



Building Event-Driven Multi-Account Activity Monitoring Solutions



Anton Aleksandrov
Principal Solutions Architect
AWS, Serverless



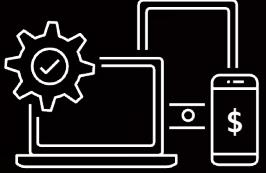
Joe Alioto
Senior Solutions Architect
AWS, CloudOps



Rob Solomon
Senior Cloud Solutions Architect
CrowdStrike



Cloud Security Industry is Evolving



New channels
and products



New threat vectors
are discovered daily



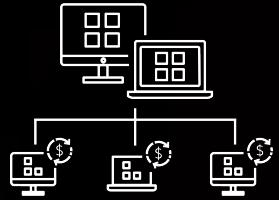
Growing customer
expectations



Yesterday's innovation
is today's commodity

Industry Challenges

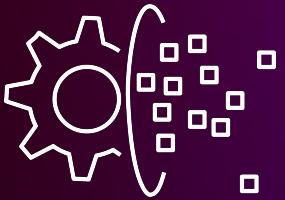
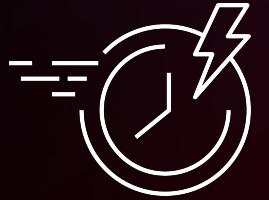
Non-functional requirements



Maintaining legacy infrastructure

High operational costs

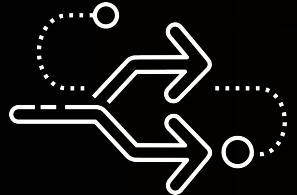
Functional commodities



Expected to be real-time

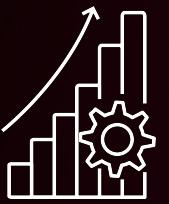
Massive volumes of cloud activities to process

Customer trust and privacy assurance



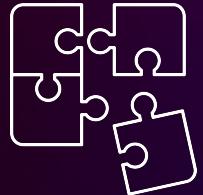
Must reach into customer's account

Considered Invasive by customers



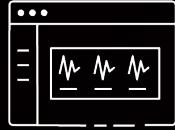
Cost sharing with customers

Features



Rapidly adding product capabilities in a highly competitive market

Real-time Threat Detection Use-cases



Keep track of **continuously changing cloud assets** inventory



Identify assets **that are out of compliance** with enterprise guardrails or regulatory frameworks



Track and audit **user and operator account activity** to detect suspicious behavior in real-time



Monitor assets for **security vulnerabilities**, such as storing secrets in clear text

“Technology and service providers that fail to adapt to the pace of cloud shift face increasing risk of becoming obsolete or, at best, being relegated to low-growth markets.”

- ***Michael Warrilow***
Research Vice President, Gartner

<https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending>



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The Modernization Cycle



Introducing AcmeShield

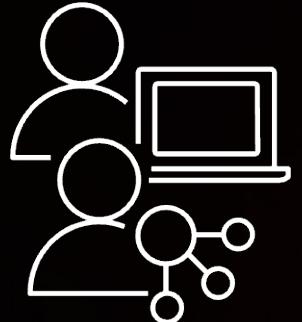
A [fictitious] Real-time Threat
Detection Cybersecurity Company



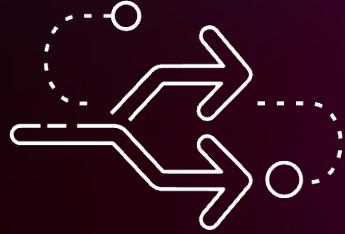
AcmeShield use-cases



**Cloud resources
inventory and change
tracking**



**Operator/user
activity analysis**

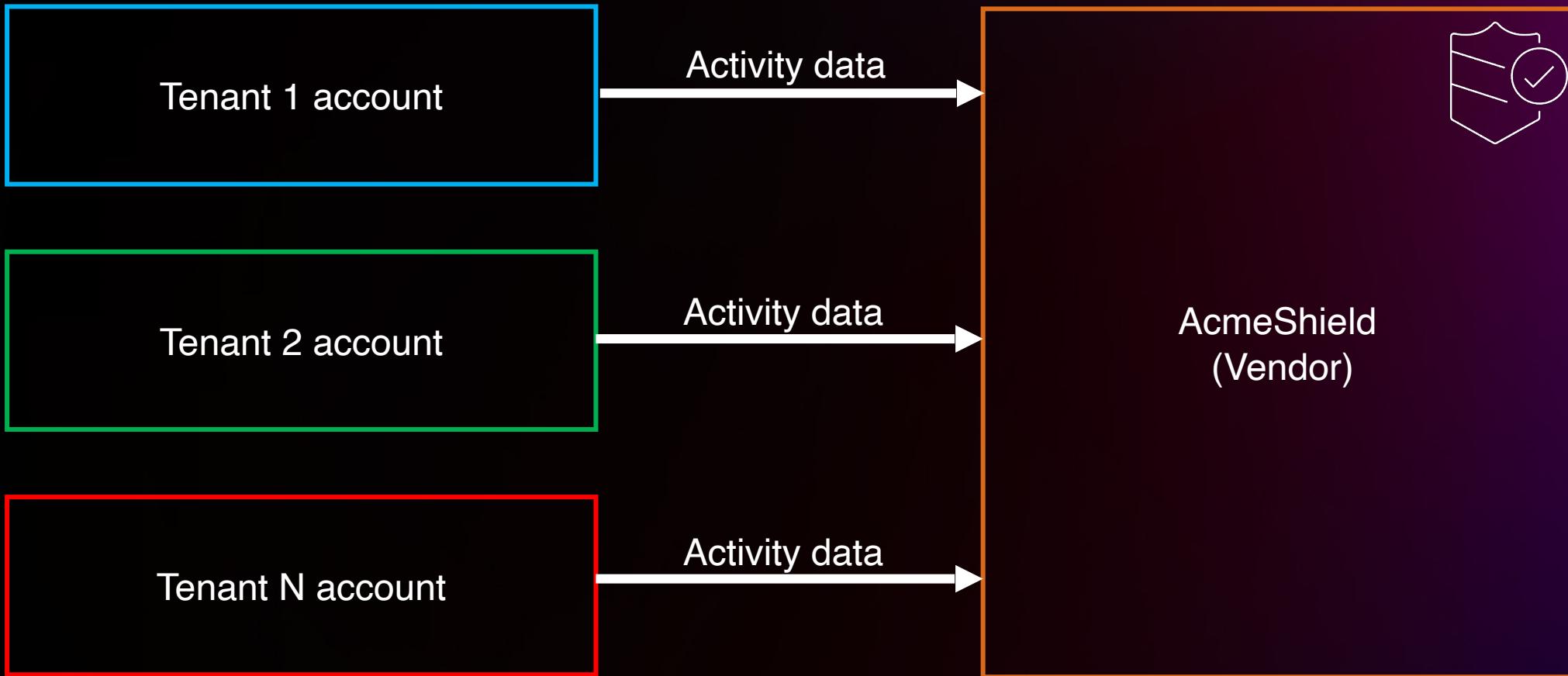


**Compliance and governance
policies violation detection**

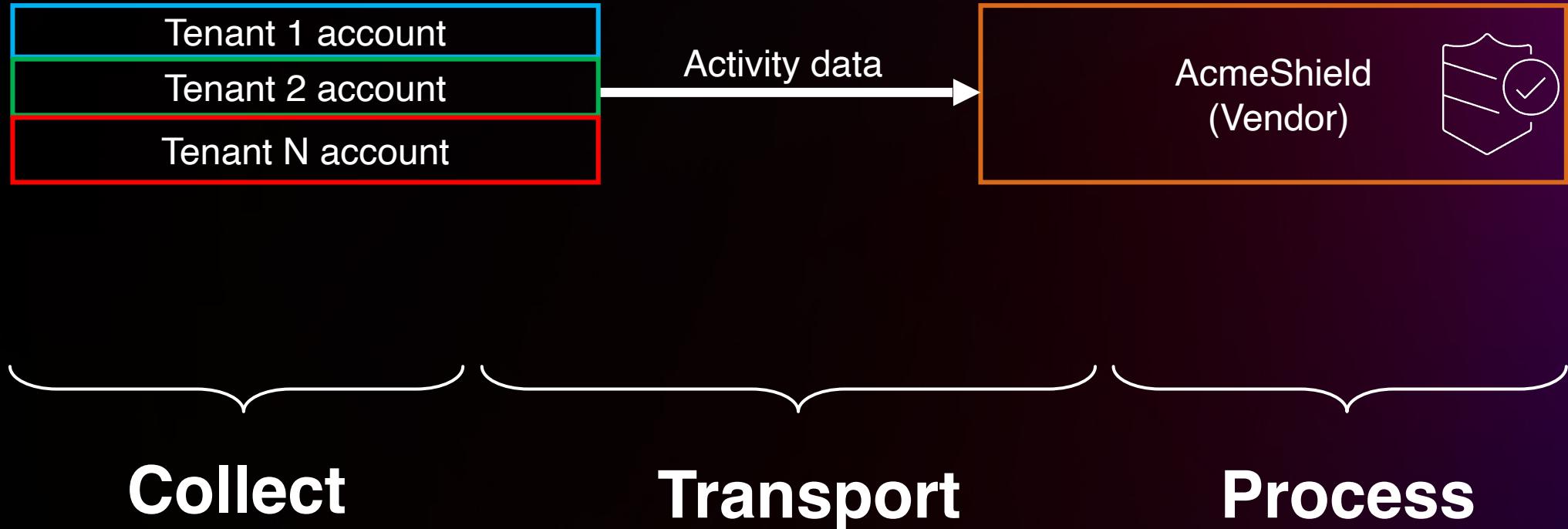


**Threat and suspicious
activity detection**

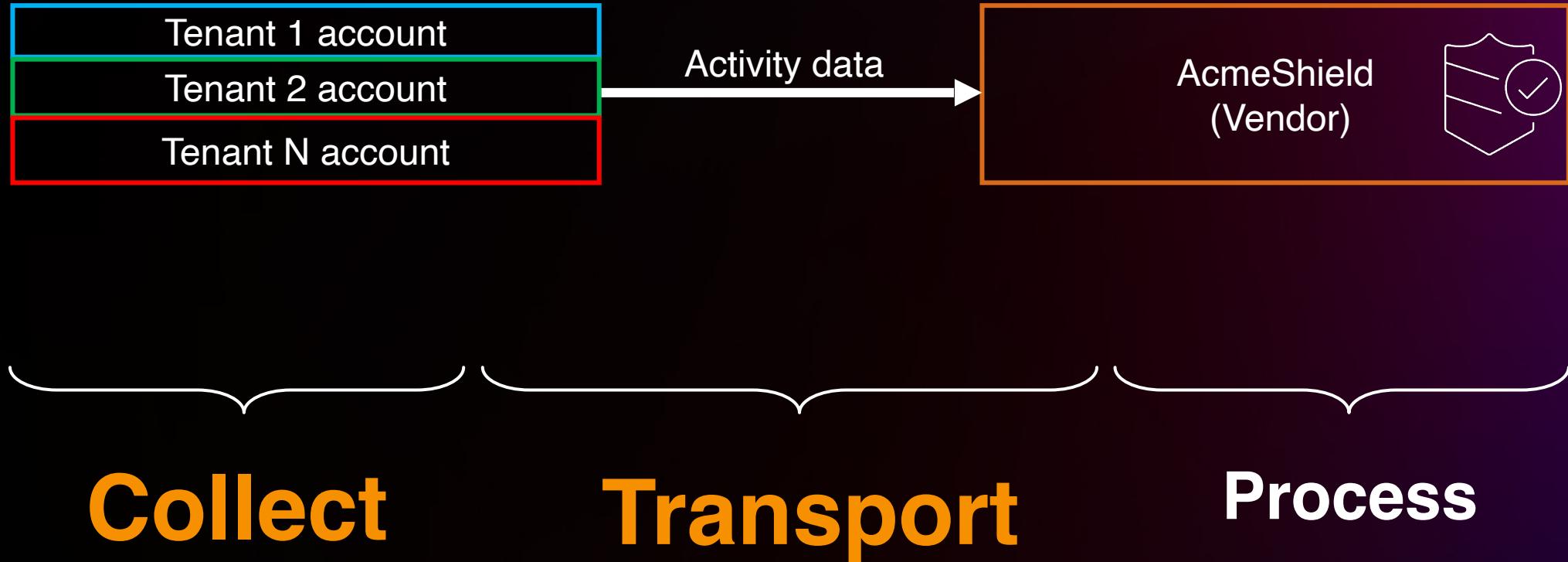
AcmeShield topology



AcmeShield topology



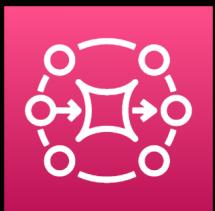
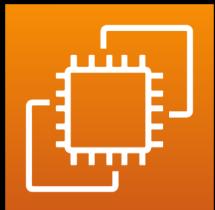
AcmeShield topology



