



Cloud Security

Migration, management, automation

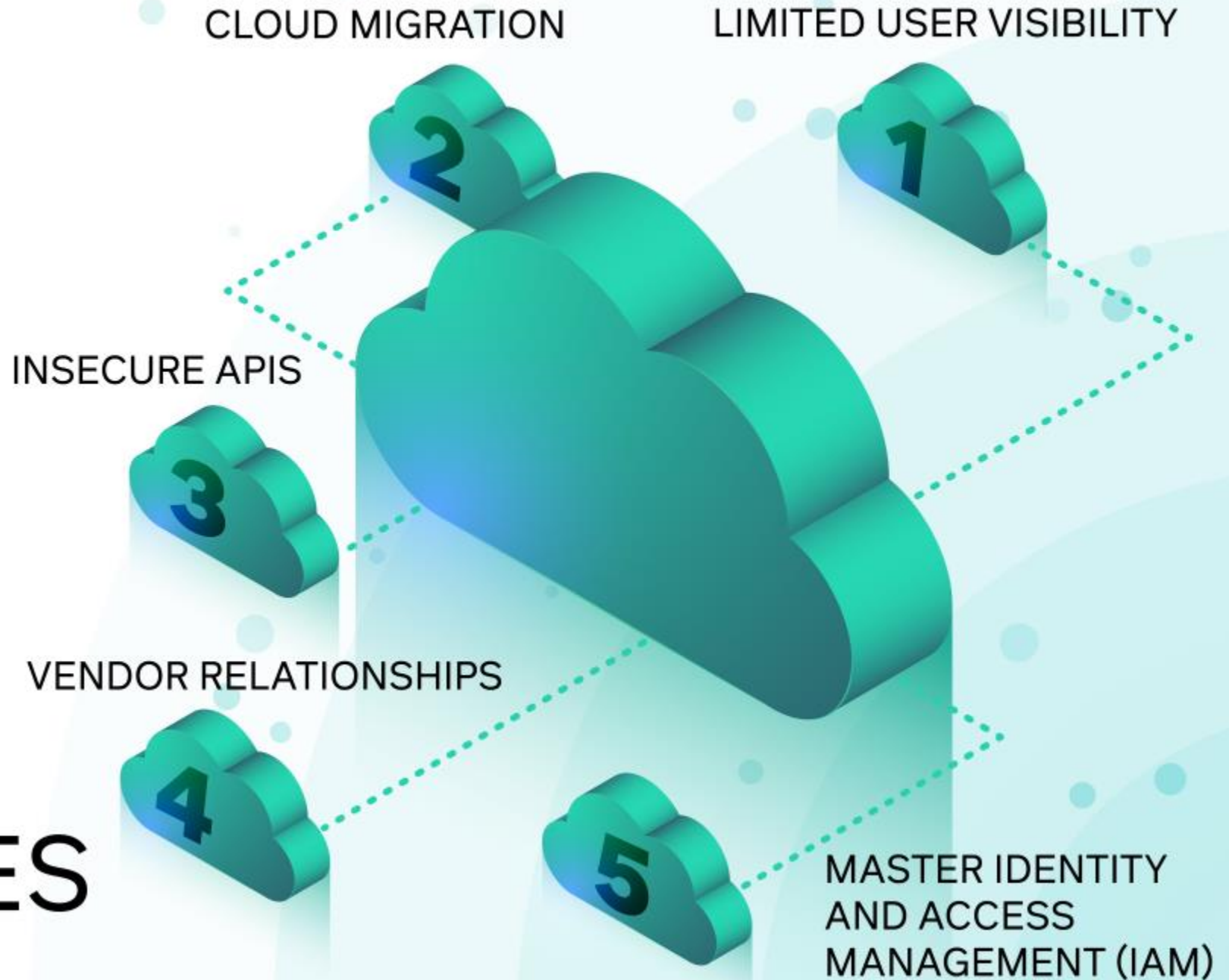
Zhuo Ding



Agenda

- Topic one: Cloud transformation & migration
- Topic two: Cloud security enhancement
- Topic three: Cloud security management
- Topic four: Cloud security automation

