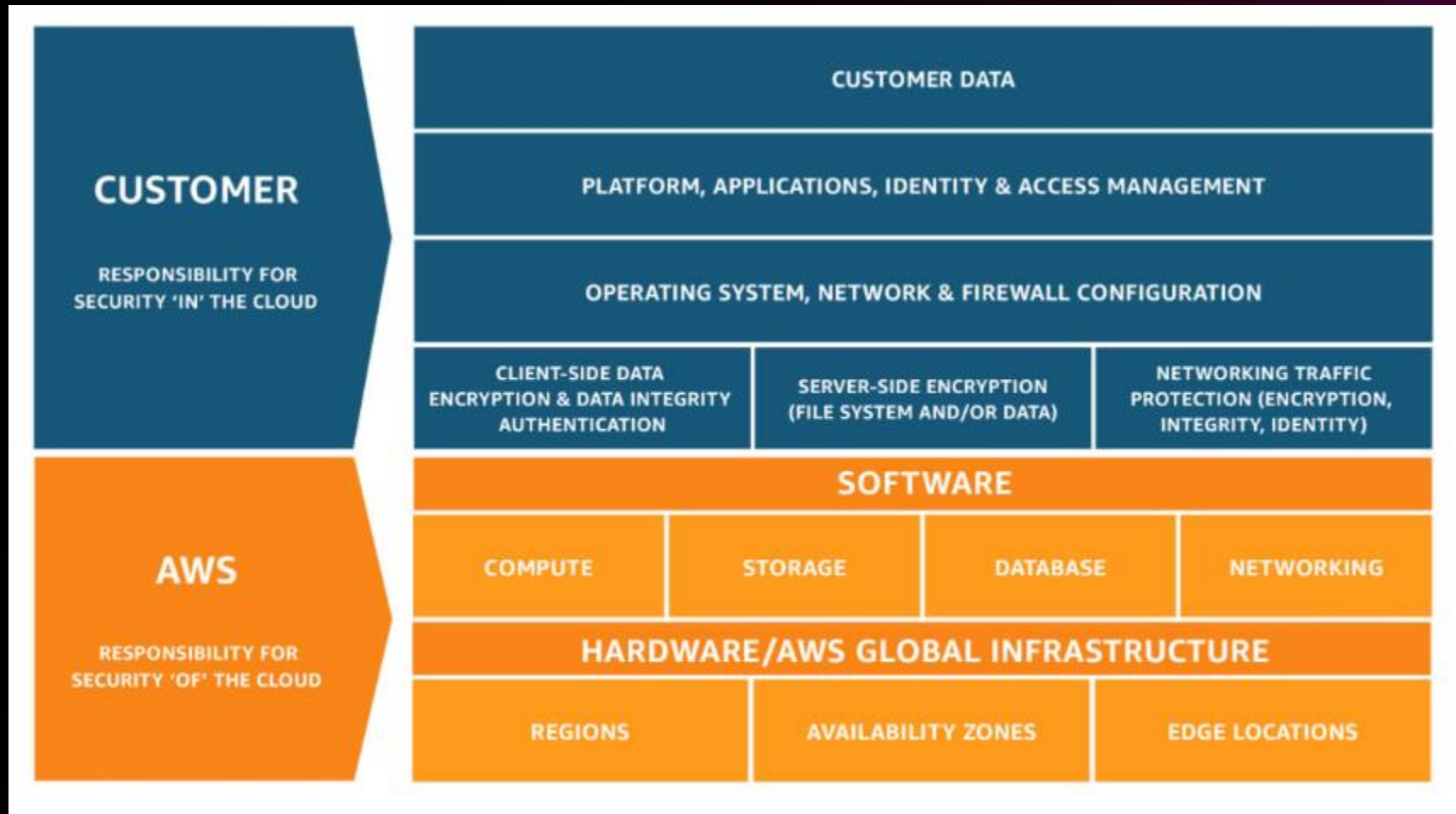
AWS
WAF

**Update malware
detection signatures**



Amazon
GuardDuty

AWS shared responsibility model



How AWS protects you

106,000

