Cloud Security Solution

Oct 2020

China – Risk Advisory | Cyber Risk Services

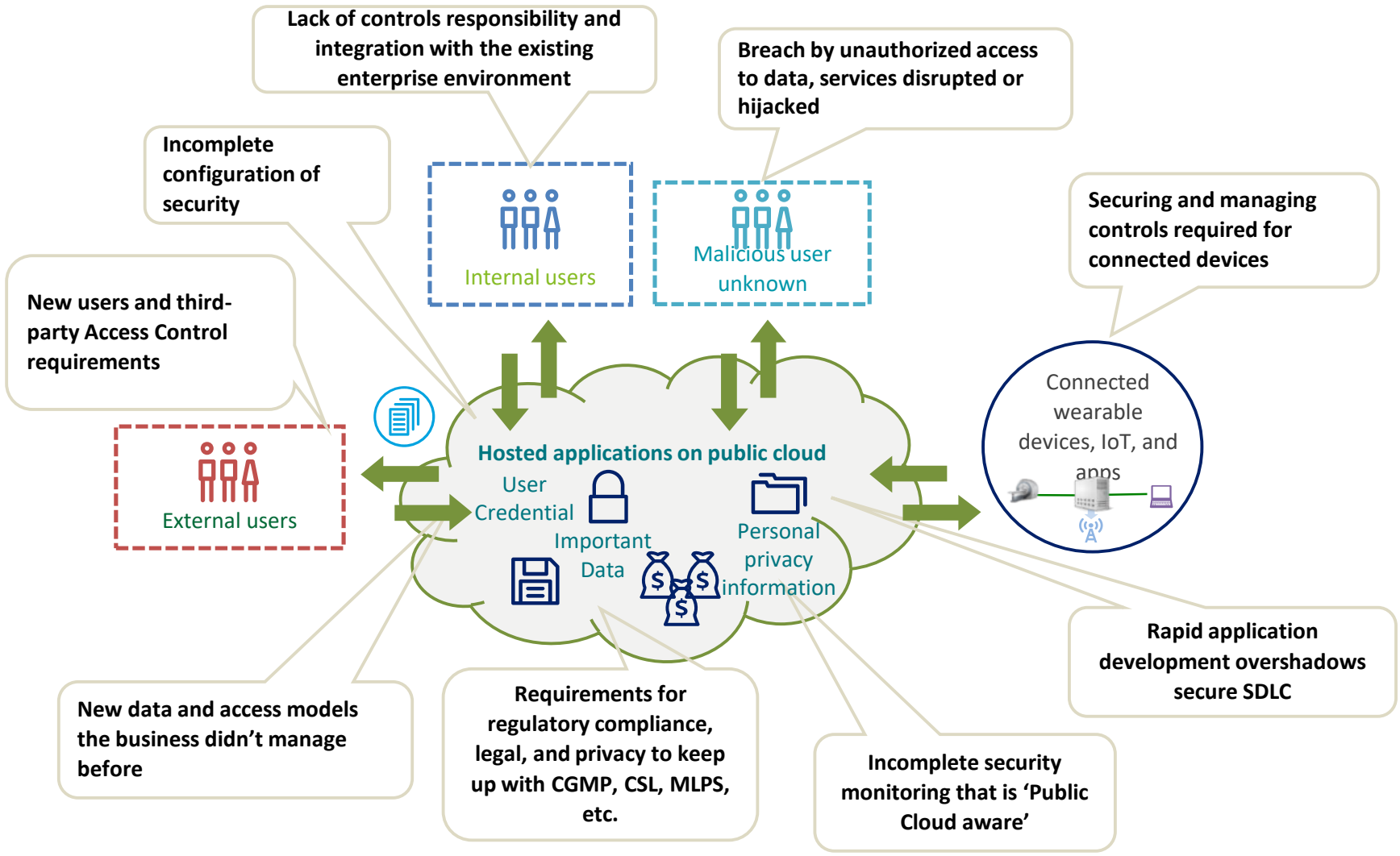
MAKING AN IMPACT THAT MATTERS since 1845

Common security challenges with client control responsibilities when adopting public clouds

Leverage Cloud Capability

Common Security control challenges

- Lack of identity and access management (IAM).
- Rapid application development overshadows secure software development life cycle (SDLC).
- Insecure data storage including sensitive information.
- Deviation of configuration by customers from public cloud leading practices.
- Incomplete logging and monitoring to efficiently detect and respond to external and insider threats.



Key Elements of Cloud Security considerations

Key elements of Cloud Cyber Security need be designed into the company AWS Cloud architecture.

Key Elements of Cloud Cyber Security

Define best practices related to **authentication and role based access controls**.

Examples include IAM, role and policy identification, AD integration mechanism etc.

Identify the **data protection and encryption/decryption solution** that should be followed by applications on cloud

Examples include data lifecycle management, encryption key management, Personal privacy information protection process etc.

Validate **network architecture** and ensure necessary zoning and protection mechanisms are in place

Examples include VLAN segregation, security group templates, VPN connect, least privilege access definition etc.

Evaluate additional requirements for increasing **security of cloud services** (PaaS) used in AWS cloud environments

Examples include application threat modeling, web scanning tools, test data sanitization approach etc.

Assess potential log sources and finalize the method for **logging and reporting** with analytics

Examples include log collection & storage architecture, tool selection, log lifecycle management etc.

Review **SIEM requirements** and define the approach for implementing it on AWS cloud

Examples include SIEM tools architecture, vulnerability assessment approach, configuration monitoring process etc.

Design **patching and update** processes for enhancing infrastructure security

Examples include OS patching and hardening tools, storage hardening policies, database patching approach in AWS Cloud.

Design and implement a **continuous monitoring and improvement model** for enhancing security architecture

Examples include periodic environments audits, security test design and approach, evaluation of new security offerings etc.

Key Elements of Cloud Security considerations

Infrastructure Security

- Infrastructure Monitoring
- Asset Management
- OS Image Hardening
- Change Management

Strategy & Governance

- Cloud Operating Model
- Policies and Standards
- Management processes

Cloud Resilience

- Backup Management & Verification
- Disaster Recovery Planning
- Operations Resiliency

Identity

- Access Federation & Single Sign-On
- Role Based Access Control
- Multi-Factors Authentication
- Third-Party Access Control

Vulnerability Management

- Configuration Compliance Monitoring
- AV & Malware Scanning
- Vulnerability Scanning
- Patch Management
- Remediation

Data Protection

- Policy governance
- Encryption of Data In Transit
- Encryption of Data At Rest
- Asset Tagging
- Key Management

Network Security

- Segmentation (Availability Zones, Subnets, Regions)
- VPN/Firewall, Security Groups Configuration

Security Monitoring & Management

- Security Event Monitoring
- Incident Response
- Log management

Deloitte will leverage China AWS best practice knowledge to design & build cloud solution aligned with China CSL, which is to ensure cyber security compliance in P.R.C.

