Incident Response

Mukhtar Kabir, CISSP

Associate Solutions Architect
Amazon Web Services

08-26-2021

Amazon Detective

What is Amazon Detective?

Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities.

Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data which allows you conduct faster and more efficient security investigations.

Why: Investigations are resource intensive & time consuming

Collect and combine terabytes of log data

Transform the data using ETL tools, custom scripting

Finding right set of visualization tools to view the data

Translate investigation questions into queries to help answer questions

Key benefits of Detective?

Faster and more effective investigations

Save time and effort with continuous data updates

Easy to use visualizations

aws

Key Use Cases?

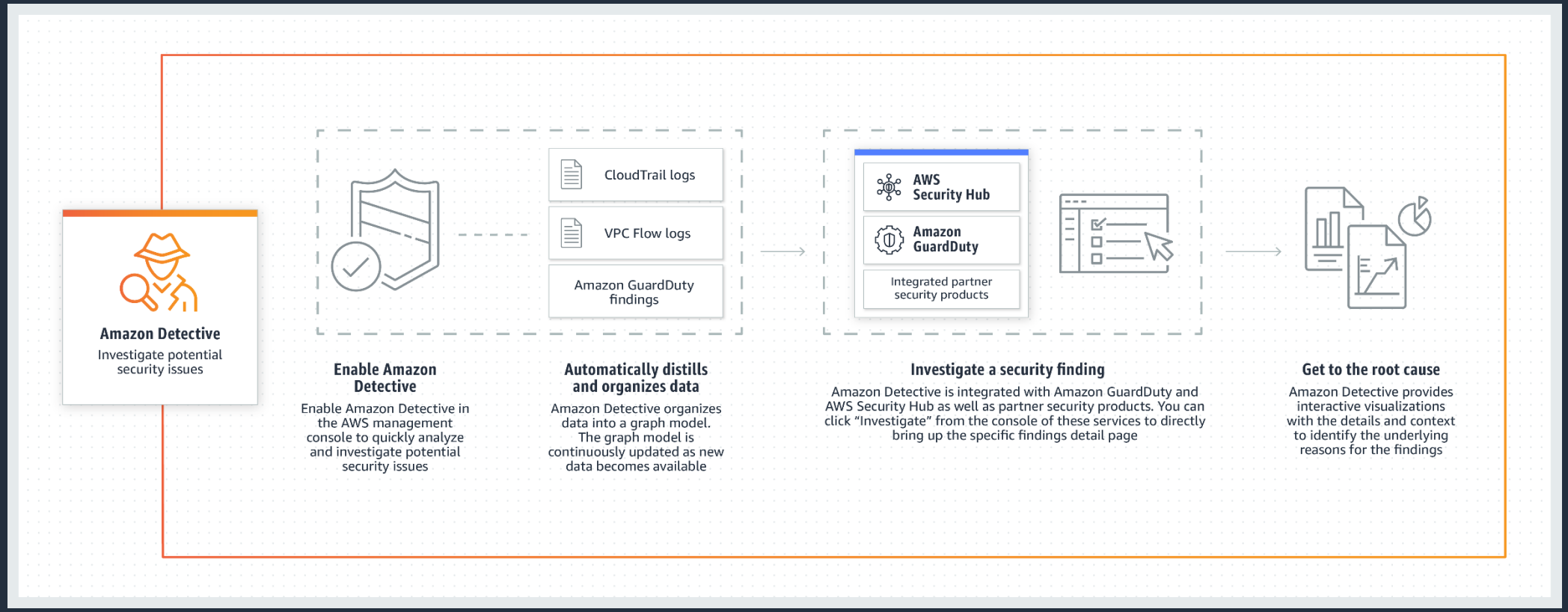
Triage Security Findings

Incident Investigation

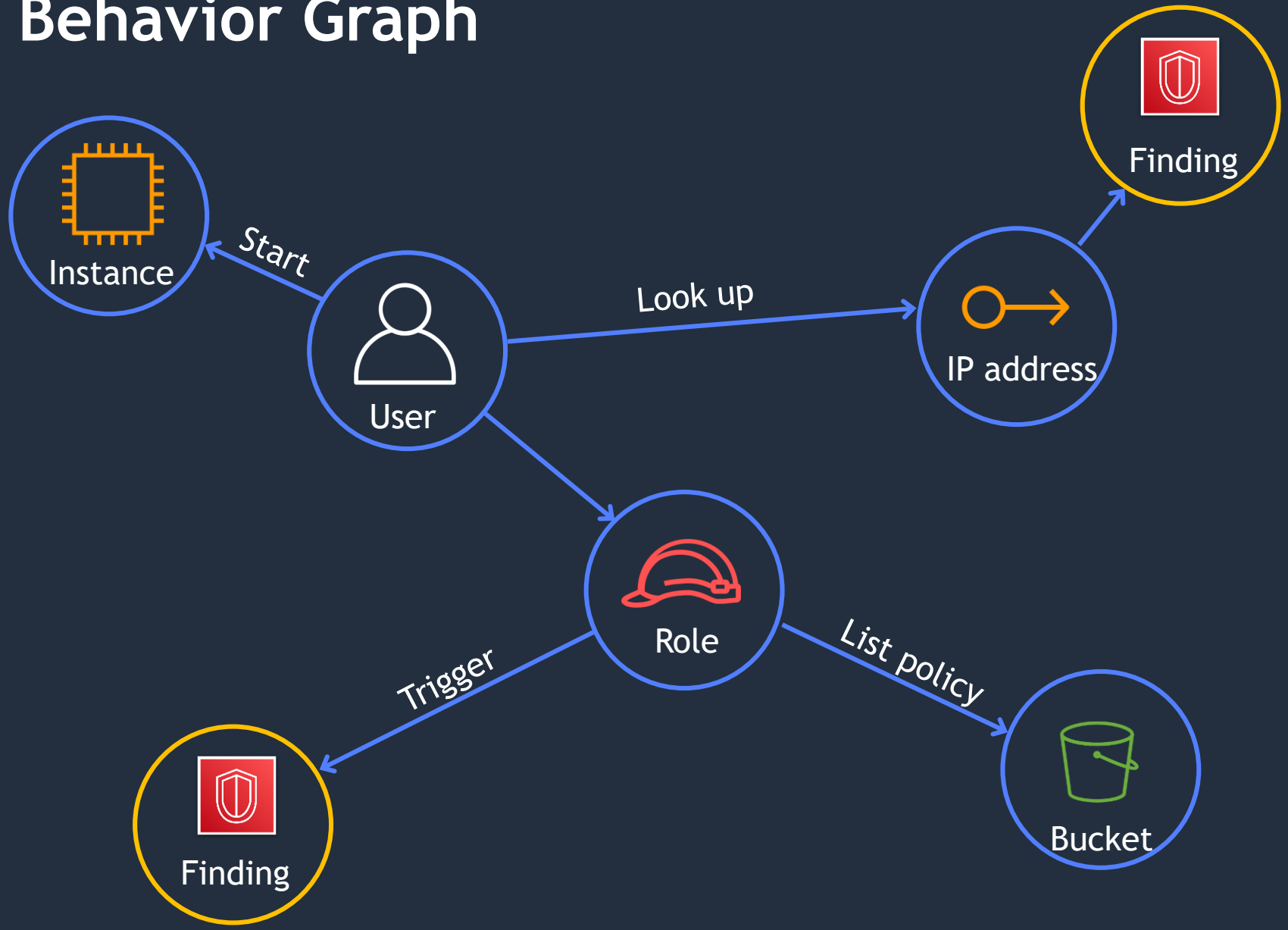
Threat Hunting

aws