5 MOST PRESSING CLOUD- BASED CYBER SECURITY CHALLENGES



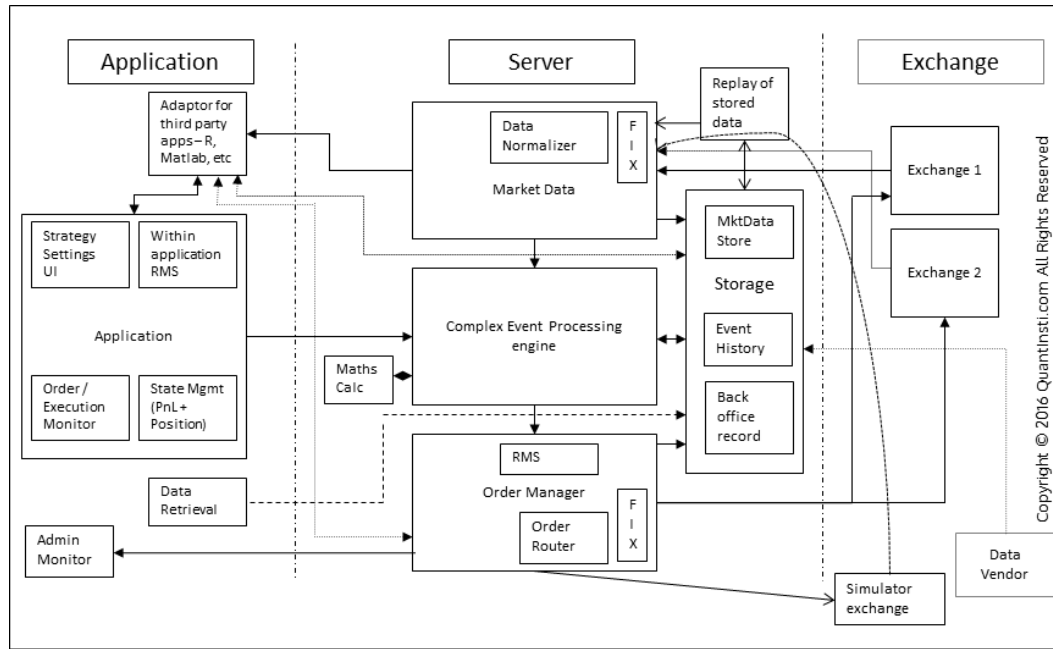


Topic one

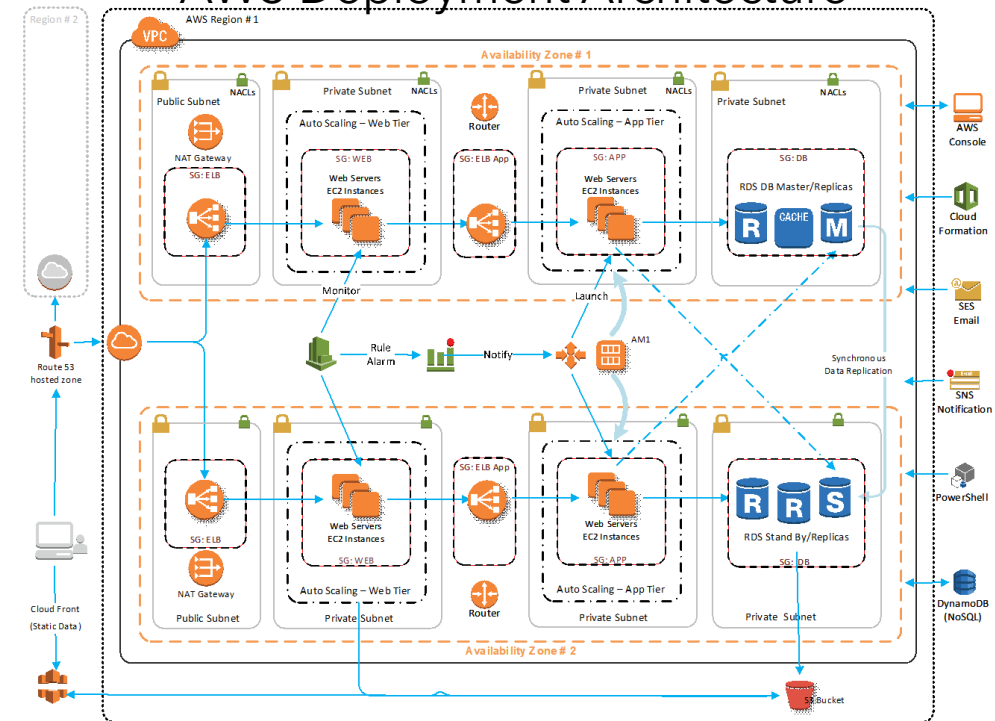
Cloud transformation & migration

Project 1: ECP1(Enterprise Cloud Platform1) -Online trading platform AWS migration

Application Architecture

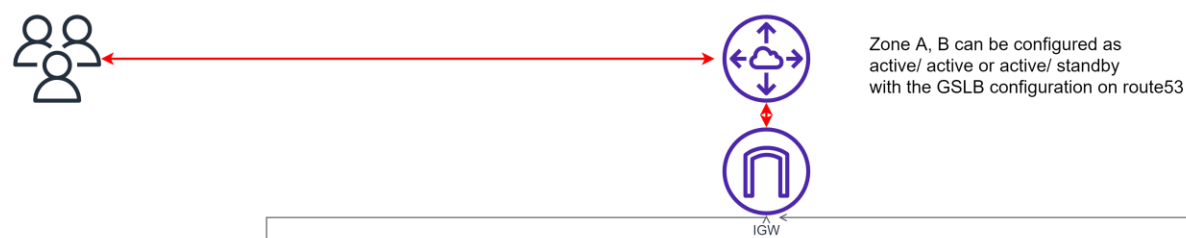


AWS Deployment Architecture



Environment: JS/Java/Springboot/apache/MQ/redis/zoomkeeper/Microservice/RDS/DynamoDB/VM/Docker container/Kubernetes
AWS Cloud deployment/provision/monitoring tools: AWS cloud formation, system manager, EC2, S3, routeS3, cloudwatch logs, etc
AWS Cloud security security hub, GuardDuty, AWS identity/Access management, Cloudtrail, Certificate manager, lambda,SNS/SQS,etc

Security design(internet trading platform)



Web Zone Subnet routing table for Zone A

Destination	Target
10.0.0.0/16	VPC-ID-AZ-A
0.0.0.0/0	IGW-ID

Web Zone security group ACL rules

Source	Destination	TCP
0.0.0.0/0	Web VIP	10.0.0.1/32 443

App Zone Subnet routing table for Zone A

Destination	Target
10.0.0.0/16	VPC-ID-AZ-A
10.1.0.0/16	VPC-ID-AZ-B

APP Zone security group Ingress ACL rules

Source	Destination	TCP
10.0.0.0/24	APP_VIP1	10.0.1.1/32 8001
10.0.0.0/24	APP_VIP2	10.0.1.2/32 8002
10.0.0.0/24	APP_VIP3	10.0.1.3/32 8003

APP Zone Security Egress ACL rules

Source	Destination	TCP
10.0.1.0/24	Zone B DB	10.1.2.0/24 3306

DB Zone Subnet routing table for Zone A

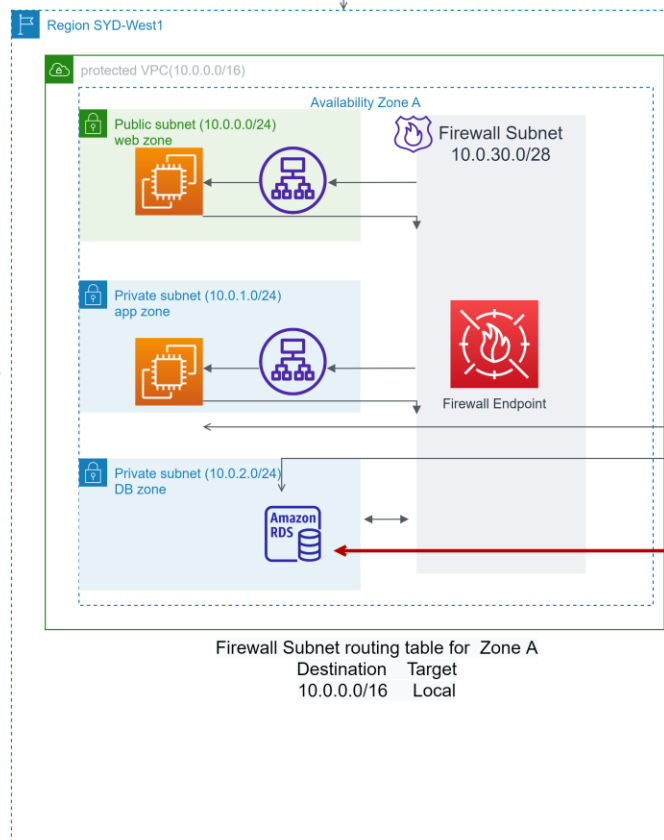
Destination	Target
10.0.0.0/16	VPC-ID-AZ-A
10.1.1.0/24	VPC-ID-AZ-B