Protect and manage my data at all times

- Enhancing data protection capabilities and processes for securing data as it is moved, processed, and stored across legacy enterprise and cloud environment
- Establishing capabilities and processes for managing increased vulnerabilities and complexity in multi-tenant cloud environments
- Adhering to regulatory requirements managing complex data residency and classification issues

Monitor and stay vigilant in the cloud environment

- Enhancing security monitoring capabilities and processes for establishing unified monitoring dashboards (single pane of glass view)
- Enhancing monitoring solutions, including connectors to meet demands cloud

Monitor and control user identity and access effectively

- Enhancing Identity and Access Management (IAM) capabilities for managing user identities across cloud platform and applications
- Extending access management capabilities to cloud platforms for streamlined control over user access
- Strengthening risk-based authentication capabilities like expanded password requirements for cloud-based resources

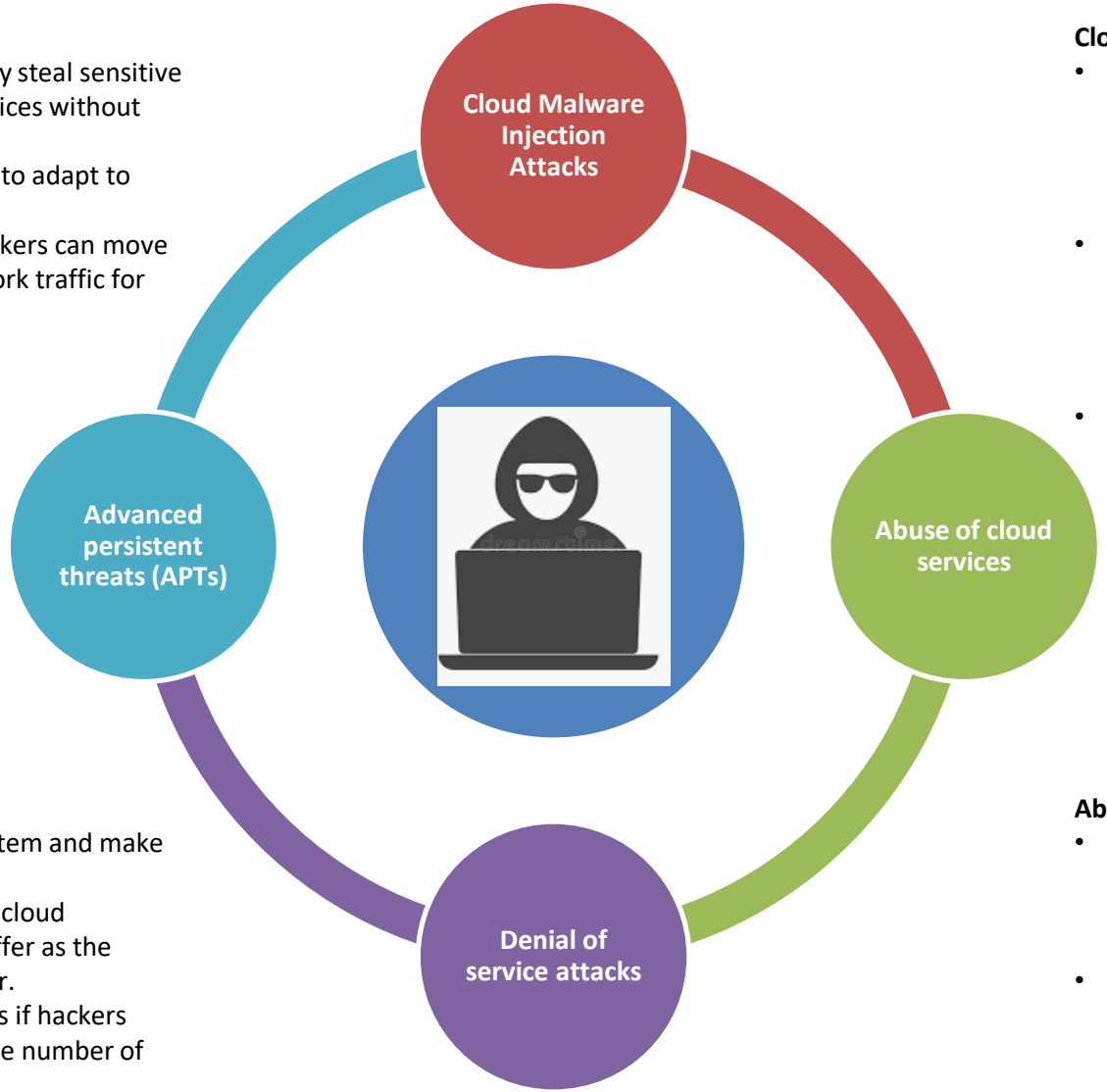
Mitigate and recover from adverse events/service failures

- Enhancing security operations and business continuity capabilities to handle cloud service failure events
- Establishing clear roles and responsibilities with the cloud service provider
- Enhancing incident response procedures considering potential impact and restrictions on shared cloud environments

Scenarios 2: Common Types of Attacks on Cloud Computing

Advanced Persistent Threats (APTs)

- APTs are attacks that let hackers continuously steal sensitive data stored in the cloud or exploit cloud services without being noticed by legitimate users.
- The duration of these attacks allows hackers to adapt to security measures against them.
- Once unauthorized access is established, hackers can move through data center networks and use network traffic for their malicious activity



Cloud Malware Injection Attacks

- Malware injection attacks are done to take control of a user's information in the cloud. For this purpose, hackers add an infected service implementation module to a SaaS or PaaS solution or a virtual machine instance to an IaaS solution.
- If the cloud system is successfully deceived, it will redirect the cloud user's requests to the hacker's module or instance, initiating the execution of malicious code. Then the attacker can begin their malicious activity such as manipulating or stealing data or eavesdropping.
- Examples: SQL injection attacks, Cross-scripting attacks and etc)

