Cloud Security

CLOUD SECURITY WEBINAR AGENDA

Introduction

1. What is Cloud Computing?
2. Why is Private Equity Moving to the Cloud?
3. What does the Journey to the Cloud look like?
4. Cloud Foundation and Architecture Framework

Panel Discussion

1. Overview of Cloud Security Risk
2. Leading Threats and Vulnerabilities Impacting the Cloud
3. Who is Responsible for Cloud Security?
4. How do I Secure my Cloud Journey?
5. Cloud Security Blueprint

WHAT IS CLOUD COMPUTING?

- Pools of virtual resources (compute, storage, operating systems, network, etc.)
- Orchestrated by management and automation software so they can be accessed by users on-demand through self-service portals
- Supported by automatic scaling and dynamic resource allocation
- Public cloud refers to the elastic computing service model used for the provisioning of storage and computational services to multiple customers over the internet while still utilizing a shared infrastructure

Public Cloud Market Share Q2 2020

33% Amazon in the lead with 500 different services

18% Microsoft stronger in mid-large enterprises

9% Google low price and focus on machine learning, big data, and artificial intelligence

Source: Synergy Research Group

WHY IS PRIVATE EQUITY MOVING TO THE CLOUD?

- The need for innovation, industry transformation, and data modernization is driving businesses to the cloud
- Moving to the cloud provides access to enterprise-class technology allowing small businesses to act faster than big established competitors
- Cloud services minimize the need for capital expenditure
- COVID created an urgency for organizations to move to the cloud
- Low-cost geographical expansion and disaster recovery

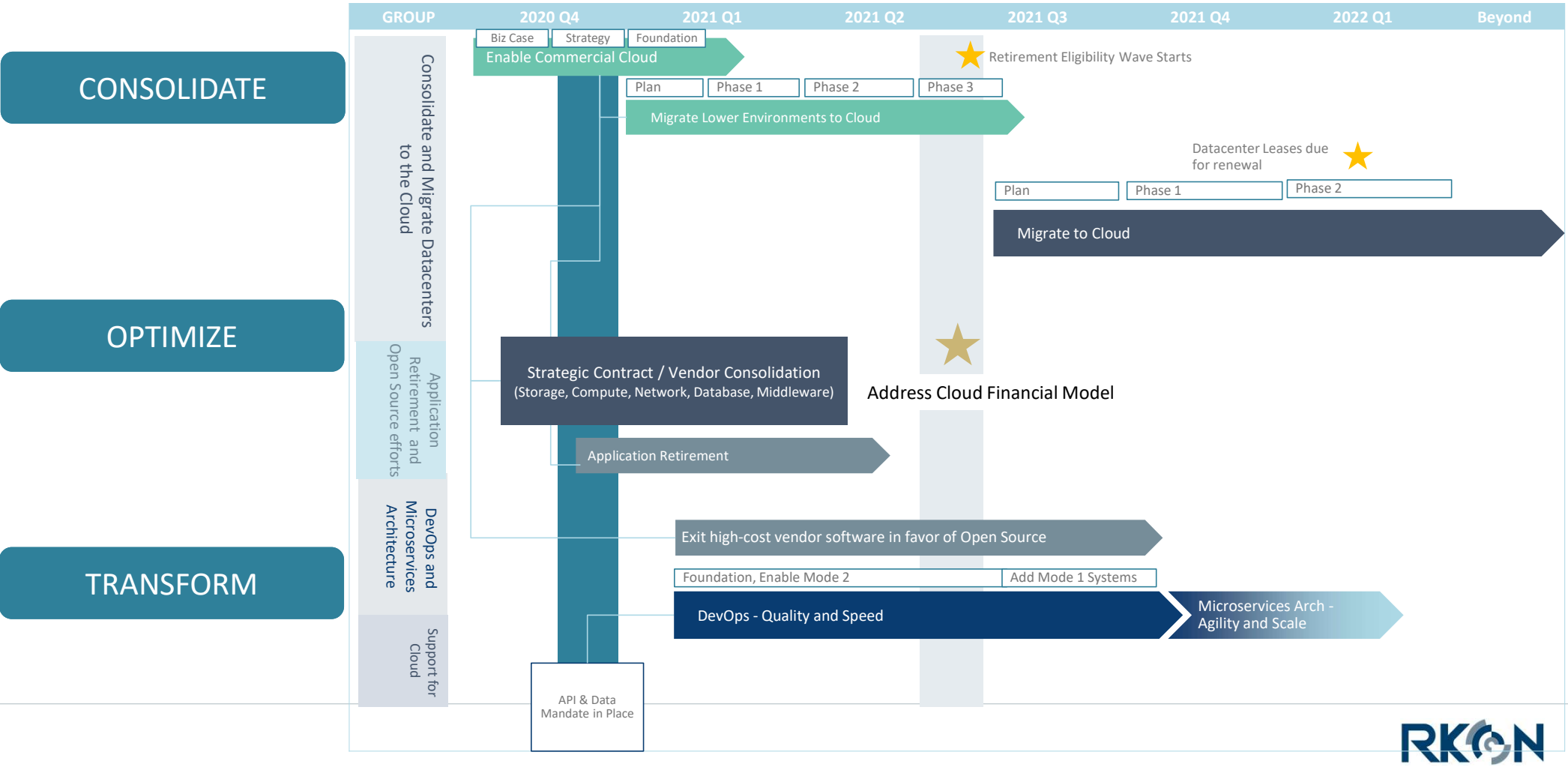
17% Cloud Service Market Forecasted to Grow[1]

