

# Introducing Amazon Detective

Luis Maldonado, Sr. Manager, Product Management, AWS

Gagan Prakash, Sr. Product Manager, AWS

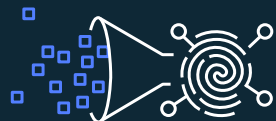
January 29<sup>th</sup> 2020



# Agenda

- Introduction
- How it works
- Demo
- Service details

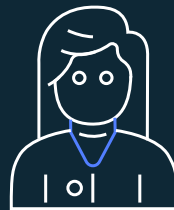
# Investigation challenges



Signal to  
noise ratio



Complexity



Skills shortage



Costs

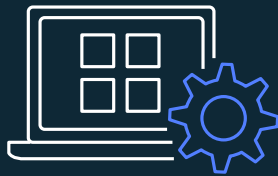
# Amazon Detective

Preview

Quickly analyze, investigate, and identify the root cause of security issues



Built-in data collection



Automated analysis



Visual insights



# Amazon Detective example use cases

A large green circle containing the text "Alert triage".

Alert  
triage

A large orange circle containing the text "Incident investigation".

Incident  
investigation

A large blue circle containing the text "Threat hunting".

Threat  
hunting



# Amazon Detective example use cases



Finding investigation

How much data was sent?

Is this traffic normal?

What happened just before?

Are these call failures common?



# Amazon Detective example use cases



Incident scoping

What API calls were made from that IP?

Do the calls indicate reconnaissance?

What other principal IDs were used?

What other instances communicated with that IP?



# Amazon Detective example use cases



## Indicator search

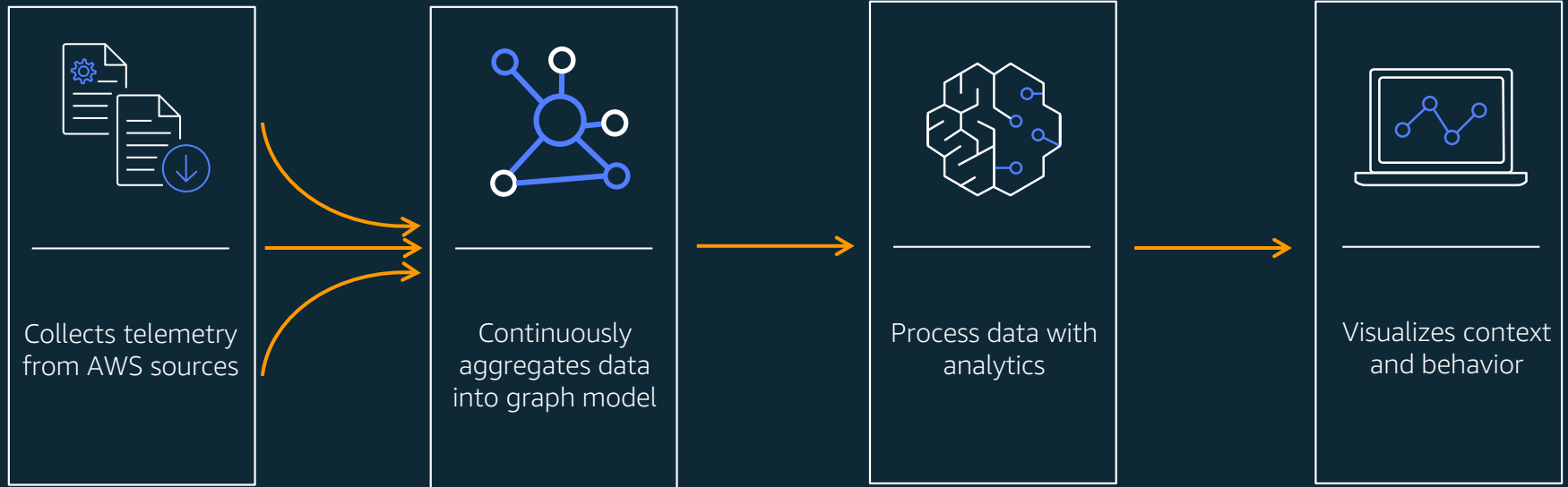
Did this IP address from our threat report communicate with any of EC2 instances over the last year?

Did this suspicious user agent issue any API calls?