Collecting data

Collecting data

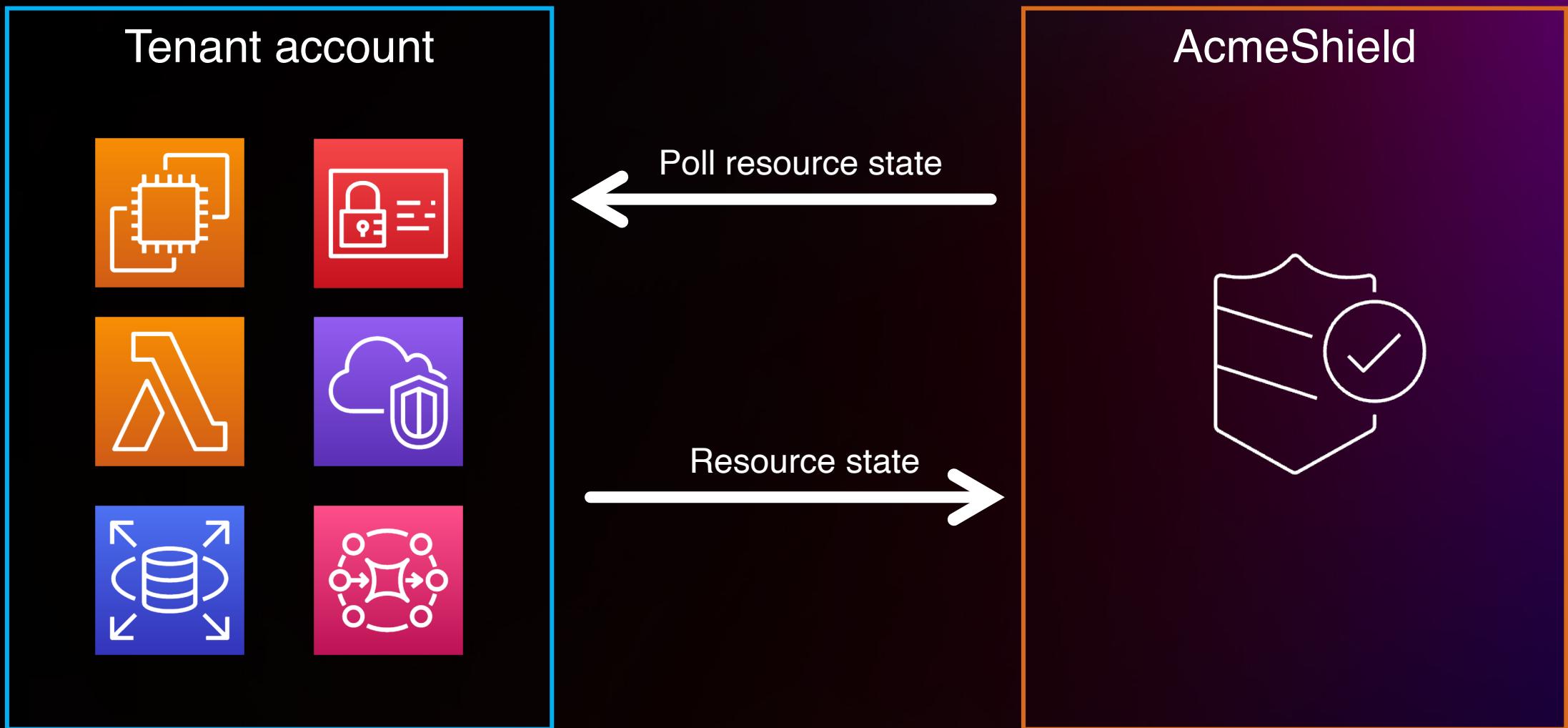
Tenant account



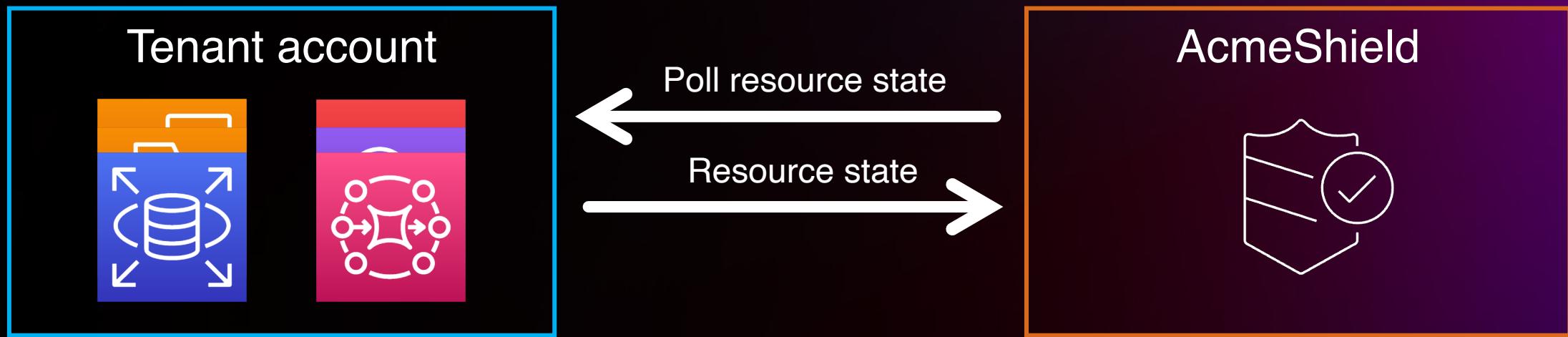
AcmeShield



Collecting data – polling AWS APIs



Collecting data – polling AWS APIs



Advantages:

- Real-time
- Provides resource state
- Good for first-time inventory building

Considerations:

- Requires maintaining polling infrastructure
- Lots of redundancy
- Consumes tenant API quota
- Doesn't handle incremental changes or activities

Event-driven architectures



What is Event?



event

[i-'vent] noun

A signal that a system's state has changed.

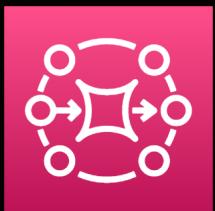
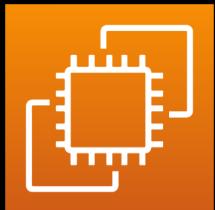
What is Event?

```
{  
  "id": "17793124-05d4-b198-2fde-7edede63b103",  
  "detail-type": "Object Created",  
  "source": "aws.s3",  
  "account": "1234567890",  
  "time": "2021-11-12T00:00:00Z",  
  "region": "us-east-1",  
  "resources": ["arn:aws:s3:::example-bucket"],  
  "detail": {  
    "bucket": {  
      "name": "my-awesome-bucket"  
    },  
    "object": {  
      "key": "my-awesome-object"  
    },  
    "source-ip-address": "1.2.3.4",  
    "reason": "PutObject"  
  }  
}
```

- A JSON object
- A signal that a system or resource state has **changed**
- Represent a fact that occurred in the past
- Immutable - you cannot change the past
- Contains metadata and detail
- Emitted automatically by **250+ AWS Services** (and growing)

Collecting data

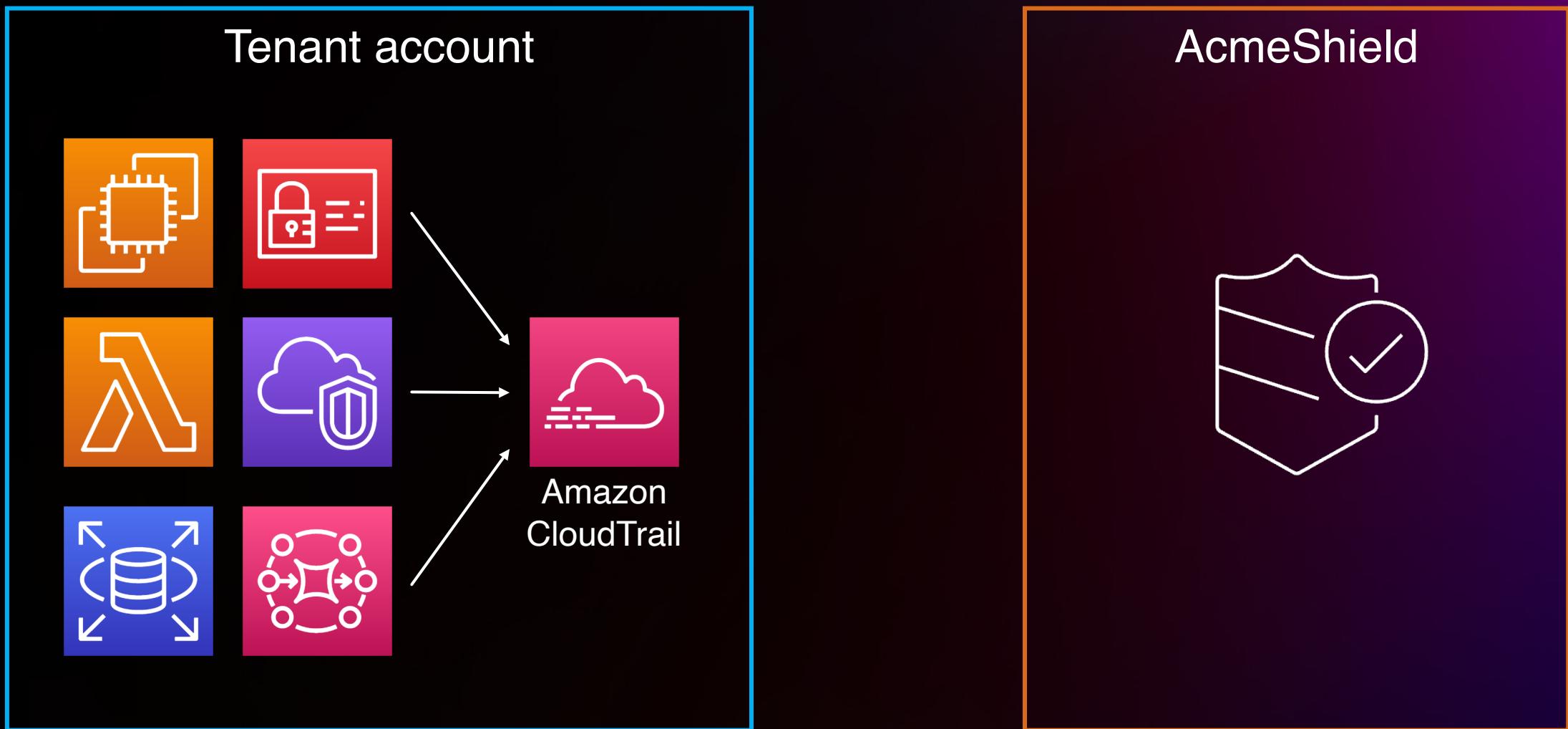
Tenant account



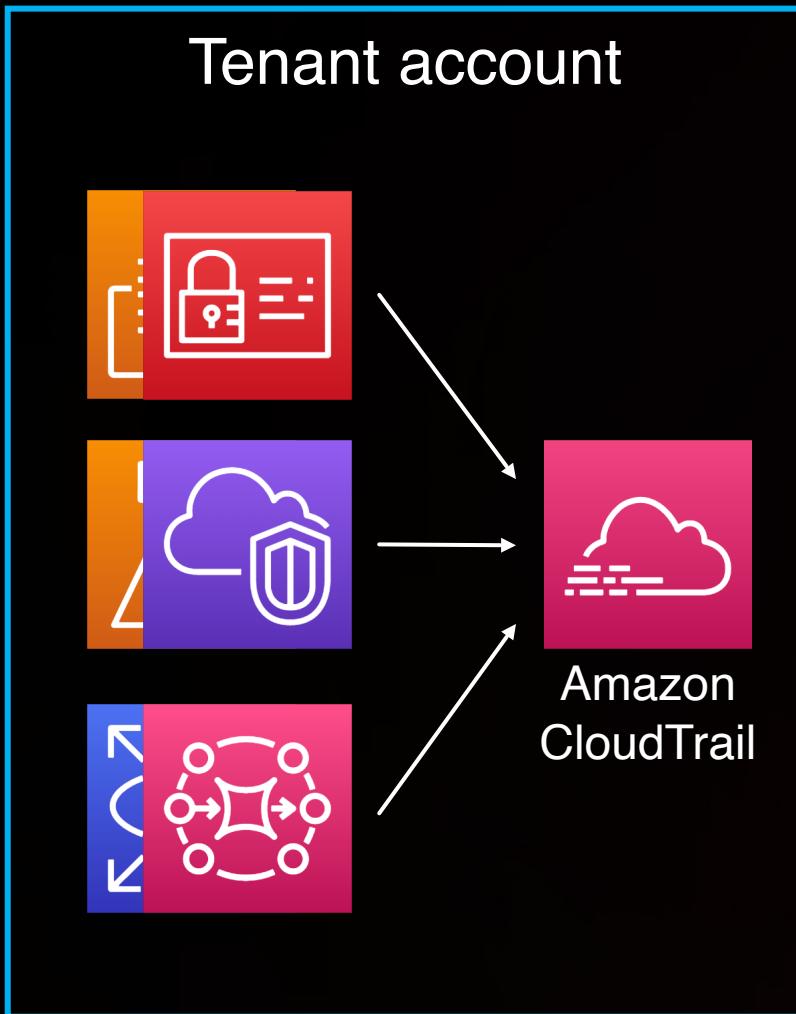
AcmeShield



Collecting data – Amazon CloudTrail



Collecting data – Amazon CloudTrail



Event history (200+) Info

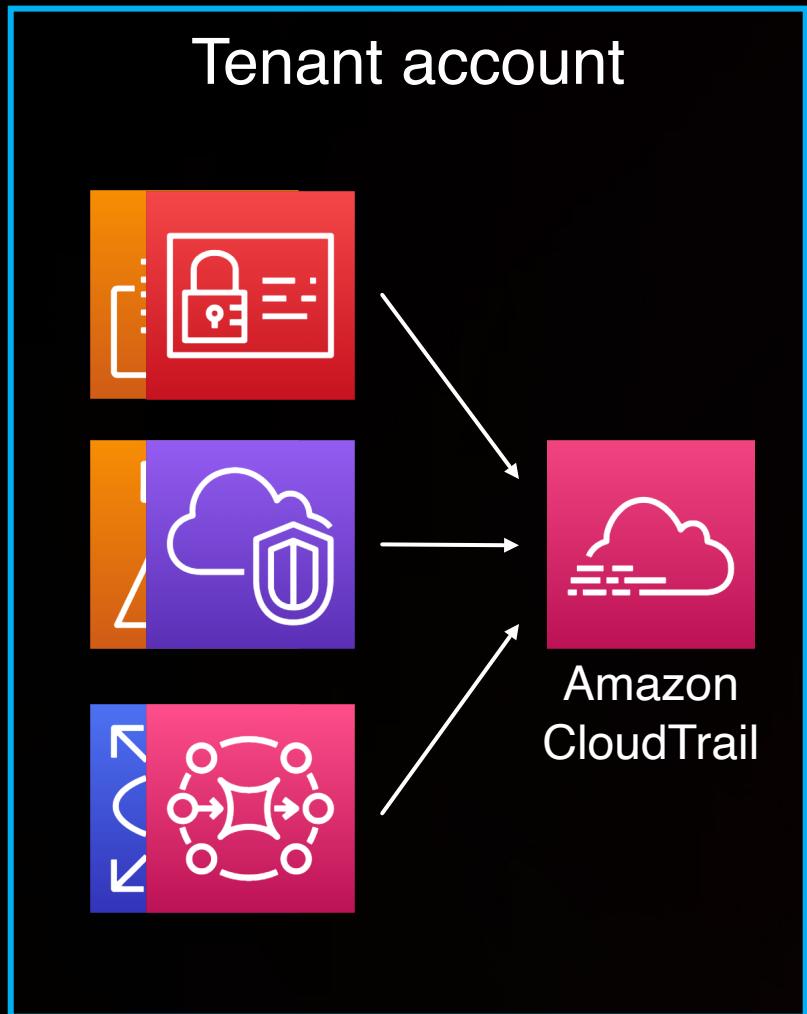
Event history shows you the last 90 days of management events.