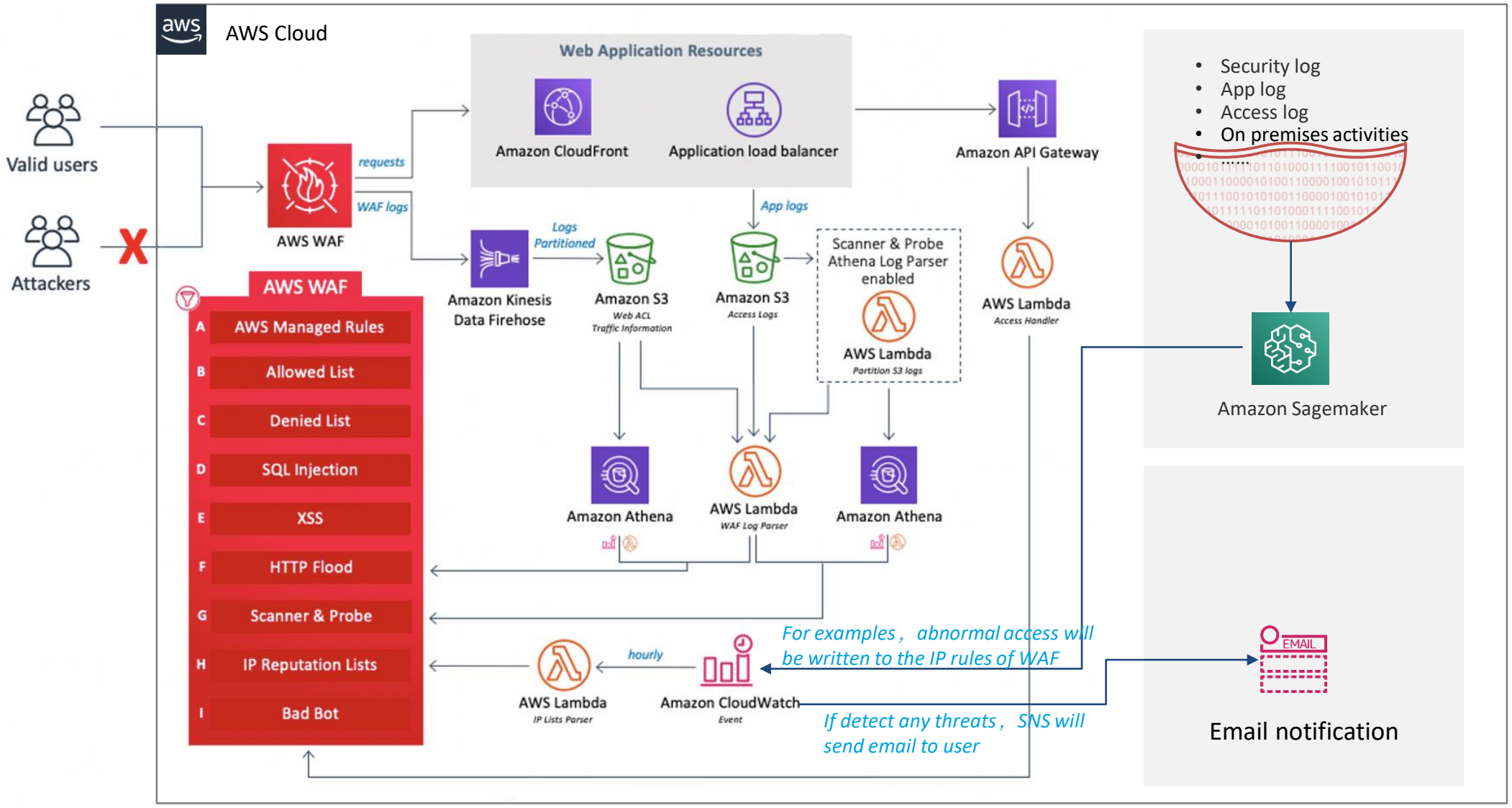
Denial of Service Attacks

- DoS attacks are designed to overload a system and make services unavailable to its users.
- These attacks are especially dangerous for cloud computing systems, as many users may suffer as the result of flooding even a single cloud server.
- DDoS attacks may be even more dangerous if hackers use more zombie machines to attack a large number of systems.

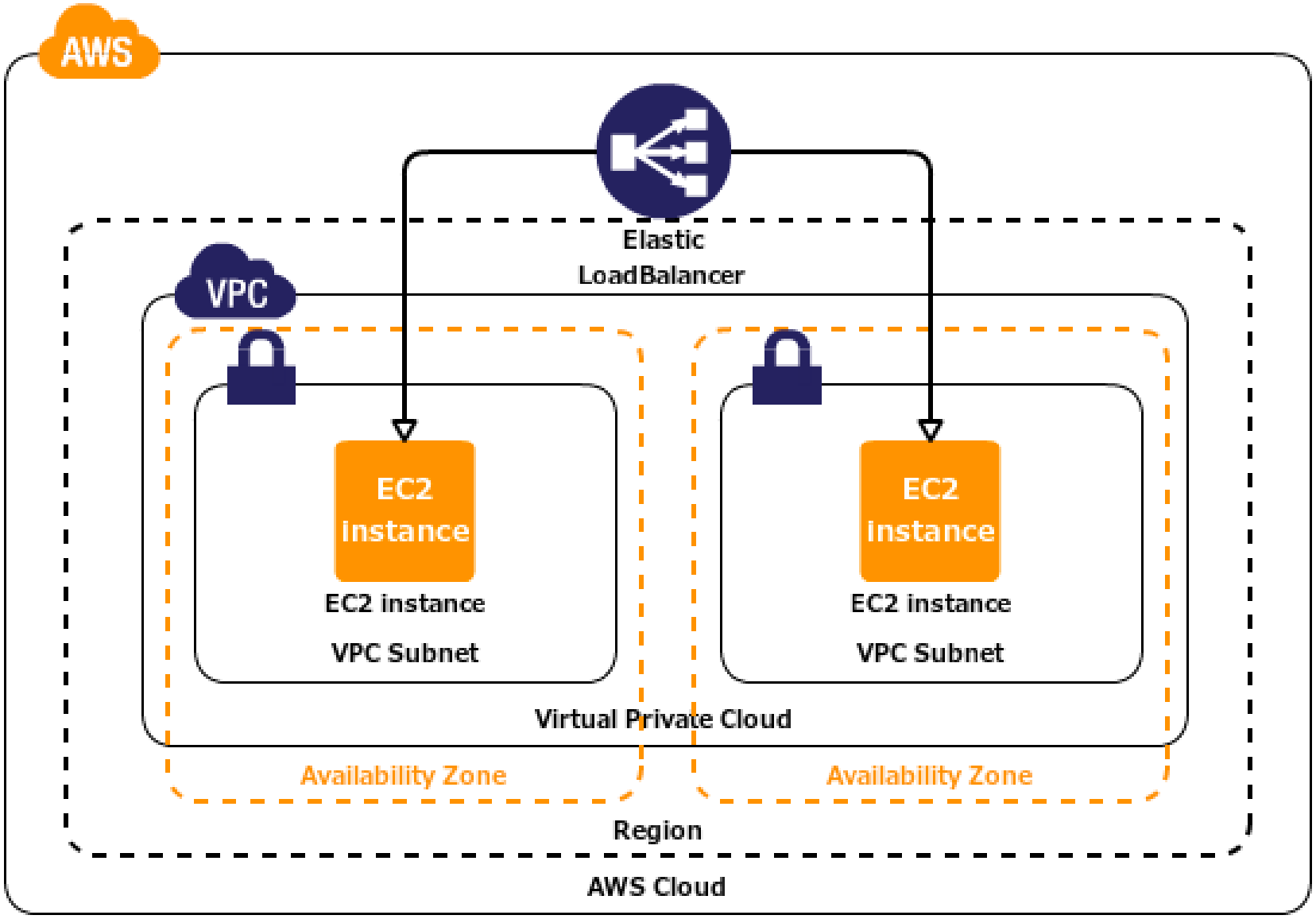
Abuse of Cloud Services

- Hackers can use cheap cloud services to arrange DoS and brute force attacks on target users, companies, and even other cloud providers.
- By renting servers from cloud providers, hackers can use powerful cloud capacities to send thousands of possible passwords to a target user's account