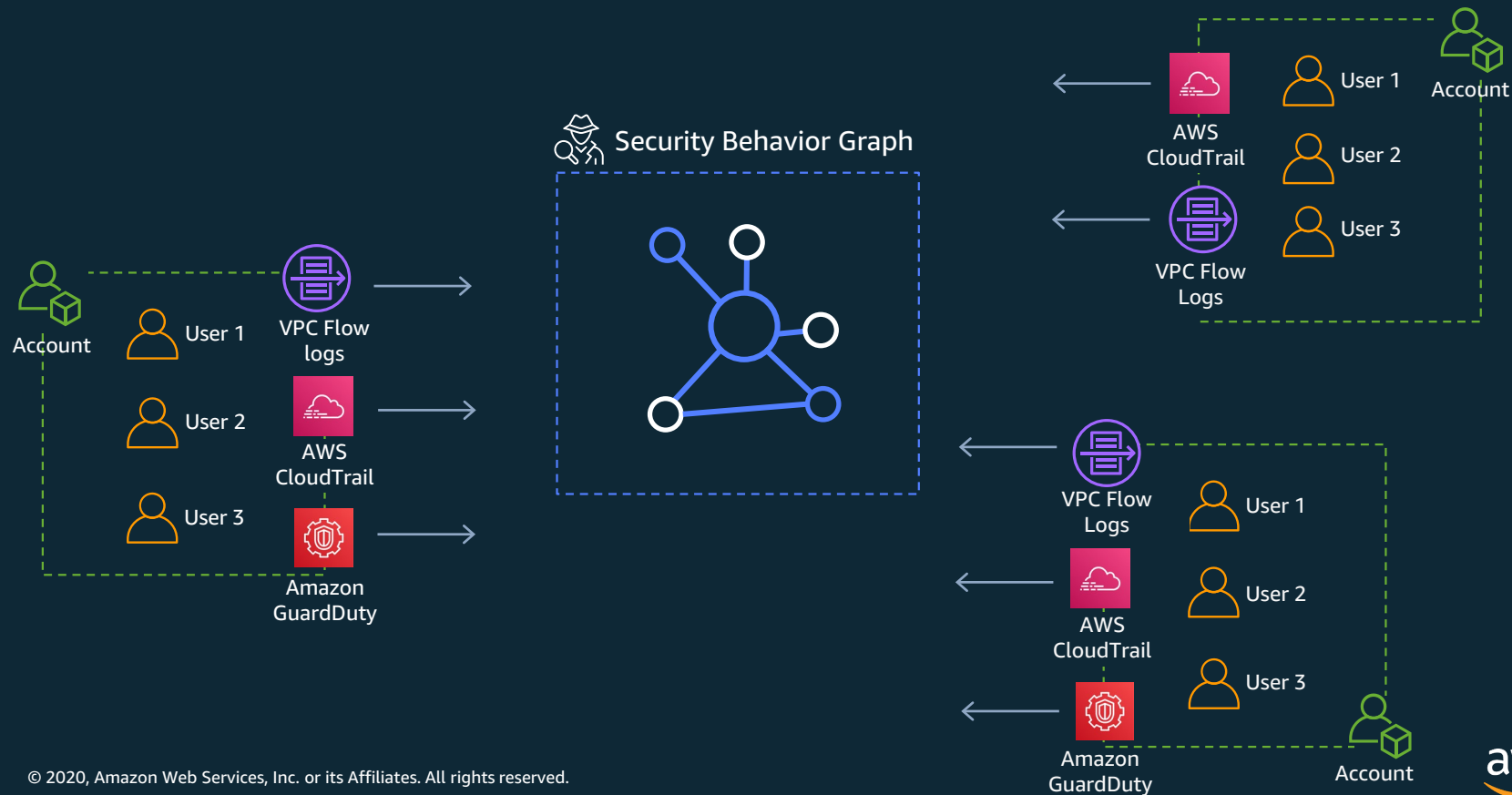


# How it works

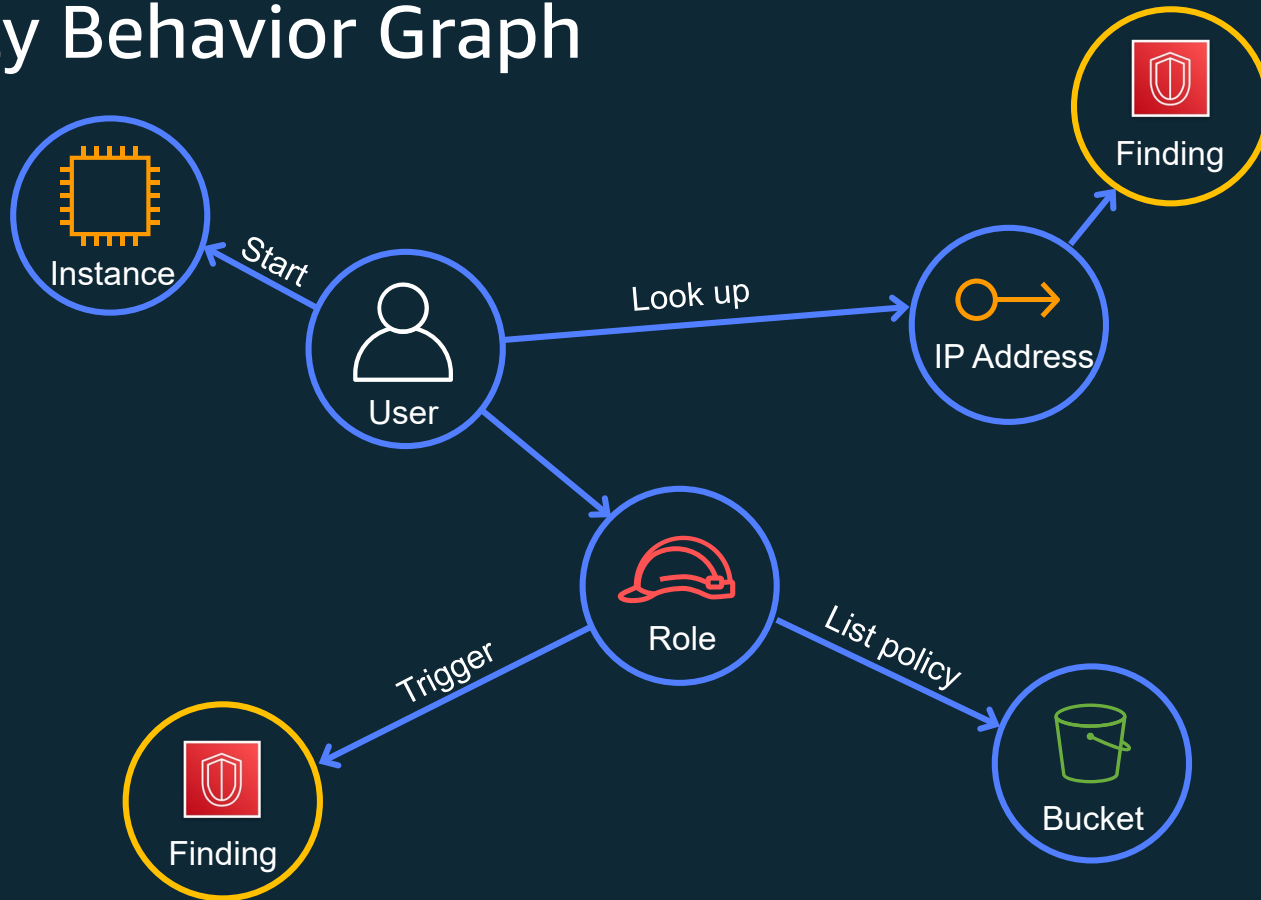
# Amazon Detective processing flow



# Multi-account telemetry collection

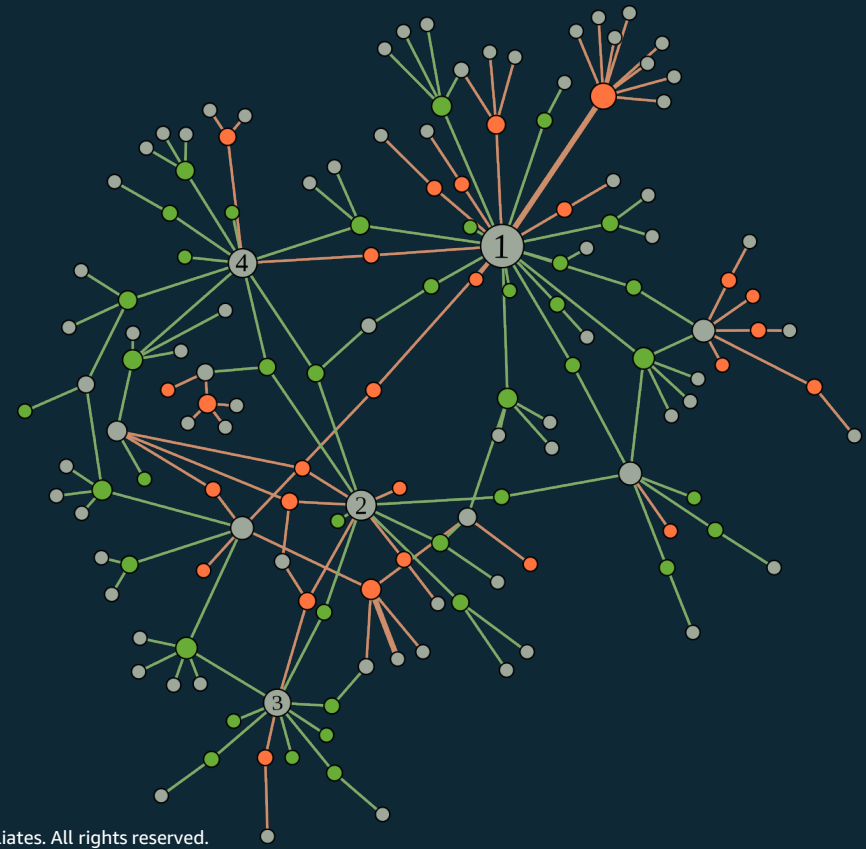


# Security Behavior Graph





# Can you see the traffic flow between the IP and the instance?



# How about now?