Lookup attributes

Read-only false

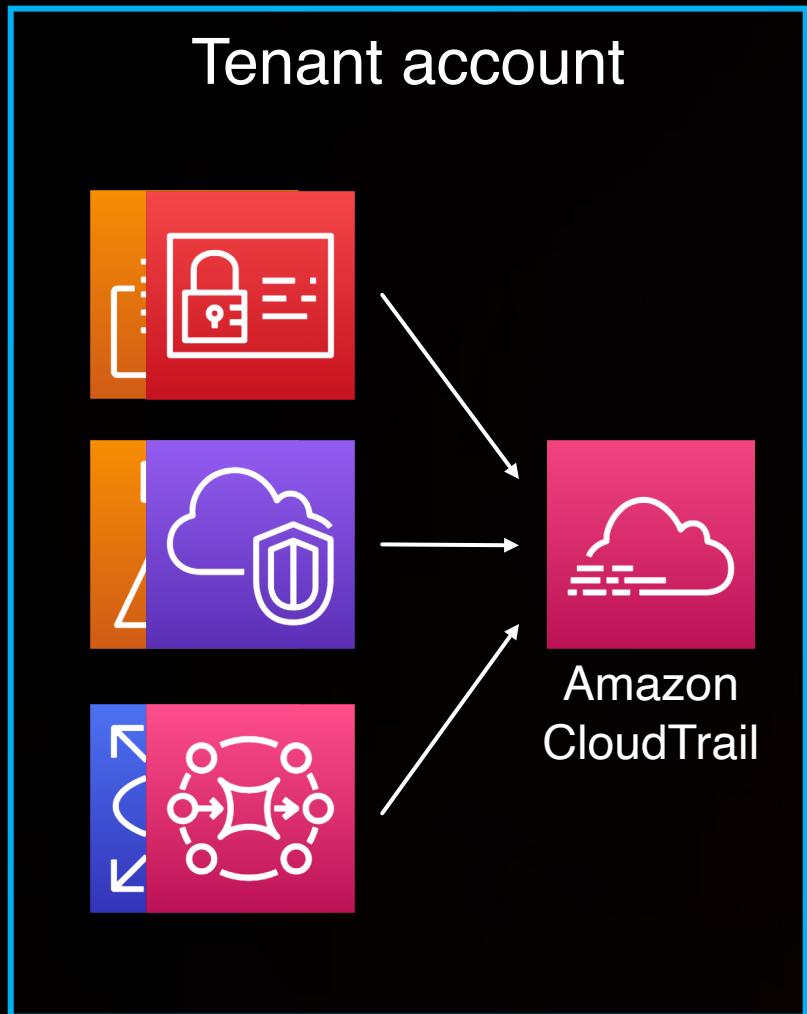
<input type="checkbox"/>	Event name	Event time	User name
<input type="checkbox"/>	UpdateInstanceAssociationStatus	August 20, 2024, 17:09:04 (UTC-05:00)	i-0c7ddfe27bfcd87c4
<input type="checkbox"/>	PutComplianceItems	August 20, 2024, 17:09:04 (UTC-05:00)	i-0c7ddfe27bfcd87c4
<input type="checkbox"/>	PutInventory	August 20, 2024, 17:09:04 (UTC-05:00)	i-0c7ddfe27bfcd87c4
<input type="checkbox"/>	UpdateInstanceAssociationStatus	August 20, 2024, 17:09:04 (UTC-05:00)	i-0c7ddfe27bfcd87c4
<input type="checkbox"/>	UpdateInstanceState	August 20, 2024, 17:09:00 (UTC-05:00)	i-0c7ddfe27bfcd87c4
<input type="checkbox"/>	UpdateInstanceAssociationStatus	August 20, 2024, 17:08:57 (UTC-05:00)	i-0c7ddfe27bfcd87c4
<input type="checkbox"/>	UpdateInstanceAssociationStatus	August 20, 2024, 17:08:57 (UTC-05:00)	i-0c7ddfe27bfcd87c4
<input type="checkbox"/>	UpdateInstanceState	August 20, 2024, 17:08:37 (UTC-05:00)	i-0c7ddfe27bfcd87c4
<input type="checkbox"/>	UpdateInstanceState	August 20, 2024, 17:08:15 (UTC-05:00)	i-011138a97e7821ebb
<input type="checkbox"/>	UpdateInstanceState	August 20, 2024, 17:03:37 (UTC-05:00)	i-0c7ddfe27bfcd87c4
<input type="checkbox"/>	UpdateInstanceState	August 20, 2024, 17:03:15 (UTC-05:00)	i-011138a97e7821ebb

Collecting data – Amazon CloudTrail



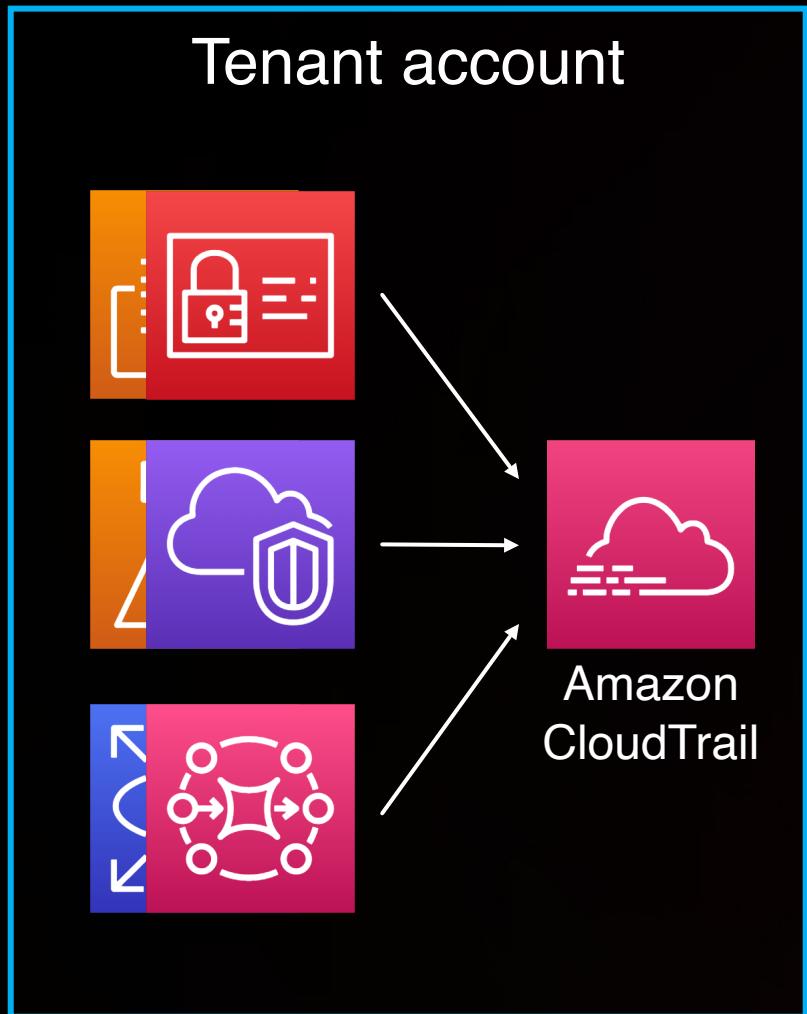
```
{  
  "eventTime": "2024-08-20T22:13:16Z",  
  "userIdentity": {  
    "type": "AssumedRole",  
    "principalId": "ABCDEFGH",  
    "arn": "arn:aws:sts::123456789:assumed-role/AWSSer",  
    "accountId": "123456789"  
  },  
  "eventSource": "ec2.amazonaws.com",  
  "eventName": "DescribeSubnets",  
  "awsRegion": "us-east-1",  
  "eventType": "AwsApiCall",  
  "managementEvent": true,  
  "recipientAccountId": "281024298475",  
  "eventCategory": "Management",  
  "sourceIPAddress": "{redacted}",  
  "userAgent": "{redacted}",  
  "requestParameters": "{redacted}"  
}
```

Collecting data – Amazon CloudTrail



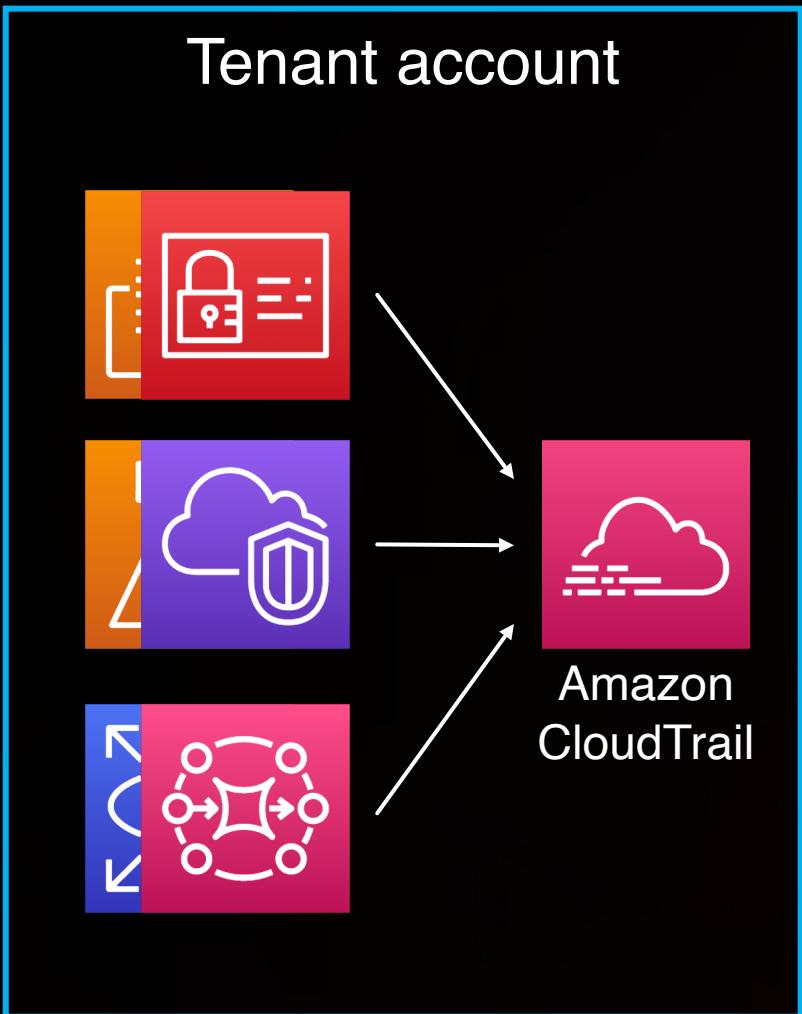
```
{  
  "eventTime": "2024-08-20T22:13:16Z",  
  "userIdentity": {  
    "type": "AssumedRole",  
    "principalId": "ABCDEFGH",  
    "arn": "arn:aws:sts::123456789:assumed-role/AWSSer",  
    "accountId": "123456789"  
  },  
  "eventSource": "ec2.amazonaws.com",  
  "eventName": "DescribeSubnets",  
  "awsRegion": "us-east-1",  
  "eventType": "AwsApiCall",  
  "managementEvent": true,  
  "recipientAccountId": "281024298475",  
  "eventCategory": "Management",  
  "sourceIPAddress": "{redacted}",  
  "userAgent": "{redacted}",  
  "requestParameters": "{redacted}"  
}
```

Collecting data – Amazon CloudTrail



```
{  
  "eventTime": "2024-08-20T22:13:16Z",  
  "userIdentity": {  
    "type": "AssumedRole",  
    "principalId": "ABCDEFGH",  
    "arn": "arn:aws:sts::123456789:assumed-role/AWSSer",  
    "accountId": "123456789"  
  },  
  "eventSource": "ec2.amazonaws.com",  
  "eventName": "DescribeSubnets",  
  "awsRegion": "us-east-1",  
  "eventType": "AwsApiCall",  
  "managementEvent": true,  
  "recipientAccountId": "281024298475",  
  "eventCategory": "Management",  
  "sourceIPAddress": "{redacted}",  
  "userAgent": "{redacted}",  
  "requestParameters": "{redacted}"  
}
```

Collecting data – Amazon CloudTrail



Advantages :

- Provides detailed data about account activity and changes
- Natively integrated with over 250 AWS services
- No maintenance / operations
- Supports AWS Organizations
- Just works out of the box

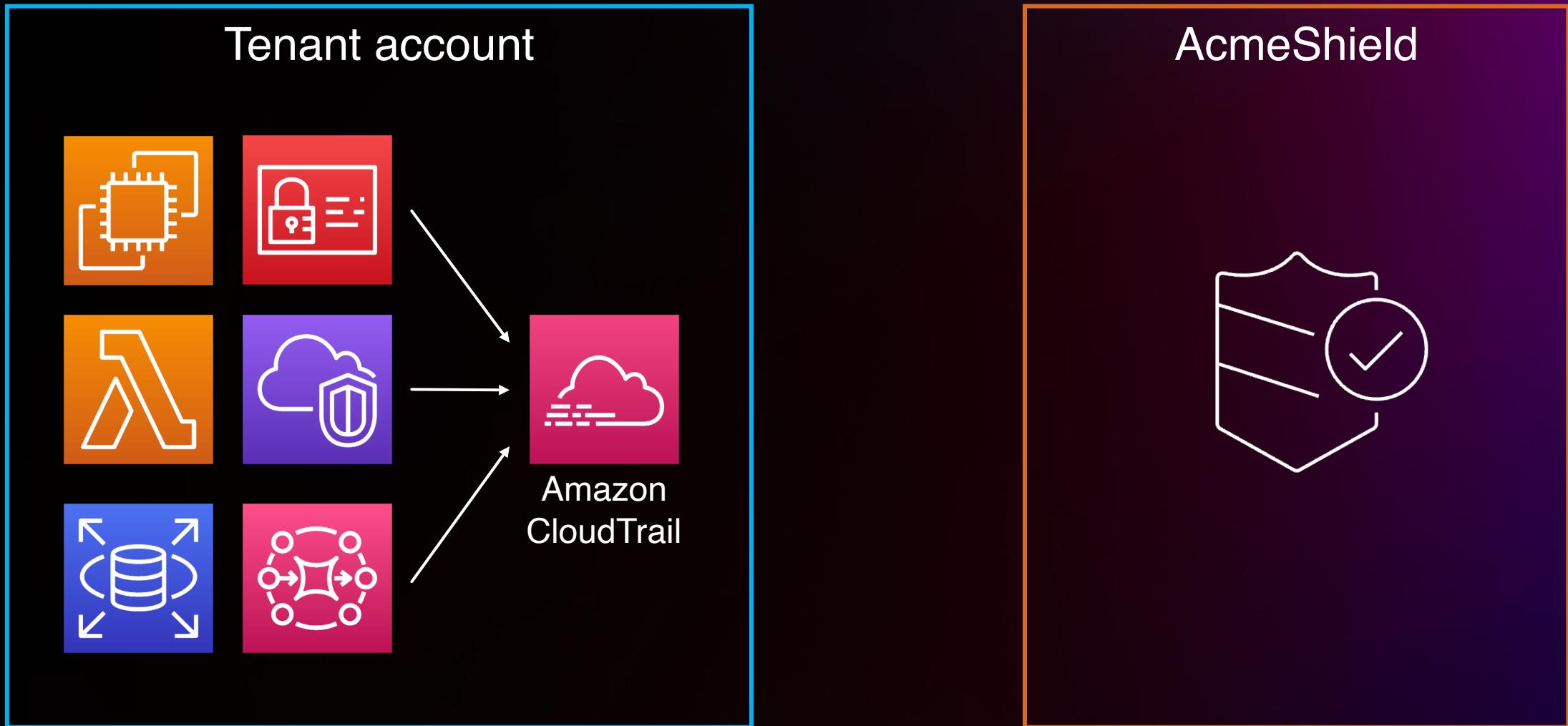
Considerations:

- Vendors still need to find a way to transport event data from tenant to vendor accounts

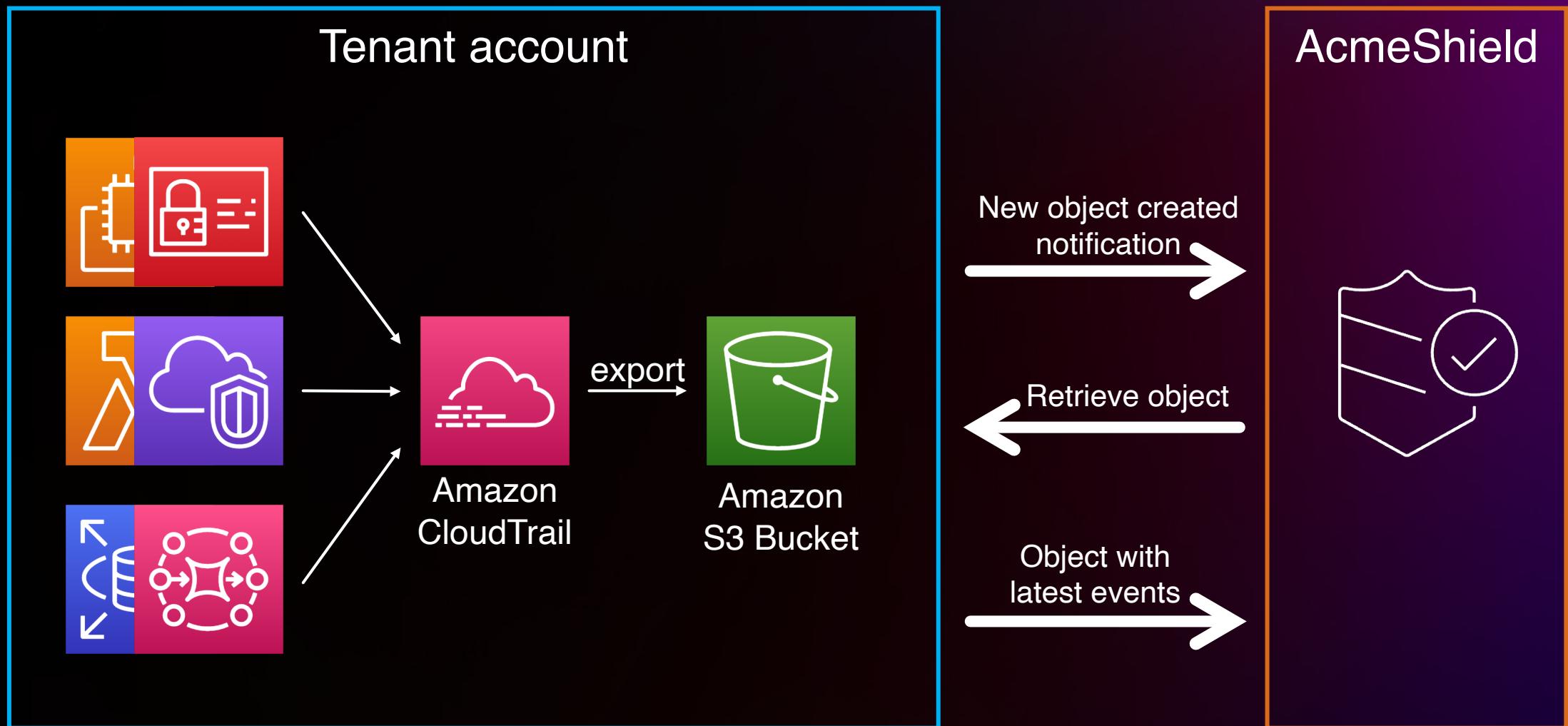
Transporting event data across accounts



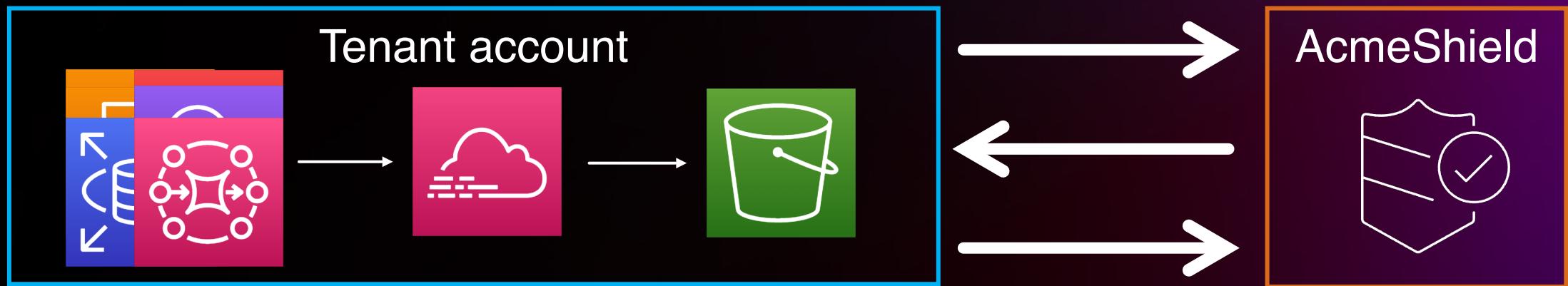
Transporting data across accounts



Traditional approach



Transporting data with S3



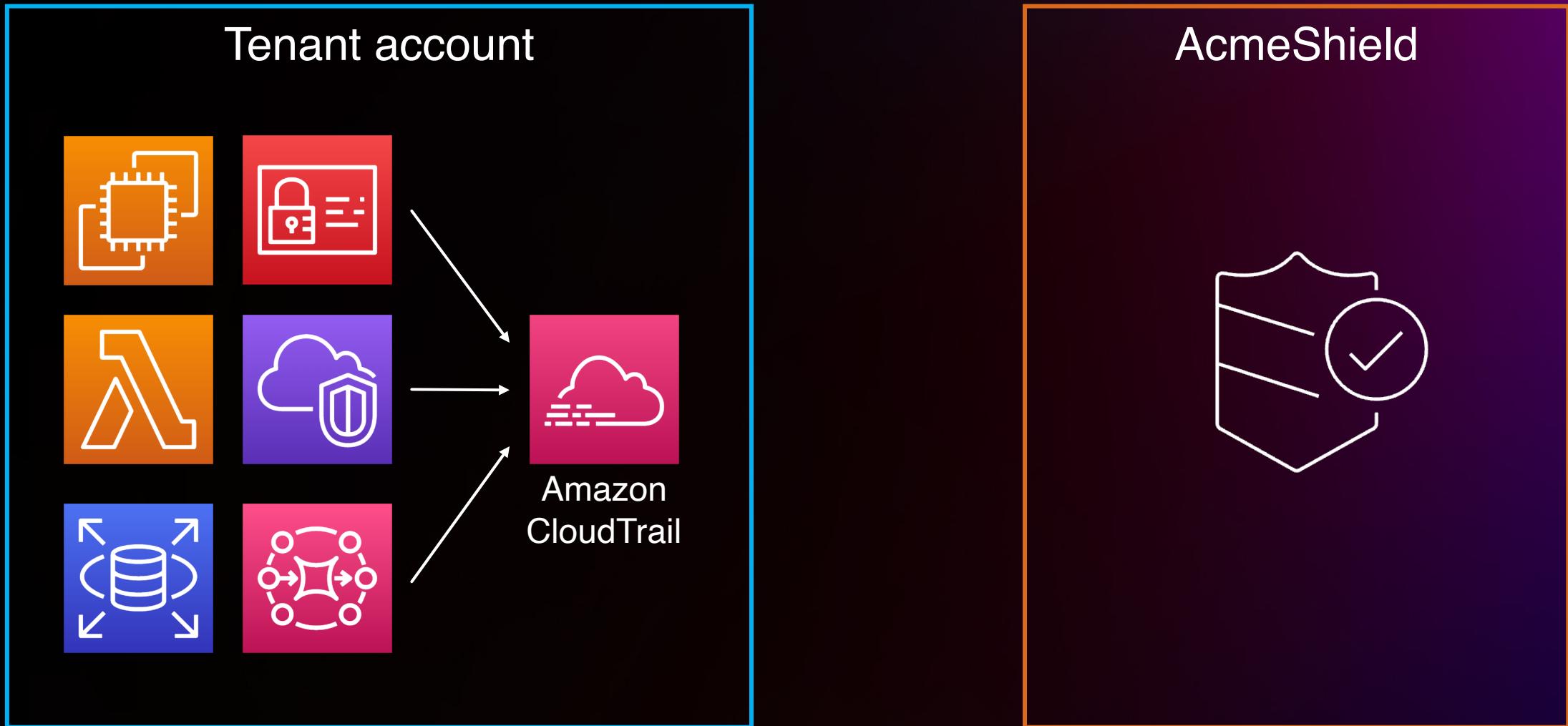
Advantages:

- Simple
- Cheap (for tenants)

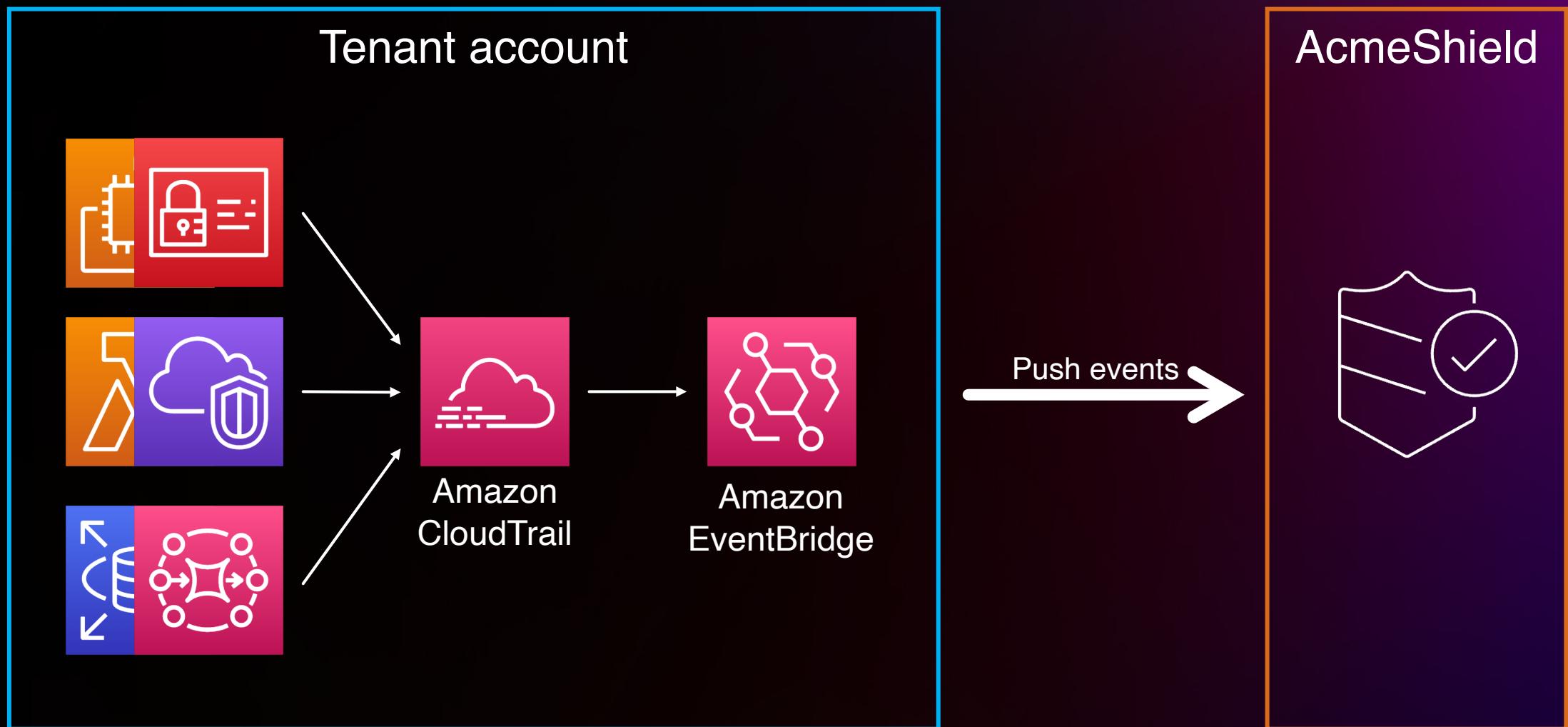
Considerations:

- All or nothing (no filtering or conditional routing)
- Not real-time, events can be delayed for minutes (higher mean-time-to-detect)
- Requires vendors to continuously maintain infrastructure for downloading and unpacking millions of S3 objects
- Requires inbound IAM permissions

