
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

NET316-R

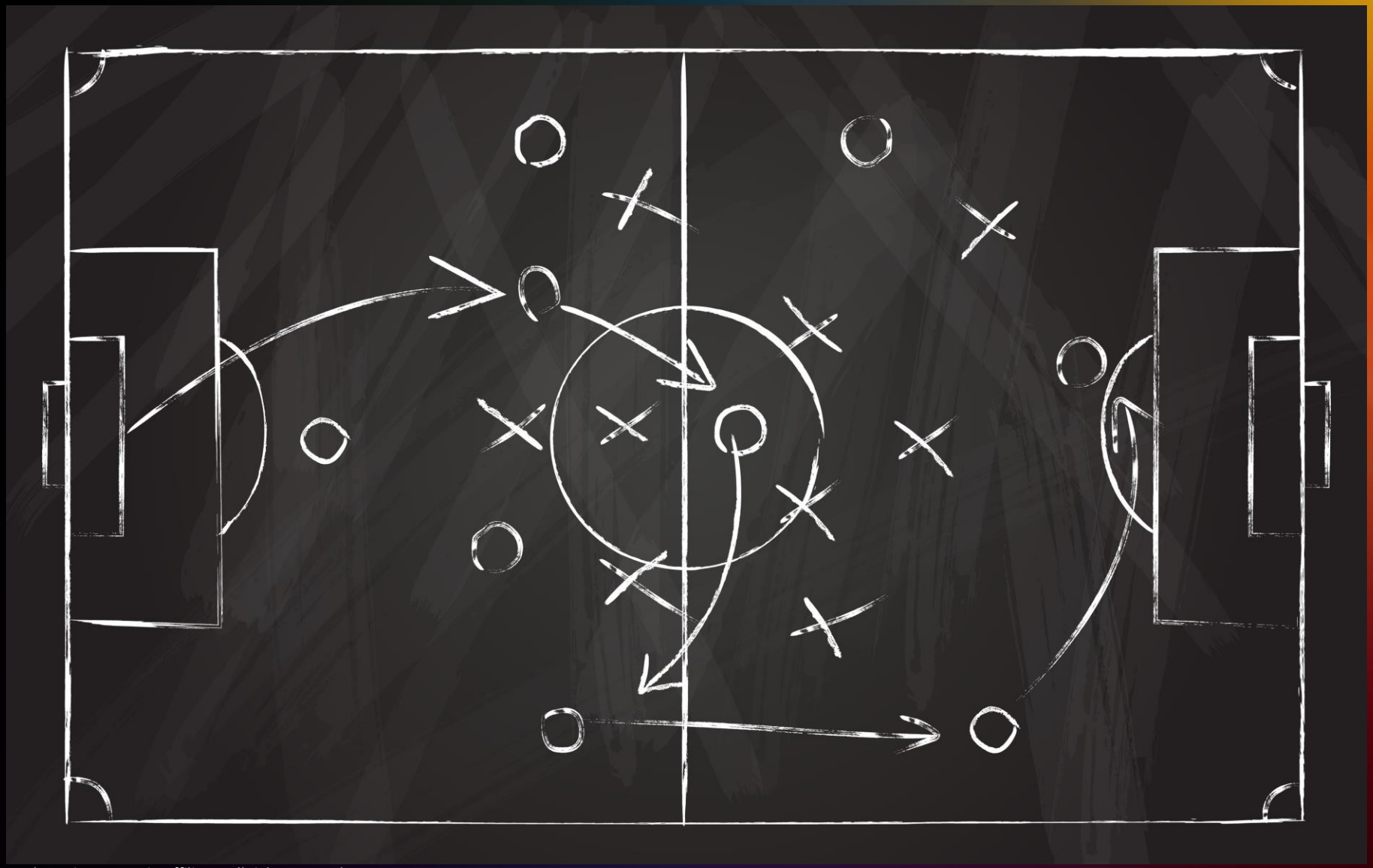
APIs: Critical for data transfer, but how do you keep them secure?

Tzoori Tamam

Principal Solutions Architect Specialist, Edge Services
Amazon Web Services

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

What is a chalk-talk



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

What to expect from this session

- API Security building blocks
- Perimeter for API architectures
- Authentication and authorization
- Bot management

