Under the Radar: Securing Multi-Cloud Deployments

Korinne Alpers
Offering Manager, QRadar Cloud Security

IBM **Security**

IBM

Today’s session: What’s in scope

- High-level overview of what’s out there today for getting your logging from your cloud environments to QRadar. Today we’ll be looking at AWS, Azure, and GCP.
- Cloud security use cases, and content extensions that cover them.
- High-level deployment options to show QRadar’s flexibility in terms of meeting you where you are.
- Resources to learn more information and dive into these integrations and deployment options.

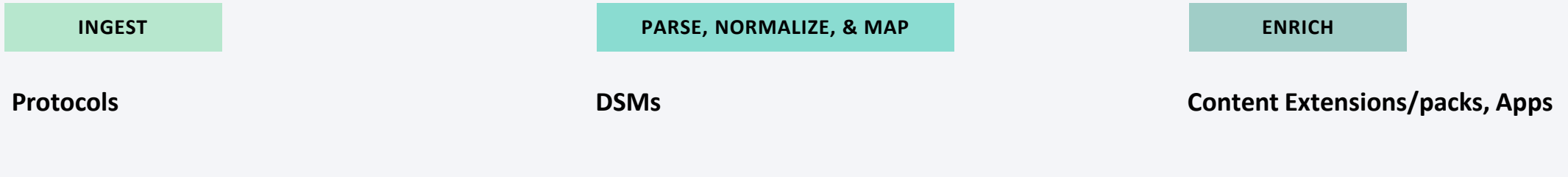
QRadar Integrations – Definitions to keep in mind

Event
An Event is a message QRadar receives and processes from a device on your network, that represents the log of some particular action on that device.

Protocol
A QRadar Protocol is the framework for getting event data off the wire.

Device Support Module (DSM)
A DSM is the way QRadar is able to parse events and categorize the data properly in the user interface.

Content Extensions
Content extensions are created by IBM and other vendors to enhance or (extend) QRadar capabilities. An extensions can contain apps, content items (such as customer rules), report templates, saved searches, or contain updates to existing content. Content extensions can be downloaded from the **IBM Security App Exchange**.



AWS integrations

AWS Logs

AWS CloudTrail Logs

Description

CloudTrail logs tell you about all user activity in your AWS account. CloudTrail makes sure that every API call made to an AWS resource in your account is recorded and written to a log.

Examples

- Starting or stopping EC2 instances
- Changes to a policy, or Security Group
- Deletions of an S3 bucket

AWS CloudWatch Logs

Description

CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS.

Examples

- Setting an alarm for monitoring root user account usage
- Understanding damage to the system after an incident

Amazon VPC Flow Logs

Description

Amazon VPC Flow Logs allow you to capture information about the network traffic moving to and from network interfaces within your VPC.

Examples

- Remote logins (such as SSH)
- Port scanning
- Data exfiltration

QRadar Integrations with AWS – Resource Roundup

All integrations

AWS CloudTrail – QRadar Integrations

- Amazon AWS S3 REST API protocol, Amazon Web Services protocol
- Amazon AWS CloudTrail DSM
- QRadar Content Extension for Amazon AWS e

Amazon VPC Flow Logs – QRadar Integrations

- Amazon AWS S3 REST API protocol
- Amazon AWS VPC Flow Logs DSM
- QRadar Content Extension for Amazon AWS

Amazon GuardDuty – QRadar Integrations

- Amazon Web Services protocol
- Amazon GuardDuty DSM
- QRadar Content Extension for Amazon AWS

AWS Security Hub– QRadar Integrations

- Amazon Web Services Protocol
- Amazon AWS Security Hub DSM
- QRadar Content Extension for Amazon AWS

Cloud Apps for AWS:

- QRadar Cloud Visibility App

AWS CloudTrail – QRadar Integrations

About

QRadar can ingest data from AWS CloudTrail using both the Amazon AWS S3 REST API protocol and/or the Amazon Web Services protocol. The first protocol is for getting data out of Amazon S3 buckets, while the second collects AWS CloudTrail logs from Amazon CloudWatch logs.
The Amazon AWS CloudTrail DSM parses and normalizes the event logs.

