AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC226

AWS Shield Advanced: A year in review

Kevin Lee
Sr. Product Manager, Tech
AWS

Chido Chemambo
Security Engineer
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Quick overview of AWS Shield and Perimeter Protection services

Deep dive into Shield’s Automatic Application Layer DDoS Mitigation

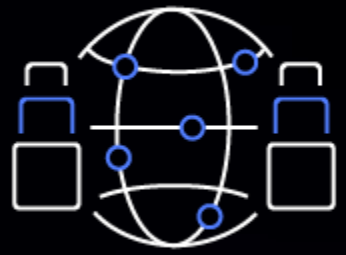
Demo!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customers want their applications to be available and responsive for their users



Uptime protection



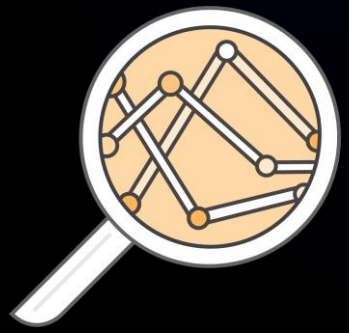
Scale on demand



Compliance

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Frequent challenges



Integrating multiple services



Resource drain



Lack of internal expertise



Expensive tools

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Comprehensive application security



AWS Shield – managed DDoS protection



AWS WAF – protection at L7 (Application Layer) for your business logic



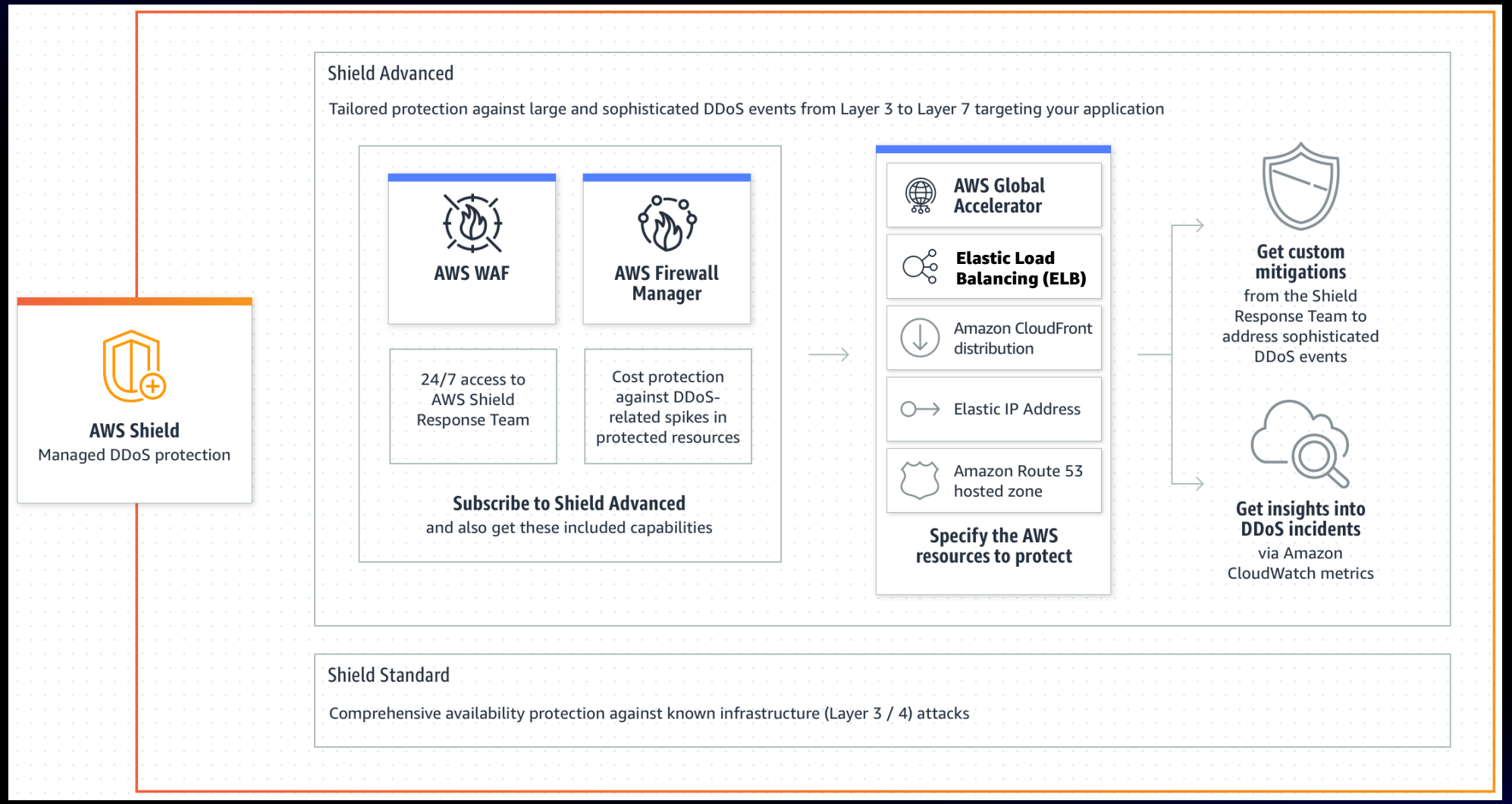
AWS Network Firewall – protection at L3/4 (Network/Transport Layer) for your VPCs