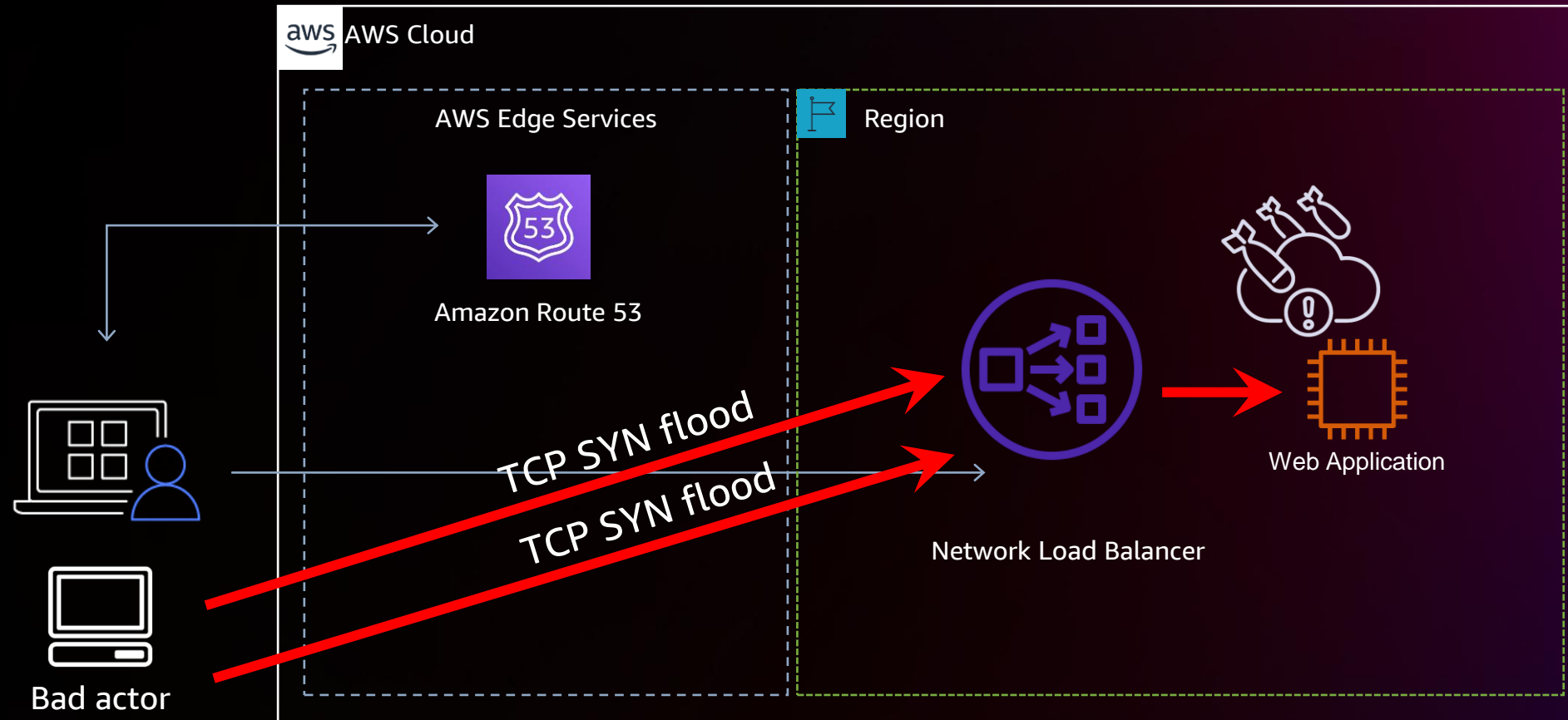
Outbound
DDoS events
Prevented

September
2022

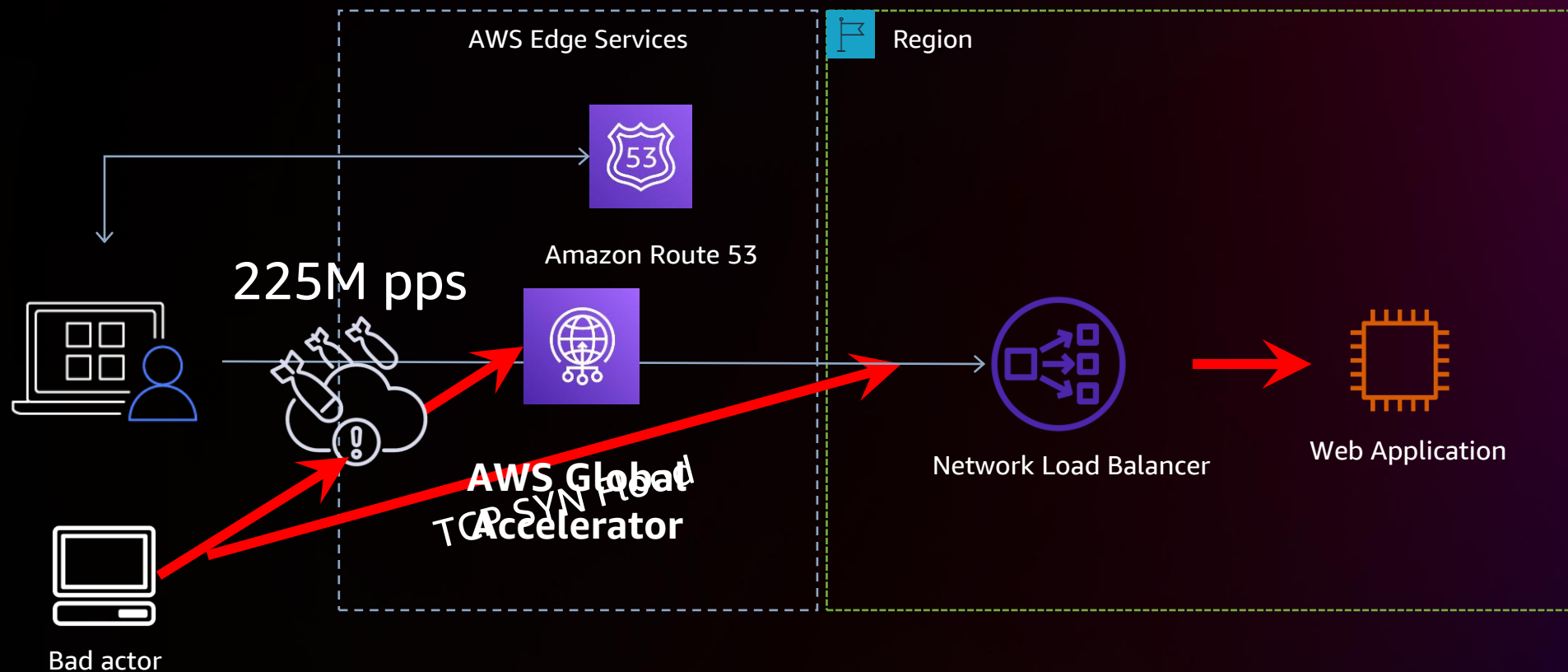


AWS Trust & Safety Team

SYN Flood: A real world example



SYN Flood: A real world example

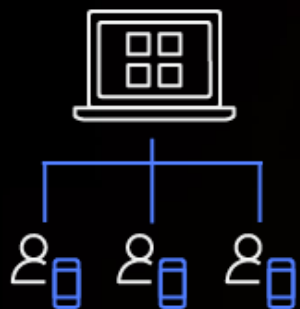


Shield Advanced protected resource



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A recipe for standing up to DDoS on AWS



