
AWS
re:Invent

SEC382-S

SPONSORED BY RAPID7

Augmenting native AWS security controls

Christopher Hertz
VP Cloud Security Sales
Rapid7

Alex Corstorphine
Cloud Solutions Architect
Rapid7

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Organizations are responsible for their own security in the cloud

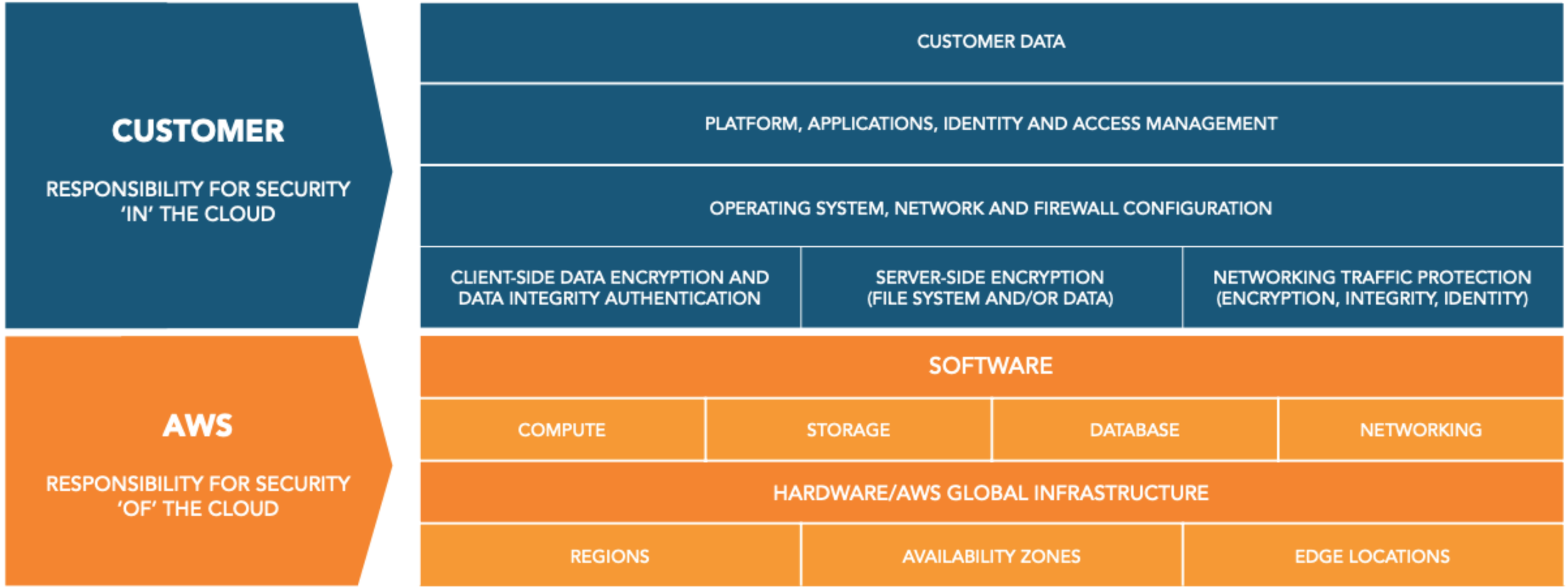
Through 2025, 90% of the organizations that do not control public cloud use will inappropriately share sensitive data

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

Through 2025, customers will be responsible for 99% of cloud security issues

Source: Gartner; October 10, 2019; Contributor: Kasey Panetta

AWS shared responsibility model



Cyber incidents are costly and increasing

In 2018, 81 major incidents

In 2019, 115 major incidents (42% increase)

Inadvertent broad data access caused by cloud misconfigurations cost enterprises an estimated $5 trillion in 2018 and 2019 alone

Source: Rapid7 2020 Cloud Misconfigurations Report

Understanding and use of frameworks is low

Out of all IT professionals surveyed, 42% do not know which frameworks their company uses to maintain compliance with standards and regulations

Almost half (49%) of all respondents whose organizations use the public cloud said that their developers and engineers, at times, ignore or circumvent cloud security and compliance policies

Source: Rapid7 2020 State of Enterprise Cloud and Container Adoption and Security

Identify, protect, detect, respond, and recover

So, what controls detect and prevent misconfigurations?