DB Zone security group ingress ACL rules

Source	Destination	TCP
10.0.1.0/24	DB_VIP1	10.0.2.1/32 3306
10.1.1.0/24	DB_VIP 1	10.0.2.1/32 3306

DB Zone security Egress ACL rules

Source	Destination	TCP
10.0.2.0/24	10.1.2.0/24	3307



Firewall Subnet routing table for Zone A

Destination	Target
10.0.0.0/16	Local

Intra AZ APP->RDS

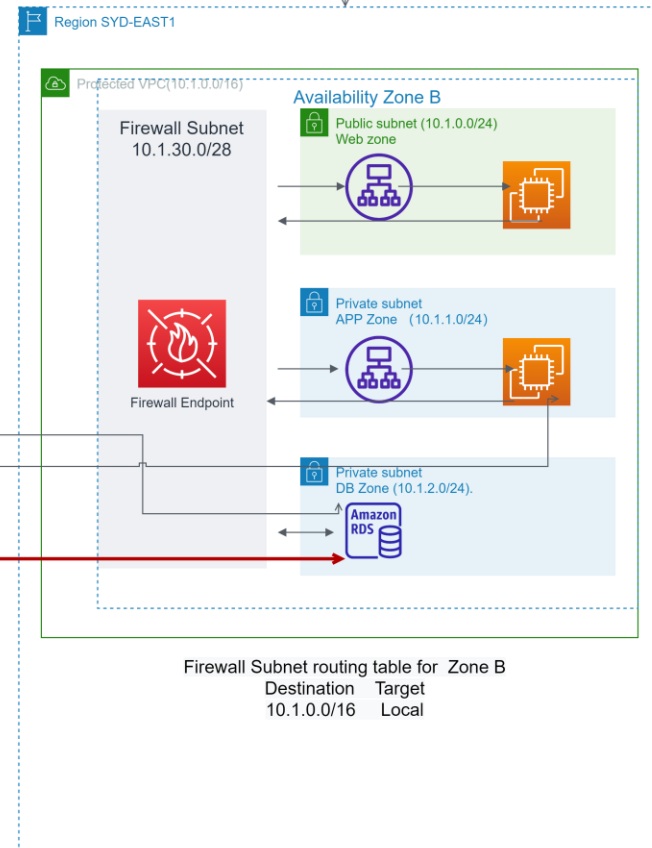
RDS sync/ replication

Intra Zone A/B traffic ACL rules

Source	Destination	TCP
10.0.1.0/24	Zone B DB	10.1.2.0/24 3306

Zone A app servers visit Zone B DB on tcp 3306

Zone B All servers visit Zone A DB on tcp 3306



Firewall Subnet routing table for Zone B

Destination	Target
10.1.0.0/16	Local

Web Zone Subnet routing table for Zone B

Destination	Target
10.1.0.0/16	VPC-ID-AZ-B
0.0.0.0/0	IGW-ID

Web Zone security group ACL rules

Source	Destination	TCP
0.0.0.0/0	Web VIP	10.1.0.1/32 443

App Zone Subnet routing table for Zone A

Destination	Target
10.0.0.0/16	VPC-ID-AZ-A
10.1.0.0/24	VPC-ID-AZ-B

APP Zone security group inbound ACL rules

Source	Destination	TCP
10.1.0.0/24	APP_VIP1	10.1.1.1/32 8001
10.1.0.0/24	APP_VIP2	10.1.1.2/32 8002
10.1.0.0/24	APP_VIP3	10.1.1.3/32 8003

intra Zone A-B traffic Source Destination TCP

Source	Destination	TCP
10.1.1.0/24	Zone A DB	10.0.2.0/24 3306

DB Zone Subnet routing table for Zone A

Destination	Target
10.1.0.0/16	VPC-ID-AZ-B
10.0.1.0/24	VPC-ID-AZ-A

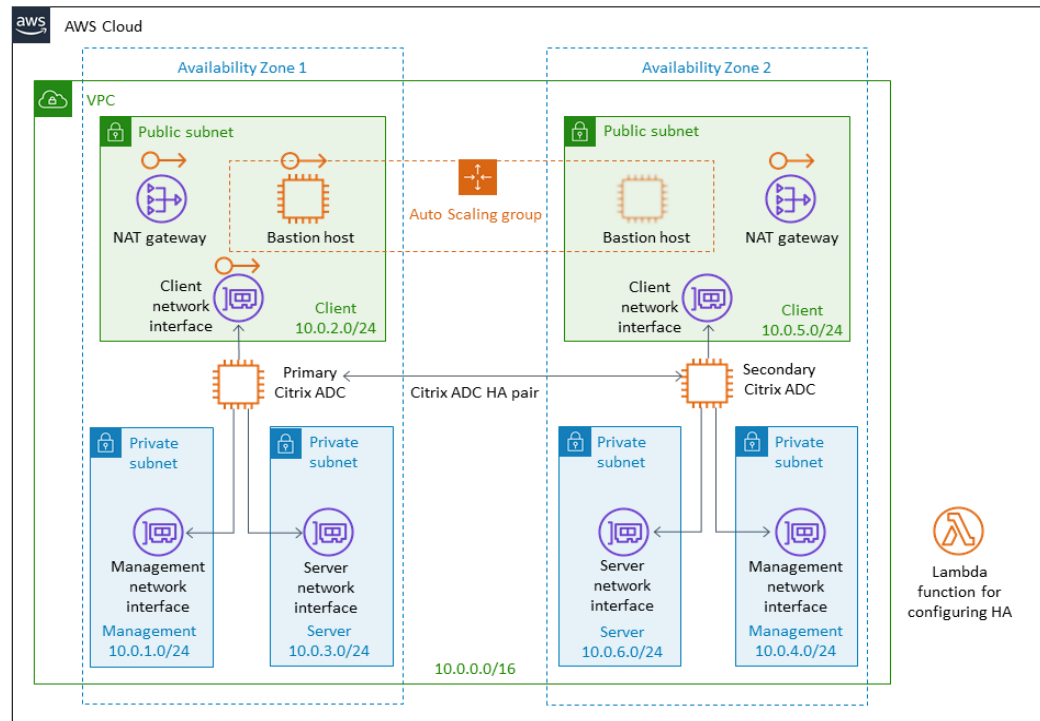
DB Zone security group ACL rules

Source	Destination	TCP
10.1.1.0/24	DB_VIP1	10.1.2.1/32 3306
10.0.1.0/24	DB_VIP1	10.1.2.1/32 3306

