aws SUMMIT

Additional Security Services on AWS

Bertram Dorn

Specialized Solutions Architect

Security / Compliance / DataProtection

AWS EMEA

aws SUMMIT

The Landscape

aws SUMMIT

Report of Independent Accountants

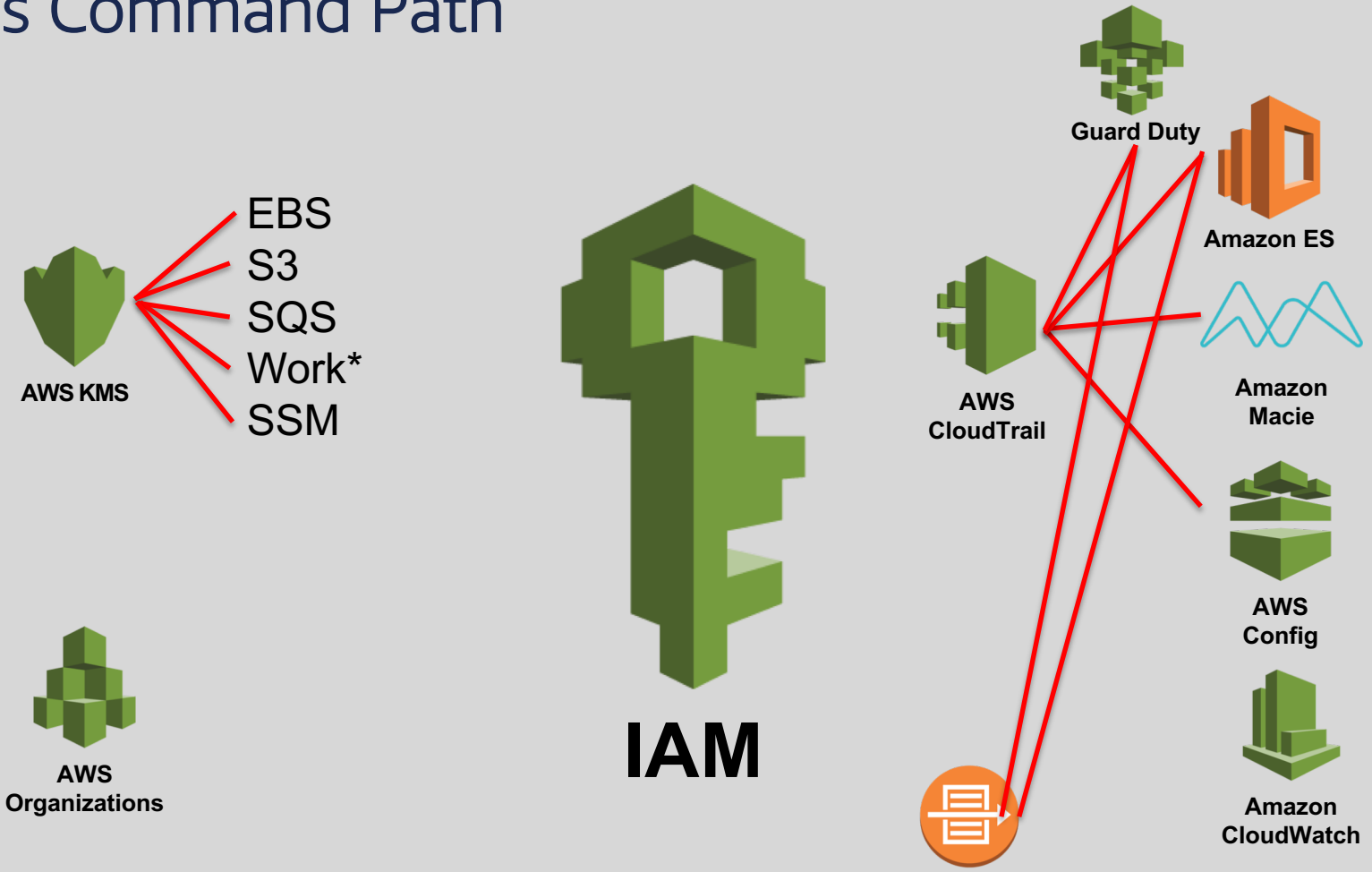
the Board of Directors of Amazon Web Services, Inc.

e have examined management's assertion that Amazon Web Services, Inc. (AWS), during the period tober 1, 2016 through March 31, 2017, maintained effective controls to provide reasonable assurance at:

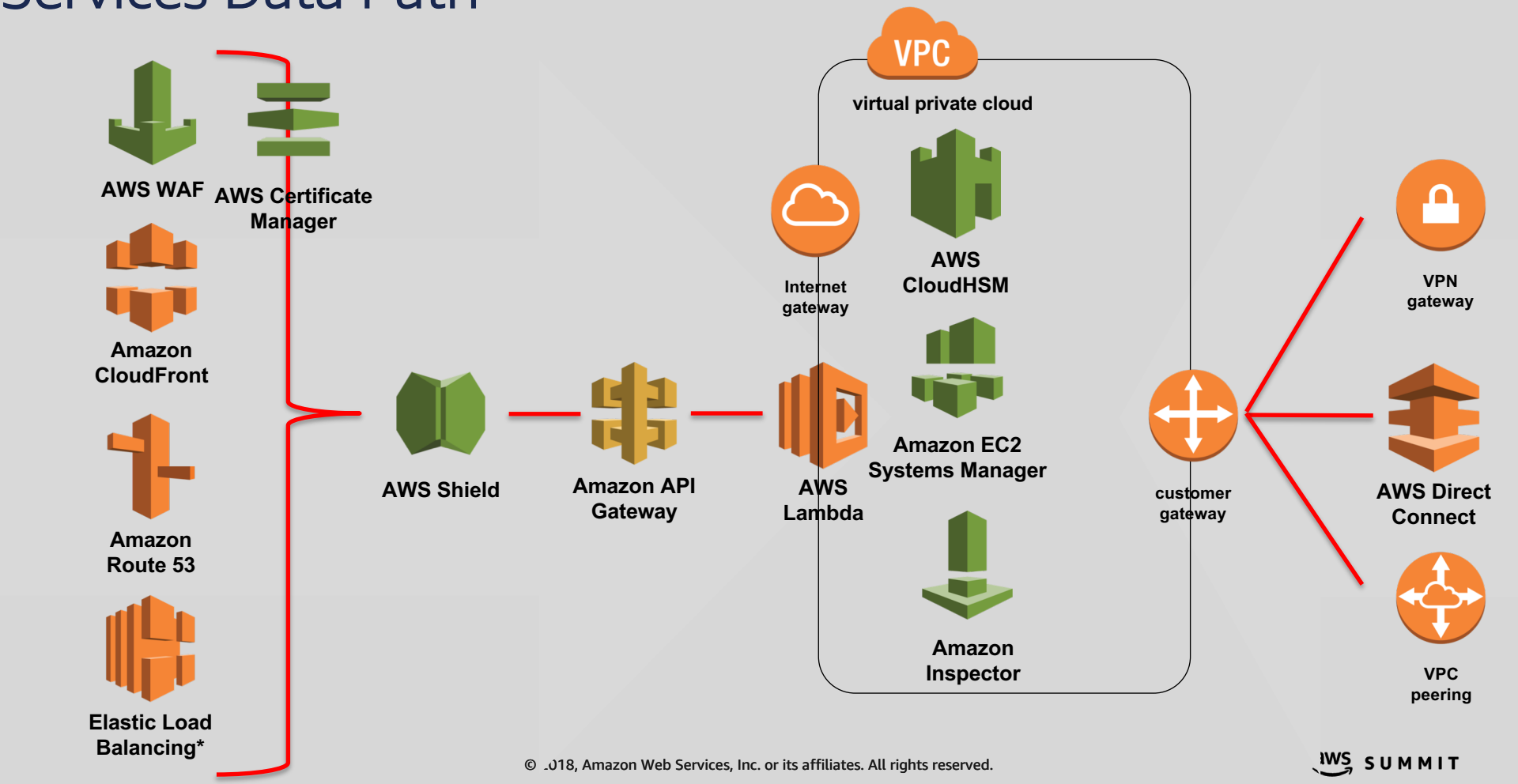
- the Amazon Web Services System was protected against unauthorized access, use, or modification to meet AWS' commitments and system requirements,
- the Amazon Web Services System was available for operation and use to meet AWS' commitments and system requirements, and
- information within the Amazon Web Services System designated as confidential was protected to meet AWS' commitments and system requirements

sed on the criteria for security, availability, and confidentiality in the American Institute of Certified blic Accountants' TSP section 100, *Trust Services Principles and Criteria for Security, Availability, ocessing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of AWS' management.