$63B Public Cloud Spend in 2021

$3.5B Cloud Security Spend in 2021

[1] *Gartner*

WHAT DOES THE JOURNEY TO THE CLOUD LOOK LIKE?



CLOUD FOUNDATION AND ARCHITECTURE FRAMEWORK

01

Accounts and subscriptions

Accounts and subscriptions

Establish account structure and segregation based on roles
- Account structure and segregation
- Environment ownership
- Billing and administration

02

Connectivity

Connectivity

Establish connectivity and networking foundations in the cloud; back to on premise
- Hybrid networking
- Network design in the cloud
- Redundancy
- IP address management and subnet design

03

Identity and Security

Identity and Security

Define identity and access policies while integrating with on premise authorization system
- Access policies
- AD integration
- Environment hardening
- Vertical specific compliance

04

Cloud Services

Cloud Services

Implement initial set of service offerings and associated administrative controls
- Initial service catalog in cloud provider
- Environment setup
- Resiliency and setup
- Service administration

05

Cloud Operations

Cloud Operations

Implement initial governance and operational dashboards
- Governance
- Operational monitoring
- Resiliency and availability
- Responsibility framework
- Automation

06

Financial Management

Financial Management

Build a cost reporting/metrics model for cloud resources
- Reporting
- Metrics
- Cost Optimization
- Financials

07

Regulatory Compliance

Regulatory Compliance

Design regulatory compliance framework to implement appropriate cloud controls
- Cloud regulatory framework
- Regulatory and compliance controls
- Compliance reporting

OVERVIEW OF CLOUD SECURITY RISK - MORE CLOUD, MORE HACKS

- The threat of attacks on cloud continue to increase as more workloads from datacenters to the cloud and hackers become increasingly savvy
- Cloud providers offer increasingly robust security measures but customers are responsible for securing their workloads
- Public cloud security threats include misconfiguration of the cloud platform/wrong setup, unauthorized access, and insecure interfaces/APIs
- Reduce complexity for non-technical stakeholders in making buying and growth decisions where a cloud enabled strategy is materially significant to the deal thesis
- Firms are realizing the hard way that Cloud Security is different than traditional IT security and that a new skill set is needed to identify and evaluate Cloud related security risks

400% Increase in Cloud Security Breaches[1]

99% Cloud Security Failures Are the Customer's Fault[2]

68% Organizations ranked misconfiguration of the cloud platform highest risk[3]

[1] *FBI Report*
[2] *Gartner*
[3] *Cybersecurity Insiders 2020 Cloud Security Report*

LEADING THREATS AND VULNERABILITIES IMPACTING THE CLOUD

Through 2024, the majority of enterprises will continue to struggle with appropriately measuring cloud security risks[1]

Advanced Cloud Security Challenges[2]

- Increased attack surface
- Lack of visibility and tracking
- Ever-changing workloads
- DevOps, DevSecOps and automation
- Granular privilege and key management
- Multi-cloud environment
- Compliance and regulations

[1] *Gartner*
[2] *Check Point*

WHO IS RESPONSIBLE FOR CLOUD SECURITY?