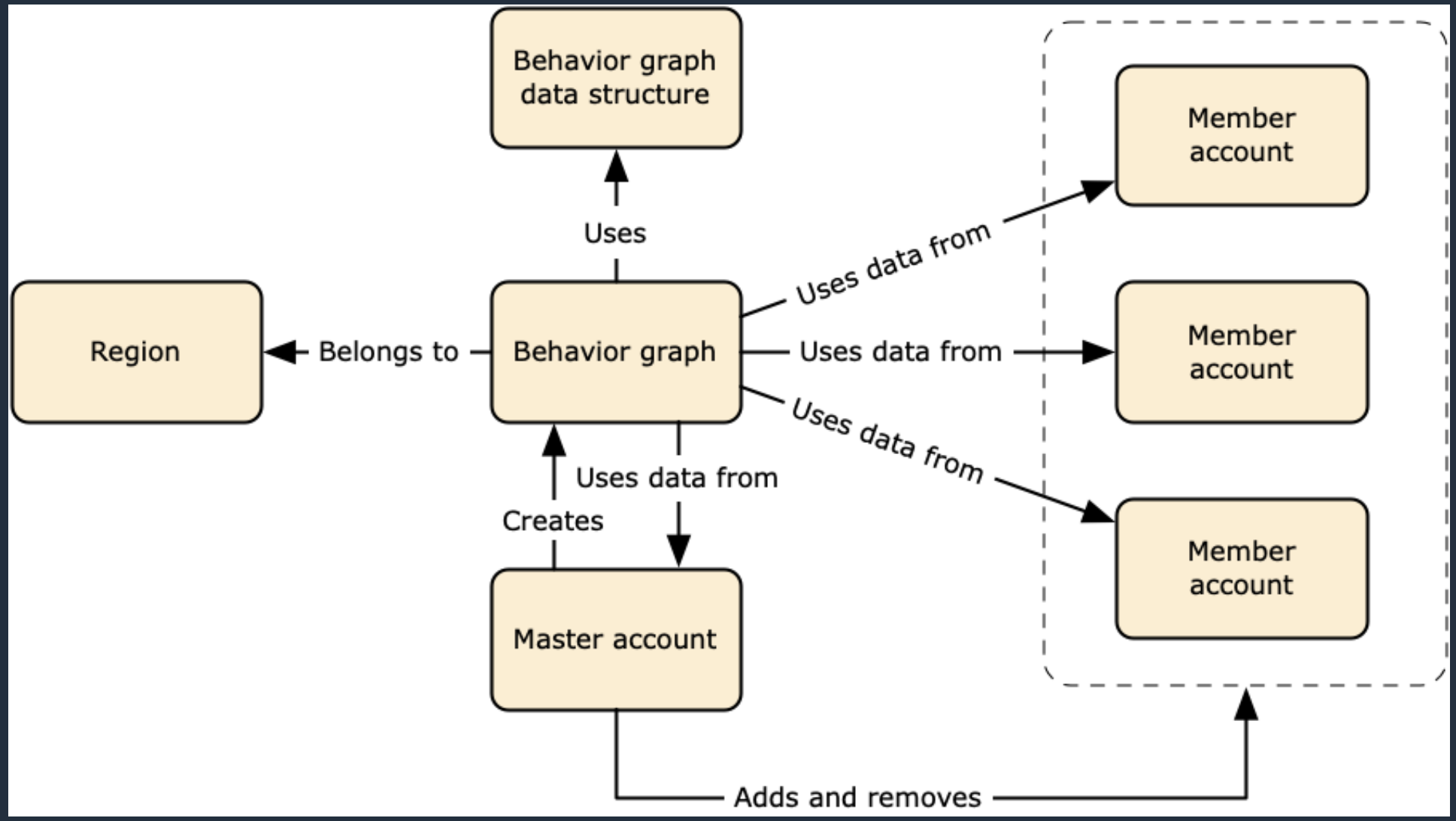
How Detective works



Security Behavior Graph



aws

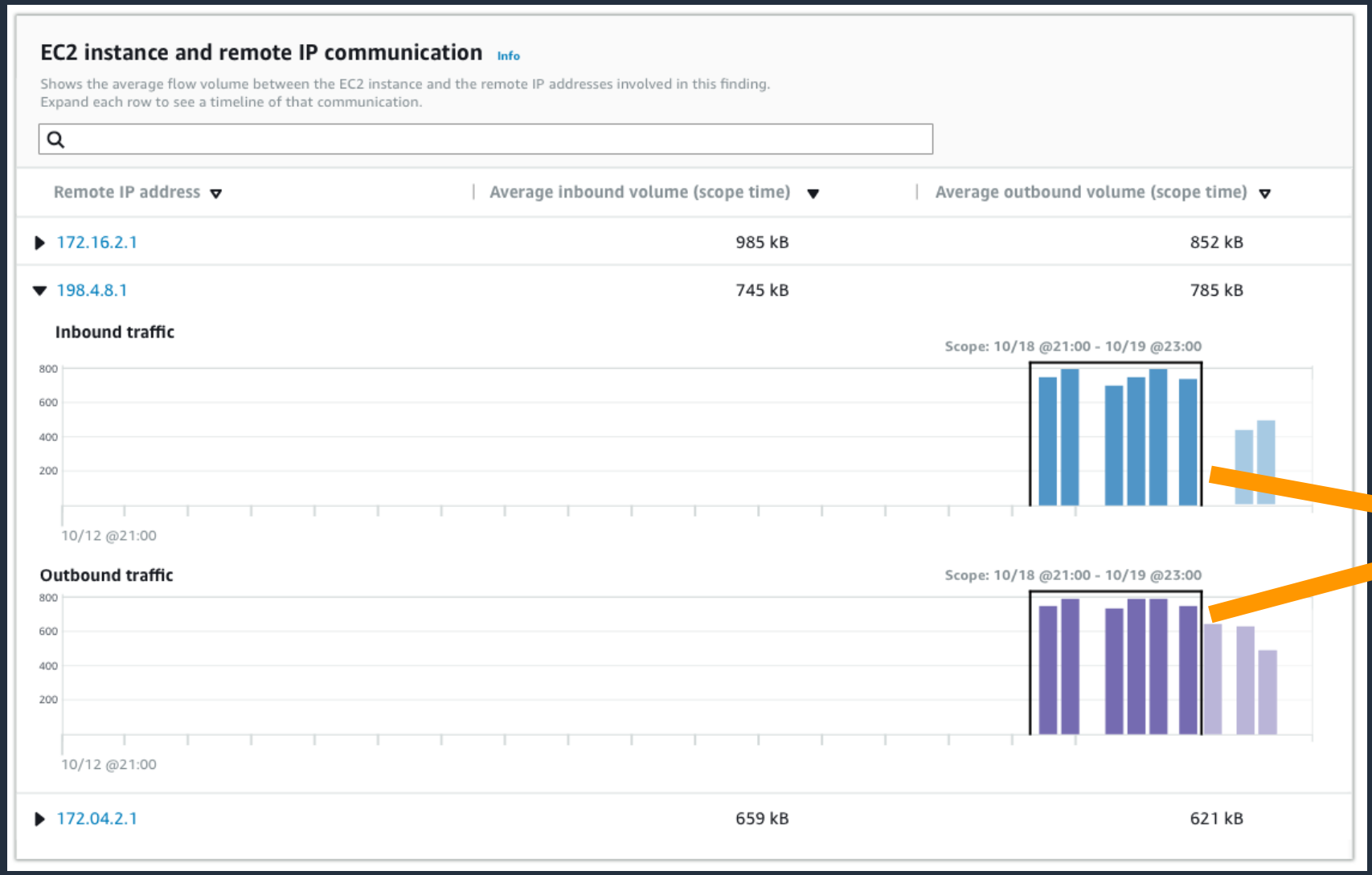


Amazon Detective - Investigations

Successful calls ramping up

Failed calls spiking and then falling

Amazon Detective - Investigations



Traffic to Bitcoin-related IPs

Partners

Technology partners

Services partners

aws

Pricing

Region: US East (N. Virginia)

Data ingested from AWS CloudTrail, Amazon VPC Flow Logs, Amazon GuardDuty	
First 1,000 GB/account/region/month	$2.00 per GB
Next 4,000 GB/account/region/month	$1.00 per GB
Next 5,000 GB/account/region/month	$0.50 per GB
Over 10,000 GB/account/region/month	$0.25 per GB

Best Practices for Amazon Detective

- Enable in all regions for multiple accounts if applicable
- Principles of least privilege: Use IAM policies, Enable MFA
- Only invite accounts you oversee
- Verify invitations from master accounts
- Communicate investigations to appropriate teams

AWS Lambda

What is AWS Lambda?

AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers, creating workload-aware cluster scaling logic, maintaining event integrations, or managing runtimes.

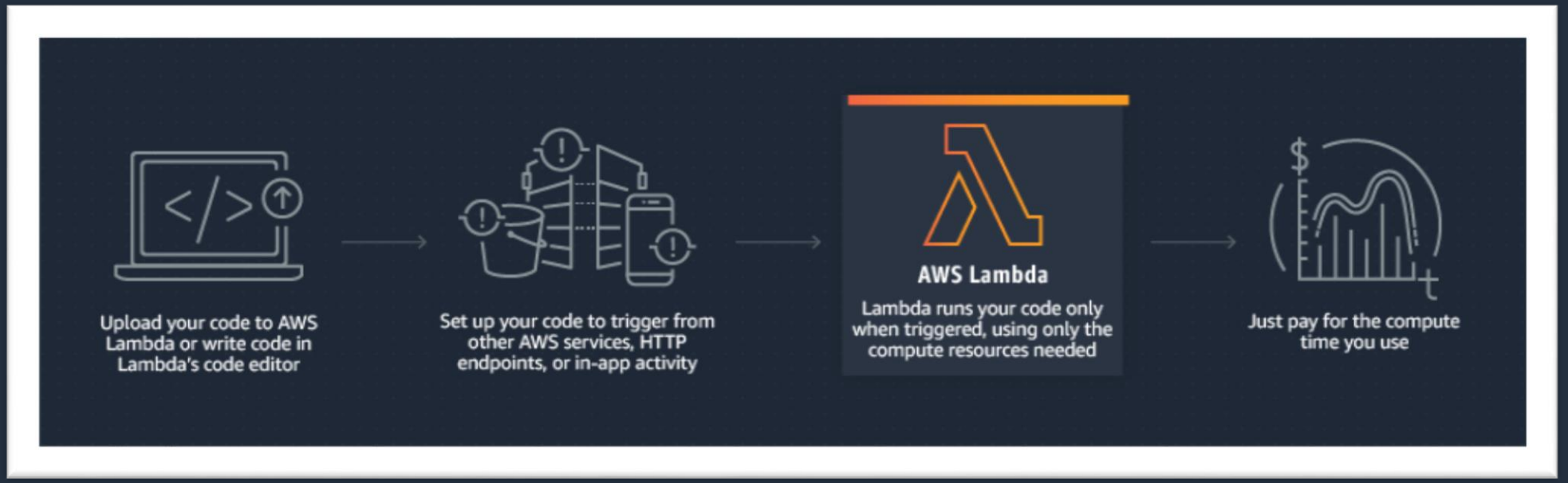
Just upload your code and Lambda automatically allocates compute execution power and runs your code based on the incoming request or event, for any scale of traffic.

Key benefits of AWS Lambda

- Absolutely no servers to manage
- Automatic Scaling in response to Events
- Get consistent performance at any scale
- Pay by the millisecond for code triggers and executions