AWS Firewall Manager – centrally configure and manage security rules across accounts and applications

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Shield: Managed DDoS protection

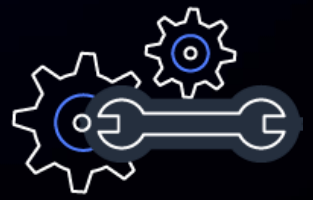


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Benefits of AWS Shield Advanced



Shield Advanced



Protection for infrastructure L3-4

L3-7 protection for your applications

Faster mitigation for your applications



Amazon CloudWatch event notification

DDoS threat environment dashboard

24x7 access to Shield Response Team (SRT)



Health-based detection

Adaptive L3-4 protection

L7 anomaly detection using AWS WAF

Automatic application layer mitigation



Proactive event response

No charge for AWS WAF for Shield Advanced protected resources

Central config and compliance
Firewall Manager cost included with Shield Advanced subscription

Cost protection for scaling during an attack

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Protect resources with AWS Shield



Amazon CloudFront



Amazon Route 53



Elastic Load Balancing (ELB)



Elastic IP address



AWS Global Accelerator

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shield Response Team: 24/7 DDoS Support

A team of security engineers dedicated to providing 24/7 support during DDoS events

- DDoS resiliency architectural guidance
- Shield Advanced onboarding
- Advanced DDoS protection consultation (before/during/after an event)
- Proactive engagement during DDoS events
- Attack analysis
- Writing custom mitigations
- Bot mitigation strategies

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS WAF



AWS WAF



Frictionless setup: Deploy without changing your existing architecture



Low operation overhead: Ready to use, built-in managed rules, and rules from AWS Marketplace



Customizable security: Highly flexible rule engine that can inspect requests with single-millisecond latency



Advanced automation: API driven architecture and fast rule propagation allows you to detect and respond to threats in real-time

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

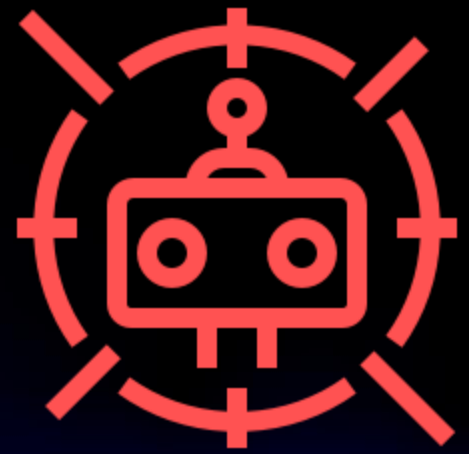
What is AWS WAF Bot Control?