## Observed EC2 instances using this IP address [Info](#)

Lorem ipsum dolor amet intelligentsia subway tile single-origin coffee tote bag. Gluten-free enamel pin ennui migas blog williamsburg street art humblebrag iceland mixtape roof party freegan before they sold out.

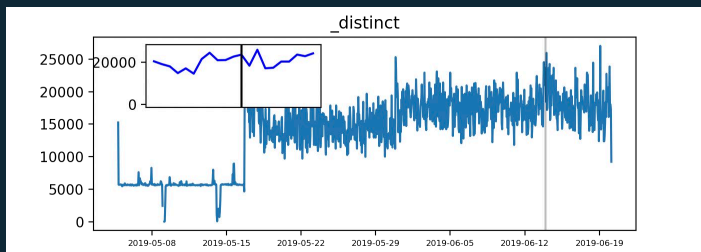
EC2 instance	First time observed	Last time observed
▶ <a href="#">i-1234a5b678c901d23</a>	11/10/18, 23:00	11/13/19, 14:00
▼ <a href="#">i-4567d8e901f234g56</a>	10/28/19, 15:00	11/12/19, 16:00

**[Time series label]** Scope: 10/18 @21:00 - 10/19 @23:00

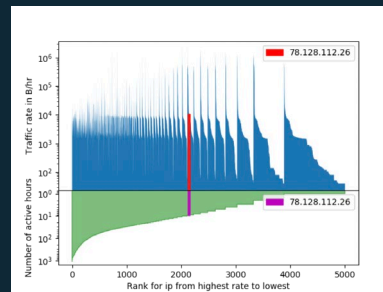
10/12 @21:00

▶ <a href="#">i-7890h1j234k567l89</a>	11/13/19, 13:00	11/13/19, 13:00
---------------------------------------	-----------------	-----------------