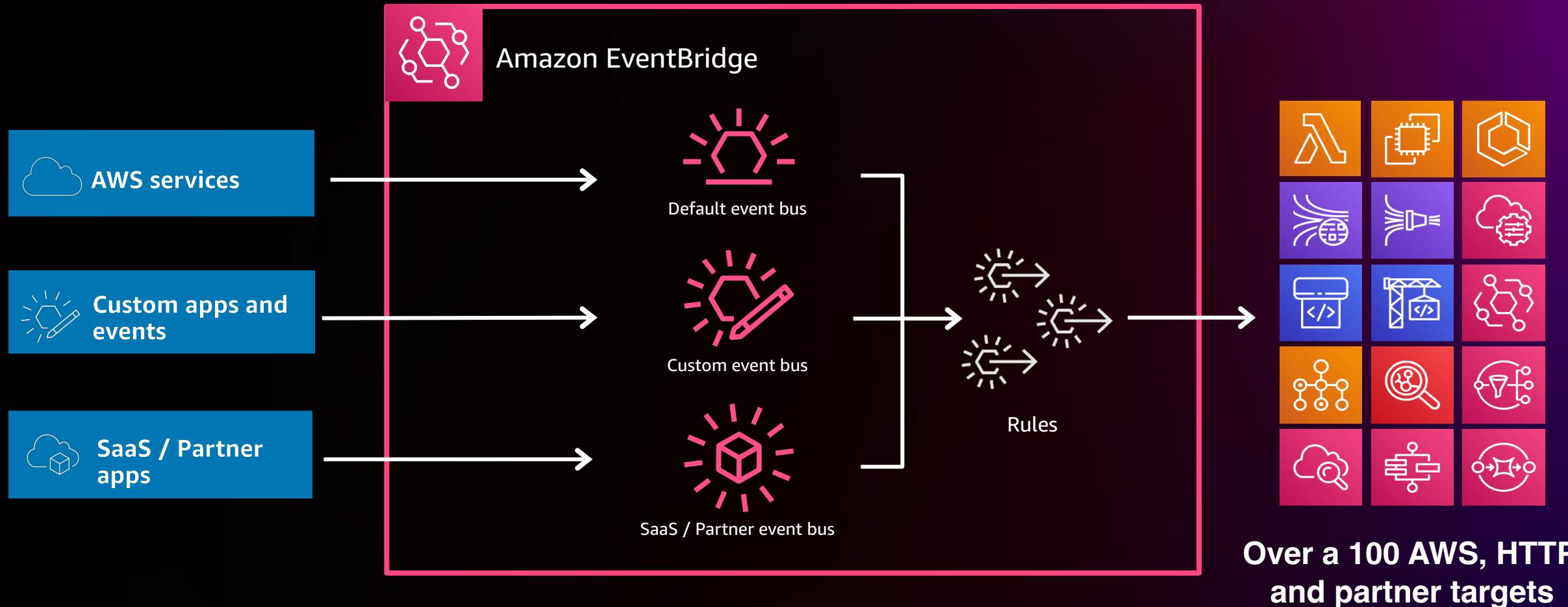
Transporting data across accounts



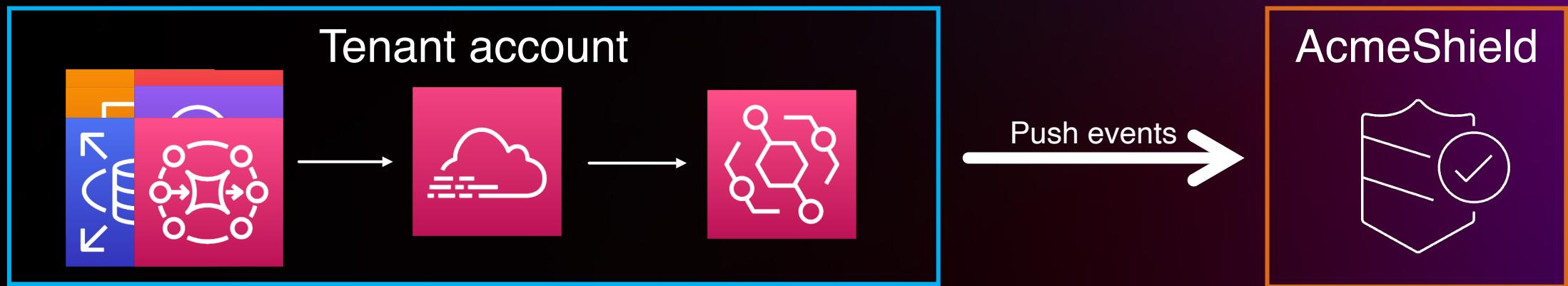
Transporting data with EventBridge



Amazon EventBridge – Serverless Event Router



Transporting data with EventBridge



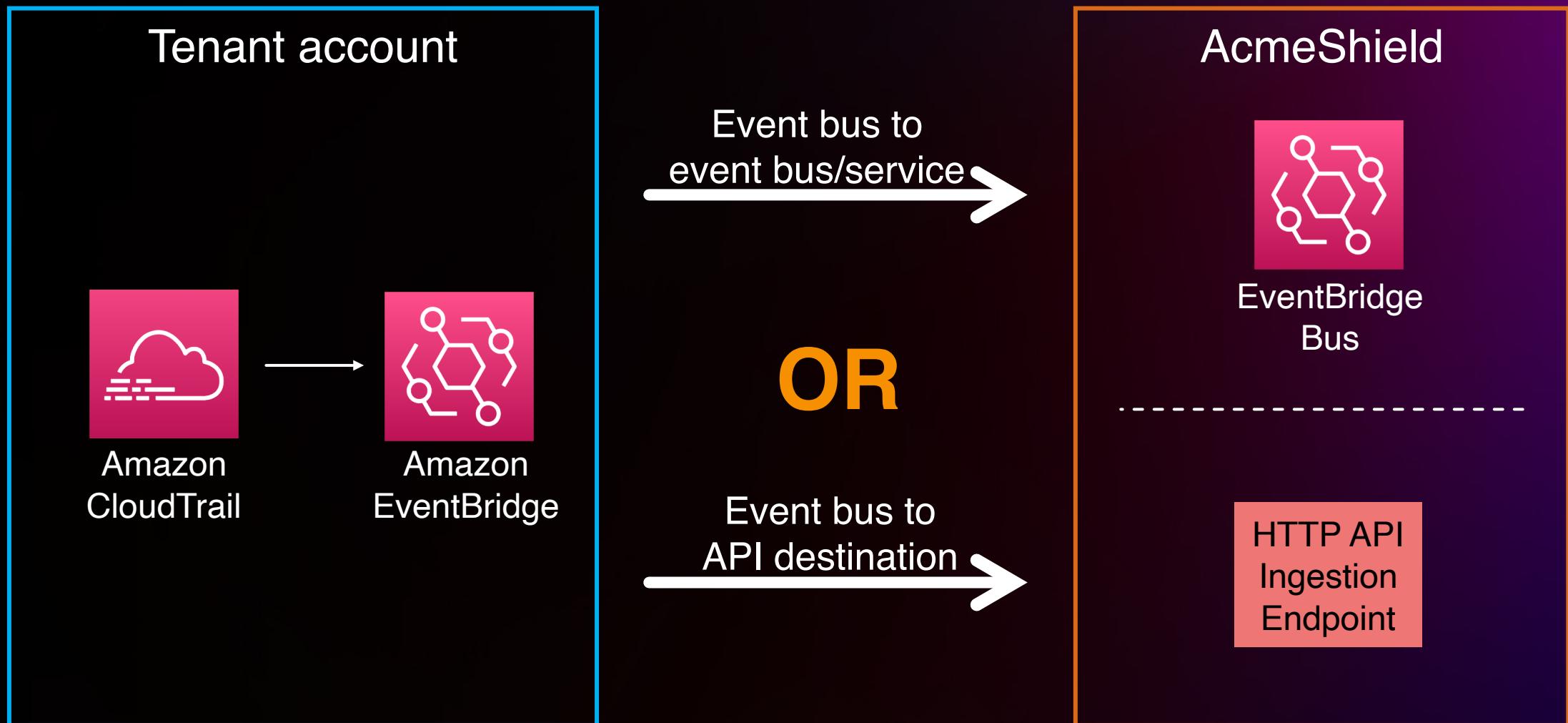
Advantages:

- Simple, serverless, just works
- No redundant polling via API calls
- Real-time, events are pushed to vendors as they occur
- Flexible filtering and routing rules
- Outbound IAM permissions only

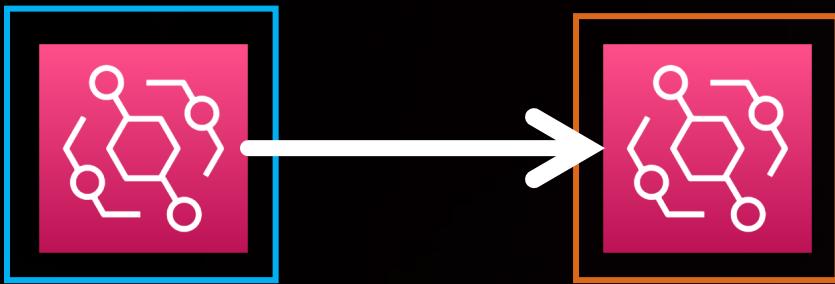
Considerations:

- Variable cost
- Consumes tenant's EventBridge quotas

Transporting data with EventBridge

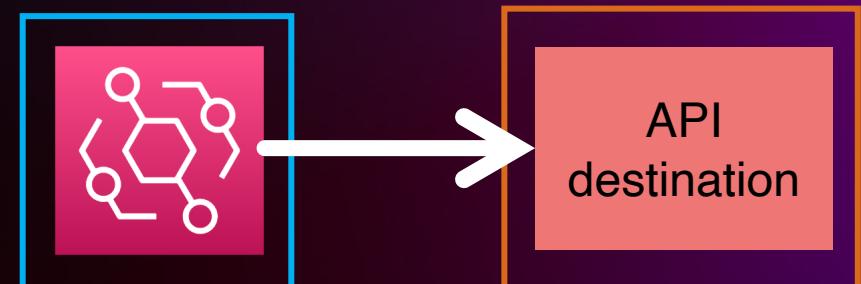


Transporting data with EventBridge



Bus-to-bus:

- Simplest to implement
 - Does not require additional endpoints on vendor side
 - Up to **18,750 TPS** by default
 - Native AWS IAM support
-
- **\$1** per million events (tenant)



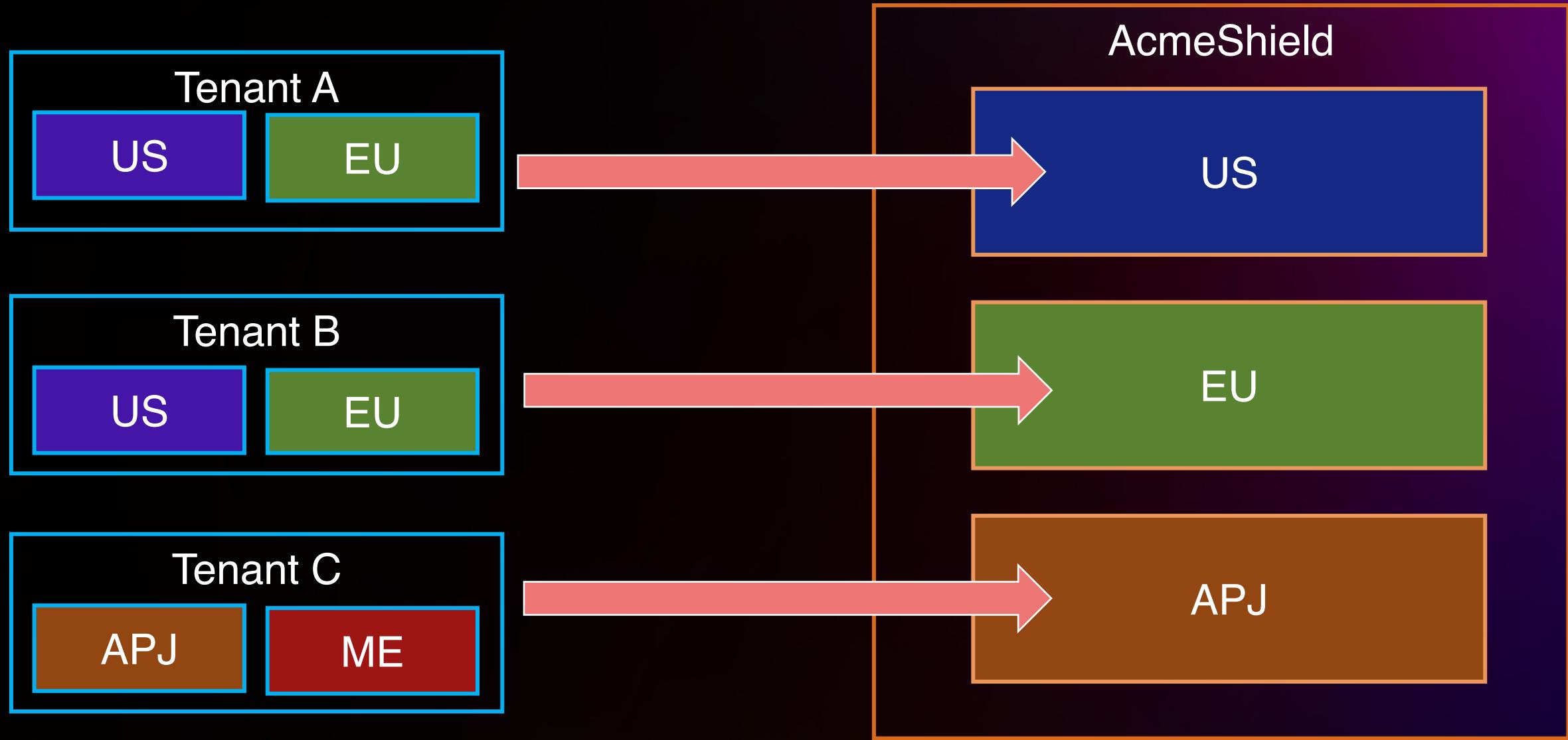
Bus-to-API:

- Simple for tenants, requires additional effort for vendors
 - **300 TPS** by default (up to 3000)
 - Vendors must implement endpoint authorization (Basic, OAuth2, or API Key)
-
- **\$0.20** per million events (tenant)

But what about cross-region?