Designed to help stop common and pervasive bot traffic on your application

Identify and categorize bots

Combine with natively available mitigation techniques on AWS WAF

Insight and visibility into bot traffic

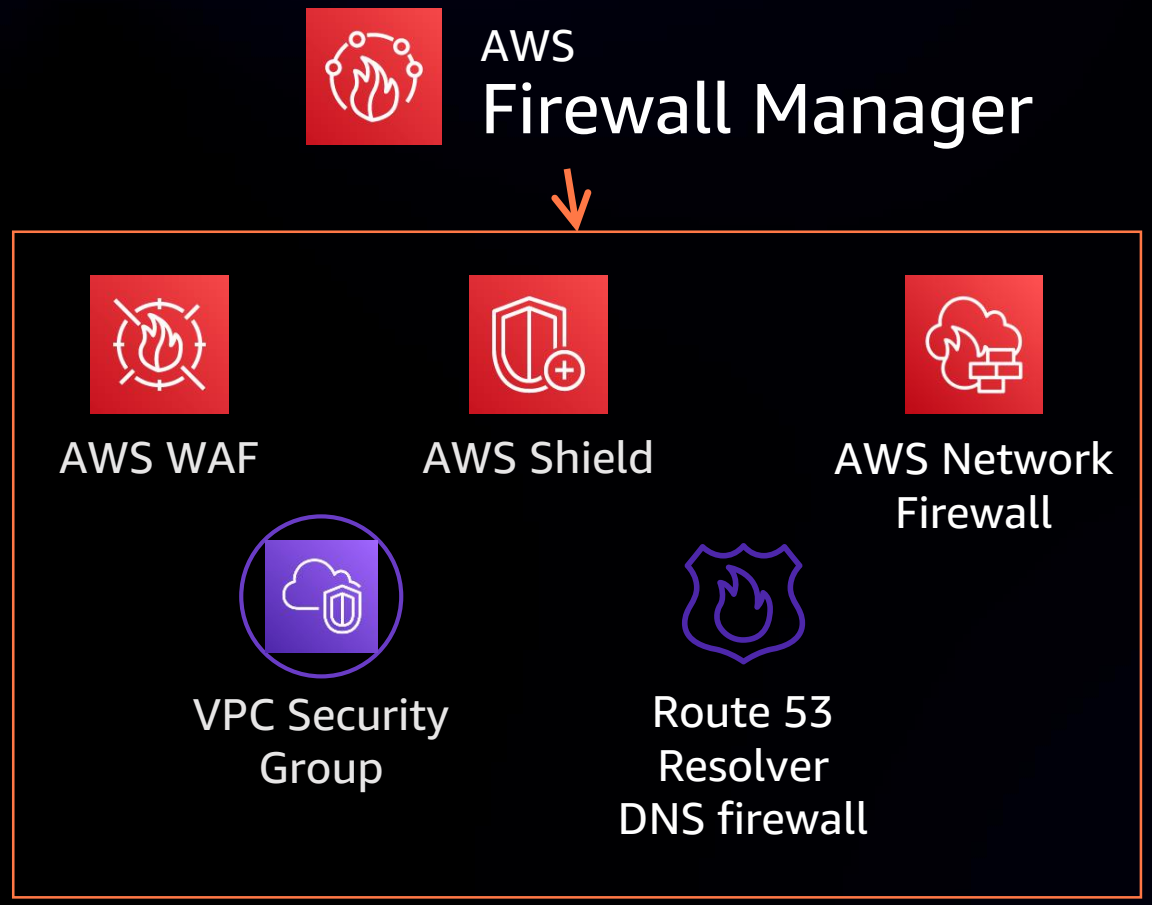


SEC313-R2 – Protecting against automated bots with AWS WAF Bot Control
Thursday, Dec. 2 @ 11:30am
Venetian, Level 4, Lando 4206

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Firewall Manager



- **Centrally enable baseline security** using Shield across AWS Organizations
- **Consistently enforce** protections, even as new applications are created
- **View compliance posture** centrally across all your AWS accounts

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Commonly used web architectures