Protecting **web**
applications



Protecting **latency**
sensitive applications

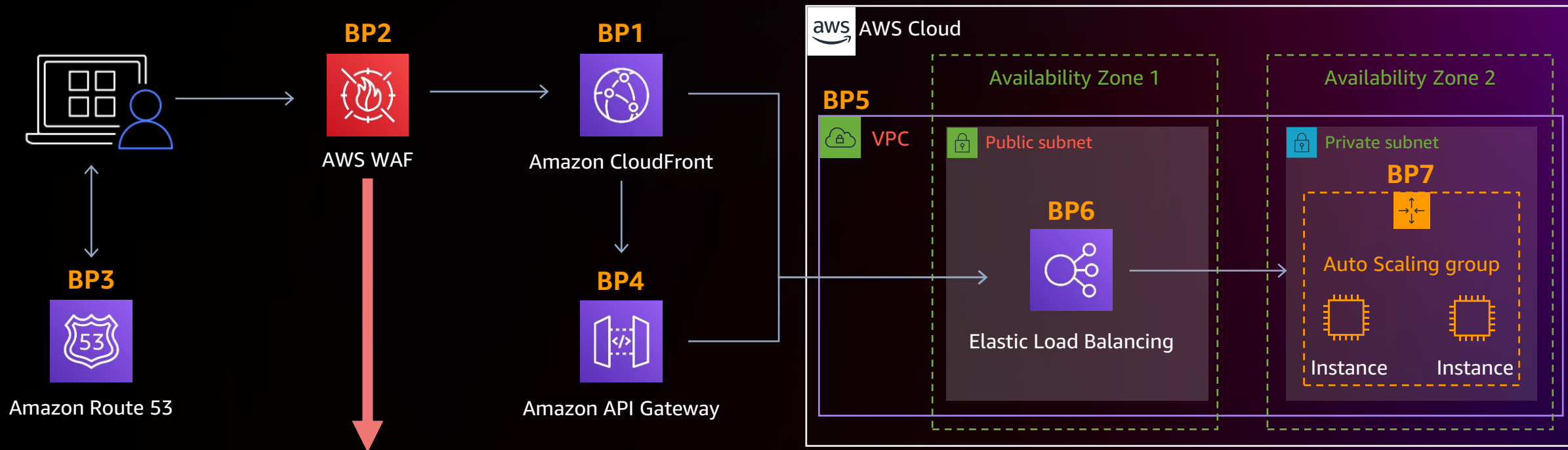


Protecting **serverless**
applications



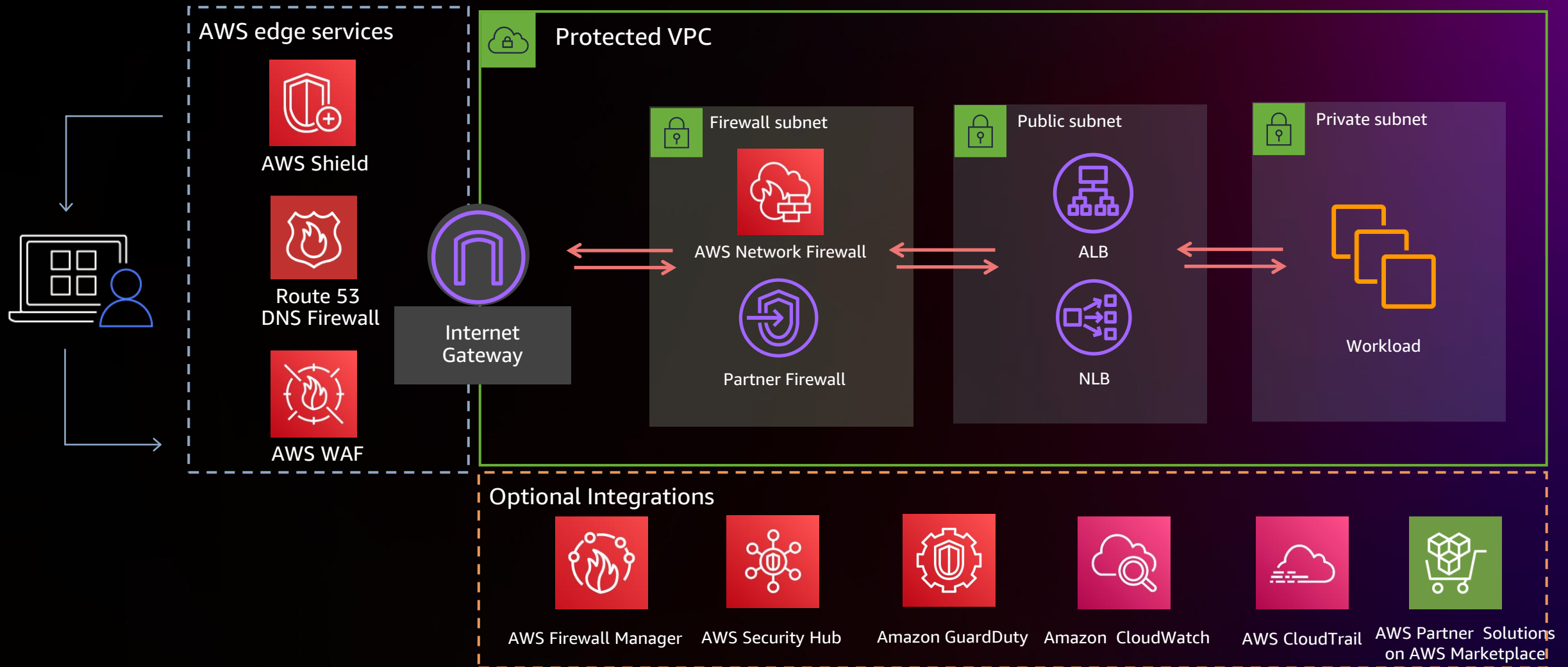
Protecting **on-premise**
applications

AWS DDoS resiliency prescriptive guidance



- ✓ Use IP reputation lists
- ✓ Rate limits on Common URLs (e.g. /, login)
- ✓ Shield Automatic Mitigation