Services Command Path



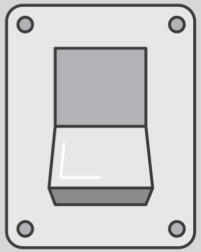
Services Data Path



Four Pillars of our approach to **Protection**

AWS Integration

DDoS protection without infrastructure changes



Always-On Detection and Mitigation

Minimize impact on application latency

Affordable

Don't force unnecessary trade-offs between cost and availability

Flexible

Customize protections for your applications

aws SUMMIT

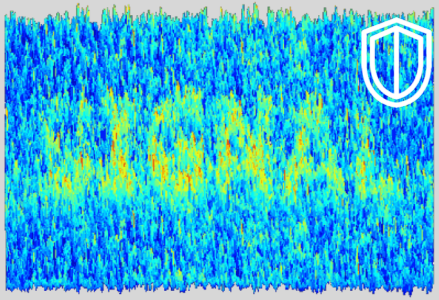
Guard Duty

aws SUMMIT

Find the Needle, Skip the Haystack

GuardDuty helps security professionals quickly find the threats (needle) to their environments in the sea of log data (haystack) so they can focus on hardening their AWS environments and responding quickly to malicious or suspicious behavior.

Amazon GuardDuty: All Signal, No Noise



GuardDuty Data Sources

VPC Flow Logs

VPC flow logs

- Flow Logs for VPCs Do Not Need to Be Turned On to Generate Findings, data is consumed through independent duplicate stream.
- Suggested Turning On VPC Flow Logs to Augment Data Analysis (charges apply).

DNS Logs

DNS Logs

- DNS Logs are based on queries made from EC2 instances to known questionable domains.
- DNS Logs are in addition to Route 53 query logs. Route 53 is not required for GuardDuty to generate DNS based findings.

CloudTrail Events

CloudTrail Events

- CloudTrail history of AWS API calls used to access the Management Console, SDKs , CLI, etc. presented by GuardDuty.
- Identification of user and account activity including source IP address used to make the calls.

Capture and save all event data via CWE or API Call for long term retention. Additional charges apply.

GuardDuty Findings: Threat Purpose Details

Describes the primary purpose of the threat. Available at launch, more coming!

- Backdoor: resource compromised and capable of contacting source home
- Behavior: activity that differs from established baseline
- Crypto Currency: detected software associated with Crypto currencies
- Pentest: activity detected similar to that generated by known pen testing tools
- Recon: attack scoping vulnerabilities by probing ports, listening, database tables, etc.
- Stealth: attack trying to hide actions / tracks
- Trojan: program detected carrying out suspicious activity
- Unauthorized Access: suspicious activity / pattern by unauthorized user

aws SUMMIT

GuardDuty Demo

aws SUMMIT

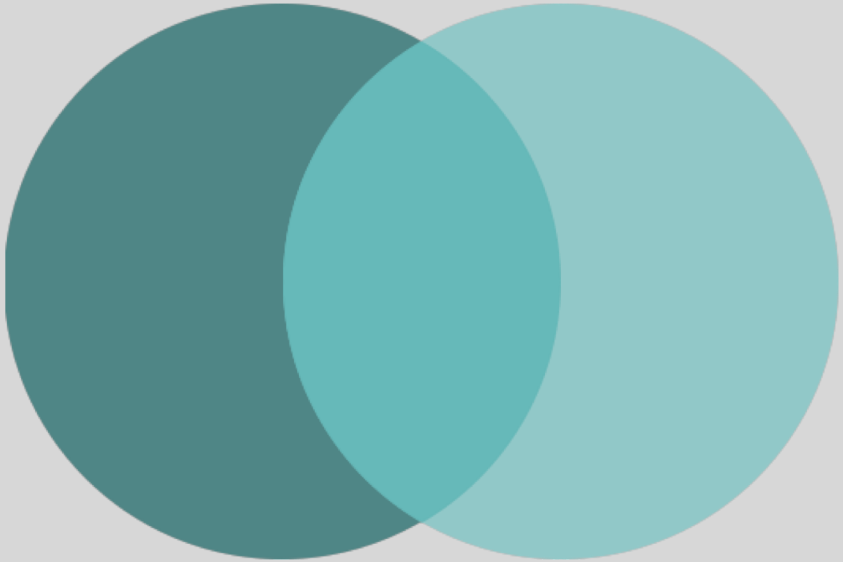
aws SUMMIT

Macies

aws SUMMIT

Macie Overview

Understand Your Data
Natural Language Processing (NLP)