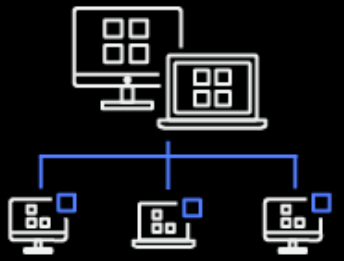
Protecting web applications



Protecting latency-sensitive applications



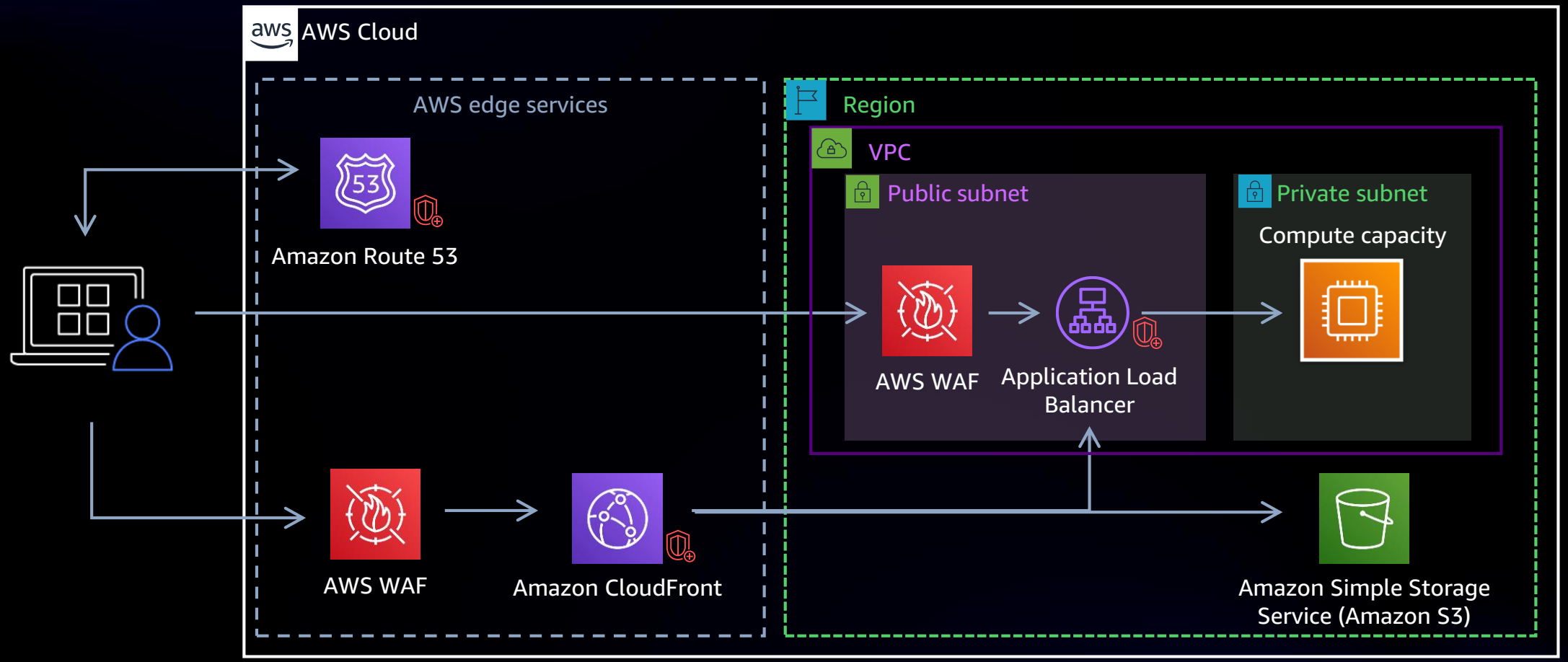
Protecting serverless applications



Protecting on-premises applications

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

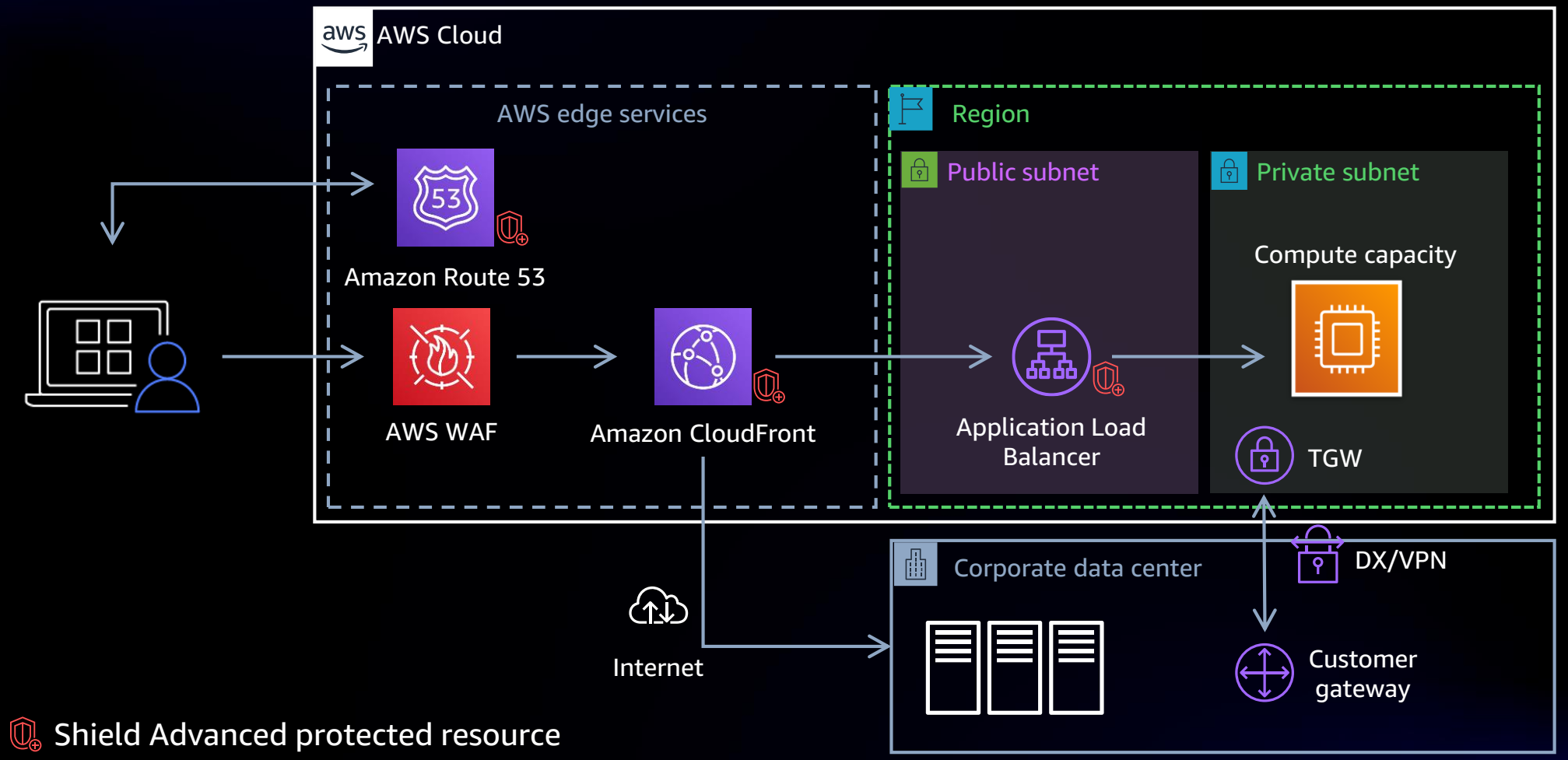
Protecting web applications



Shield Advanced protected resource

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Protecting on-premises applications



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automatic application layer DDos mitigation

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Launched today: Automatic application layer DDoS mitigation