Cross-region events collection – what's common



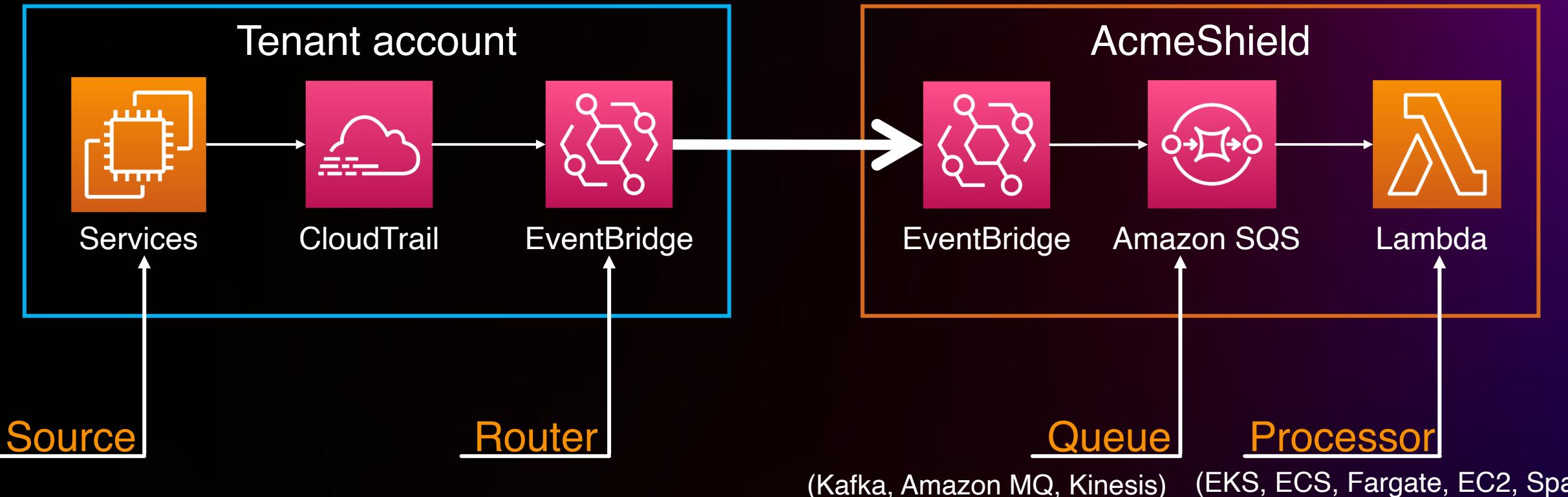
Best Practices



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

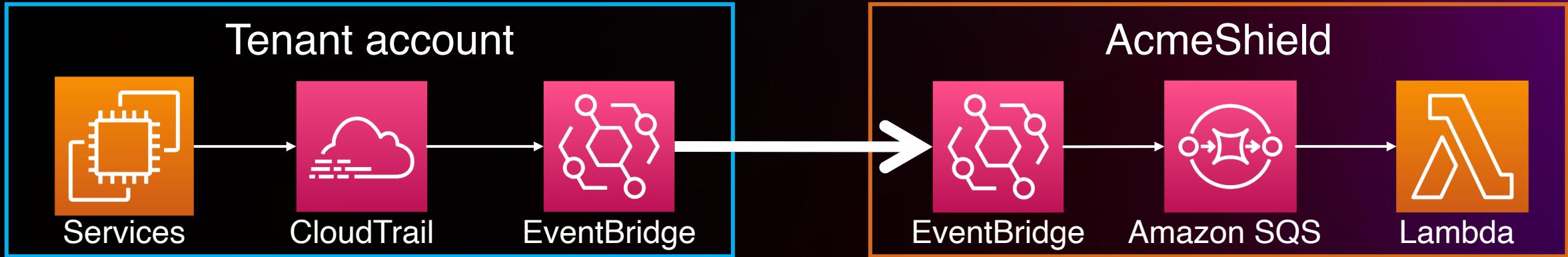
Buffer events before processing

**Normalize ingestion, reduce spikes and unpredictability
by queueing / buffering events before processing**



Not all events are equal

Differentiate between different event types



Control plane (mutating/non-mutating)

Resource **created**
Resource **updated**
Resource **deleted**

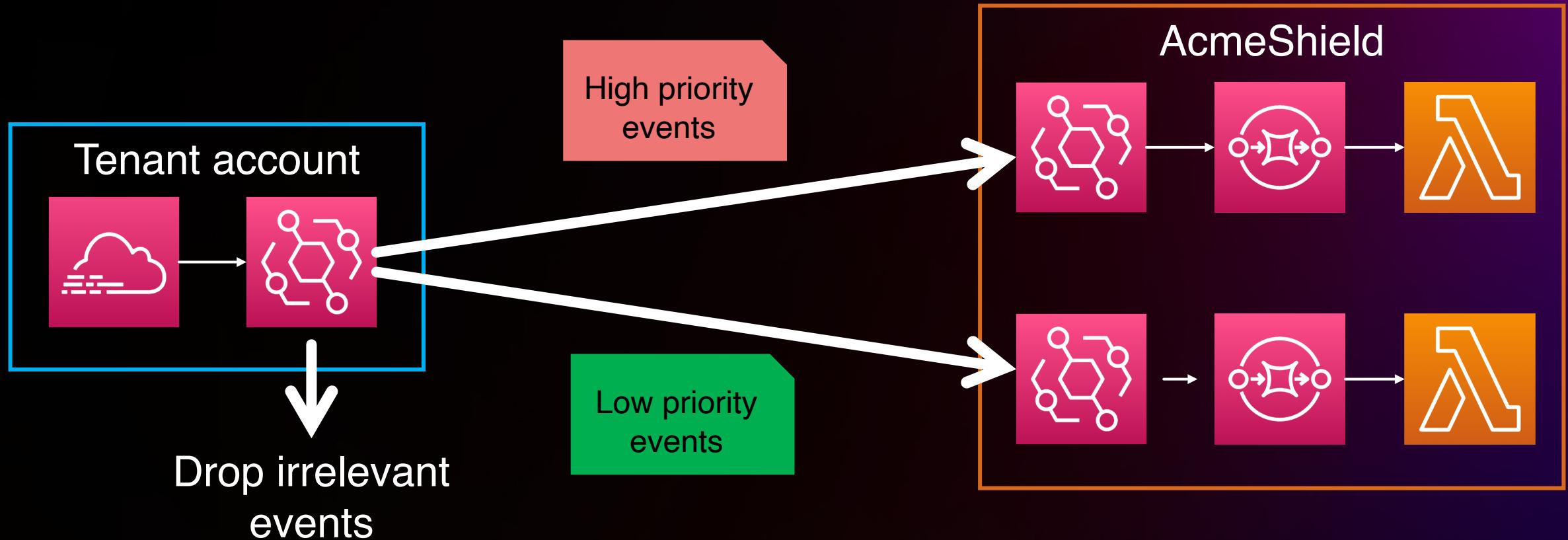
Resource **listed**
Resource **retrieved**
Resource **described**

Data plane

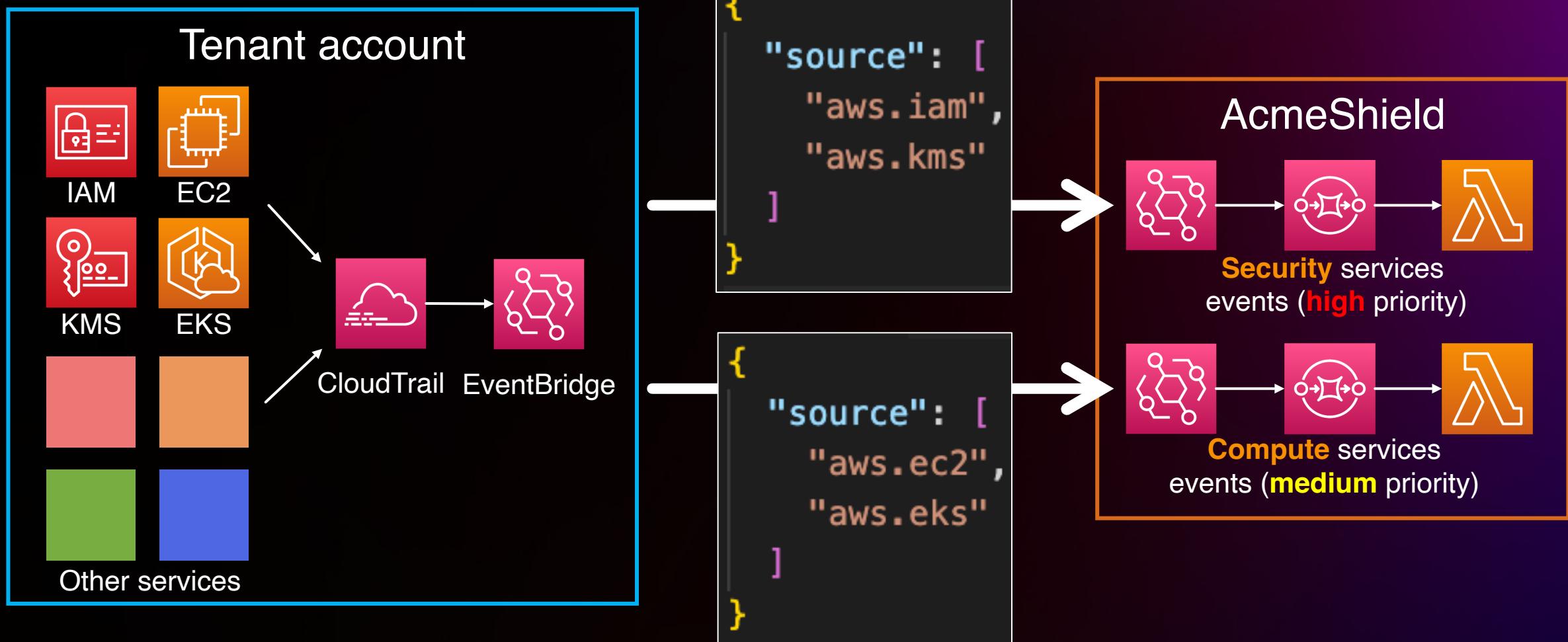
Lambda **invoke**
SNS **publish**
DynamoDB **putItem**

