Unlocking Cloud Compliance: Optimizing Audit With Automation

Anil Kumar GK- Senior Director (IT & Cyber Security- MetricStream)

Neha Singh Rajpurohit- Senior Product Manager (AWS Audit Manager)

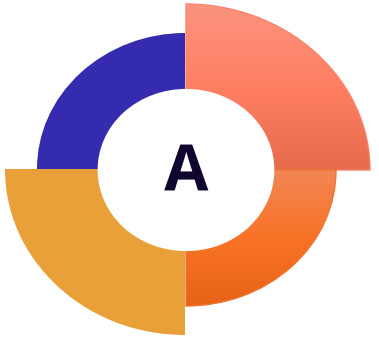
Agenda

1. Traditional audit experience
2. Challenges faced by customer
3. Compliance at cloud scale
4. Enabling compliance through automation
5. About AWS Audit Manager
6. Example walkthrough
7. Leveraging GRC to optimize audits

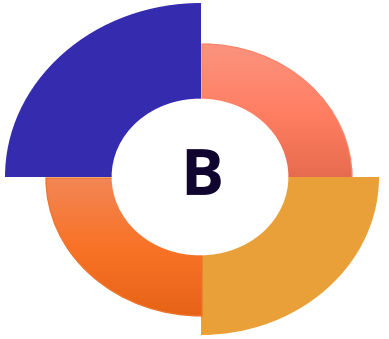
How do you see your organization towards **automating evidence extraction** for audits and compliance requirements.

Spectators – We extract evidence manually as this is the easiest solution for us now and are waiting to see what others are doing
Explorers – We are evaluating opportunities for automation, and we are still new to this area

Innovators – We have taken steps to automate our controls and will look to do so as much as possible
Visionary – our goal is to develop a path to automate everything



Spectators & Explorers



Innovators & Visionary

Typical Audit Experience

- **Tedious**
- **Time-Consuming**
- **Redundant**

What makes audits inefficient?

Manual collection of Evidence

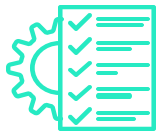
Difficulty in searching & reuse of Evidence

Incorrect or Incomplete Evidence

Redaction and sharing of Evidence

Broad classification of controls

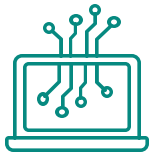
Area of applicability



40%

Infrastructure

- They help to protect the organizations infrastructure from a variety of threats, including unauthorized access, data breaches, and malware attacks.



30%

Applications

- They are designed to protect specific applications from a variety of threats, including unauthorized access, data breaches, and malware attacks.