Reduce time-to-mitigation and respond to application availability threats immediately

- ✓ AWS WAF rules are automatically created to mitigate detected DDoS events
- ✓ AWS WAF rules are tested against legitimate traffic to minimize false positives
- ✓ AWS WAF rules can be created in Count mode to observe effectiveness before deploying in Block mode
- ✓ AWS WAF rules are automatically removed after an event subsides
- ✓ No manual intervention required

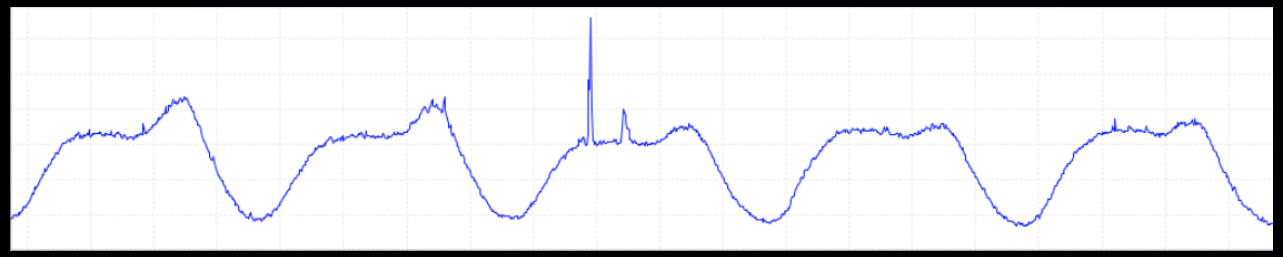


aws

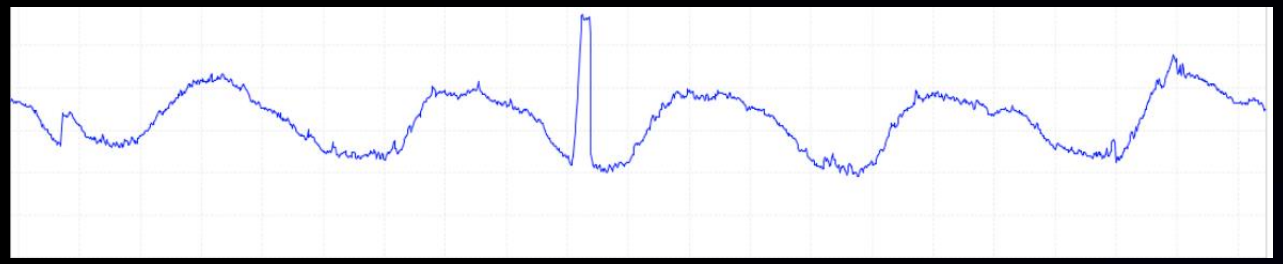
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detecting Layer 7 traffic anomalies