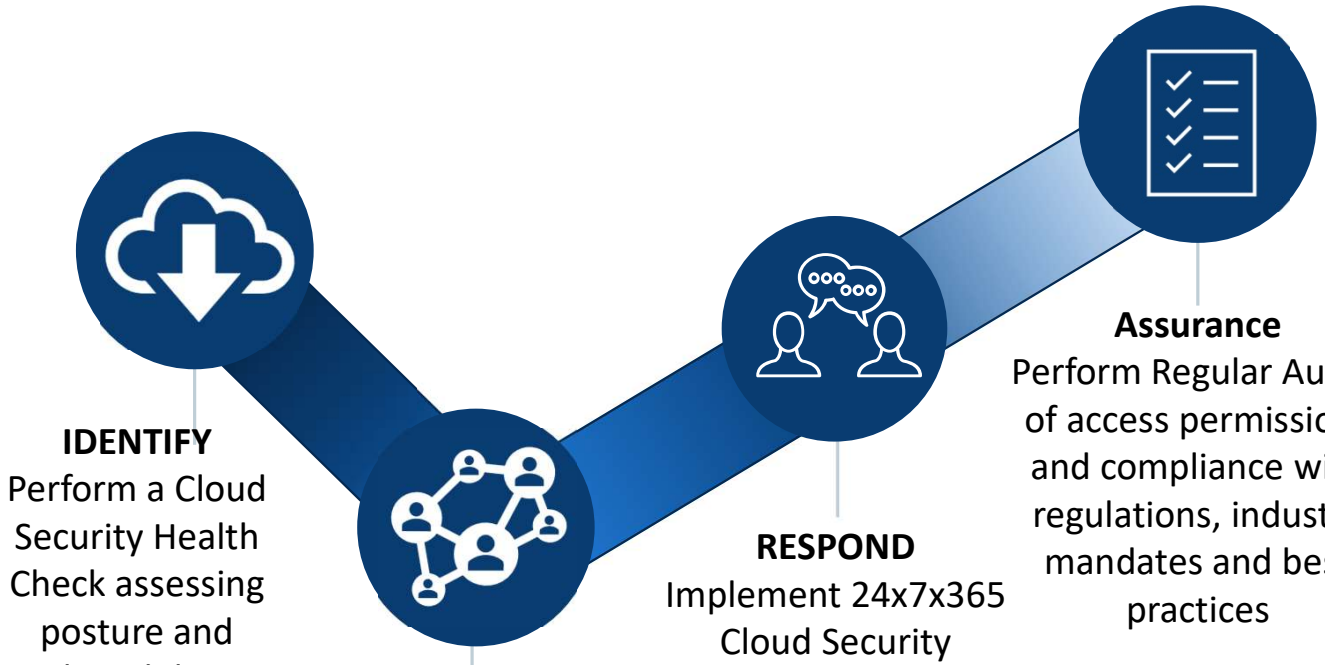
Cloud Security is a Shared Responsibility

SECURITY "OF" THE CLOUD

- Cloud Asset Management
- Network Security
- Identity and Access Management
- Encryption and Key Management
- Vulnerability and Threat Management
- Logging
- Monitoring
- Backup and Disaster Recovery

SECURITY "IN" THE CLOUD

HOW DO I SECURE MY CLOUD JOURNEY?



IDENTIFY
Perform a Cloud Security Health Check assessing posture and vulnerabilities

PROTECT
Develop a Cloud Security Blueprint to implement security controls

RESPOND
Implement 24x7x365 Cloud Security Monitoring responding to security incidents

Assurance
Perform Regular Audits of access permissions and compliance with regulations, industry mandates and best practices

IDENTIFY - CLOUD SECURITY HEALTH CHECK

Assesses the security posture of cloud environments by aligning to gold standard policies, identifying critical security control misconfiguration, and remediating potential attack and insider threat vectors

Posture Assessment

Provides intuitive visibility into all cloud assets, networks and security groups

Assess gold standard policies across accounts, projects, regions and virtual networks