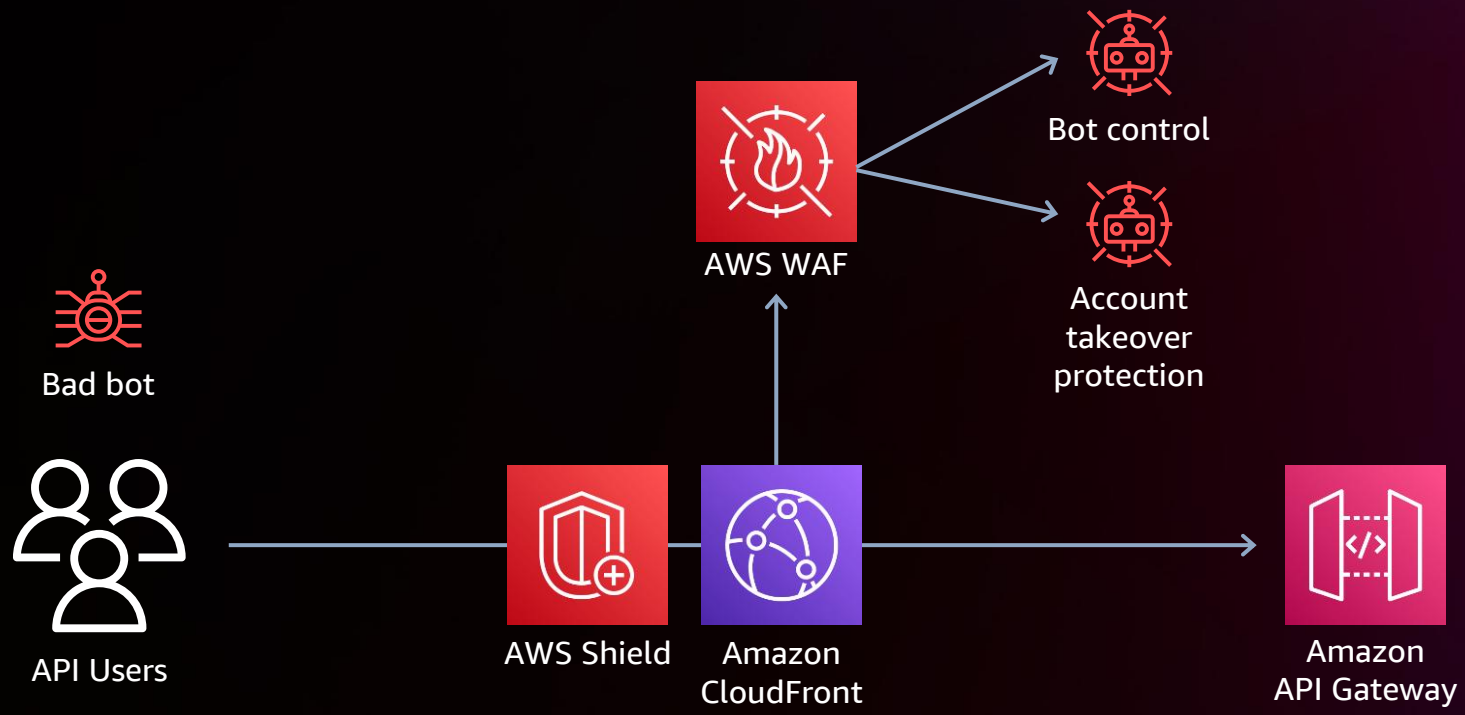
~30%

- Open discussion

~70%

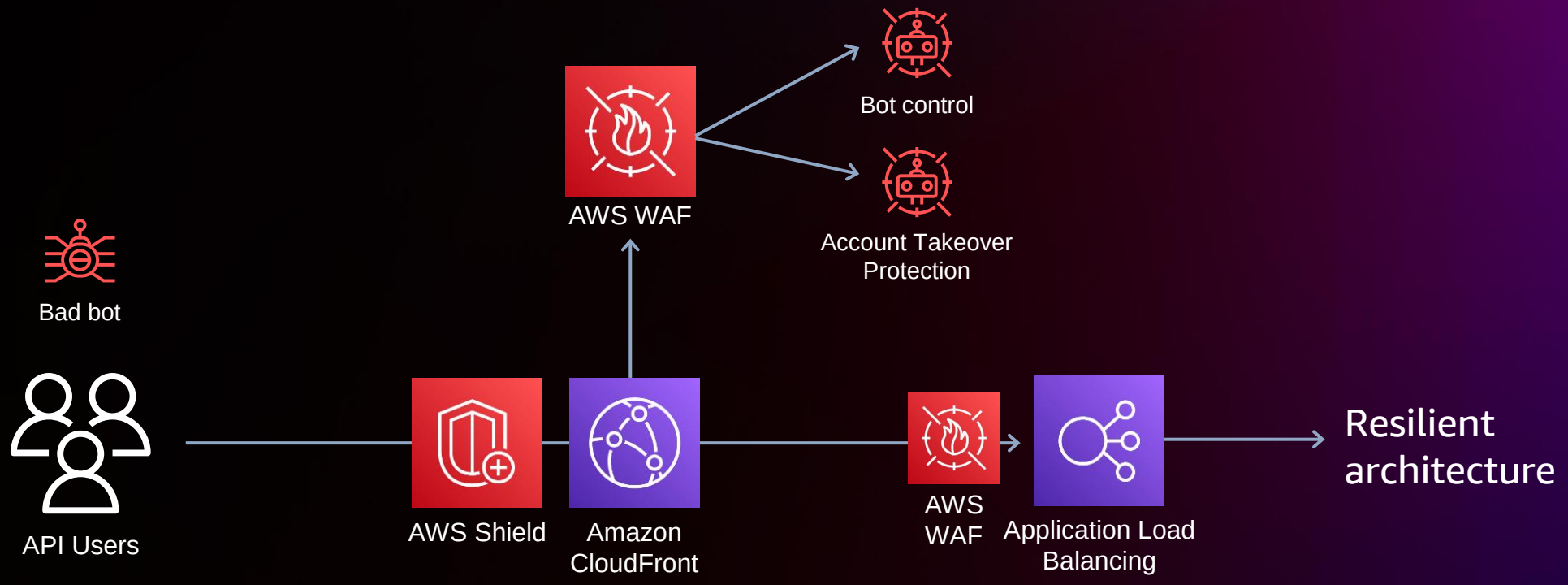
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Protecting your API perimeter