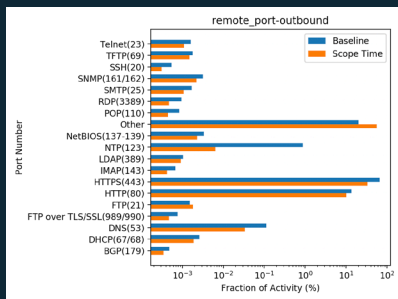
# Powered by data scientists



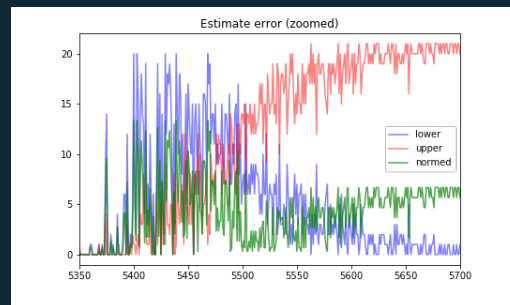
## Behavioral baselines



## Distributions

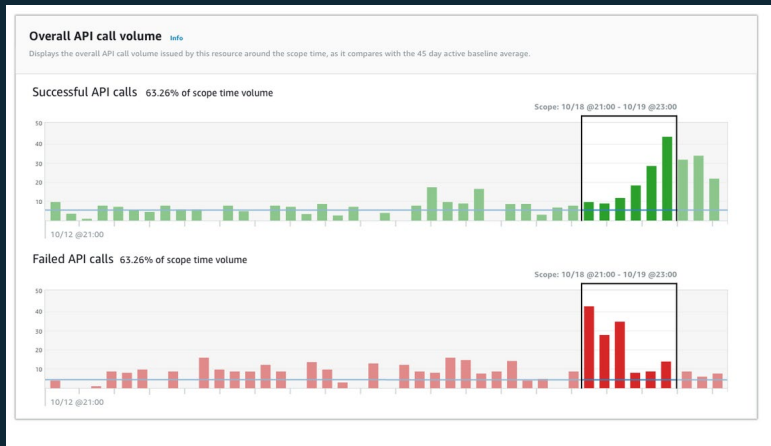


## Time series analysis



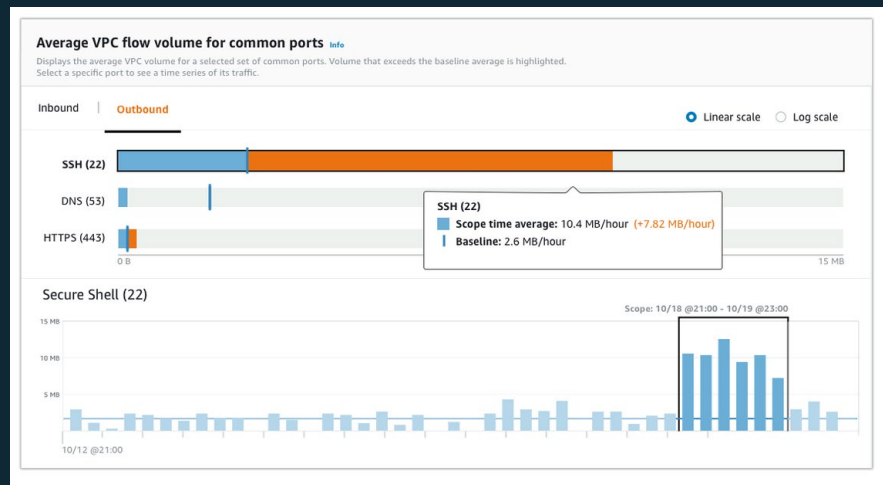
## Data stream analytics

# Visualized for security analysts



How much data was sent?

Is this traffic normal?



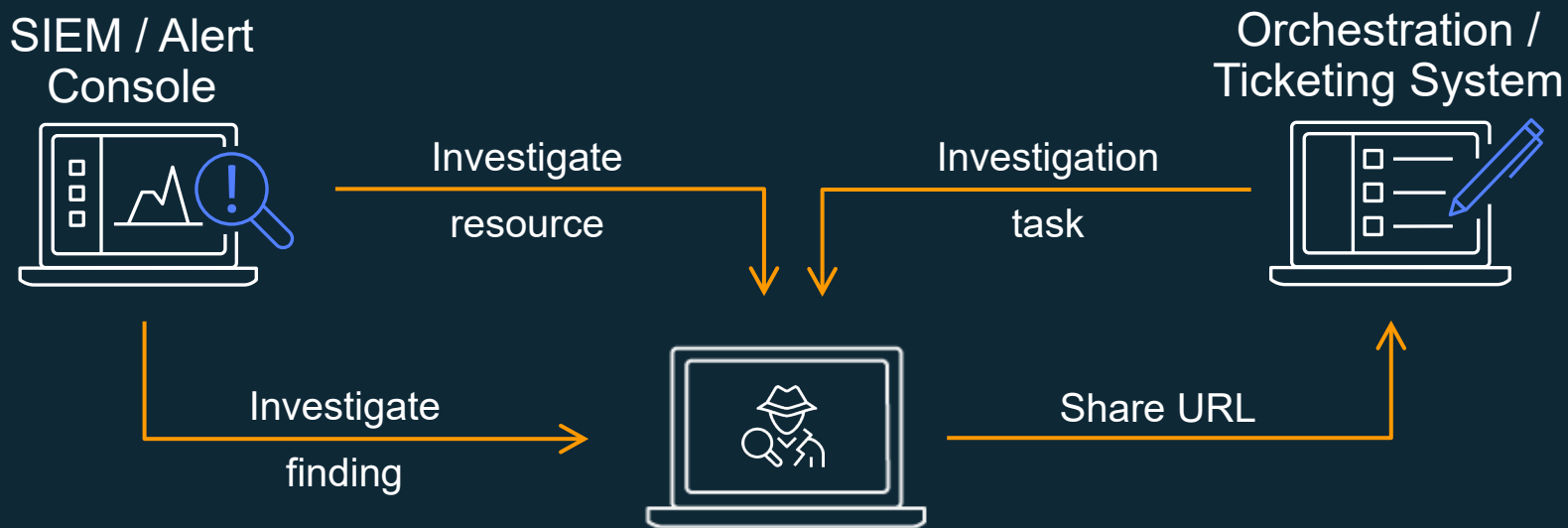
What happened just before?