Understand Data Access
Predictive User Behavior Analytics (UBA)

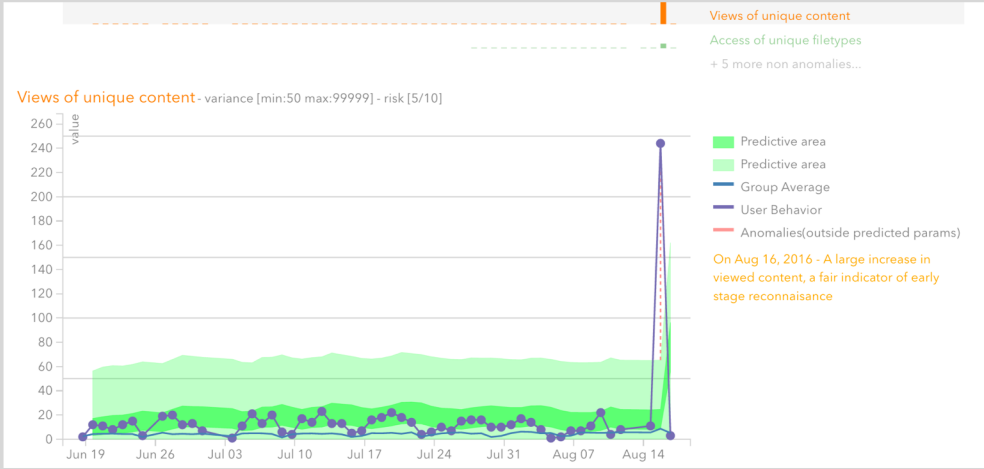
Macie User Behavior Analytics

We use behavioral analytics to baseline normal behavior patterns.

Contextualize by value of data being accessed.

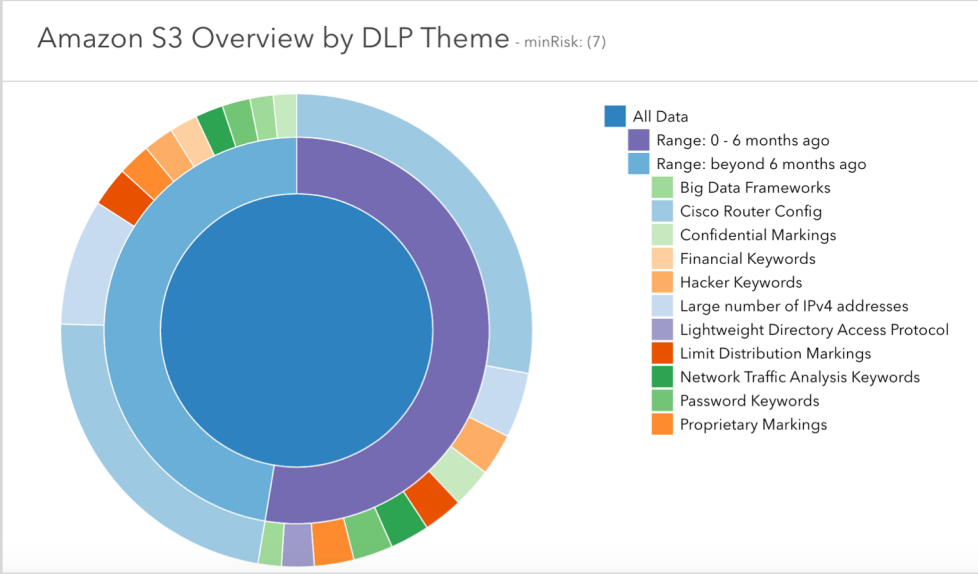
Goals:

- Go to crazy lengths to avoid false positives
- Features, features
- Compare peers
- Tell a narrative



Macie Content Classification

- PII and personal data
- Source code
- SSL certificates, private keys
- iOS and Android app signing keys
- Database backups
- OAuth and Cloud SAAS API Keys