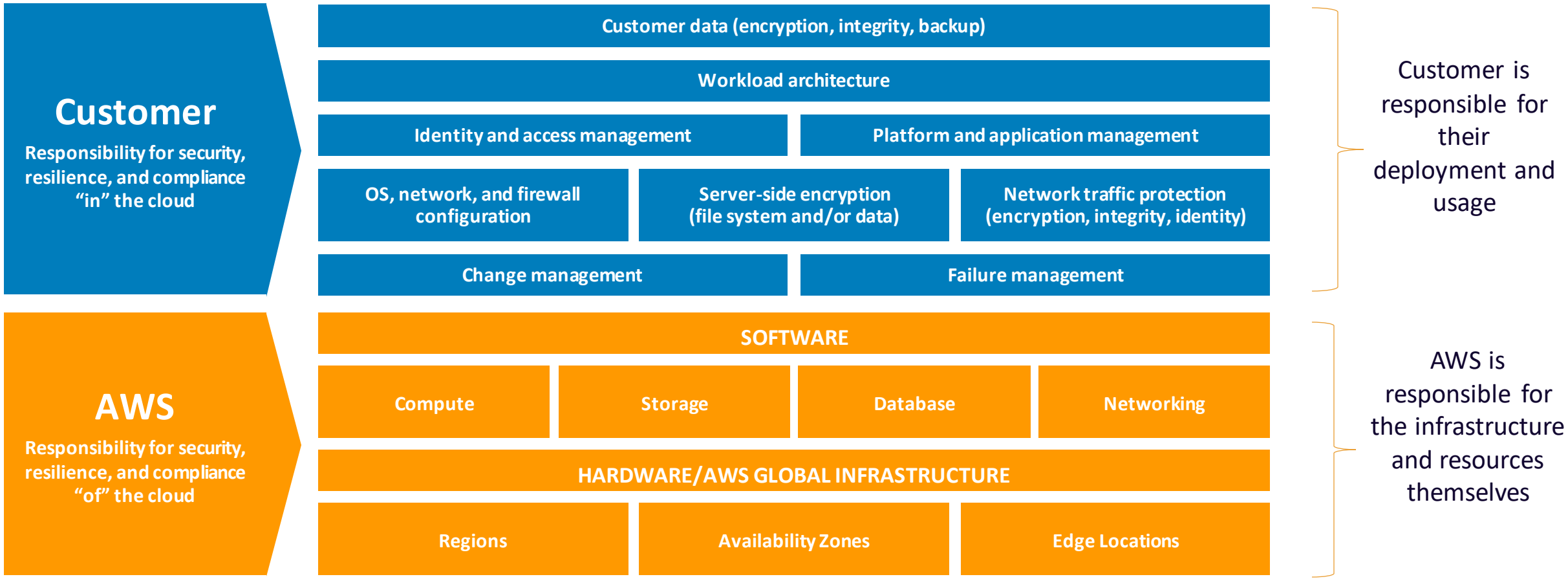
30%

Policies and Procedures

- Policy and procedural controls are an important part of an organization's overall information security program.

Cloud Compliance is a shared responsibility

Security and Compliance is a shared responsibility between AWS and the customer.