Use built-in routing and filtering capabilities

Add rules to intelligently route and filter events, as well as save costs

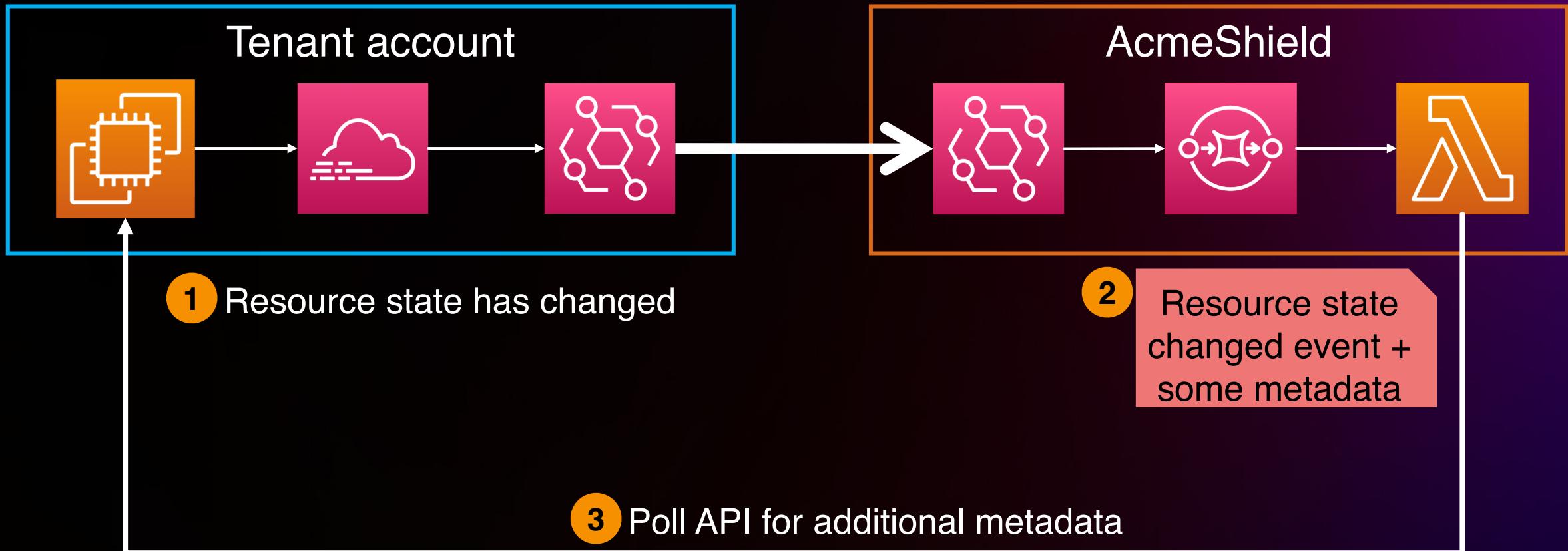


Use built-in routing and filtering capabilities



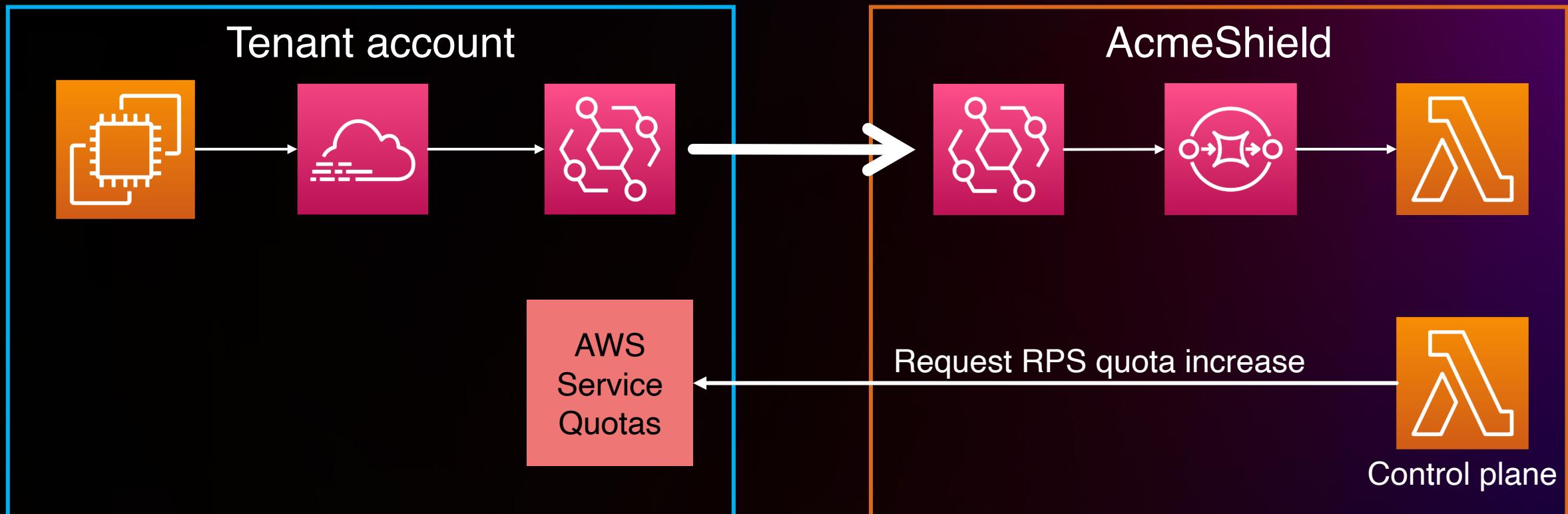
Sometimes polling is still OK

**Intelligently poll for additional metadata
when resource state has changed**



Help tenants with quotas increases

Use the Service Quotas API to request quota increases in tenant accounts

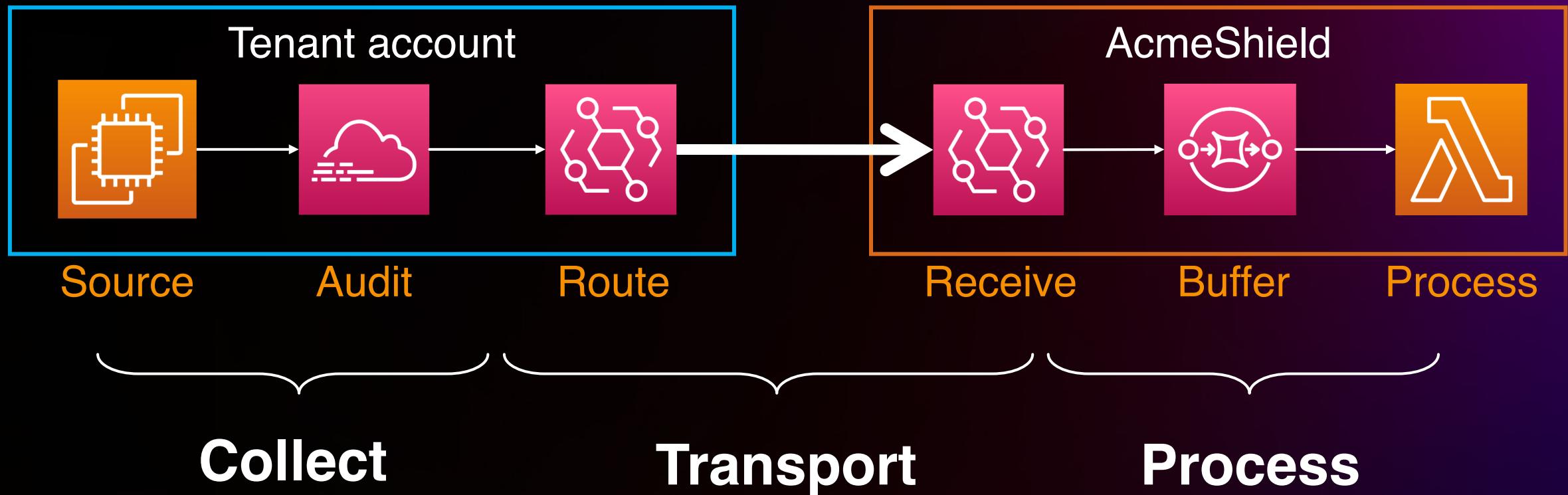


Bringing everything together



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bringing everything together