To answer this question, we align AWS controls against core aspects of the NIST Cybersecurity Framework (NIST CSF)

Identify	Protect	Detect	Respond	Recover
Asset management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures		Mitigation	
Risk Assessment Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective			
	Technology			

AWS foundational and layered security services



Amazon Macie

DISCOVER AND PROTECT YOUR SENSITIVE DATA AT SCALE



Gain visibility and evaluate

- Bucket inventory
- Bucket policies



Discover sensitive data

- Inspection jobs
- Flexible scope



Centrally manage at scale

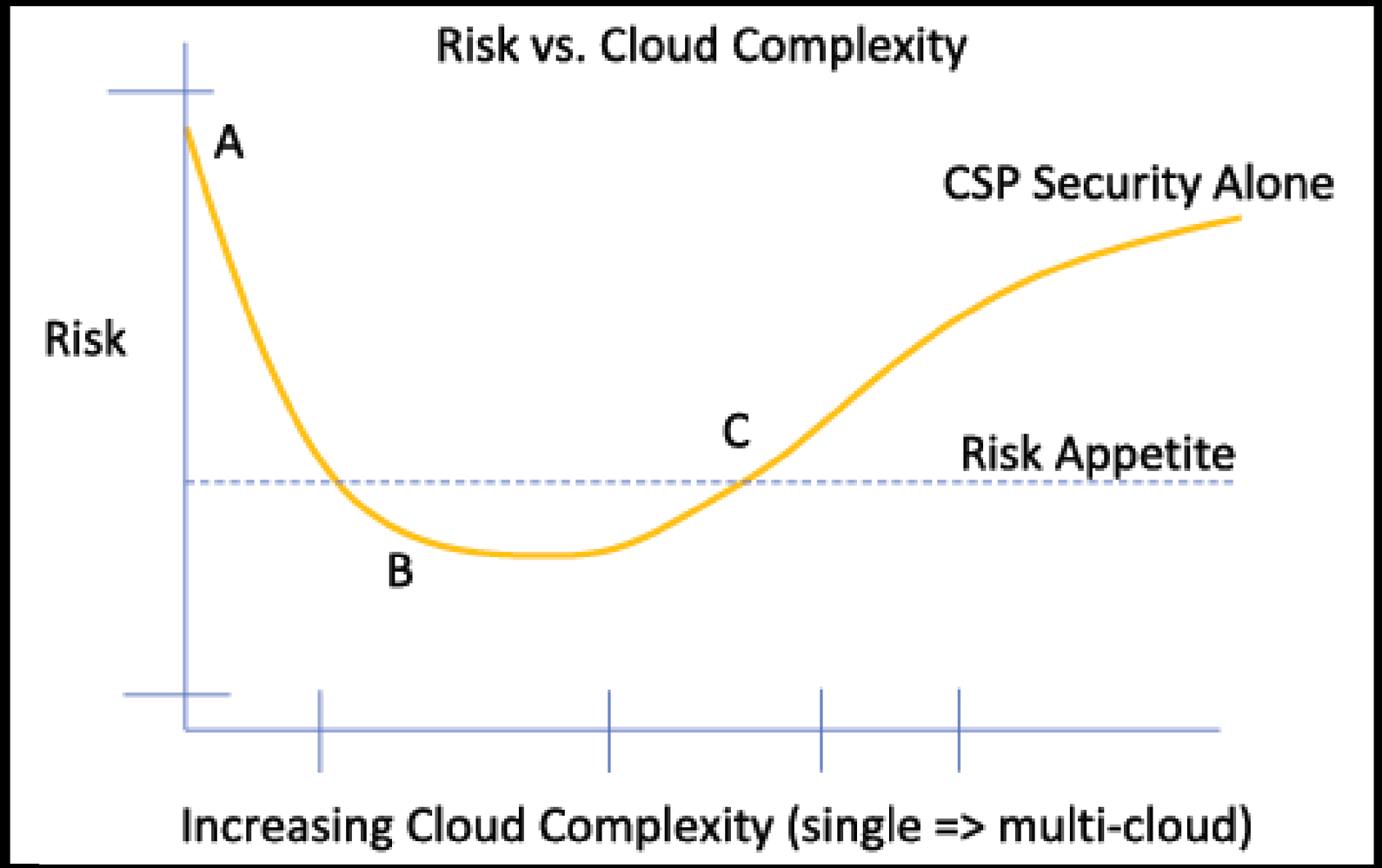
- AWS Organizations
- Managed & custom data detections