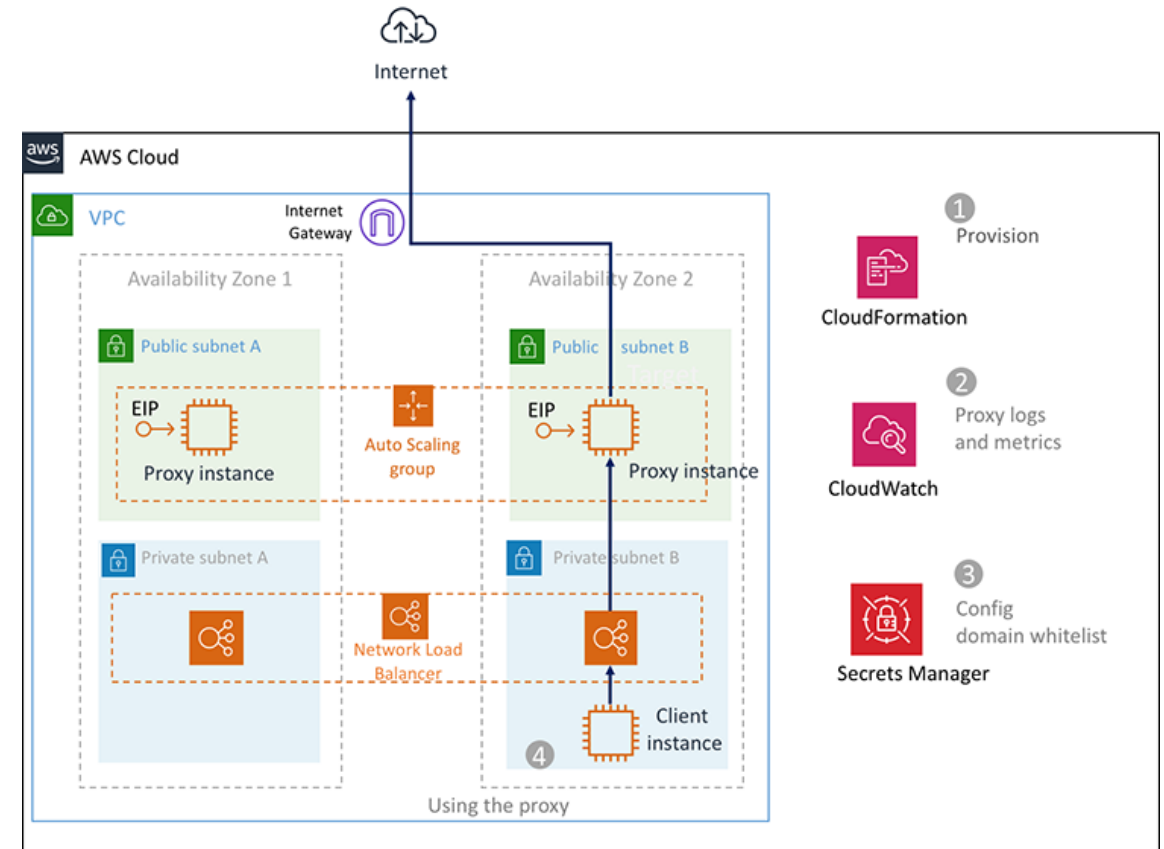
DB Zone security Egress ACL rules

Source	Destination	TCP
10.1.2.0/24	10.0.2.0/24	3307

Project 2: ECP1 AWS cloud VMFW/citrix ADC/SG security enhancement



AWS enhancement stage1: WAF /load balancer citrix ADC netscaler, F5 WAF/LTM deployment(BYOL)



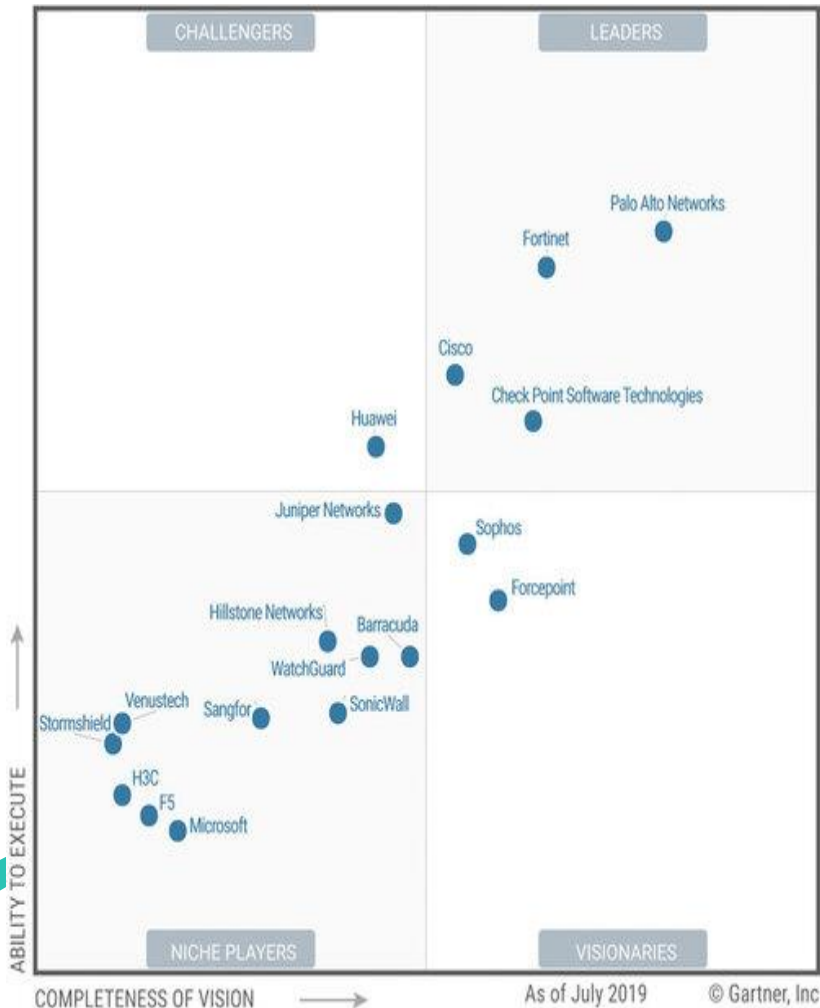
AWS enhancement stage 2: Secure SG proxy deployment(BYOL)

Project 3: Unified Cloud Security Management CSPM/CWPP

Project **background:** Company A has been using **AWS, Azure, GCP** as CSPs for several years. It has typical **multi cloud /vendors** environment. As the **SOC** and **SecOps** getting more **complex** and **difficult** to manage all the security events/threats/attacks for different CSP's VMs, containers and orchestration/kubernetes, serverless, plus the multi incident investigations.