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

Protecting your API perimeter



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

API-specific web ACLs

- Rate limiting rules (specific, generic)
- Bot control rules
- Account takeover rules
- JSON body inpsection rules
- Positive security rules (allowed endpoints and HTTP methods)
- Default to BLOCK, custom response
- IP-based managed/custom rules
- Partner managed rules

☐	AWS-AWSManagedRulesAnonymousIpList	Use rule actions
☐	AWS-AWSManagedRulesAmazonIpReputationList	Use rule actions
☐	AWS-AWSManagedRulesKnownBadInputsRuleSet	Use rule actions
☐	AWS-AWSManagedRulesCommonRuleSet	Use rule actions
☐	AWS-AWSManagedRulesATPRuleSet	Use rule actions
☐	AWS-AWSManagedRulesBotControlRuleSet	Use rule actions
☐	Allowed-GET-URIs	Count
☐	Allowed-POST-URIs	Count
☐	Allowed-DELETE-URIs	Count
☐	Rate-Limit-to-Signup-URI	Block
☐	JSON-Inspection	Block
☐	Allowed-Bypassed-AMRs	Allow
☐	Allowed-Conformant-API-Calls	Allow

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

DDoS and APIs

Utilize CloudFront's distributed and resilient nature to block attacks close to the attacker

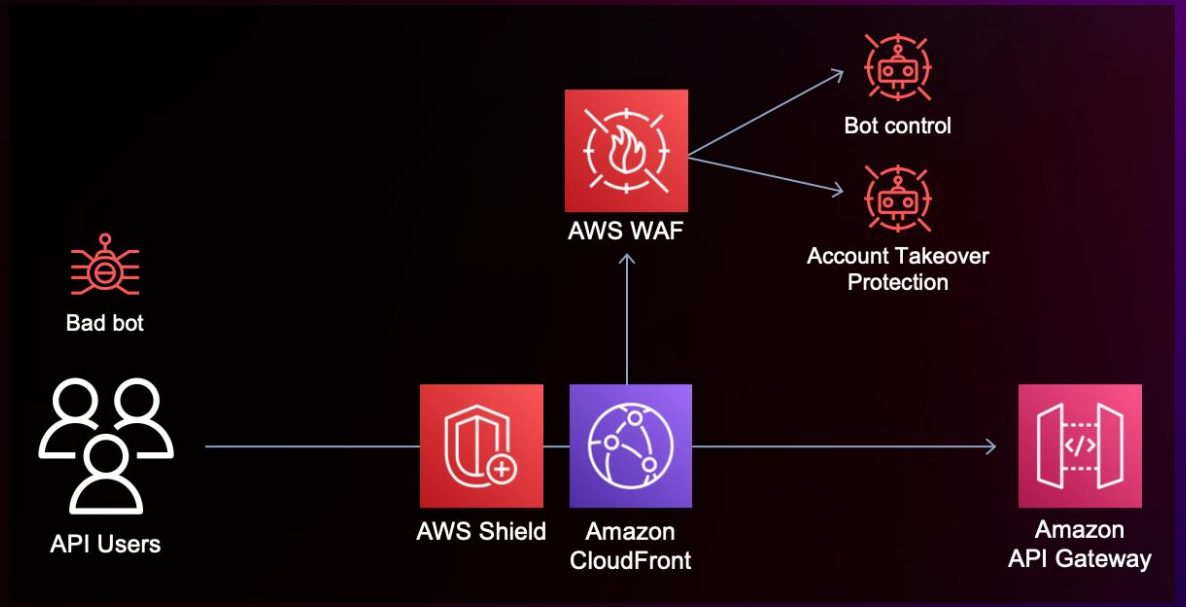
Shield for network level DDoS

Shield Advanced for L7 DDoS, together with AWS WAF

Use rate-based rules with AWS WAF

Use Shield Advanced Automatic L7 Rules

Architect your application resiliently



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

Token validation and authentication

Validating JWT tokens at the edge

Fine-grain authorization at the application

Run custom logic at the edge with

- Lambda@Edge
- CloudFront Functions



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

Let’s talk about it!

- AWS WAF for APIs
- APIs and DDoS protection
- Authentication and authorization
- Bot management
- Partner solutions

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

Thank you!

Tzoori Tamam
tzoorit@amazon.com
/in/tzoorit



Please complete the session survey in the **mobile app**

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