Continuous compliance requires insight and automation

Precise Visibility

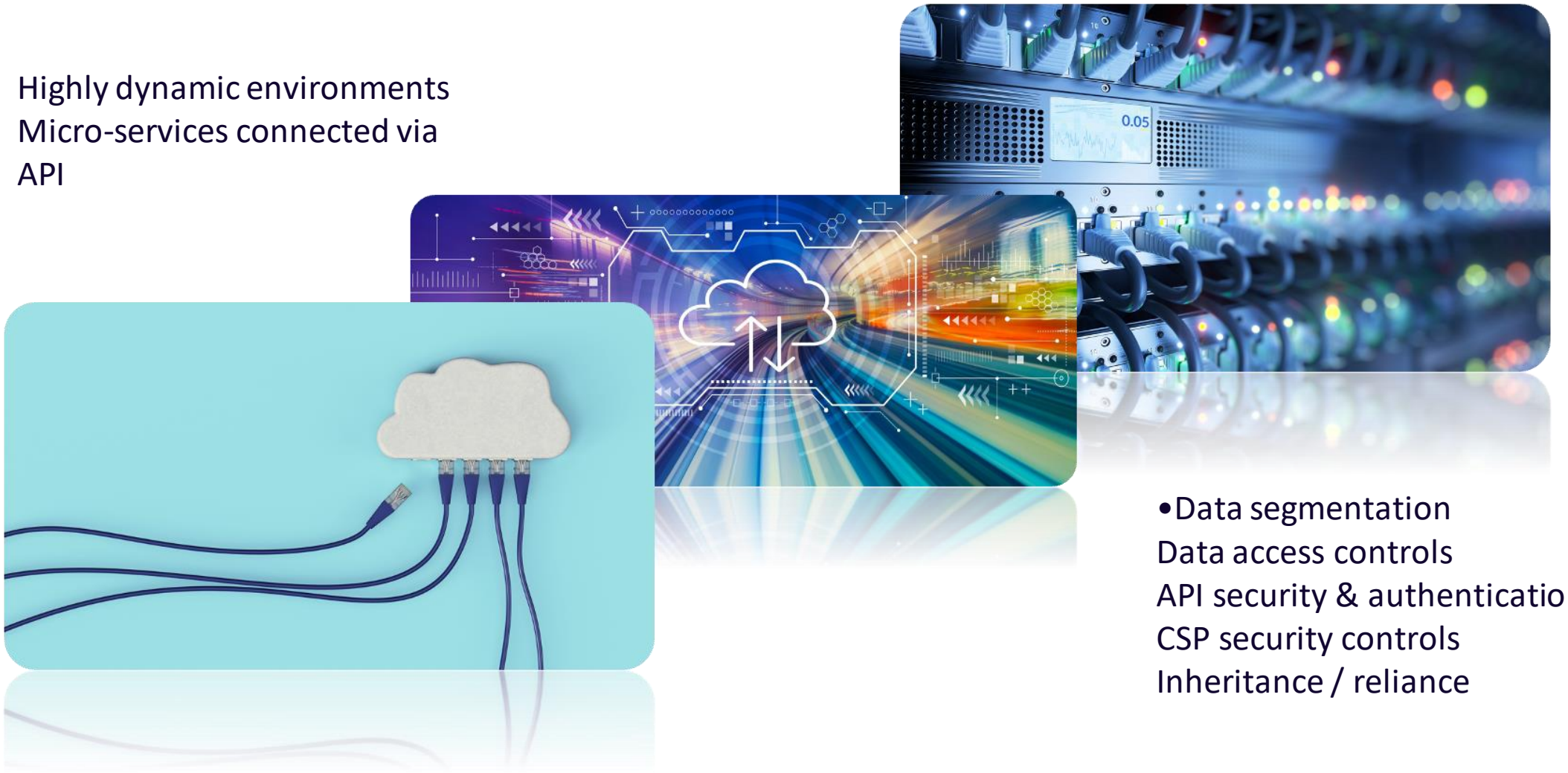
Near-Real-Time Automation

Continuous Compliance

Having the visibility into **WHO** made **WHAT** change from **WHERE** in near-real time enables you to **DETECT** mis-configurations and non-compliance and **RESPOND** quickly to **PREVENT** risks from materializing.

Cloud audits : where automation is not an option but a necessity

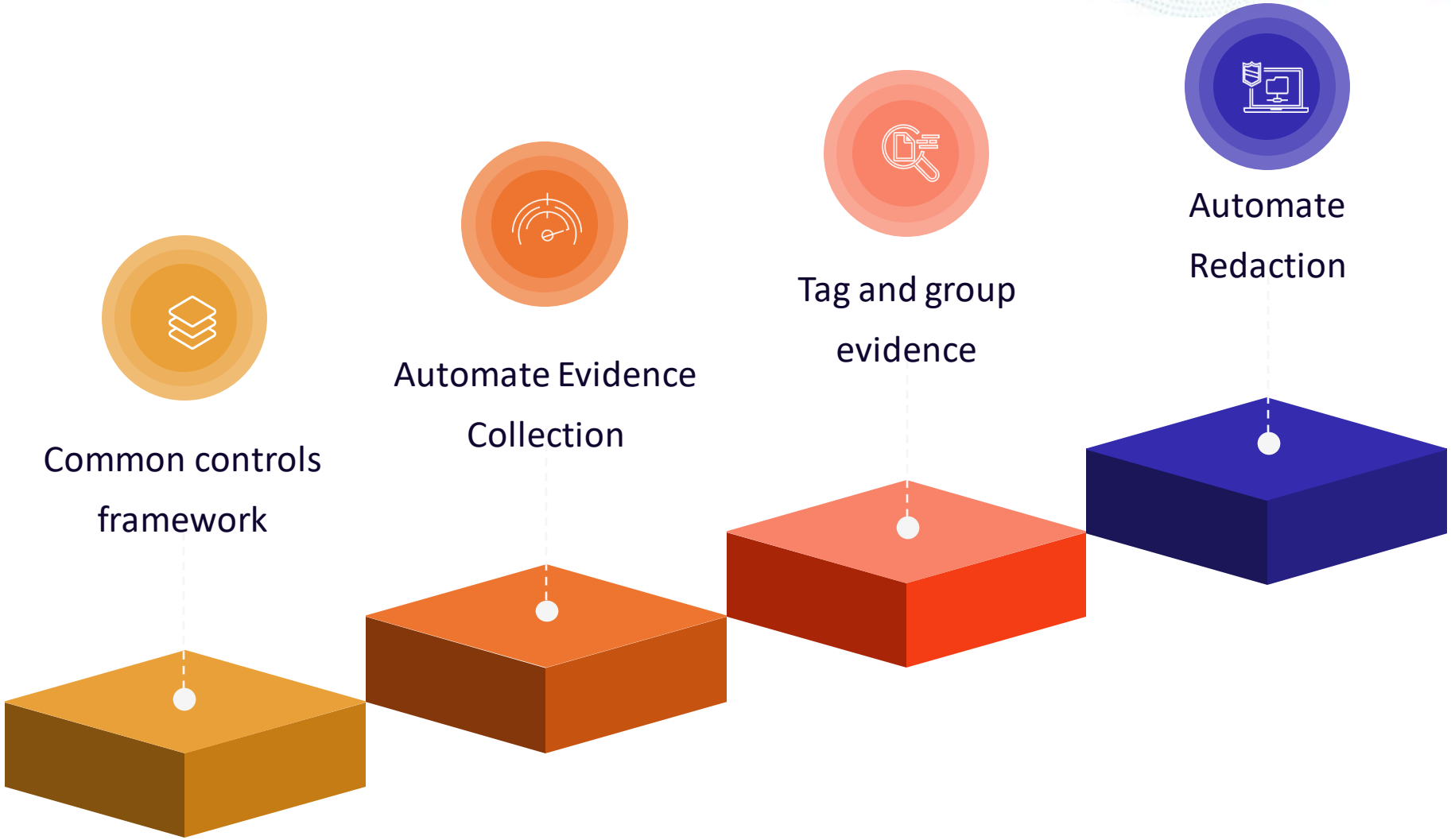
Highly dynamic environments
Micro-services connected via API