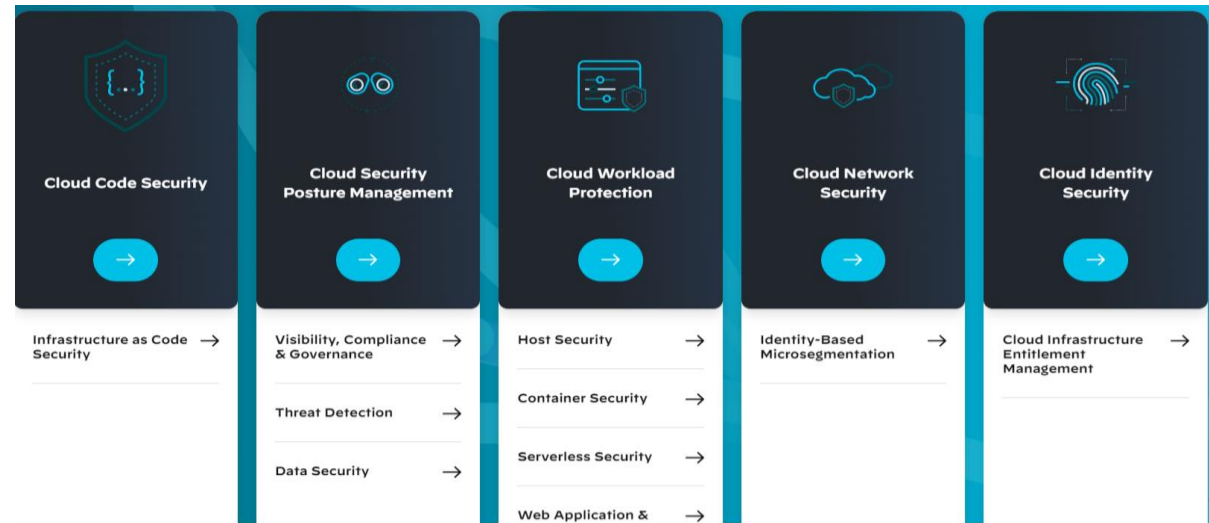
Project **Goal:** to **Simply** the **SOC** and **SecOps** management. To **unify cloud security management** for virtual assets include instances, containers, Orchestrations, micro services, etc, further **enhance** the **cloud security standards** with industry leader's most recent automation solution.

Project 3: Unified Cloud Security Management CSPM/CWPP

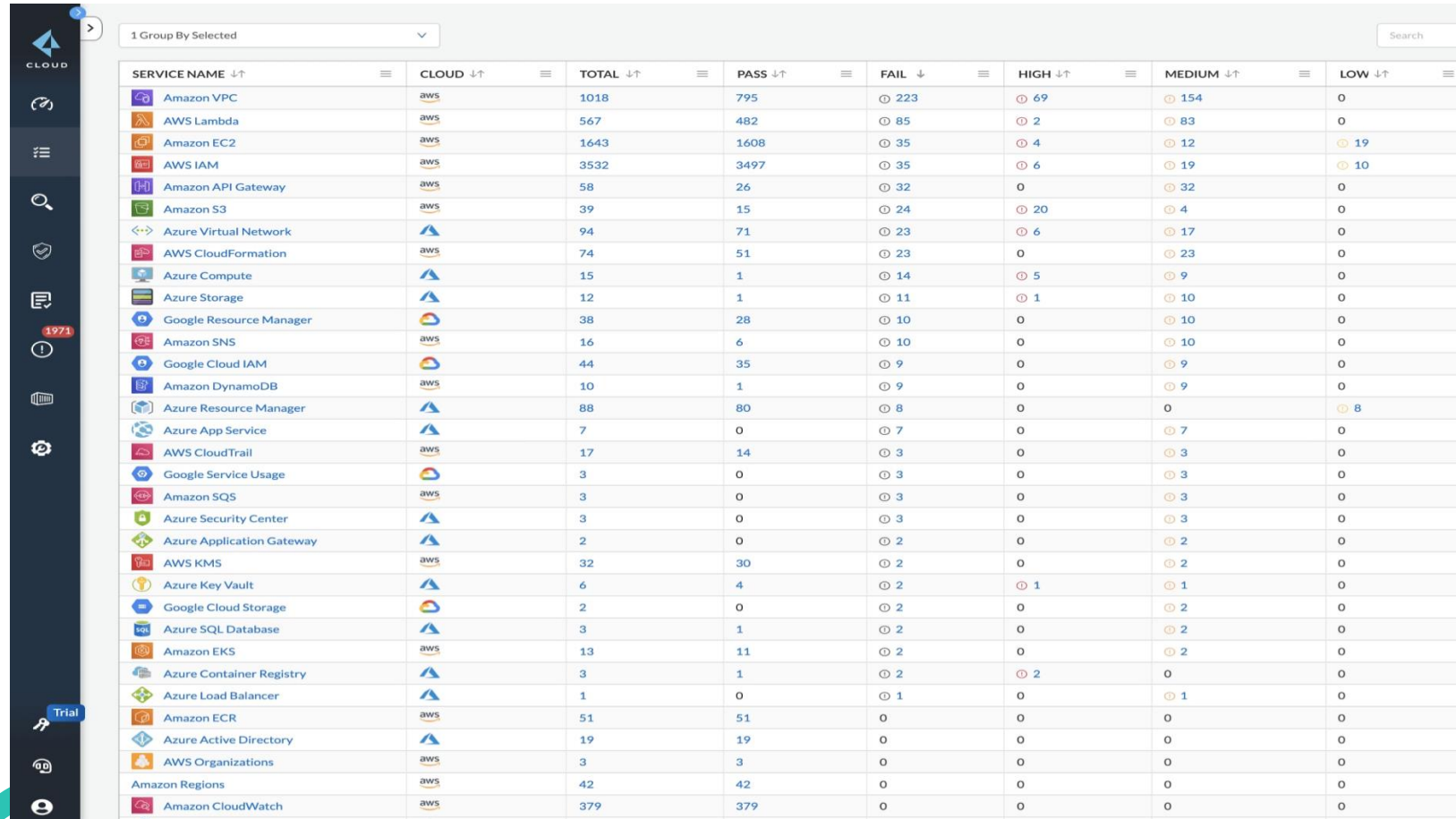


✓ SAAS/PAAS product : VMWARE, Azure, AWS, Cisco, F5, Citrix, checkpoint, Juniper, Redhat, Palo Alto + Prisma Cloud security