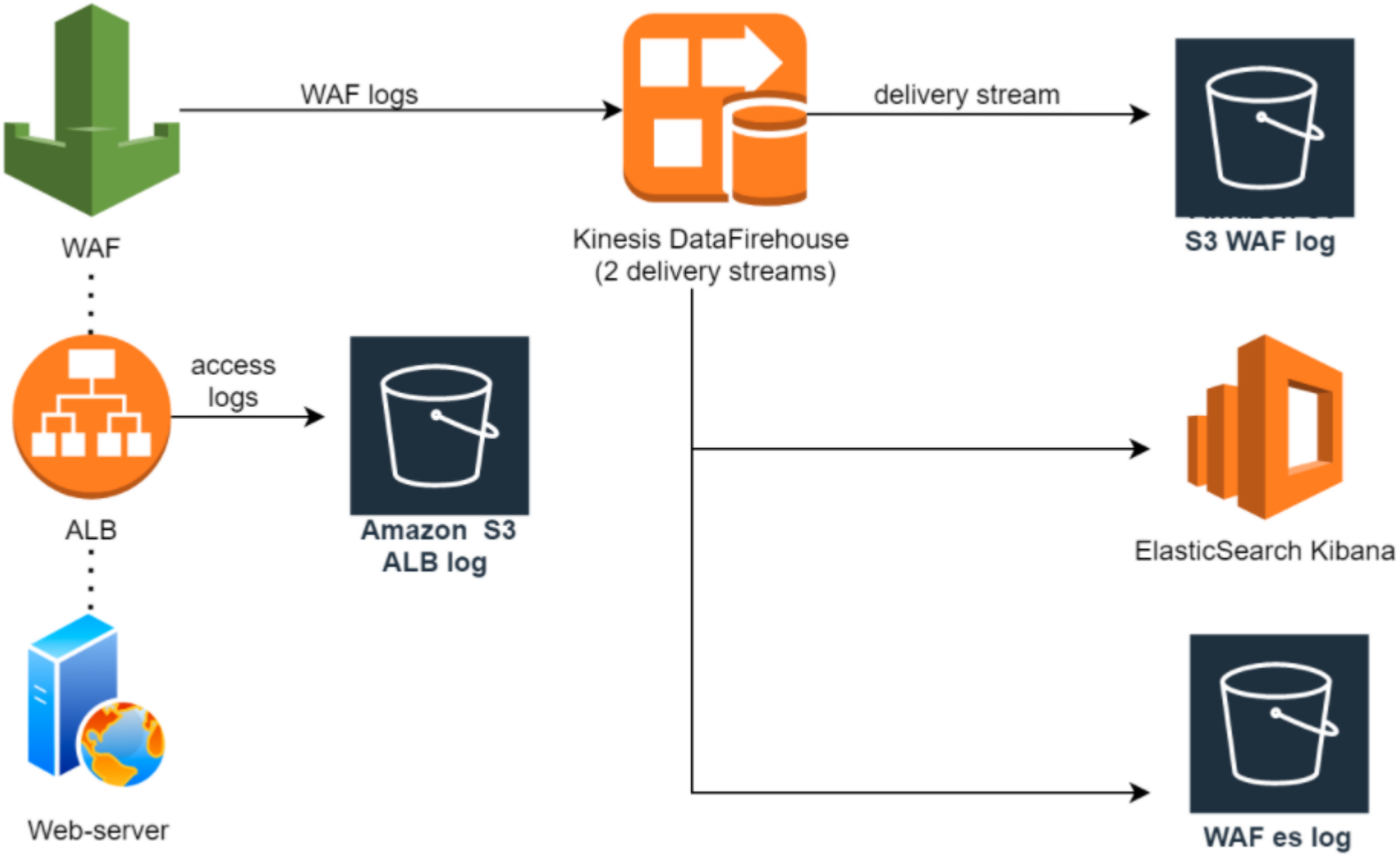
AWS Security implementation architecture for WAF Automation



Basic Infrastructure

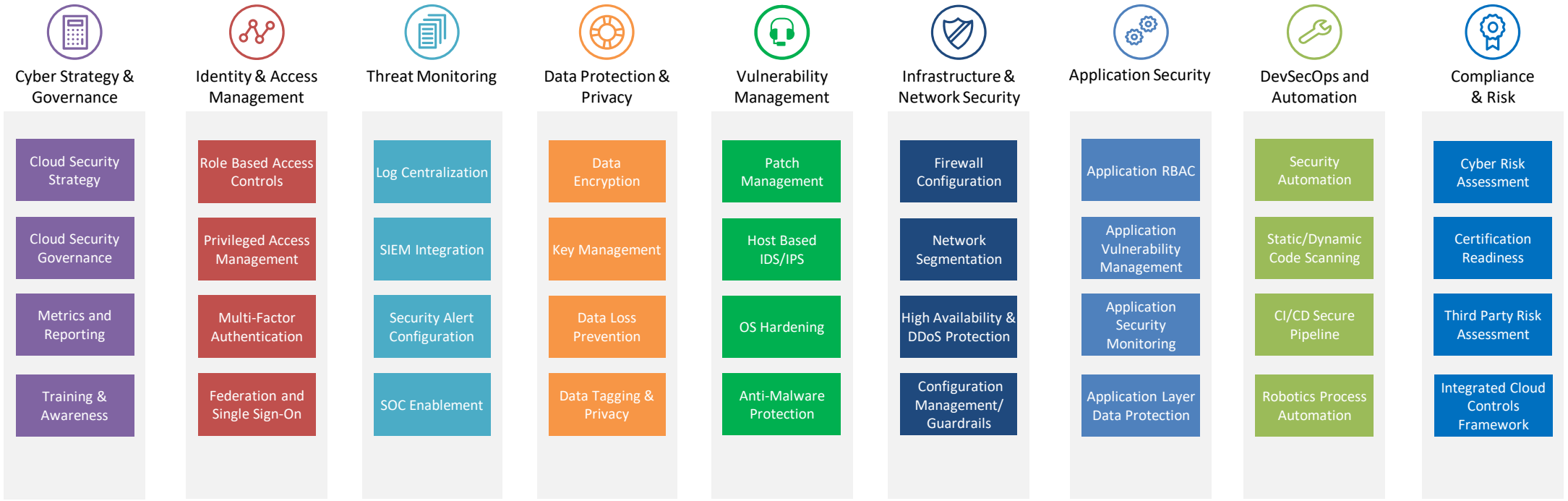


AWS WAF Demo architecture



Deloitte Cloud Cyber Risk Services

Our Cloud Cyber Risk Team can enable required capabilities across the entire spectrum of security domains



- **Services can be customized based on client requirements and deployed in multiple ways**
- **Flexible pricing based on consumption or solution based services**
- **Services should be included as part of AWS Cloud Migration and Transformation projects**
- **Cyber Risk assessment typically done prior to the design and implementation of security capabilities**

AWS Solution

Gartner Magic Quadrant for AWS

- AWS Named as a Cloud Leader for the 10th Consecutive Year in Gartner's Infrastructure & Platform Services Magic Quadrant
- Magic Quadrant for Operational Database Management Systems
- Magic Quadrant for Cloud AI Developer Services