aws

How it Works



aws

AWS Lambda Use Cases

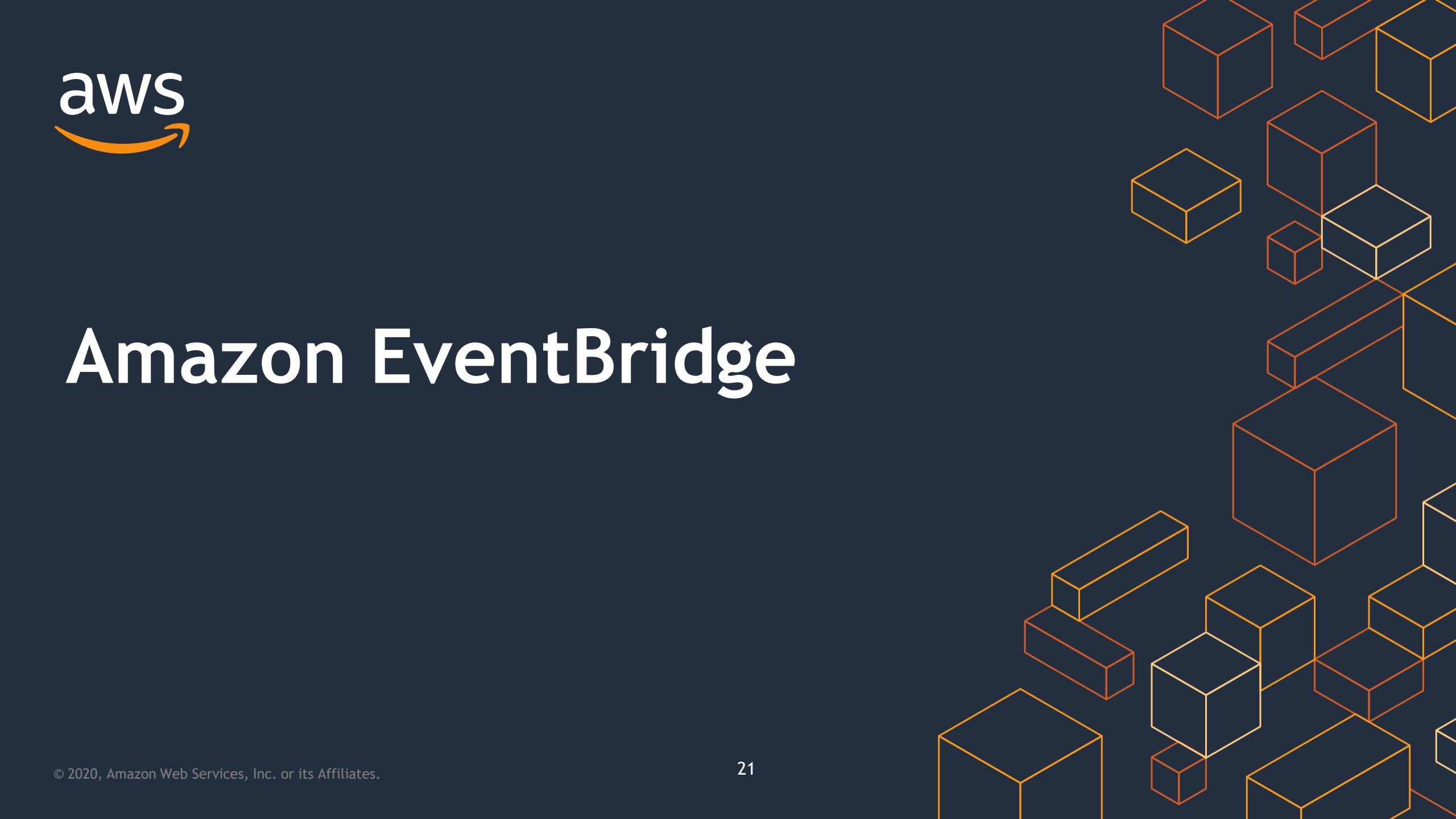
- Web Applications
- Data Processing
- Real time file processing
- Build Serverless Backends
- Machine Learning

aws

Pricing

Region: US East (N. Virginia)

	Price
Requests	$0.20 per 1M requests
Duration	$0.0000166667 for every GB-second



Amazon EventBridge

What is Amazon EventBridge?

Amazon EventBridge is a serverless event bus that makes it easier to build event-driven applications at scale using events generated from your applications, AWS services and integrated Software-as-a-Service (SaaS) applications.