✓ Result: Palo Alto received the highest score
Azure has the second highest score
Cisco the third



CSPM Project outcome: unified Multi Cloud /Multi hybrid cloud asset inventory management



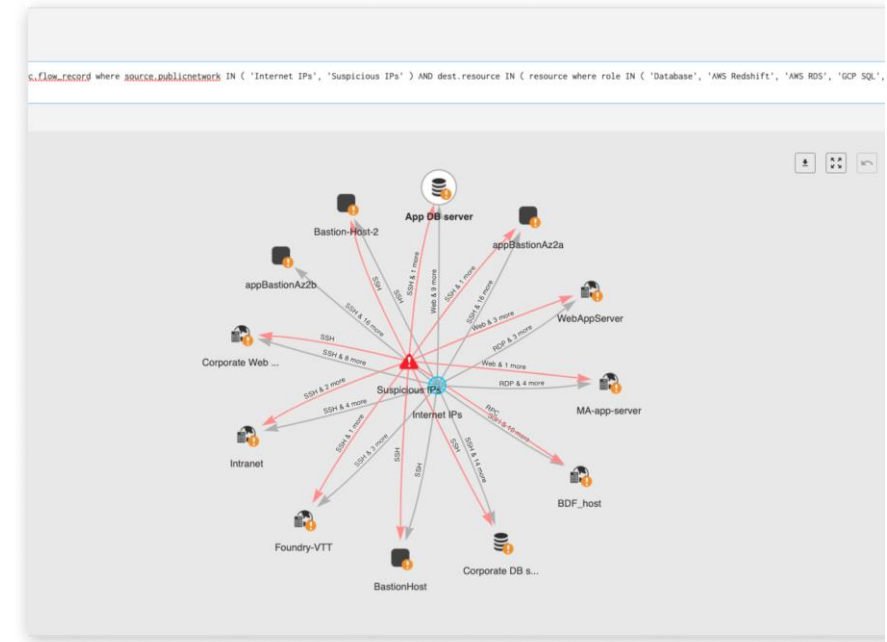
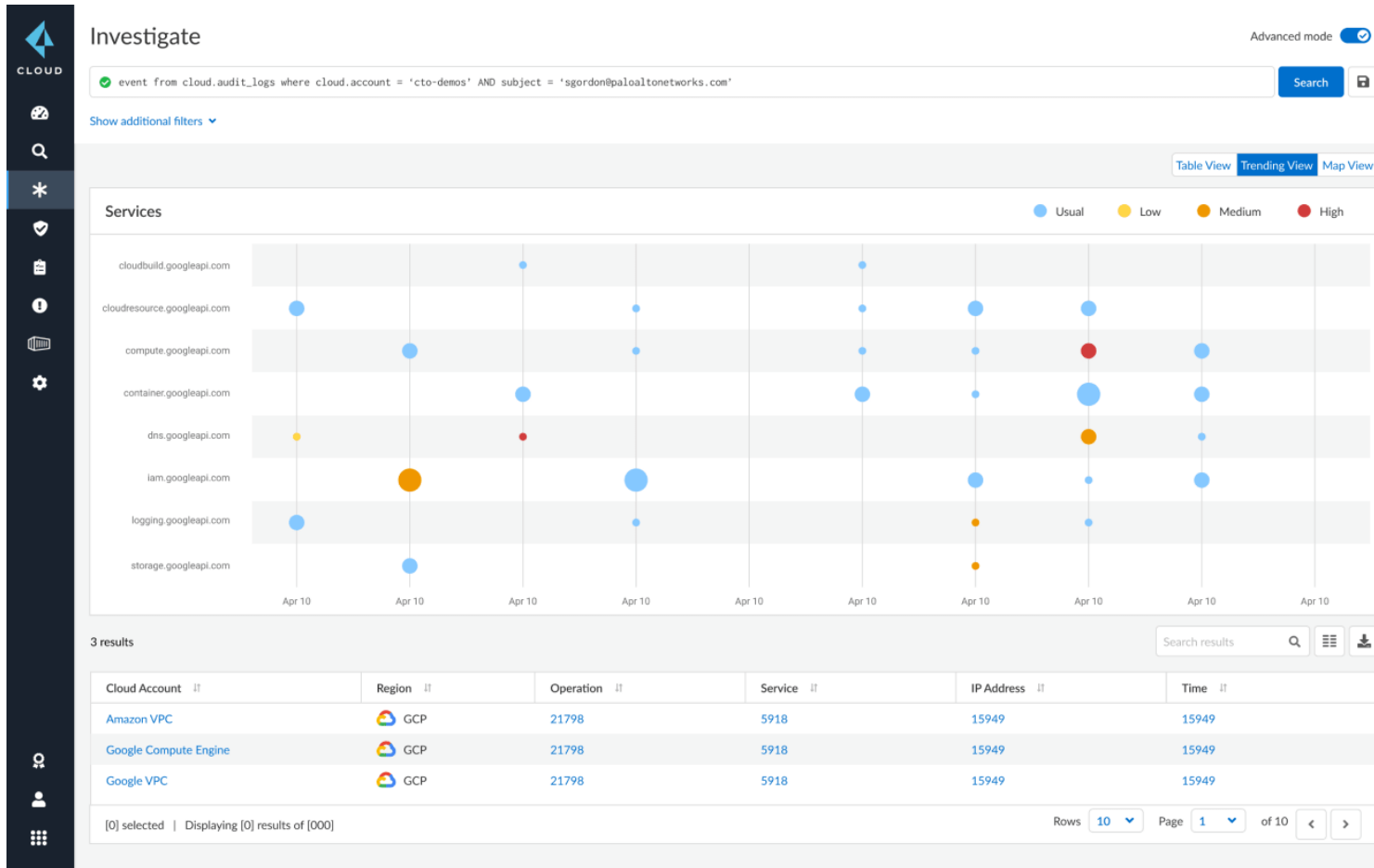
1 Group By Selected