Completing the cycle with SaaS Partner Integrations

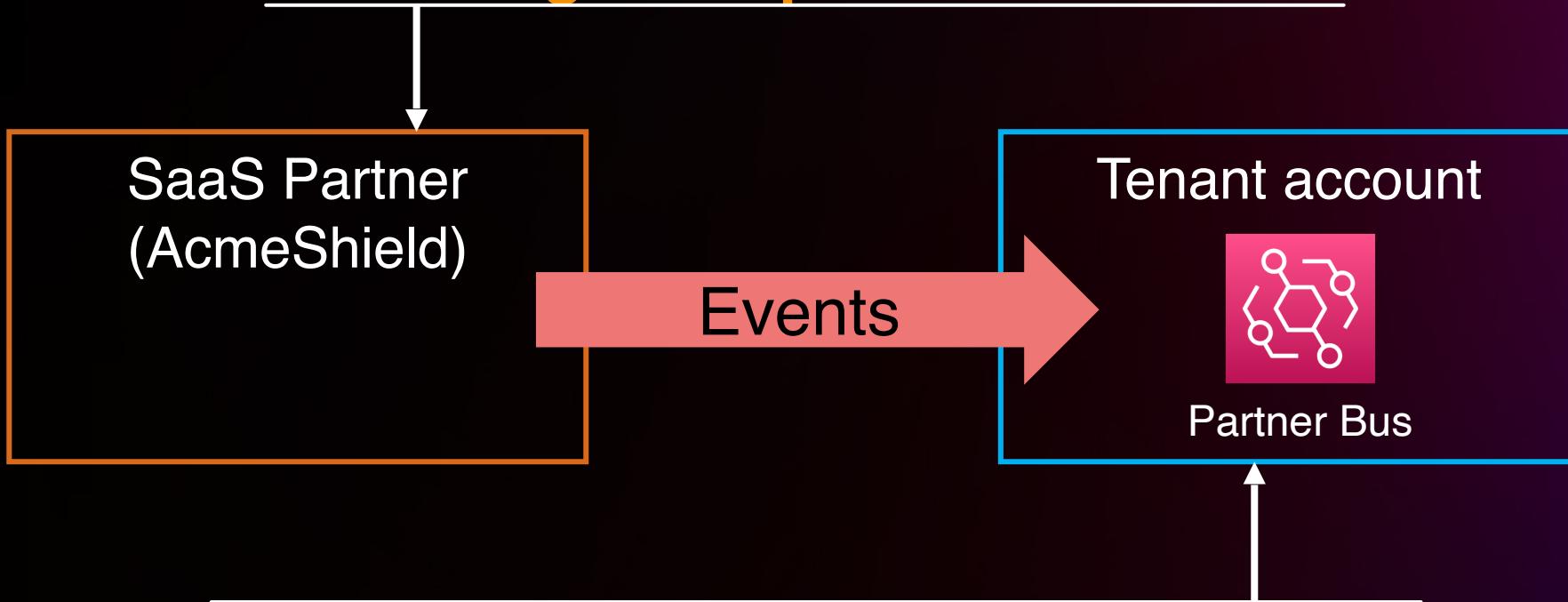


SaaS Partner Event Sources



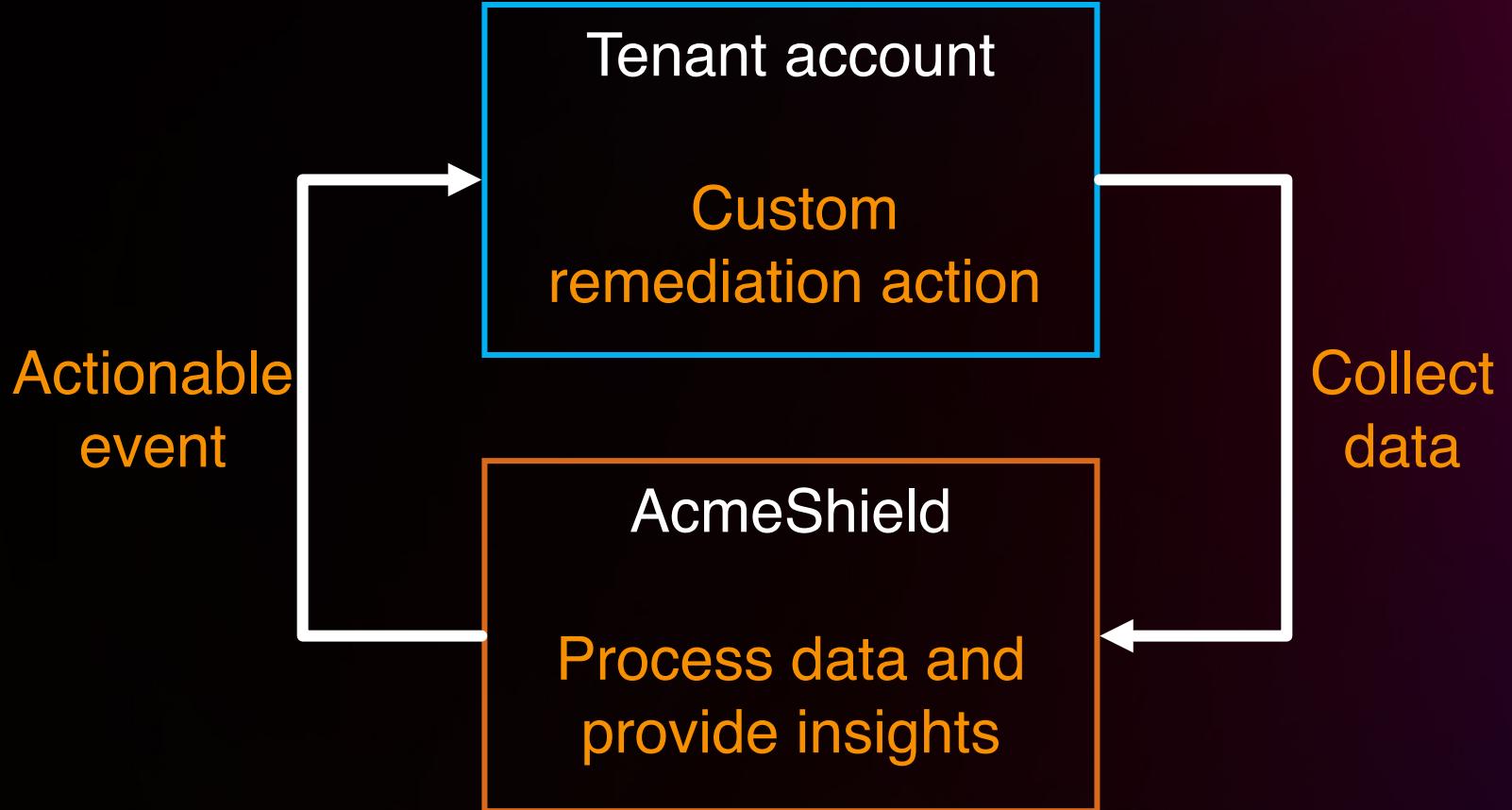
SaaS Partner Event Sources

SaaS partners can publish events to a designated partner event bus

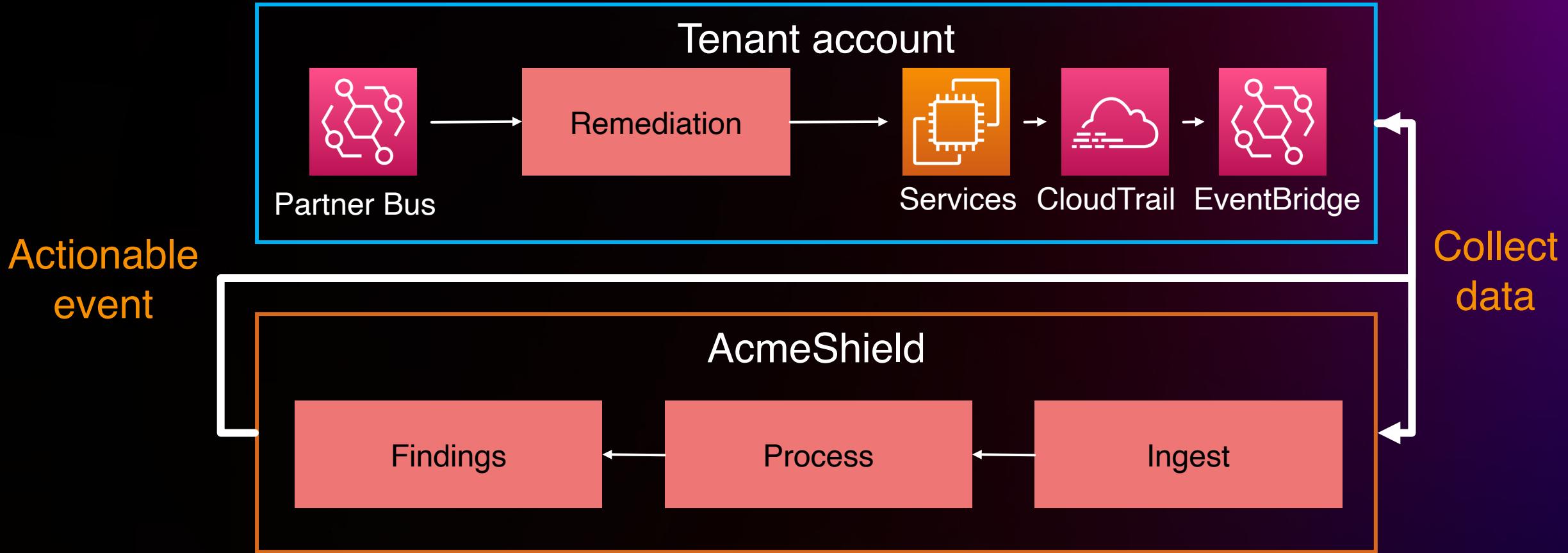


Tenants can subscribe to those events and trigger event-based automations

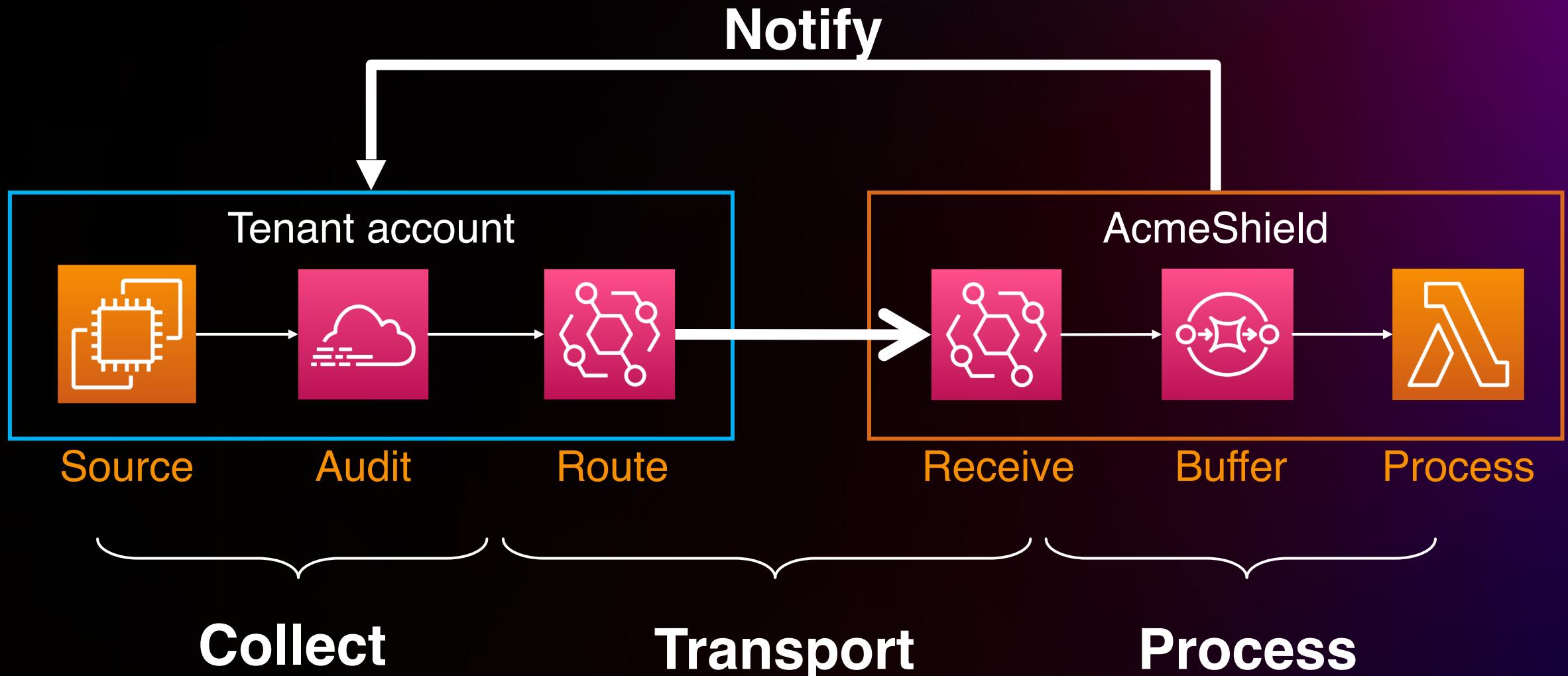
SaaS Partner Event Sources



SaaS Partner Event Sources



Bringing everything together

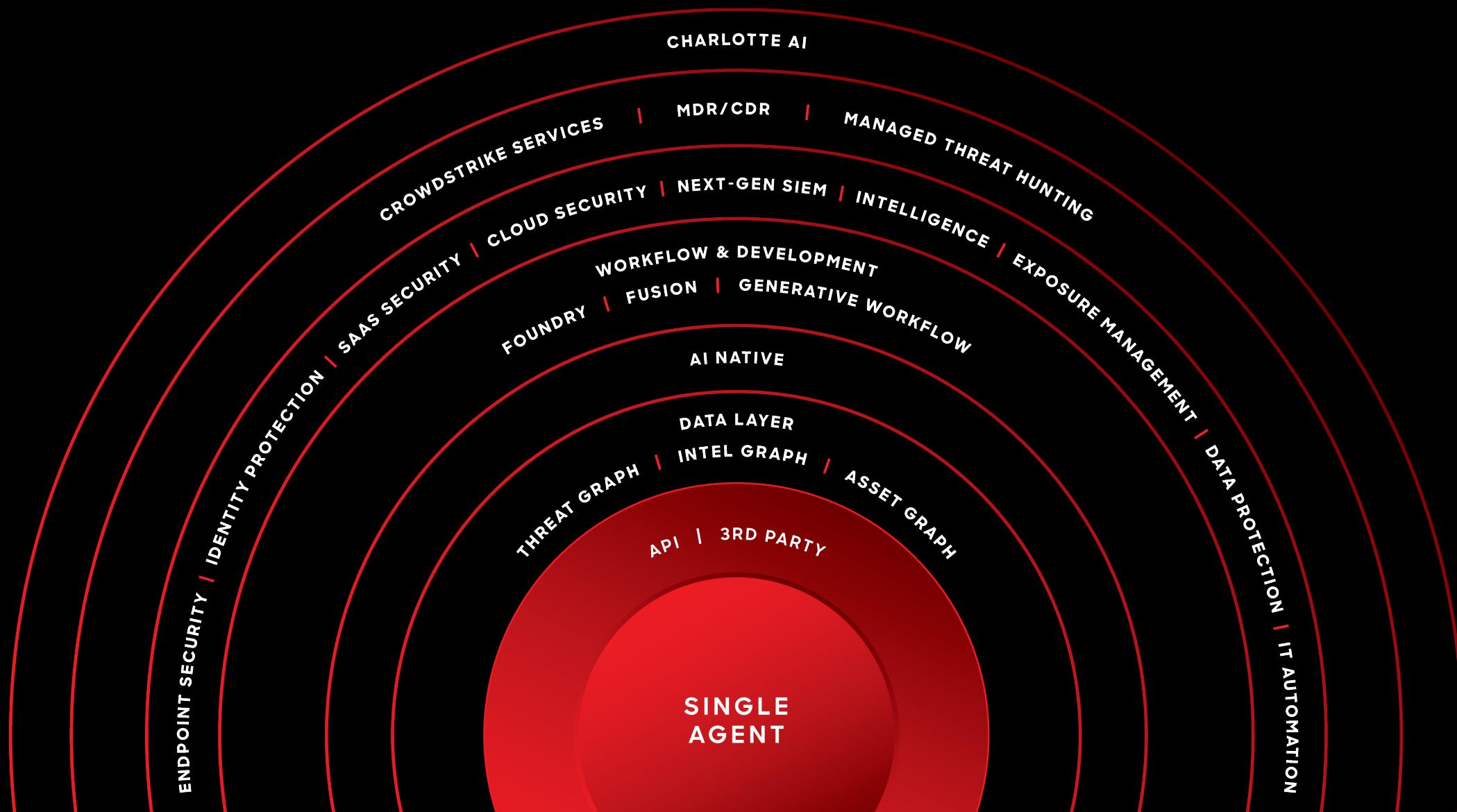


CrowdStrike's story



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CROWDSTRIKE'S AI-NATIVE PLATFORM STOPS BREACHES





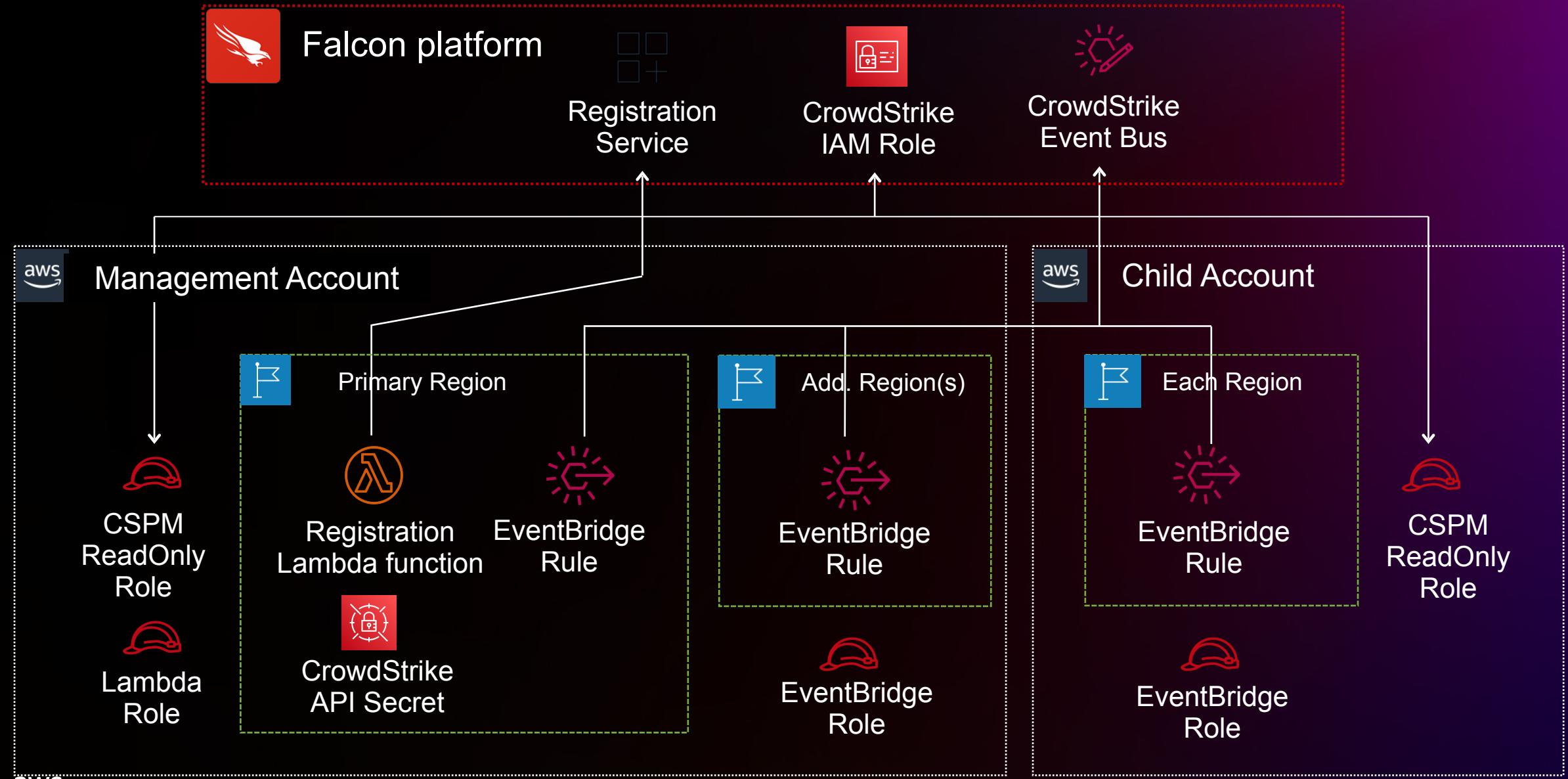
Detect Adversary Behavior in Milliseconds with CrowdStrike and Amazon EventBridge

CrowdStrike maximizes the advantages of event-driven architecture by integrating with EventBridge. CrowdStrike Falcon Horizon IOA, powered by EventBridge, **observes end-to-end cloud activities at high speeds at scale**. Paired with targeted detection algorithms from in-house threat detection experts and threat intelligence data, Falcon Horizon IOA **combats emerging threats against the cloud control plane with its cutting-edge event-driven architecture**.

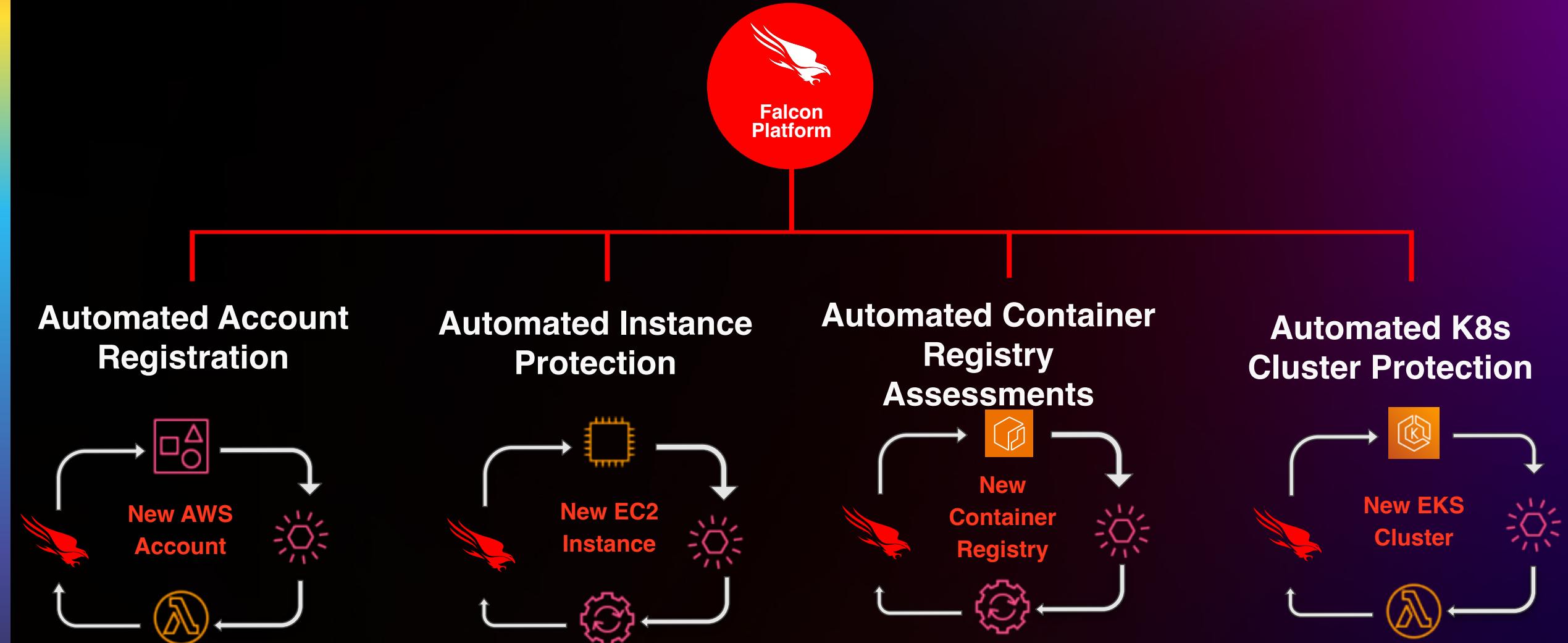
<https://aws.amazon.com/blogs/compute/enhancing-multi-account-activity-monitoring-with-event-driven-architectures/>
<https://aws.amazon.com/blogs/architecture/detect-adversary-behavior-in-seconds-with-crowdstrike-and-amazon-eventbridge/>



CrowdStrike Falcon Cloud Security - EventBridge architecture



Event-driven deployment automation



Conclusion



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Conclusion

1

Event-driven activity monitoring scales efficiently across large AWS footprints

2

Implement comprehensive security and operational insights via real-time alerts

3

Make informed choices and balance trade-offs when architecting your solutions



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



Anton Aleksandrov

antonal80

aal80.github.io/whoami



Joe Alioto

josephalioto



Rob Solomon

solorob33