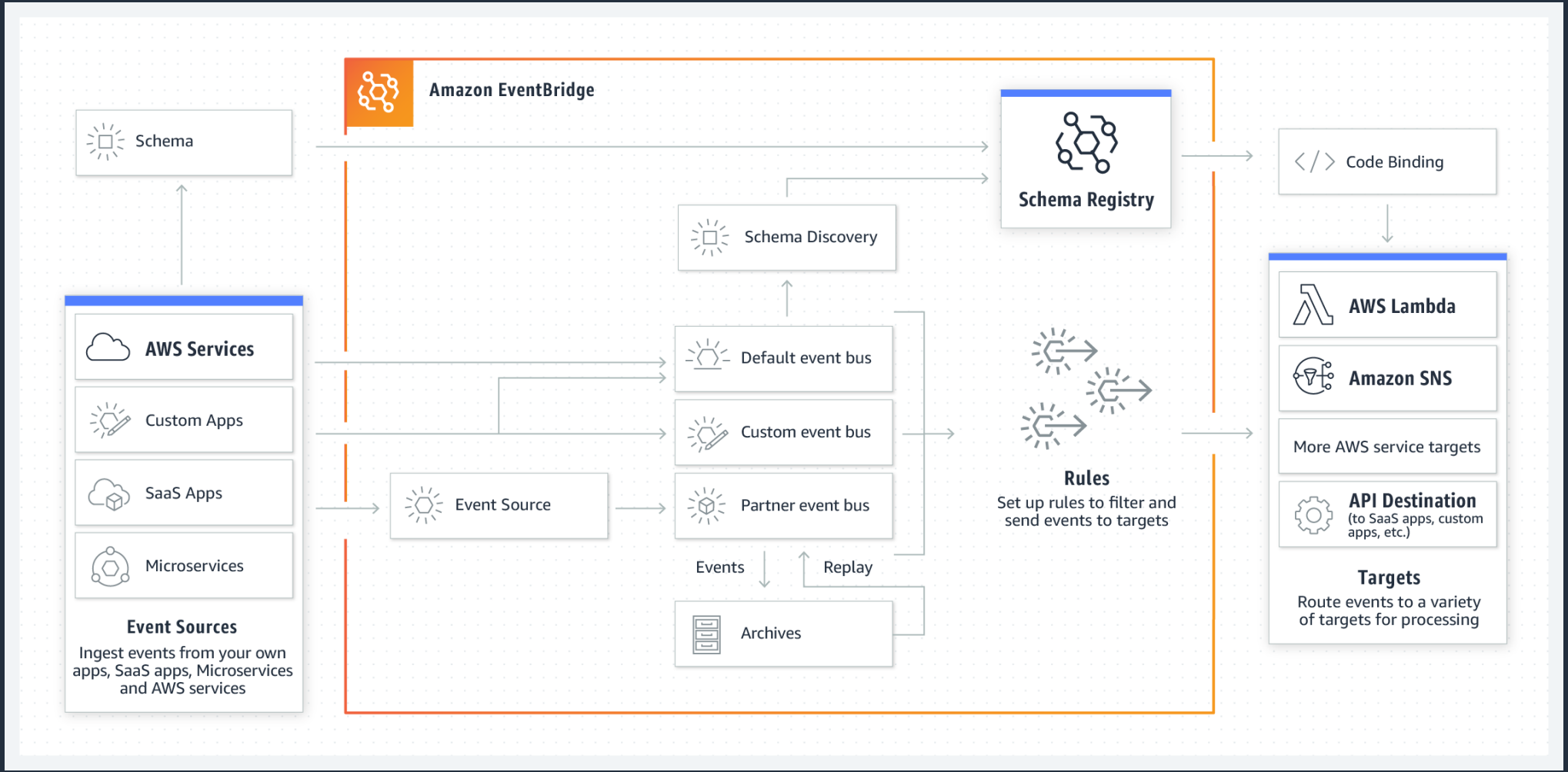
EventBridge delivers a stream of real-time data from event sources such as AWS Securtity Hub and GuardDuty and third party sources such as Shopify or Zendesk to targets like AWS Lambda, EC2 Instances and other SaaS applications.