- Data segmentation

Data access controls
API security & authentication
CSP security controls
Inheritance / reliance

Gaining Efficiency via automation



Advantages of Automation

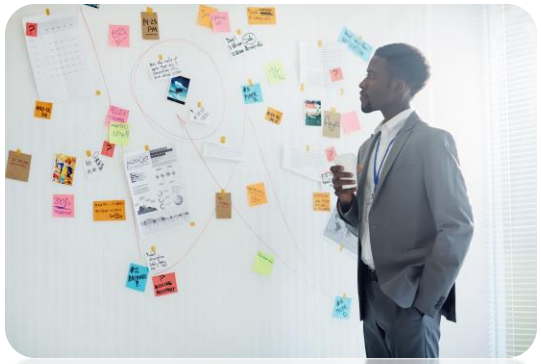
- Save time, effort
- Improve speed and accuracy
- Better reporting
- Build employee morale

How does Audit Manager help?

Immutable storage of evidence

Verifiable provenance

Automated testing



Evidence mapped to framework controls

PCI audit example

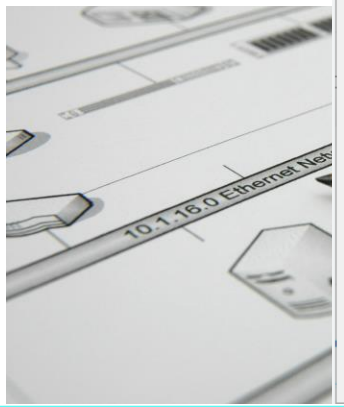
Requirement: 1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement….

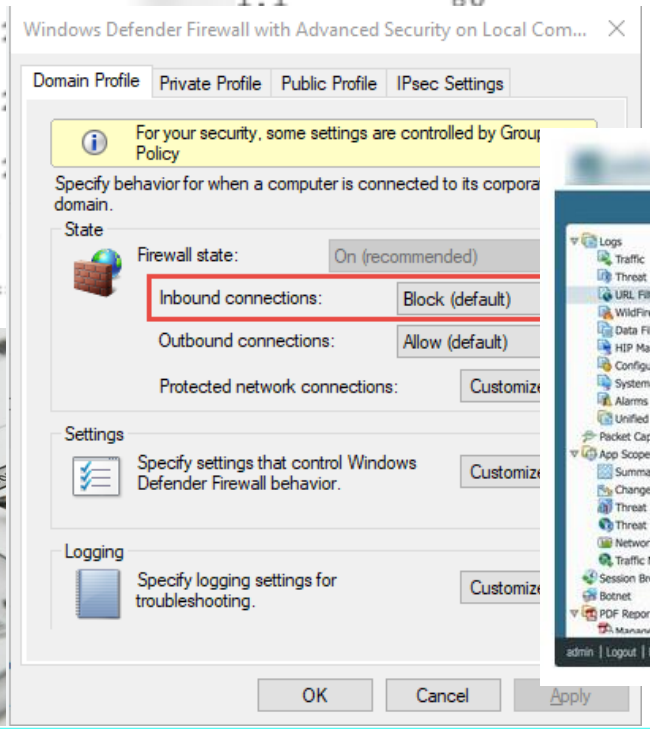
On-premise audit considerations	Cloud audit considerations
• firewalls	• security groups
• routers	• network access control lists (NACLs)
• switches	
• WAN / LAN considerations	