Attacks during traffic peaks



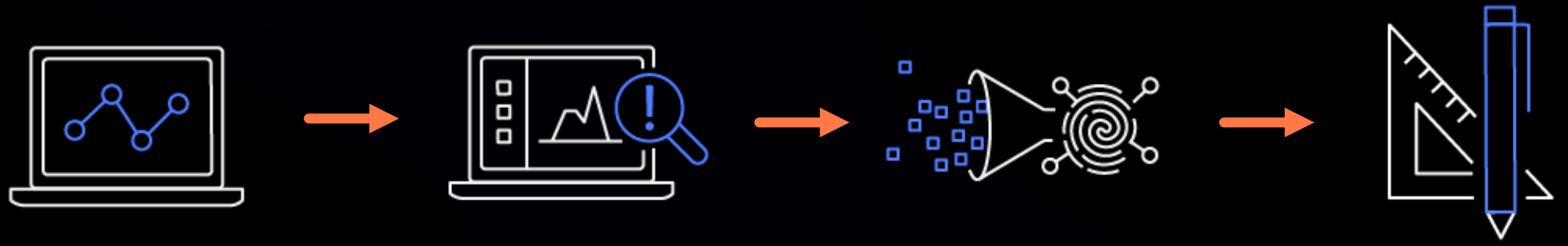
Attacks during traffic valleys



- Traffic baseline is established for your Shield-protected web application resources
- Baselines cover up to 30 days and time of day is factored into detection decisions
- Example of traffic anomalies detected:
  - Attacks posing a risk to application availability
  - Attacks that match known pattern
  - Events where traffic increases may impact application availability

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Confirm an attack signature is safe to block