Are these call failures common?



# Demo

# Amazon Detective workflow integration



# Amazon Detective integrations and managed services

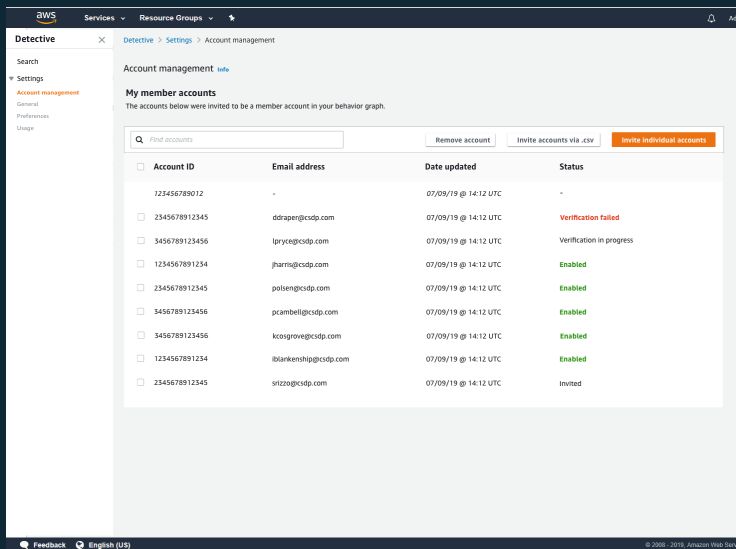
## Technology partners



## Services partners

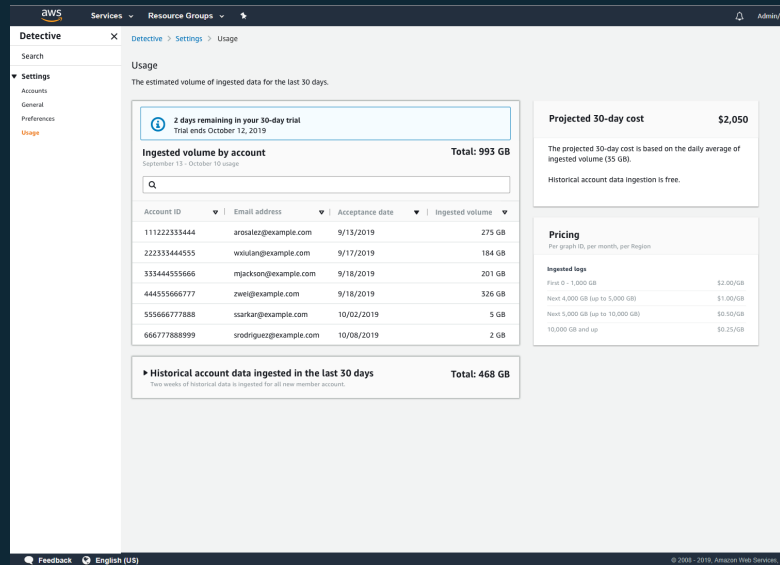


# Getting started



Simple multi-account management

## 30 day free trial and cost estimator



2 weeks of preloaded data

# US-East Pricing

			Price
First	1000	GB/month	\$2.00 / GB
Next	4000	GB/month	\$1.00 / GB
Next	5000	GB/month	\$0.50 / GB
Above	10000	GB/month	\$0.25 / GB

## What's included

- Data sources
  - Amazon Virtual Private Cloud (Amazon VPC) Flow Logs
  - CloudTrail management events
  - GuardDuty findings
- 1 year of Security Graph data

# Preview available in 5 regions



General Availability (GA) in all commercial regions Q1 2020



# Learn more and sign up

[aws.amazon.com/detective](https://aws.amazon.com/detective)

# Q&A