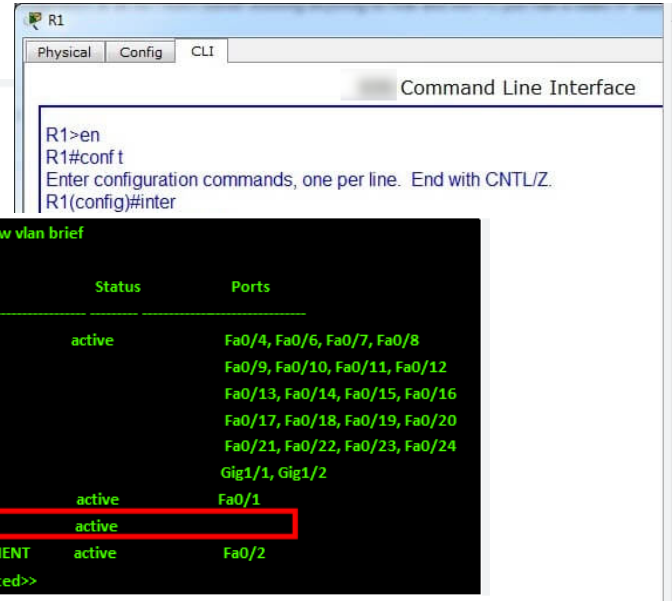
PCI audit example – on premise evidence

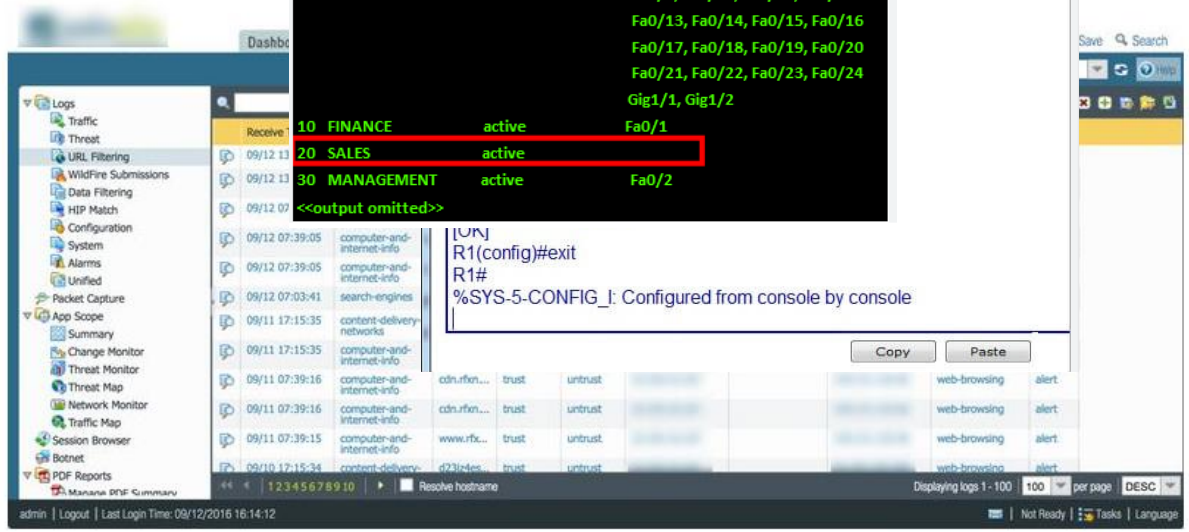
Requirement: 1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement….