Figure 1. Magic Quadrant for Cloud Infrastructure and Platform Services

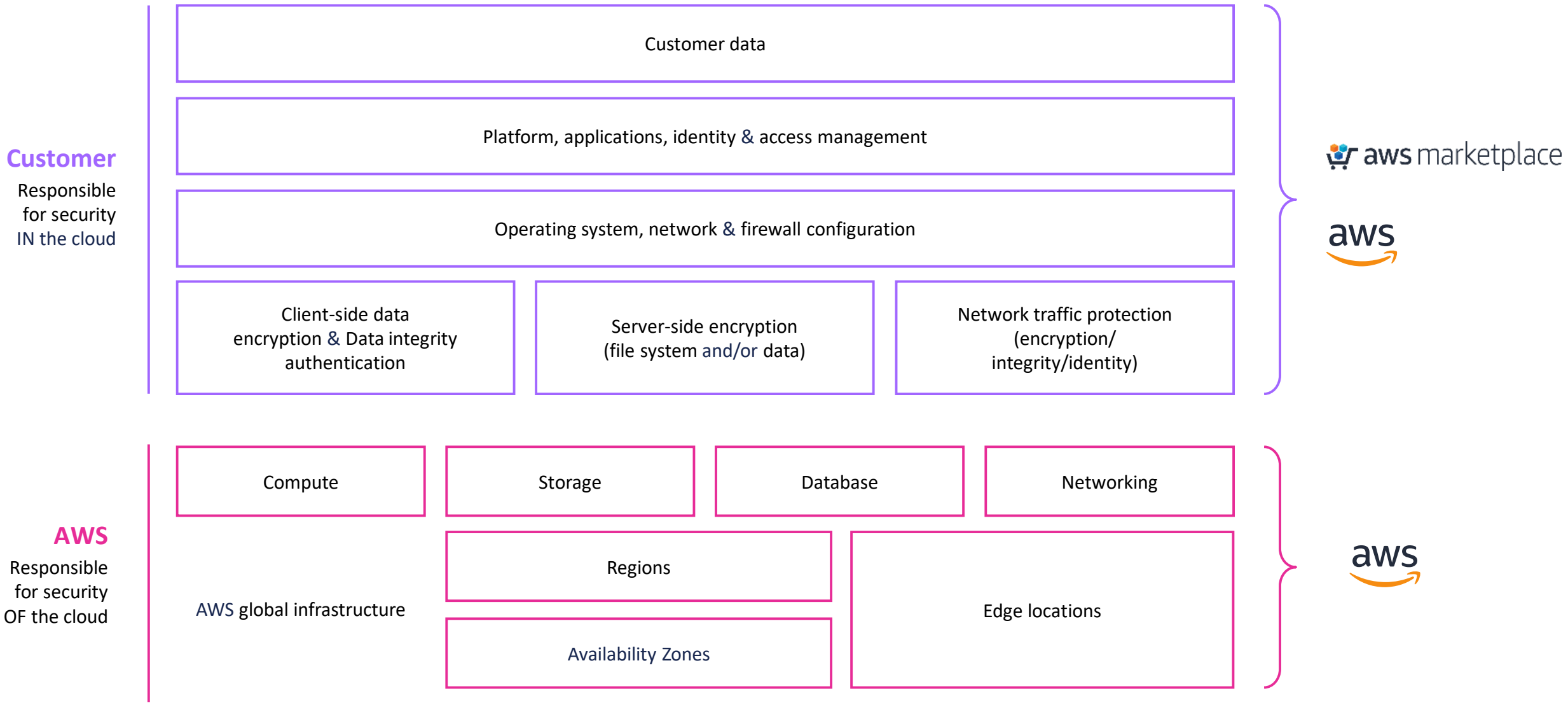
Figure 1. Magic Quadrant for Operational Database Management Systems

Source: Gartner (November 2019)

Figure 1. Magic Quadrant for Cloud AI Developer Services

Source: Gartner (February 2020)

Security & compliance is a shared responsibility



AWS security Services by function

Identity & access management

AWS Identity & Access Management (IAM)

AWS Single Sign-On

AWS Directory Service

Amazon Cognito

AWS Organizations

AWS Secrets Manager

AWS Resource Access Manager

Detective controls

AWS Security Hub

Amazon GuardDuty

AWS Config

AWS CloudTrail

Amazon CloudWatch

VPC Flow Logs

Infrastructure protection

AWS Systems Manager

AWS Shield

AWS WAF – Web application firewall

AWS Firewall Manager

Amazon Inspector

Amazon Virtual Private Cloud (VPC)