Automate and take actions

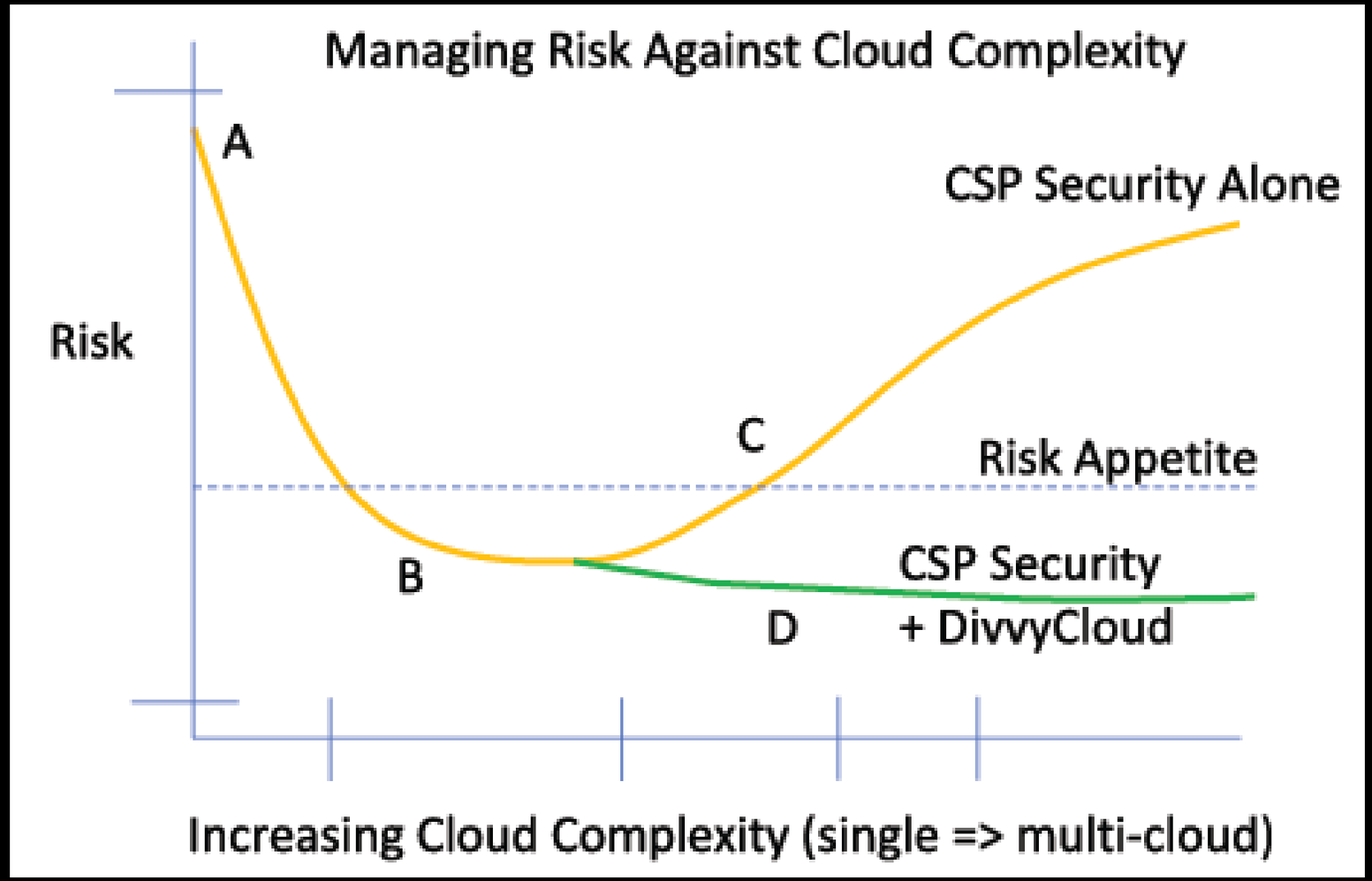
- Detailed findings
- Management APIs

Essential and sufficient to a point



Source: DivvyCloud; Augmenting Native Cloud Service Provider Security

Gaining security effectiveness while managing risk



Source: DivvyCloud; Augmenting Native Cloud Service Provider Security

The 4 levels of automated remediation

Level 1: Ensure visibility and accountability through logging

Level 2: More impactful best practices

Level 3: Governance and account hygiene