SERVICE NAME ↓↑	CLOUD ↓↑	TOTAL ↓↑	PASS ↓↑	FAIL ↓	HIGH ↓↑	MEDIUM ↓↑	LOW ↓↑
Amazon VPC	aws	1018	795	223	69	154	0
AWS Lambda	aws	567	482	85	2	83	0
Amazon EC2	aws	1643	1608	35	4	12	19
AWS IAM	aws	3532	3497	35	6	19	10
Amazon API Gateway	aws	58	26	32	0	32	0
Amazon S3	aws	39	15	24	20	4	0
Azure Virtual Network	aws	94	71	23	6	17	0
AWS CloudFormation	aws	74	51	23	0	23	0
Azure Compute	aws	15	1	14	5	9	0
Azure Storage	aws	12	1	11	1	10	0
Google Resource Manager	aws	38	28	10	0	10	0
Amazon SNS	aws	16	6	10	0	10	0
Google Cloud IAM	aws	44	35	9	0	9	0
Amazon DynamoDB	aws	10	1	9	0	9	0
Azure Resource Manager	aws	88	80	8	0	0	8
Azure App Service	aws	7	0	7	0	7	0
AWS CloudTrail	aws	17	14	3	0	3	0
Google Service Usage	aws	3	0	3	0	3	0
Amazon SQS	aws	3	0	3	0	3	0
Azure Security Center	aws	3	0	3	0	3	0
Azure Application Gateway	aws	2	0	2	0	2	0
AWS KMS	aws	32	30	2	0	2	0
Azure Key Vault	aws	6	4	2	1	1	0
Google Cloud Storage	aws	2	0	2	0	2	0
Azure SQL Database	aws	3	1	2	0	2	0
Amazon EKS	aws	13	11	2	0	2	0
Azure Container Registry	aws	3	1	2	2	0	0
Azure Load Balancer	aws	1	0	1	0	1	0
Amazon ECR	aws	51	51	0	0	0	0
Azure Active Directory	aws	19	19	0	0	0	0
AWS Organizations	aws	3	3	0	0	0	0
Amazon Regions	aws	42	42	0	0	0	0
Amazon CloudWatch	aws	379	379	0	0	0	0

Solution Benefit:

- A single dashboard for all the cloud assets
- Support for all major cloud providers include AWS, Azure, GCP asset
- provides detailed resource classification
- Real-time and historical views into risk management

CSPM Project outcome: unified threat detection



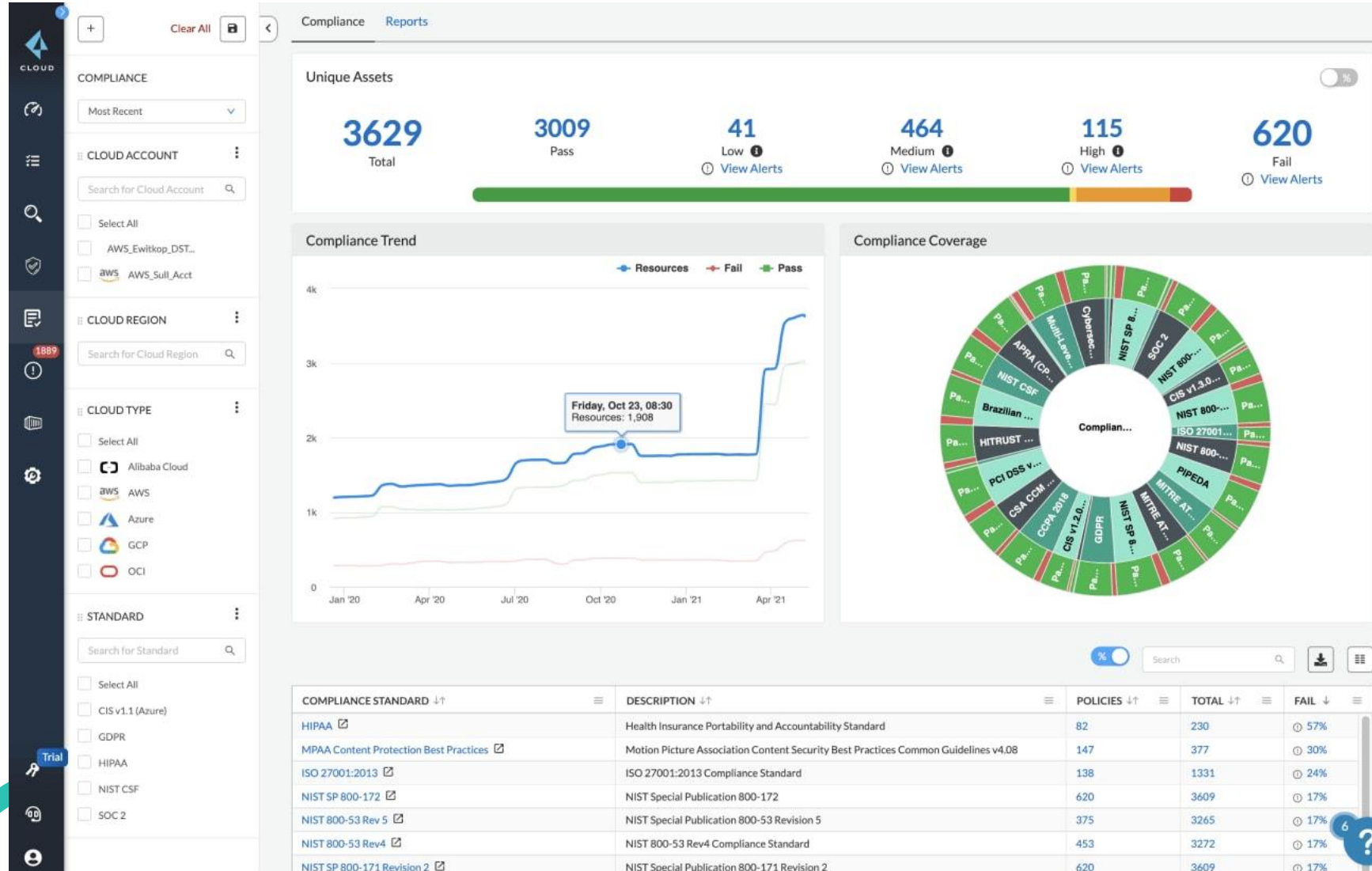
Alerts Overview

Grouped By Policy Type 868 alerts on 168 policies

Policy Type	Policy Name	Alerts	Severity
Config (163)	163 Policies	730	34 High, 84 Medium, 45 Low
Anomaly (3)	3 Policies	99	1 High, 2 Medium, 0 Low
Unusual user activity		92	High
Excessive login failures		6	High
DDoS activity (External)		1	Medium
Audit Event (2)	2 Policies	39	0 High, 0 Medium, 2 Low
Sensitive network configuration updates in AWS		31	Low
AWS IAM sensitive activities by User		8	Low