Data protection

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

Amazon Macie

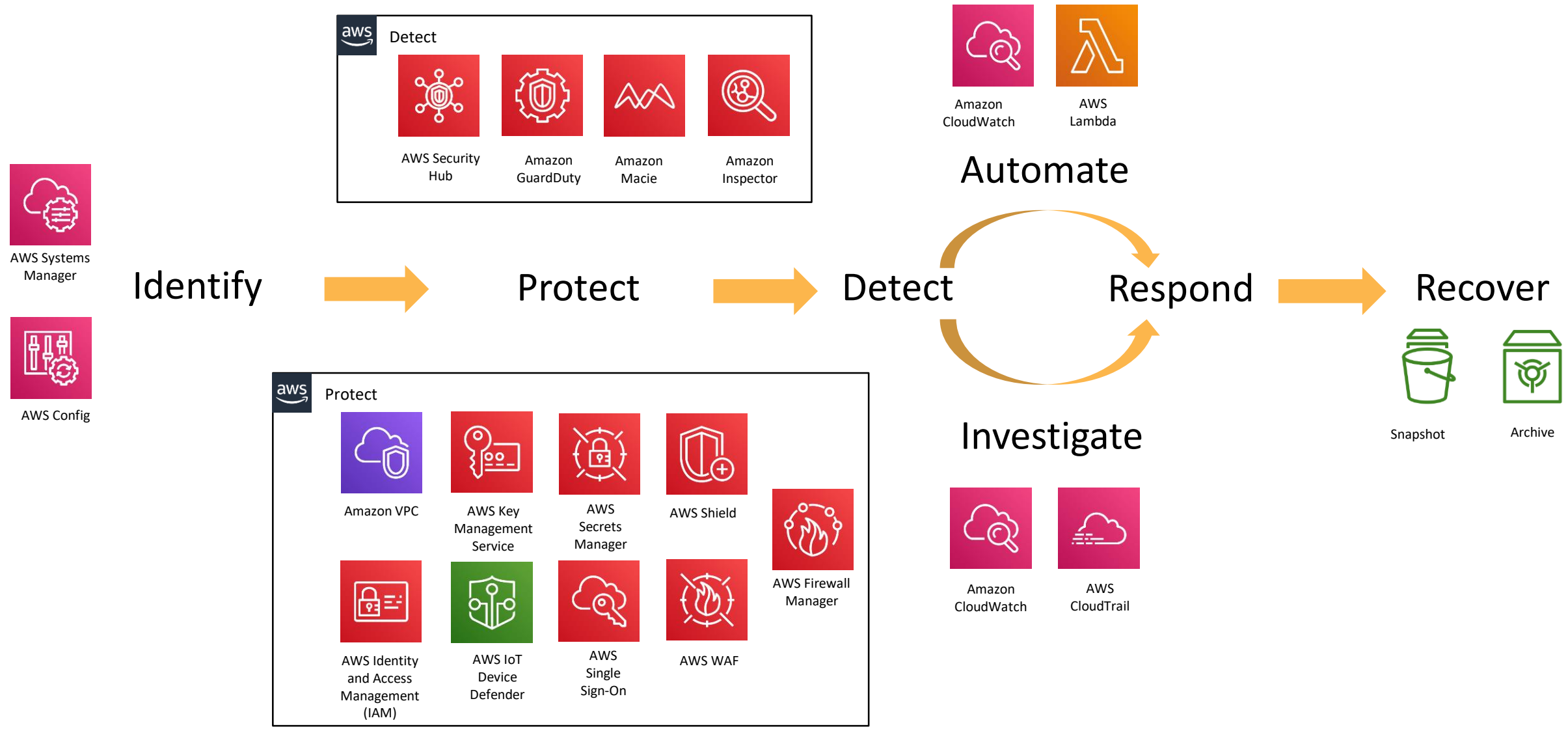
Server-Side Encryption

Incident response

AWS Config Rules

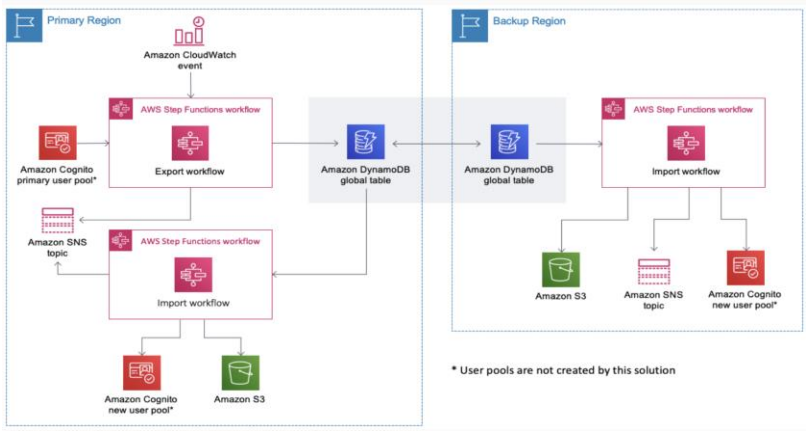
AWS Lambda

AWS Security Services by process



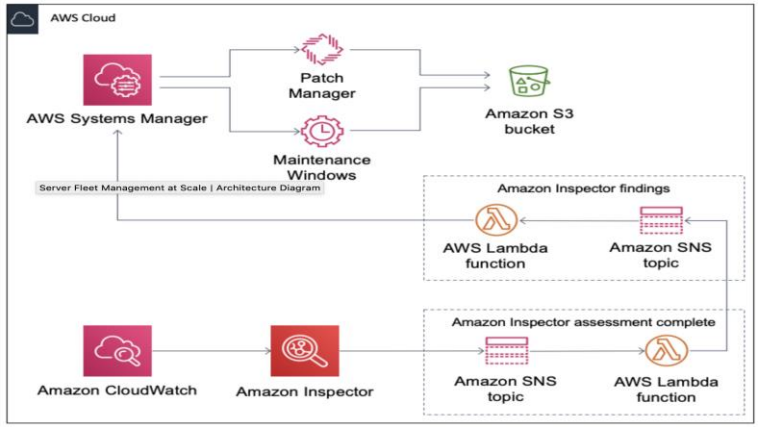
AWS Security reference architecture (extracts)

Cognito User Profiles Export Reference Architecture



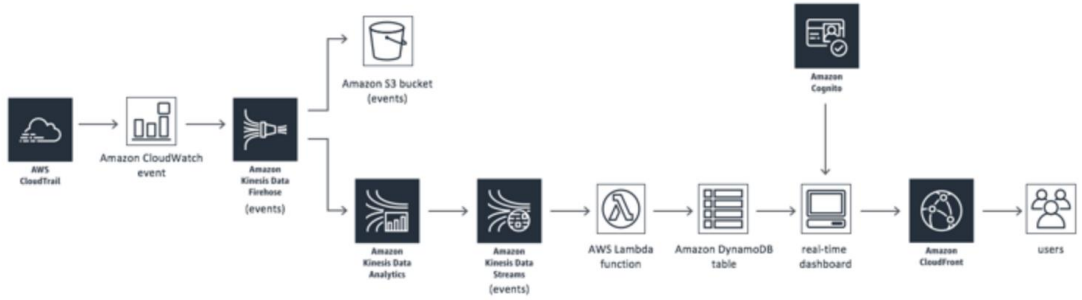
Many Amazon Web Services (AWS) customers use Amazon Cognito User Pools to provide a scalable and secure user directory for their applications. Amazon Cognito customers often need to export user information to facilitate more complex user queries, or to provide resiliency in case of Regional failure or accidental deletion of their users' profiles.

Server Fleet Management at Scale



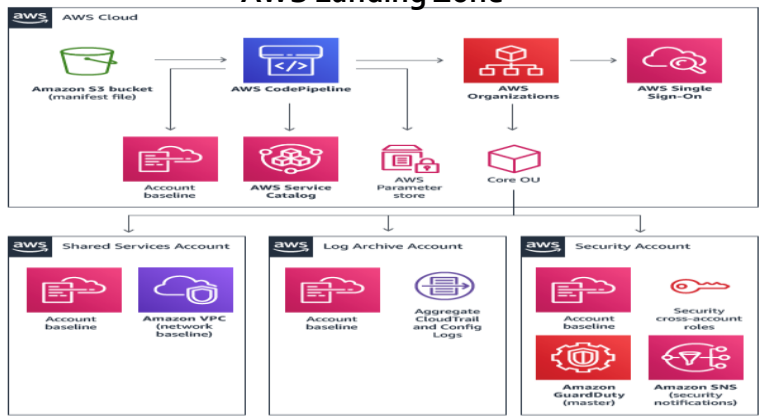
Amazon Web Services (AWS) customers who own a fleet of servers are sometimes unsure of how to best automate their fleet management for operational efficiency and maintenance. AWS Systems Manager provides a unified user interface so customers can view operational data from multiple AWS services, and allows customers to automate operational tasks across your AWS resources.

Real-Time Insights on AWS Account Activity



Monitoring Amazon Web Services (AWS) account activity can provide valuable insight into who is accessing your resources and how your resources are being used. This insight can help you make better-informed decisions that increase security and efficiency, facilitate compliance auditing, and optimize costs.

AWS Landing Zone



The AWS Landing Zone solution includes four accounts, and add-on products that can be deployed using the AWS Service Catalog such as the Centralized Logging solution and AWS Managed AD and Directory Connector for AWS SSO.