aws SUMMIT

Macies Demo

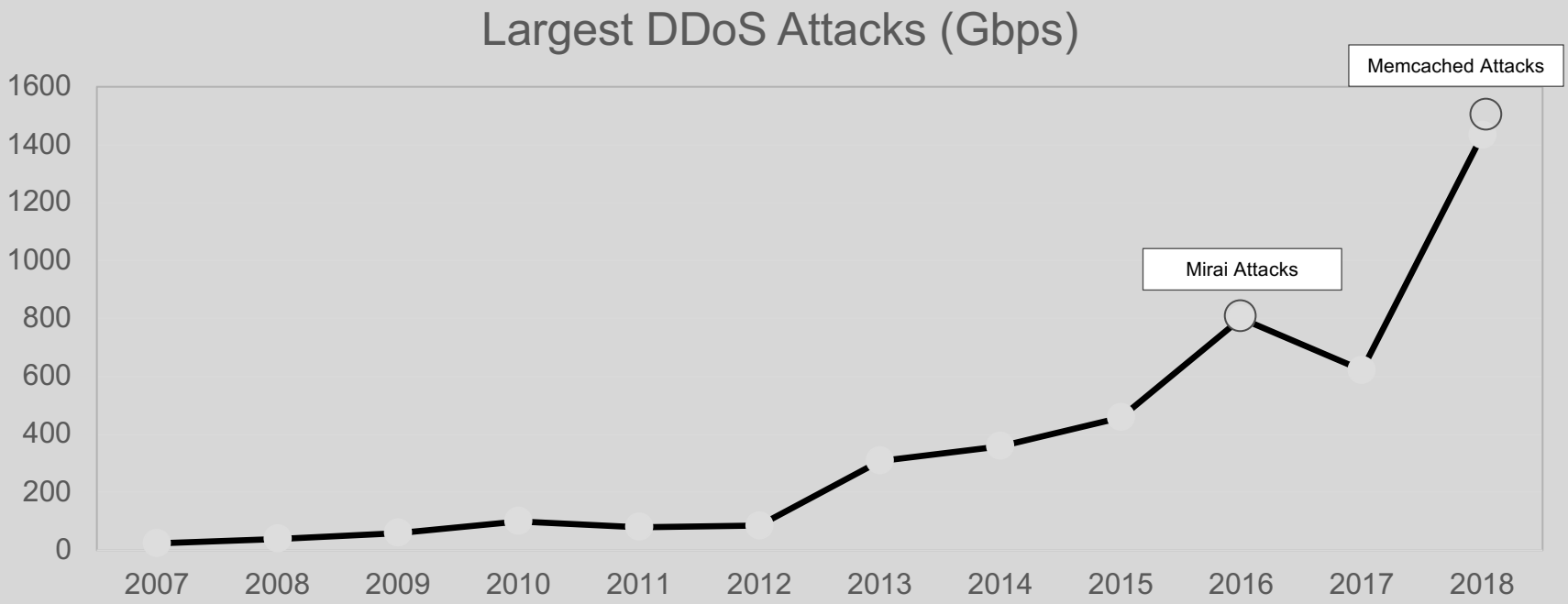
aws SUMMIT

aws SUMMIT

WAF/Shield

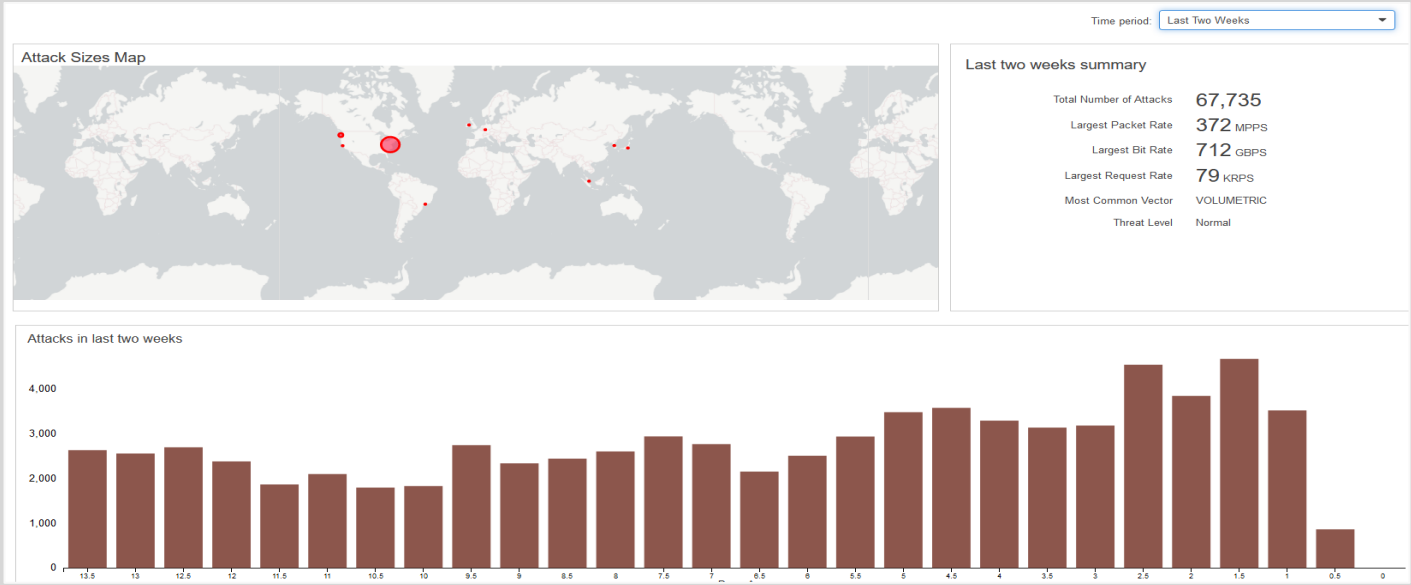
aws SUMMIT

DDoS Size Trend



DDoS Threats and Trends

AWS Shield detects and mitigates **1,000's of DDoS Attacks Daily**



*Source: AWS Global Threat Dashboard (Available for **AWS Shield Advanced** customers)*

AWS Shield
Standard

AWS Shield Standard

Layer 3/4 Protection for Everyone

- ✓ Automatic defense against the most common network and transport layer DDoS attacks for any AWS resource, in any AWS Region
- ✓ Comprehensive defense against all known network and transport layer attacks when using Amazon CloudFront and Amazon Route 53
- ✓ SYN Floods, UDP Floods, Reflection Attacks, etc.

AWS WAF

Layer 7 Protection Available via AWS WAF

- ✓ Self-service & pay-as-you-go
- ✓ Flexible rule language
- ✓ Fast rule propagation

AWS Shield Advanced:
Enhanced Protection

Detection

- Layer 7 attack detection (HTTP Floods, DNS Query Floods)
- Baselining and Anomaly detection
- Enhanced Layer 3 attack detection
- Granular detection thresholds (for regional services EC2/ELB only)

Mitigation

- Proprietary packet filtering stacks
- Suspicion-based filtering
- Advanced mitigations like SYN Throttling
- Pre-configured mitigations according to resource type
- Customer defined Mitigations
- Traffic Engineering for Large DDoS Attacks
- Network ACLs executed at the border for EIPs

AWS Shield Advanced:
DDoS Response Team (DRT)