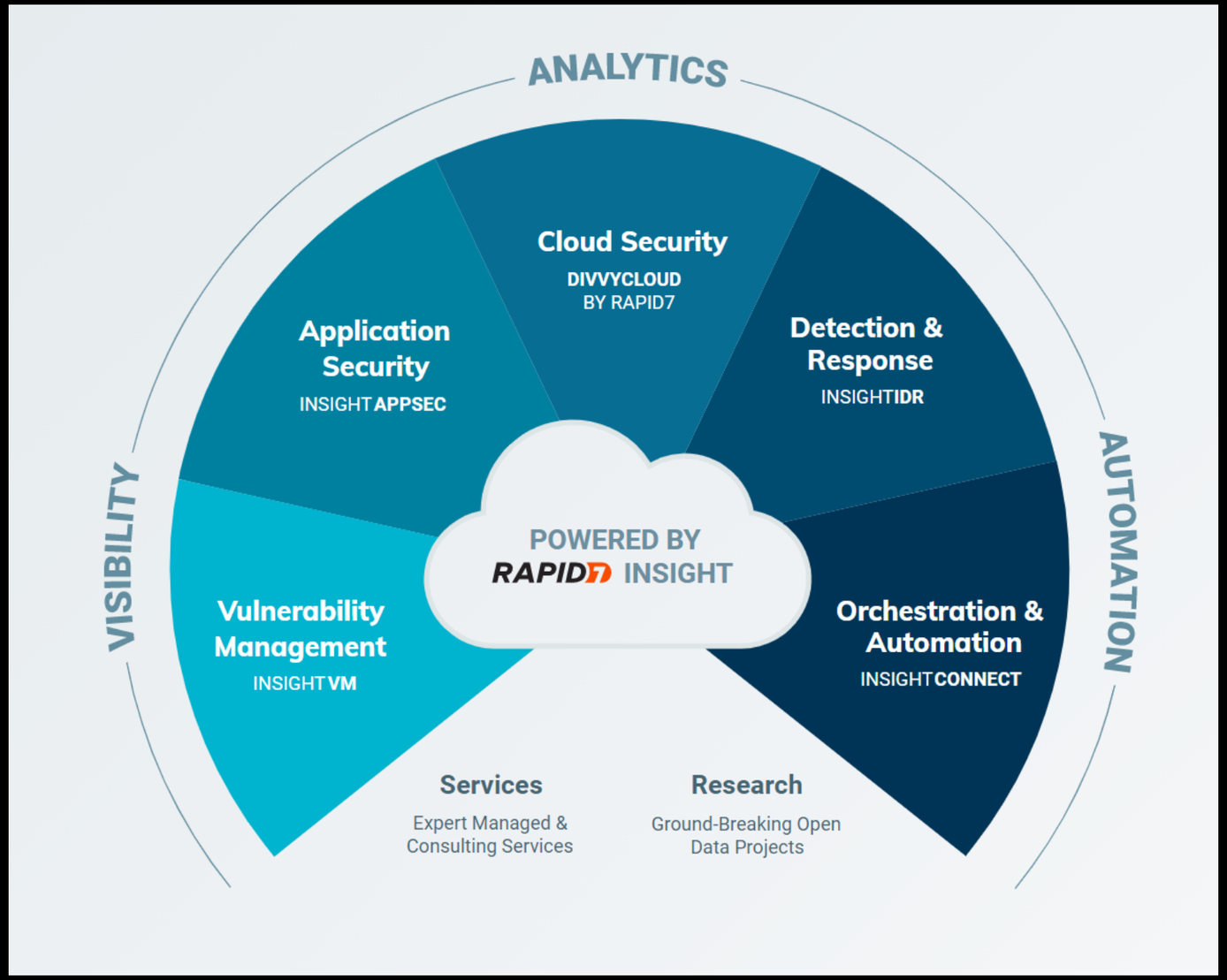
Level 4: “Classic” automated remediation

Nearly continuous security and compliance

DivvyCloud by Rapid7 protects customer cloud and container environments from

- Misconfigurations
- Policy violations
- Risks
- IAM challenges

Now is not the time to wonder about security



Gain full-lifecycle cloud security today with a free 30-day trial of DivvyCloud by Rapid7

divvycloud.com/free-trial/

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.