No.	Protocol	Source IP	Destination IP	Dest. Port	Action
1	TCP	10.1.1.1	1.1	80	Accept
2	TCP	10.1.1.2	1.1	80	Deny
3	TCP	10.1.1.0/			Deny
4	TCP	10.1.1.3			Acce
5	TCP	10.2.2.0/			Deny
6	TCP	10.2.2.5			
7	TCP	10.3.3.0/			
8	TCP	10.3.3.9			
9	IP	0.0.0.0/0			









PCI audit example – cloud configuration evidence

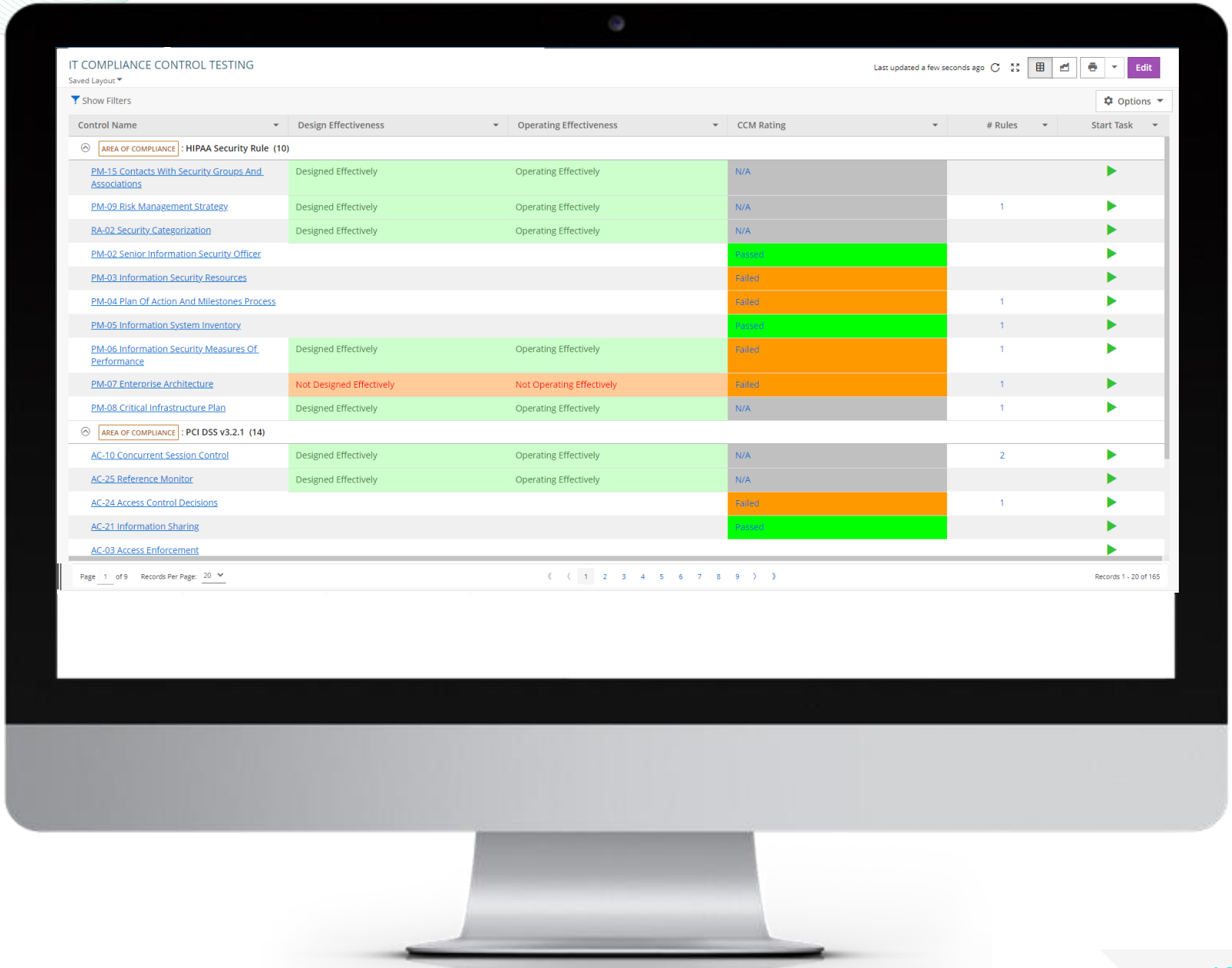
Requirement: 1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement….