Key benefits of Amazon EventBridge

- No servers to manage
- Build event-driven architectures
- Connect SaaS applications
- Write less custom code

aws

How it Works



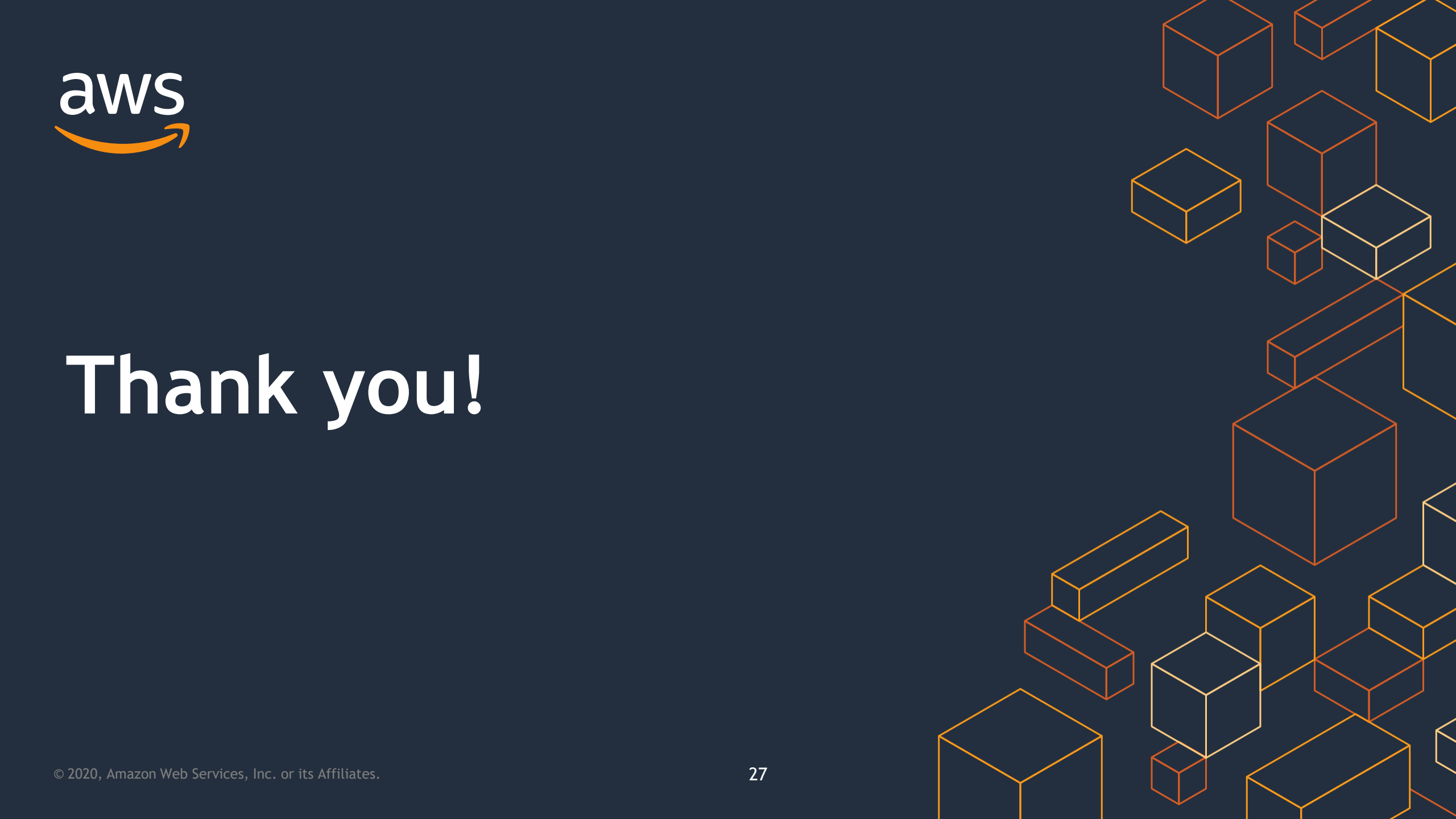
Amazon EventBridge use cases

- Monitor and audit your AWS environments
- Modernize and re-orchestrating your architecture
- Extend functionality via SaaS integrations
- Customize SaaS with AI/ML

aws

Pricing

Region: US East (N. Virginia)	
AWS service events	Free
Custom events	$1.00/million custom events published
Third-party (SaaS) events	$1.00/million events published
Events to another Bus	$1.00/million events sent



Thank you!