Compliance & Governance

Conform to regulatory requirements and security best practices

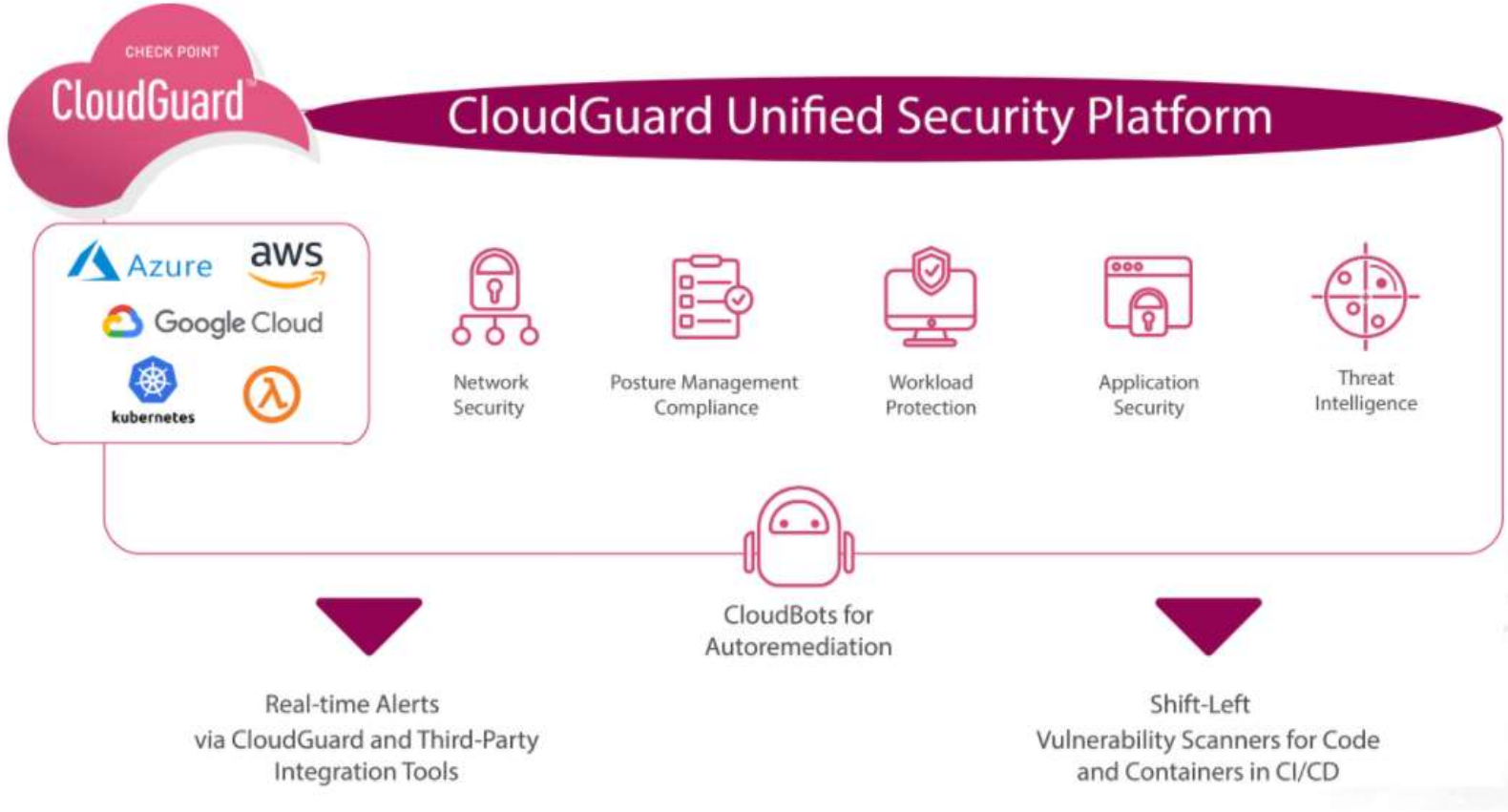
Comprehensive assessment status reports for security and compliance posture