Out of the box framework support

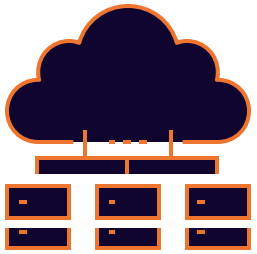
- HIPAA Security Rule 2003
- SOC 2
- GxP EU Annex 11
- GxP 21 CFR Part 11
- NIST 800-53 (Rev. 5) Low-Moderate-High
- NIST Cybersecurity Framework version 1.1
- NIST SP 800-171 Rev. 2
- Essential Eight
- PCI DSS V3.2.1
- Canadian Centre for Cyber Security - Medium
- AWS Foundational Security Best Practices
- ISO-IEC 27001:2013 Annex A
- FedRAMP Moderate Baseline
- CIS Controls v8 IG1

Consolidated View of Control testing

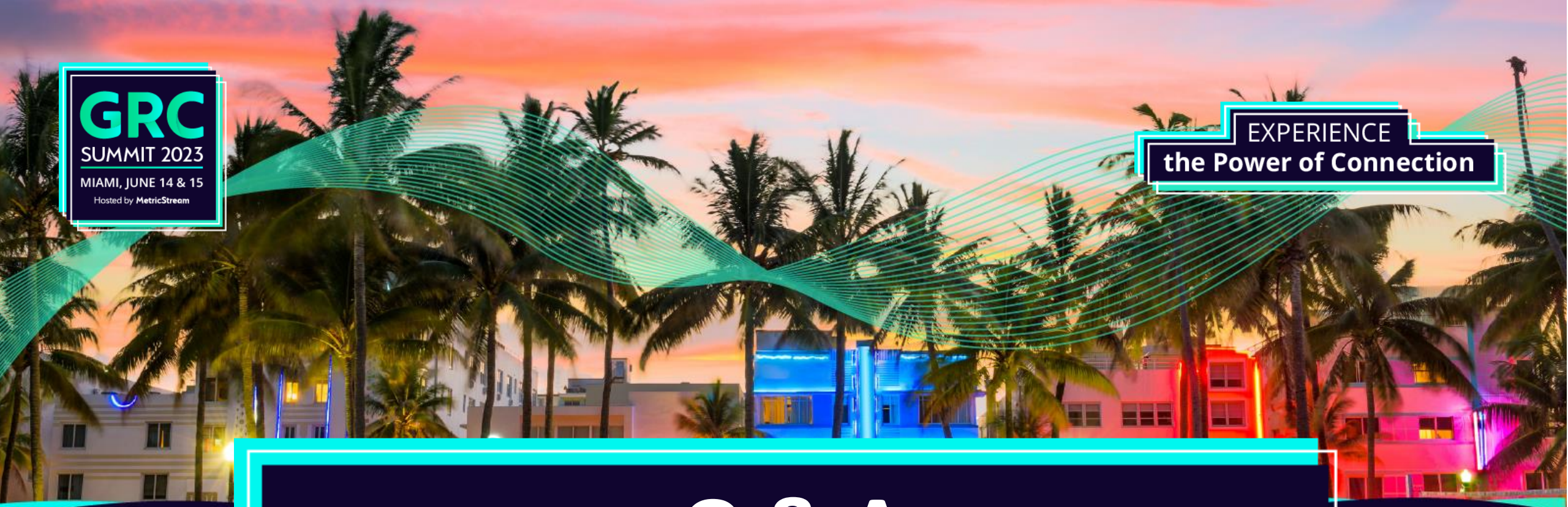
- Integrated test results for GRC controls from Manual and Automated testing
- Easy Access to evidences gathered across control testing



Forward and Future outlook



- Cloud provides access to a ‘**continuous compliance**’ mindset in risk management
- As technology continues to evolve, **audit quality** increases as organizations deploy automated solutions
- Audit space is swamped with data and there are many **AI opportunities** to intelligently analyze this data and make some sense of it for the end user
- Need for **upskilling** of current audit professionals to increase cloud fluency


GRC
SUMMIT 2023
MIAMI, JUNE 14 & 15
Hosted by MetricStream
EXPERIENCE
the Power of Connection

Q & A

Thank You

metricstream
thrive on risk™