Check to see if attack is isolatable

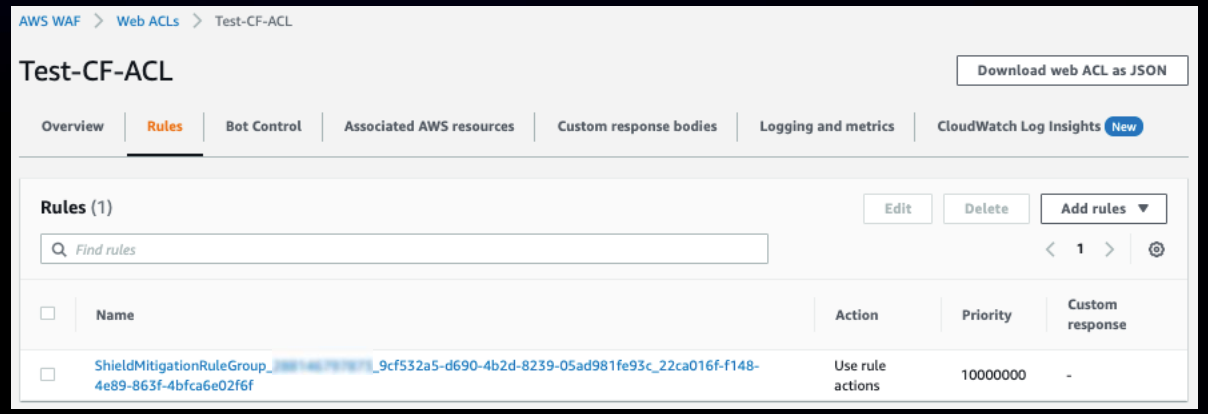
Determine confidence score

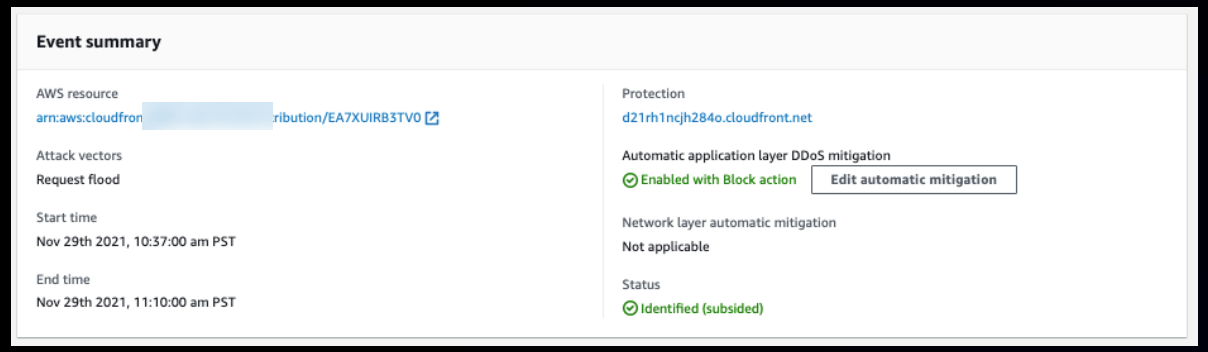
Assess for false-positive

Create AWS WAF rules

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automatically place mitigations using WAF

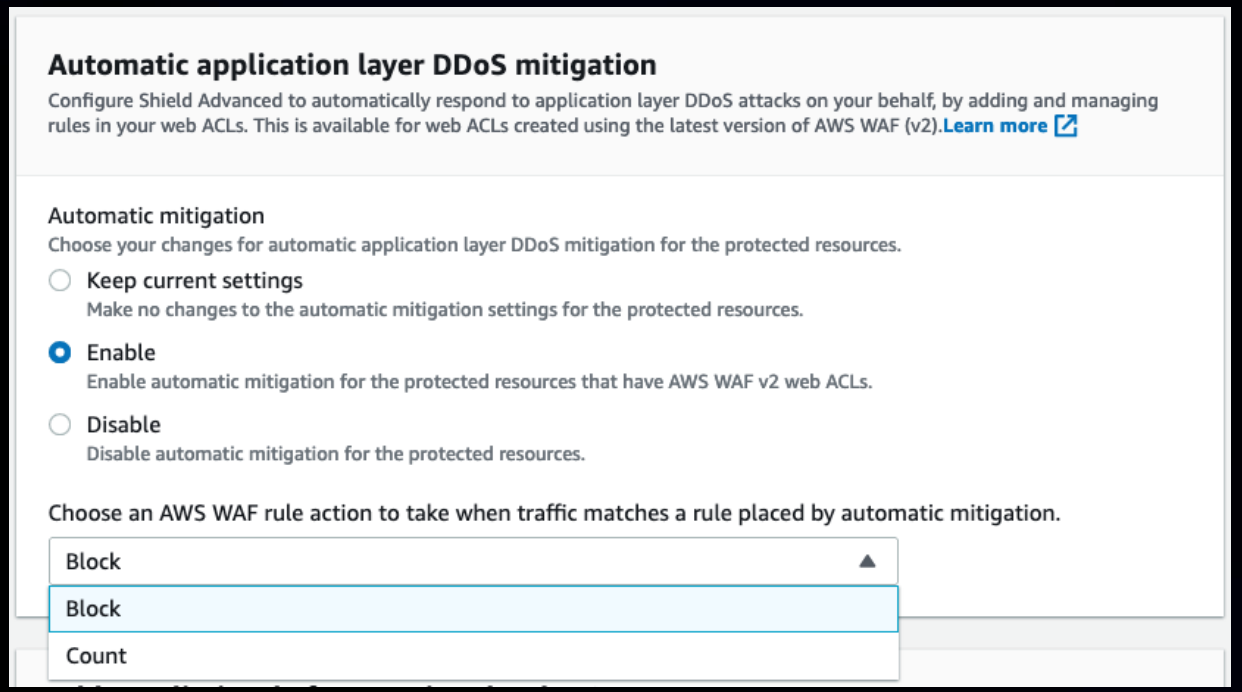




- Enabling automatic mitigation creates a Shield managed rule group associated with the Web ACL of protected resources
- Shield Advanced automatically creates AWS WAF rules in the Shield managed rule group in response to layer 7 DDoS events
- Only AWS Shield Advanced can create rules within this managed rule group