Identity Protection

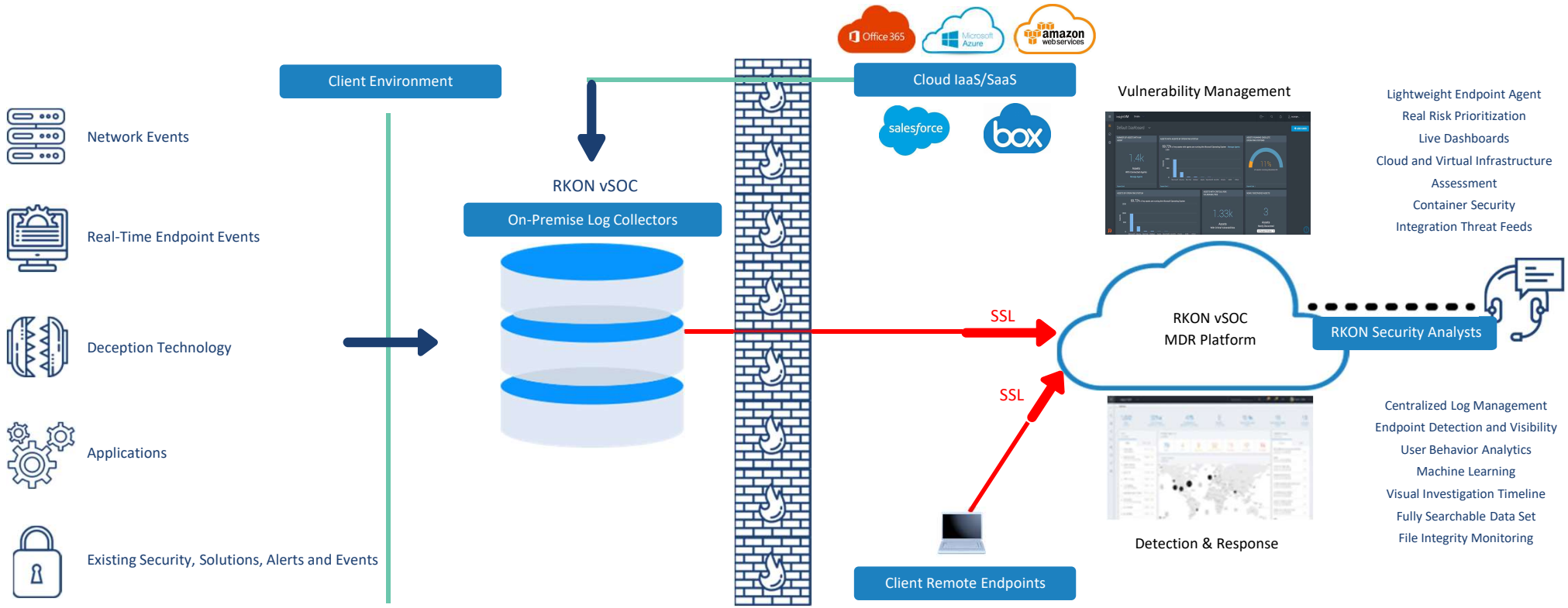
Ensure proper access to sensitive operations and actions are enforced based on users and roles

Analysis of IAM users and rules for suspicious activity

PROTECT - CLOUD SECURITY BLUEPRINT

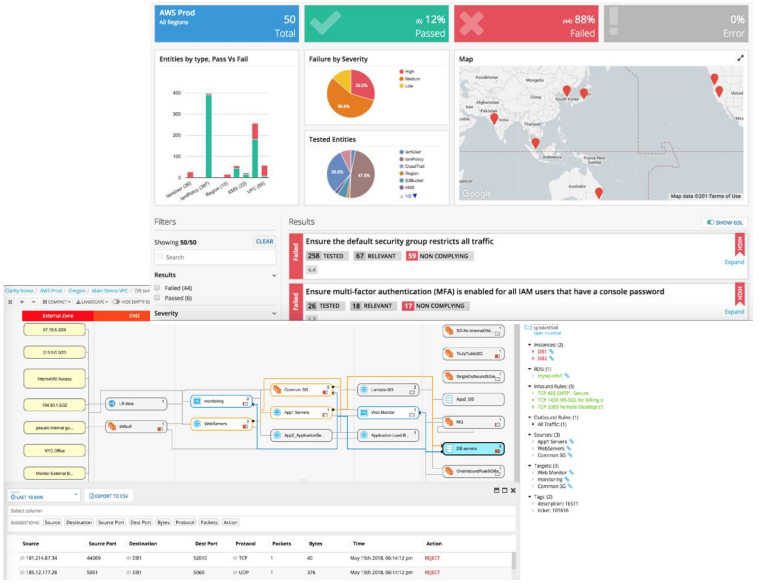


RESPOND – CLOUD SECURITY MONITORING



ASSURANCE – CLOUD SECURITY CONTROLS AUDIT

- ✓ Regular review of user access, permissions, roles, and terminated user access disabled or removed
- ✓ Regular review of privileged/administrative access and separation of duties
- ✓ Regular review of third-party vendor access
- ✓ Continuously assess and enforce security best practices and compliance standards
- ✓ Ensure Business Continuity Plan includes Cloud Security Controls and perform regular testing



THANK YOU