Case study - Pacific Magazines Moves to AWS for Stability and Scalability

Pacific Magazines is an Australian magazine publisher owned by Seven West Media. The company publishes *New Idea*, *InStyle*, *Marie Claire*, *Women's Health,* and other popular Australian lifestyle brands.

Customer's voice

" Everyone at Pacific Magazines—whether on the technical or business side—agrees that by moving to AWS we are effectively platformed for the future."

Will Everitt,
Director of Digital Products and Technology, Pacific Magazines

Benefits of AWS

- Withstood a 500% spike during a DDoS attack
- Increased availability to 99.99%
- Reduced hosting costs by 16%
- Exceeded benchmarks by 21%
- Expanded audience traffic by 24%

AWS Services used

- AWS Auto Scaling
- AWS Web Application Firewall (WAF)
- Amazon Elastic Container Service
- Amazon CloudFront

https://aws.amazon.com/cn/solutions/case-studies/pacific-magazines-case-study/?nc1=h_ls

Case study - Siemens Handles 60,000 Cyber Threats per Second Using AWS Machine Learning

Siemens AG is a global electrification, automation, and digitalization leader. The company provides solutions for power generation and transmission, medical imaging, laboratory diagnostics, and industrial infrastructure and drive systems.

Customer's voice

"On AWS, our AI-driven cybersecurity platform easily exceeds the strongest published benchmarks in the world."

-Jan Pospisil, Senior Data Scientist, Siemens Cyber Defense Center

Benefits of AWS

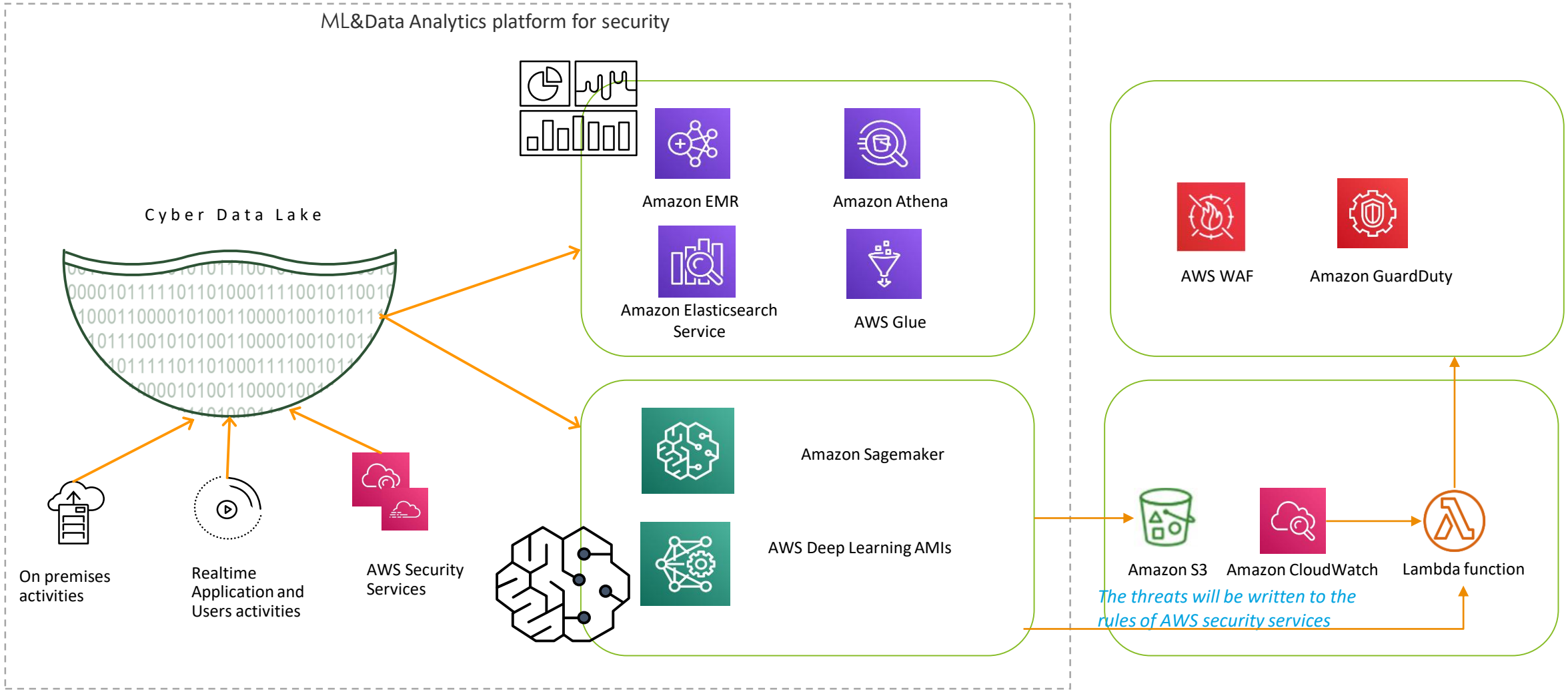
- Cybersecurity solution exceeds published benchmarks
- Evaluates 60,000 threats per second
- Forensic analysis doesn't slow system performance
- Solution is managed by 12 employees

AWS Services used

- Amazon SageMaker
- AWS Glue
- AWS Lambda
- Amazon Simple Storage Service

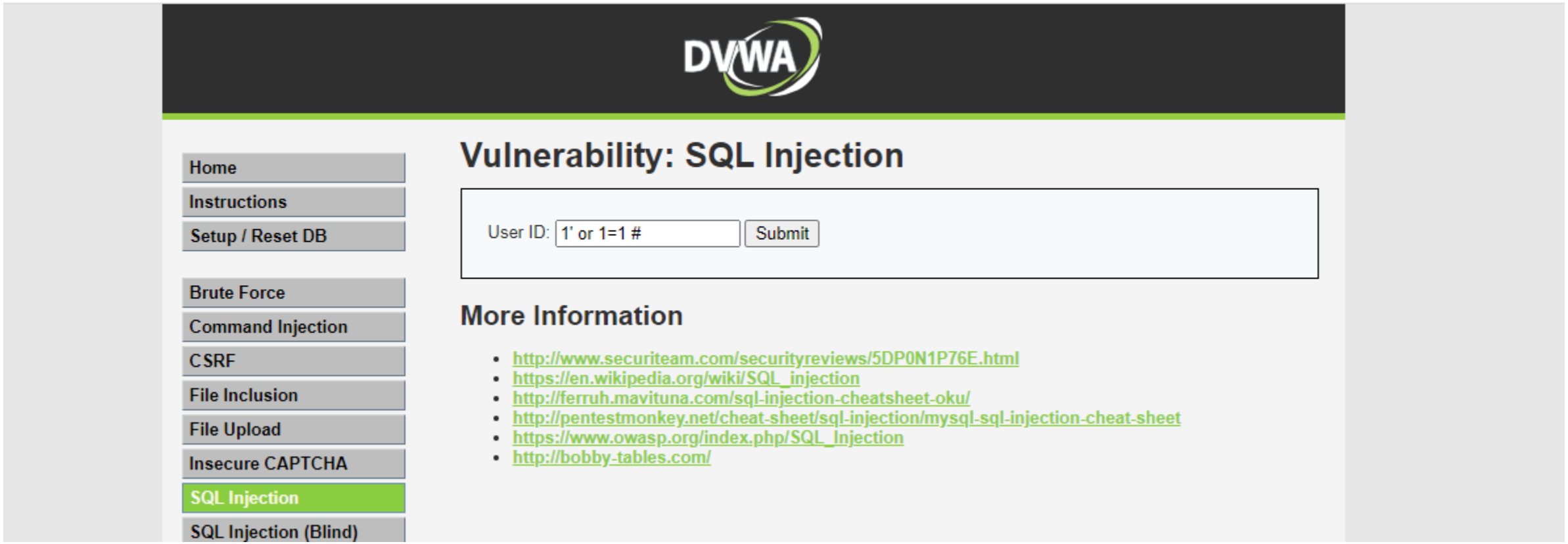
https://aws.amazon.com/solutions/case-studies/siemens-cybersecurity/?nc1=h_ls