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

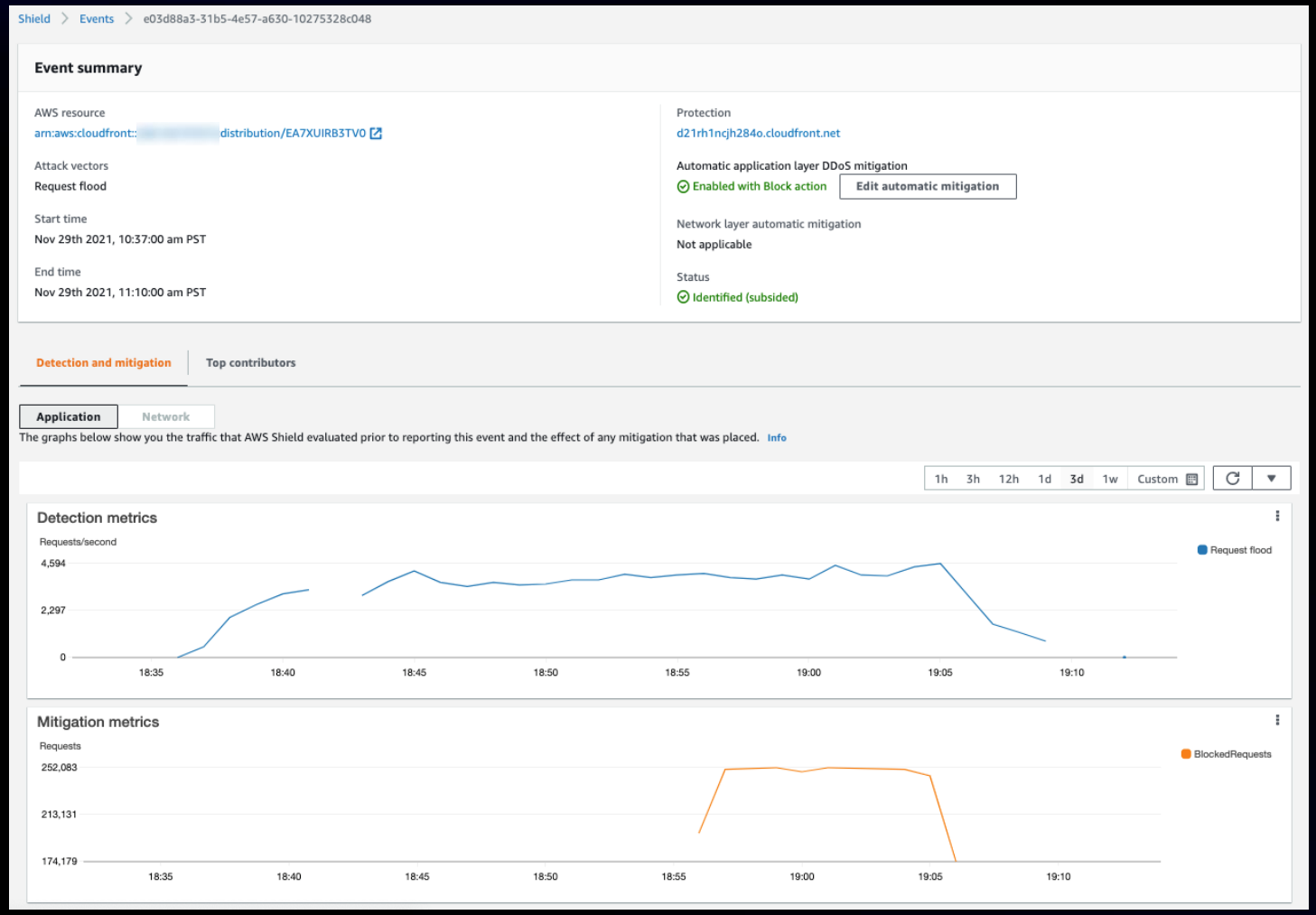
Edit automatically placed mitigations



- The action taken by automatically created AWS WAF rules can be changed to Count or Block per protected resource
- Automatic mitigation can be disabled at any time
- When attack subsides, AWS WAF rules will be removed automatically by Shield

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Report on application layer DDoS events



- Detection & mitigation metrics
  - Volume of requests to the resource
  - Volume of requests blocked
  - Event-specific timeline
- Top contributors
  - Report on top 5 by source/destination IP, country, URL, user agent, referrer
- All metrics populated by Amazon CloudWatch

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shield Advanced getting started checklist

- ✓ Specify your resources that you want to protect
- ✓ Configure Route 53 health checks
- ✓ Enable proactive DDoS response
- ✓ Enable automatic application layer DDoS mitigation
- ✓ Configure Amazon CloudWatch alarms
- ✓ Add rate-based rules

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.