For more sophisticated and complex attacks

Pre-emptive Engagements

- DDoS Architecture Review
- Fire Drills and basic DDoS WAF rules consultation
- Custom mitigation templates for EIPs (EC2/NLBs)

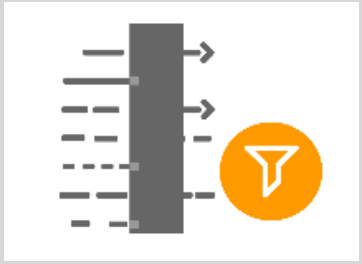
24x7 Incident Response

- Automatically engaged for availability impacting L3/4 events
- Customer driven support cases through AWS Support or AWS Shield Engagement Lambda
- Incident triaging
- Manual traffic engineering

AWS Shield
Standard & **Advanced**

DDoS Expertise	Built-in DDoS Protection for Everyone	Enhanced Protection	24x7 access to DDoS Response Team (DRT)
Visibility & Compliance	CloudWatch Metrics	Attack Diagnostics	Global threat environment dashboard
Economic Benefits	AWS WAF at no additional cost *for protected resources*	Cost Protection for scaling	

What is AWS WAF

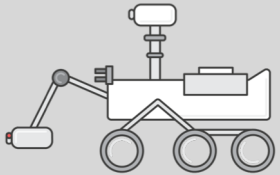


Web traffic filtering with custom rules

Malicious request blocking

Active monitoring and tuning

Biggest Threats to Applications today



	DDoS	OWASP Top 10	Bad Bots
Application Layer 	HTTP floods Abusive users	SQL injection XSS Application exploits	Crawlers Content scrapers Scanners & probes

What can we do with an AWS WAF?

1. Malicious traffic blocking

- SQLi
- XSS
- IP Blacklists

2. Web traffic filtering

- Rate based rules
- IP Match & Geo-IP filters
- Regex & String Match
- Size constraints
- Action: Allow/Block

3. Active monitoring & tuning

- CloudWatch Metrics/Alarms
- Sampled Logs
- Count Action mode