Network edge protections on AWS



**“By failing to prepare, you
are preparing to fail”**

Benjamin Franklin

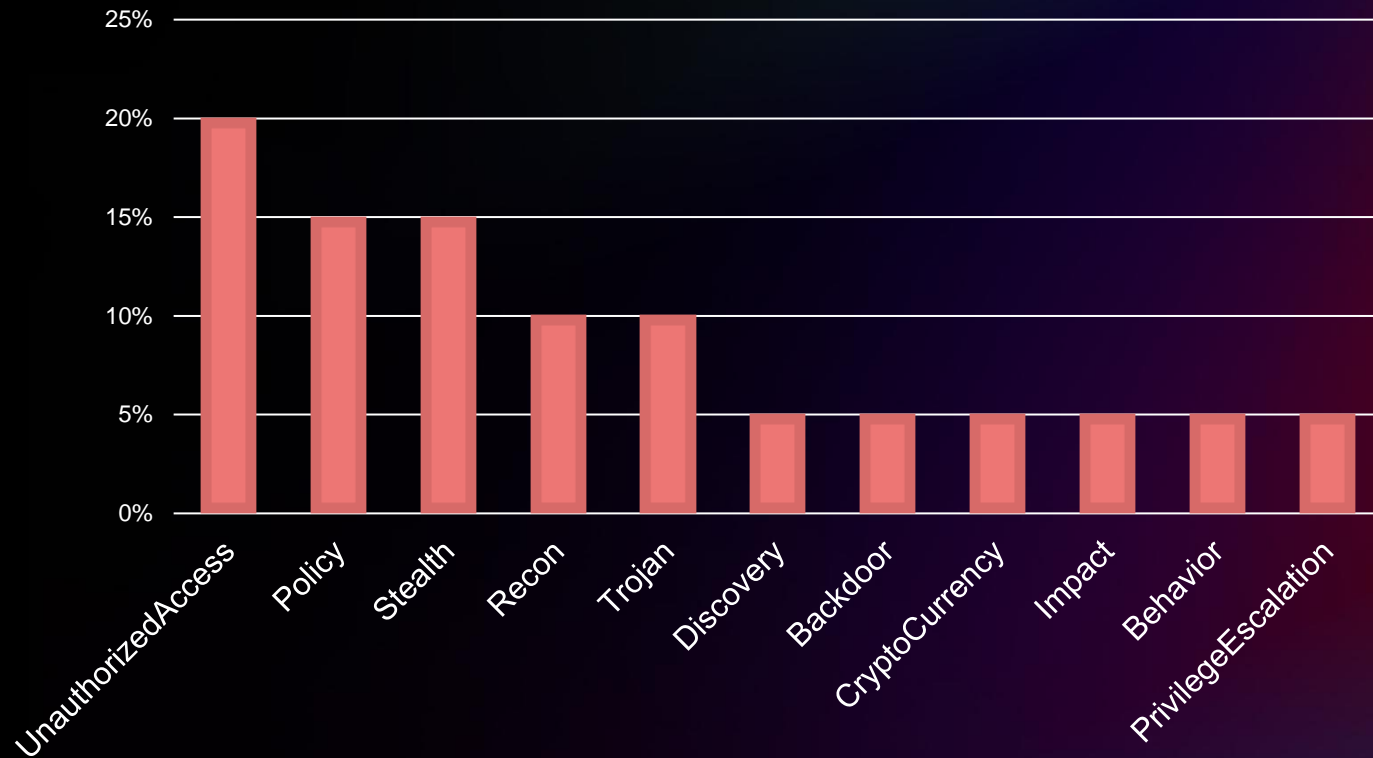
Founding Father of the United States

Common AWS account and resource threats

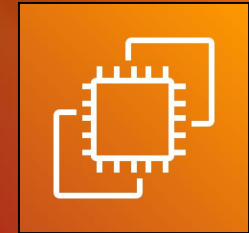


Top threats detected by Amazon GuardDuty

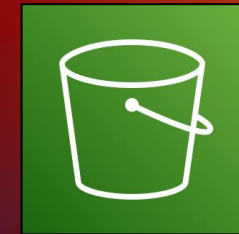
THREAT PURPOSES FOR TOP FINDING TYPES
JULY 1ST 2022 TO SEPTEMBER 30TH 2022



Amazon GuardDuty



Amazon EC2



Amazon S3

Top threats detected by Amazon GuardDuty

The most common threat purposes were...



Unauthorized
Access



Policy



Stealth

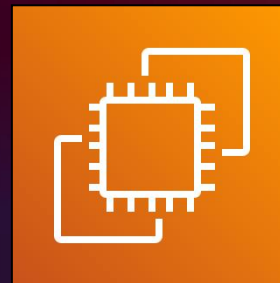
Top EC2 Threats



Unauthorized Access:

EC2/RDP Brute Force

EC2/SSH Brute Force



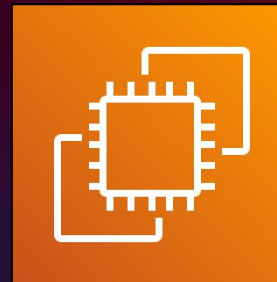
Top EC2 Threats



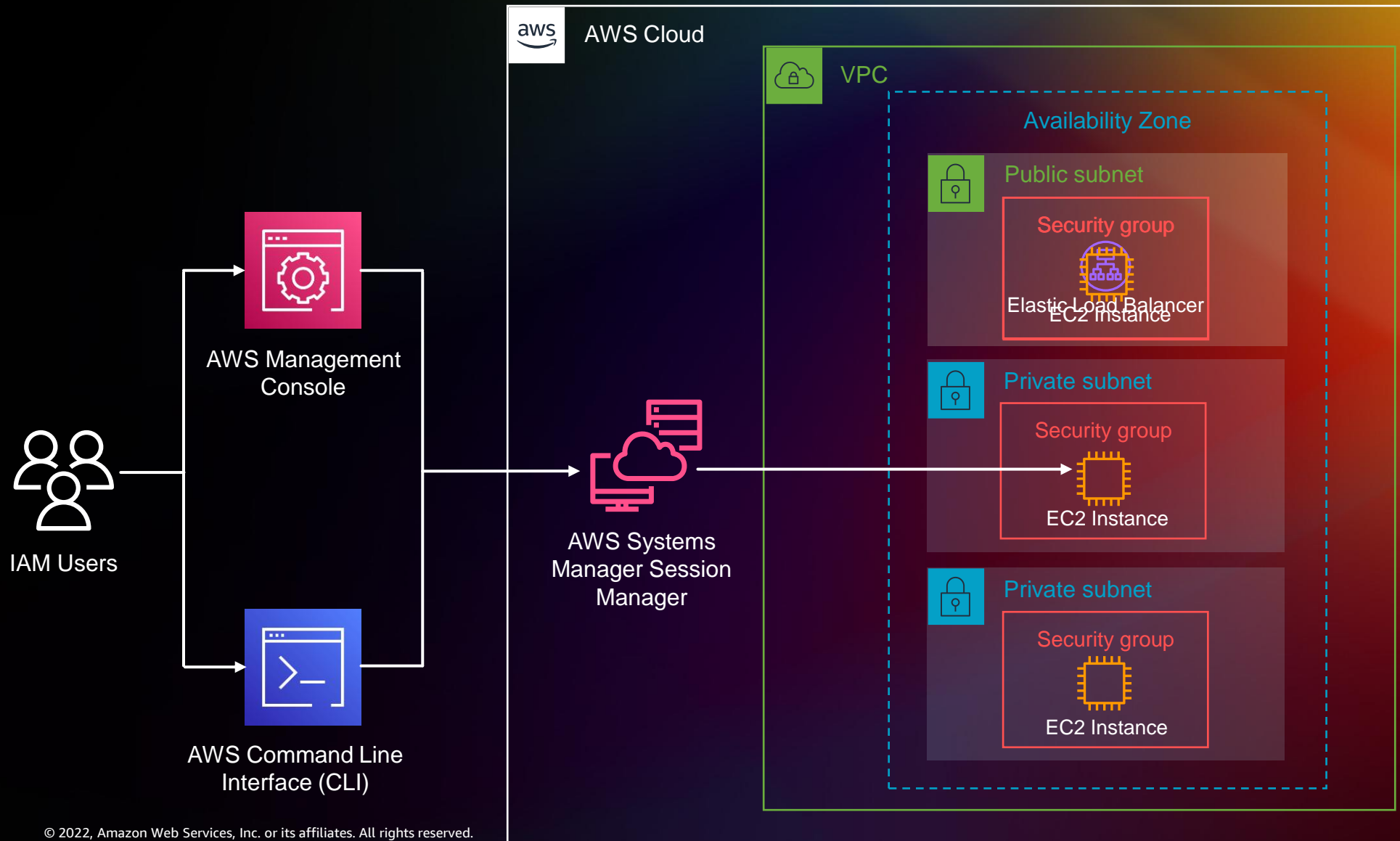
Unauthorized Access:

EC2/RDP Brute Force

EC2/SSH Brute Force



Securing EC2 instance access



Top policy related threats



Policy:

IAM User/Root Credential Usage



S3/Bucket Block Public Access Disabled



S3/Bucket Anonymous Access Granted

Root credential best practices



✓ Protect your AWS account root user with Multi-Factor Authentication



✓ Avoid creating an access key for the AWS account root user

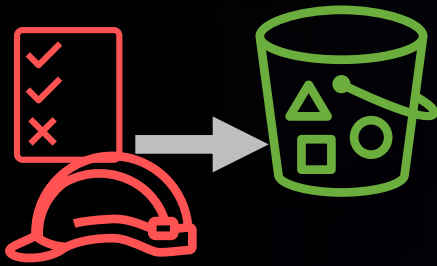


✓ Limit use of the AWS root account

S3 access best practices



✓ Enable S3 Block Public Access



✓ Grant IAM roles access to S3 buckets

✓ Implement least privilege access



✓ Encrypt your data

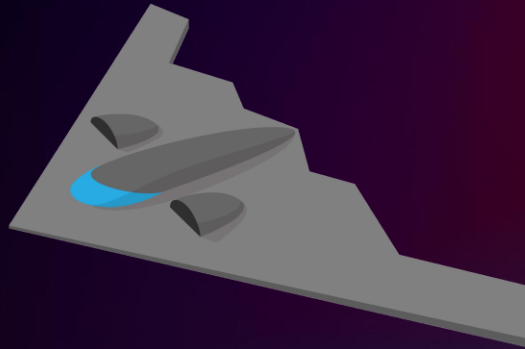
Top Stealth Related Finding



Stealth:

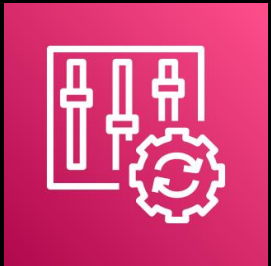
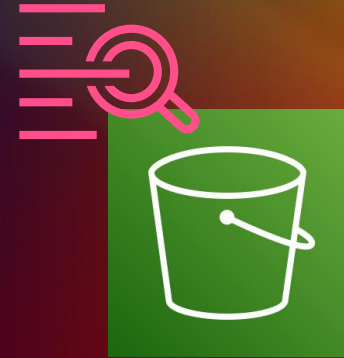


S3/Server Access Logging Disabled



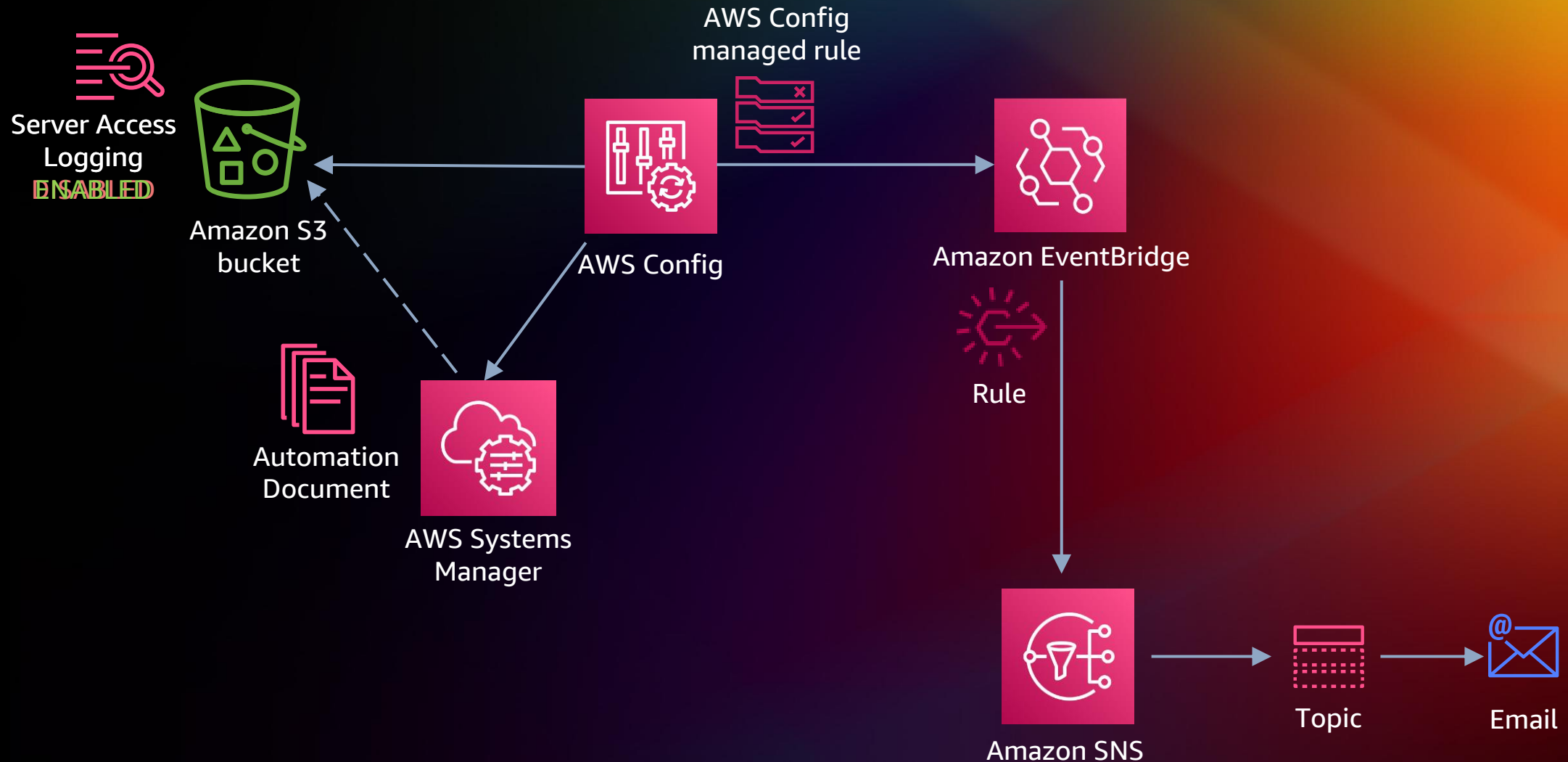
S3 Logging Best Practices

- ✓ Enable server access logging for S3



- ✓ Use the AWS Config rules to know when S3 logging is disabled and take action

Automatic configuration remediation



Observations from CIRT about Security Events



Ransomware

Ransom

Data destruction

Check out session [WPS305](#)
and chalk talk [STG305-R1](#)

Observations from CIRT about Security Events

Ransomware



Unauthorized users gain access

Malware Deployed

Malware encrypts data

A ransom demand

Observations from CIRT about Security Events

Ransom



Unauthorized users gain access

Exfiltrate data

Hold data for ransom

Observations from CIRT about Security Events

Data destruction



Most common scenario!