Siemens ML&Data Analytics platform for security



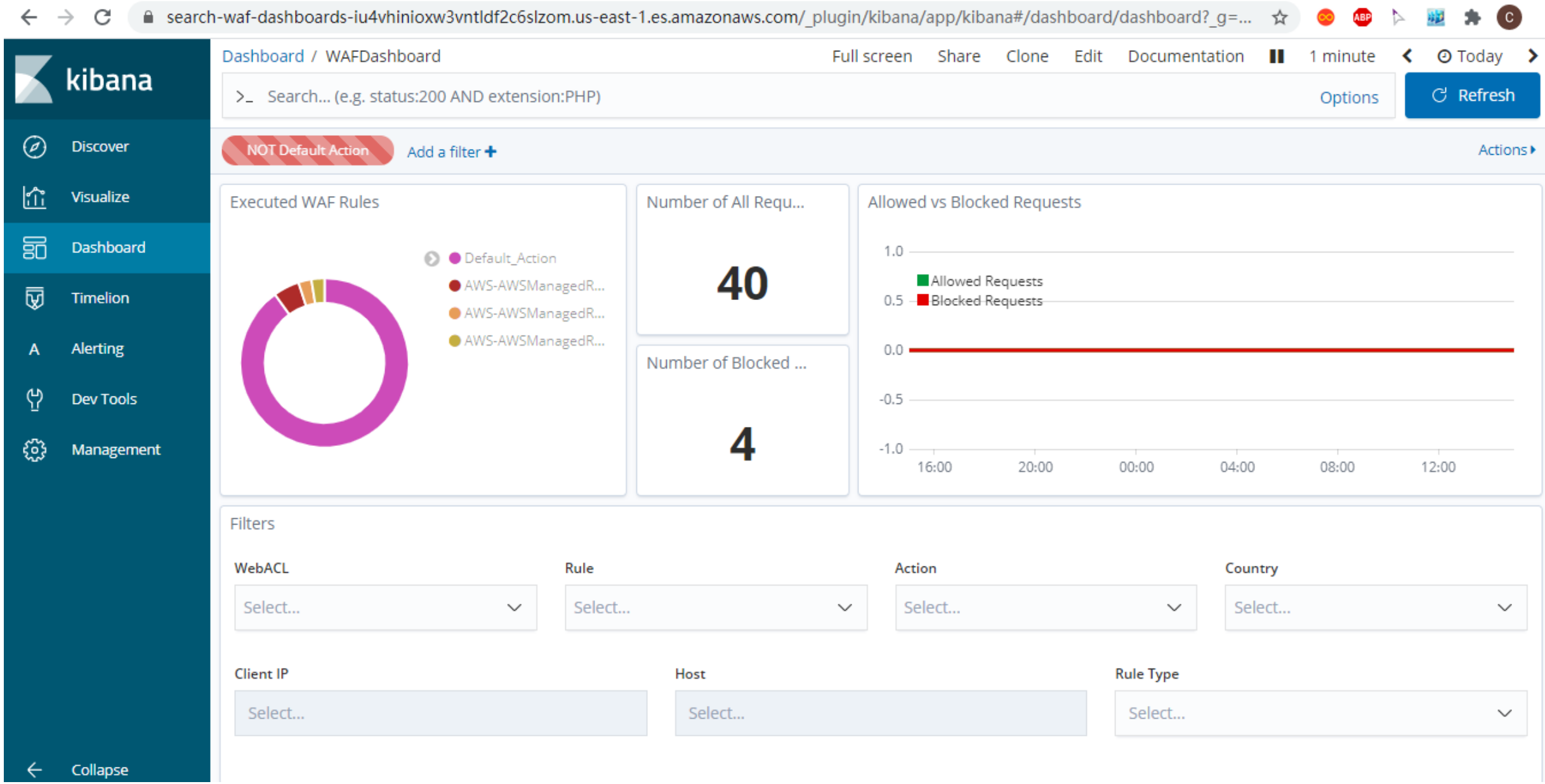
DEMO

不安全 | waf-alb-demo-1353180285.us-east-1.elb.amazonaws.com/DVWA/vulnerabilities/sqli/



不安全 | waf-alb-demo-1353180285.us-east-1.elb.amazonaws.com/DVWA/vulnerabilities/sqli/?id=1%27+or+1%3D1+%23&Submit=Submi...

403 Forbidden


search-waf-dashboards-iu4vhinioxw3vntldf2c6slzom.us-east-1.es.amazonaws.com/_plugin/kibana/app/kibana#/dashboard/dashboard?_g=...
kibana
Discover
Visualize
Dashboard
Timelion
Alerting
Dev Tools
Management
Collapse
Dashboard / WAFDashboard
Full screen
Share
Clone
Edit
Documentation
1 minute
Today
Search... (e.g. status:200 AND extension:PHP)
Options
Refresh
NOT Default Action
Add a filter +
Actions
Executed WAF Rules
Default_Action
AWS-AWSManagedR...
AWS-AWSManagedR...
AWS-AWSManagedR...
Number of All Requ...
40
Number of Blocked ...
4
Allowed vs Blocked Requests
1.0
0.5
0.0
-0.5
-1.0
Allowed Requests
Blocked Requests
16:00
20:00
00:00
04:00
08:00
12:00
Filters
WebACL
Rule
Action
Country
Select...
Client IP
Host
Rule Type

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 312,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

The Deloitte brand entered the China market in 1917 with the opening of an office in Shanghai. Today, Deloitte China delivers a comprehensive range of audit & assurance, consulting, financial advisory, risk advisory and tax services to local, multinational and growth enterprise clients in China. Deloitte China has also made—and continues to make—substantial contributions to the development of China's accounting standards, taxation system and professional expertise. Deloitte China is a locally incorporated professional services organization, owned by its partners in China. To learn more about how Deloitte makes an Impact that Matters in China, please connect with our social media platforms at www2.deloitte.com/cn/en/social-media.