Rows 25 Page 1

CSPM Project outcome: Unified cloud Compliance monitoring and reporting/SOC automation



One-click audit reportings, more than 20 compliance standards, including PCI DSS, HIPAA, GDPR, SOC2, NIST 800-171, NIST 800-53, NIST CSF, ISO 27002, CCPA, CCM and any custom frameworks. Generate audit-ready reports with a single click.

(Investigated project): Cloud Ops automation

Terraform(HashiCorp) orchestration for multi cloud provision, change and version control

Infrastructure as code

Use infrastructure as code to automate the provisioning of your infrastructure including servers, databases, firewall policies, and almost every other aspect.



Multi-cloud deployment

Deploy serverless functions with AWS Lambda, manage Microsoft Azure Active Directory resources, provision a load balancer in Google Cloud, and more.



Manage Kubernetes

Provision and manage Kubernetes clusters on AWS, Microsoft Azure, or Google Cloud, and interact with your cluster using the Kubernetes Terraform provider.



Manage network infrastructure

Automate key networking tasks, like updating load balancer member pools or applying firewall policies.



Manage virtual machine images

Deploy and manage virtual machine images with Terraform and Packer.

Integrate with existing workflows

Automate infrastructure deployments through existing CI/CD workflows.

Enforce policy as code

Enforce policies before your users create infrastructure using Sentinel policy as code.

Inject secrets into Terraform

Automate using dynamically generated secrets and credentials within Terraform configurations.

Terraform(HashiCorp)'s Automate infrastructure provisioning on all clouds. lets Ops use the same workflow to manage multiple CSP providers and handle cross-cloud dependencies. This simplifies management and orchestration for large-scale, multi-cloud infrastructures.

Team Collaboration



Architect/Engineer



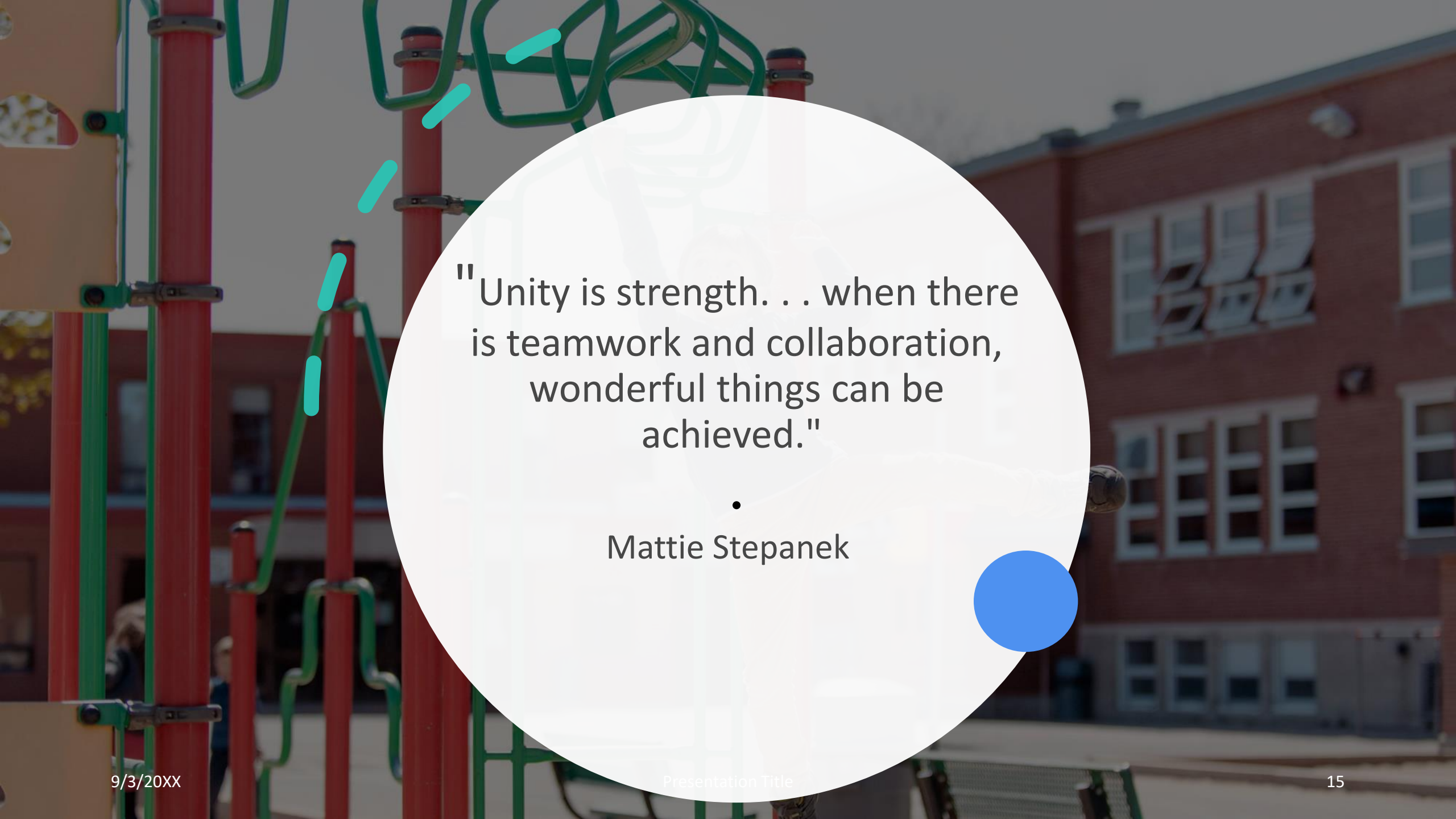
SOC/SecOps



CSP



Business Owner



"Unity is strength. . . when there
is teamwork and collaboration,
wonderful things can be
achieved."

•
Mattie Stepanek



Thank you

Zhuo Ding

dingzhuo2019@gmail.com