Unauthorized users gain access

Deletes some data

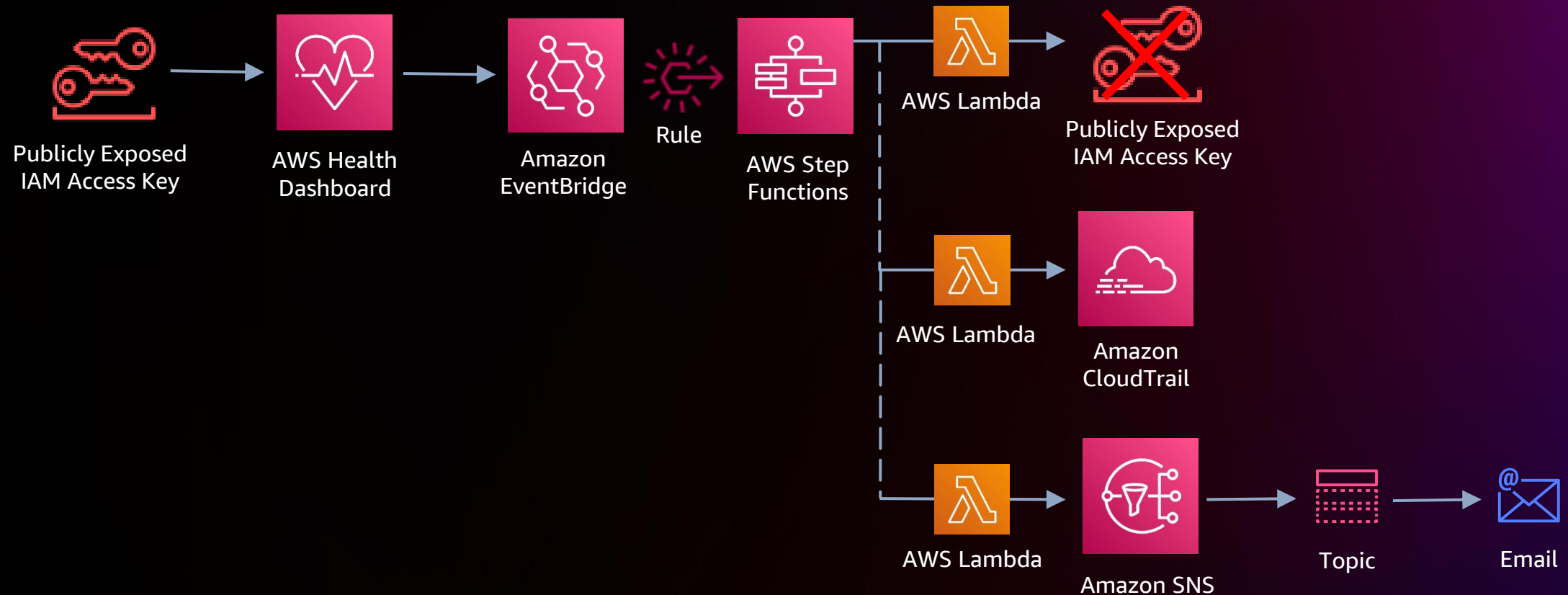
A ransom demand

Bad actor does not return data

“The most common cause of customer security events is the unintended disclosure of security credentials and secrets by customers.”

AWS Customer Incident Response Team (CIRT)

Automatic remediation of exposed credentials



Key takeaways

What is the data telling you? **Eat your veggies!!!**







Protect your AWS infrastructure and applications

🧄 AWS DDoS resiliency prescriptive guidance.

🥒 Use AWS WAF managed rules to protect applications

Key takeaways

Protect your AWS accounts

-  Limit the use of the root account, and long-term credentials.
-  Ensure proper security and access controls for EC2 instances and S3 buckets.
-  Use a defense in depth strategy when protecting your AWS resources.
-  Schedule regular tests of your backup and recovery plan.

Additional resources



[AWS Best Practices for DDoS Resiliency](#)
AWS Whitepaper



[Protecting against ransomware](#)
AWS Cloud Security Guidance



[AWS Best Practices for Securing the Root User](#)
Reference Guide



[AWS Health Exposed Credentials Event Automated Action](#)
Example Architecture and CloudFormation Stack



[Amazon S3 Preventative Security Best Practices](#)
Amazon S3 User Guide



[Amazon S3 Monitoring and Auditing Best Practices](#)
Amazon S3 User Guide

Thank you!

Fola Bolodeoku
obbolode@amazon.com

Steve Bollers
sboller@amazon.com