How QRadar integrates with AWS CloudTrail

- Amazon AWS S3 REST API protocol, Amazon Web Services protocol
- Amazon AWS CloudTrail DSM
- QRadar Content Extension for Amazon AWS

INGEST

Amazon AWS S3 REST API protocol, Amazon Web Services protocol

Recorded events
• AWS CloudTrail JSON logs

PARSE, NORMALIZE, & MAP

Amazon AWS CloudTrail DSM

Parsed events
• AWS CloudTrail logs stored in S3 buckets • AWS CloudTrail logs stored in a Log group in CloudWatch logs

ENRICH

AWS Content Extension

What it does
The QRadar content extension for AWS adds rules, reports, and saved searches to build on the existing QRadar event parsing capabilities for AWS deployments. For CloudTrail specifically, this content extension provides rules for use cases such as deleting, disabling, or changing CloudTrail logs.

Amazon VPC Flow Logs – QRadar Integrations

About

QRadar collects Amazon VPC Flow Logs via the Amazon AWS S3 REST API protocol. The Amazon VPC Flow Logs DSM parses and normalizes the flow logs.

How QRadar integrates with AWS VPC Flow Logs:

- Amazon AWS S3 REST API protocol
- Amazon AWS VPC Flow Logs DSM
- QRadar Content Extension for Amazon AWS

INGEST

Amazon AWS S3 REST API protocol

Recorded events
• Amazon VPC Flow Logs

PARSE, NORMALIZE, & MAP

Amazon VPC Flow Logs DSM

Parsed events
• Amazon VPC Flow Logs

ENRICH

AWS Content Extension

What it does
The QRadar content extension for AWS adds rules, reports, and saved searches to build on the existing QRadar event parsing capabilities for AWS deployments.

Amazon GuardDuty – QRadar Integrations

About

QRadar's integration with Amazon GuardDuty involves the Amazon Web Services protocol for collection, and the Amazon Guard Duty DSM for parsing/normalization.

How QRadar integrates with Amazon GuardDuty:

- Amazon Web Services protocol
- Amazon GuardDuty DSM
- QRadar Content Extension for Amazon AWS

INGEST

Amazon Web Services protocol

Recorded events
• Amazon GuardDuty findings from the log group of AWS CloudWatch logs.

PARSE, NORMALIZE, & MAP

Amazon GuardDuty DSM

Parsed events
• Amazon GuardDuty findings.

ENRICH

AWS Content Extension

What it does
The QRadar content extension for AWS adds rules, reports, and saved searches to build on the existing QRadar event parsing capabilities for AWS deployments. For CloudTrail specifically, this content extension provides rules for use cases such as deleting, disabling, or changing CloudTrail logs.

AWS Security Hub – QRadar Integrations

About

QRadar's integration with AWS Security hub can work two ways: pulling from Security Hub, and pushing to AWS Security Hub. With QRadar's AWS protocol and Security Hub DSM, QRadar can pull in events from Security Hub to QRadar, and build rules to create offenses.
With the Cloud Visibility App, users can push all findings related to AWS resources from QRadar to AWS Security Hub. In this way, Security Hub can act as a central repository

How QRadar integrates with AWS Security Hub:

- Amazon Web Services Protocol
- Amazon AWS Security Hub DSM
- QRadar Content Extension for Amazon AWS

INGEST

Amazon Web Services Protocol

Recorded events
• AWS CloudWatch logs • Amazon Kinesis Data Streams **Note:** You'll need to configure a log source on the QRadar Console for AWS to communicate with QRadar using this protocol. Specific parameters for this log source can be found **here.**

PARSE, NORMALIZE, & MAP

Amazon AWS Security Hub DSM

Parsed events
• Security Hub findings

ENRICH

AWS Content Extension

What it does
The QRadar content extension for AWS adds rules, reports, and saved searches to build on the existing QRadar event parsing capabilities for AWS deployments. For CloudTrail specifically, this content extension provides rules for use cases such as deleting, disabling, or changing CloudTrail logs.

QRadar Cloud Visibility App

About

QRadar can detect potential problems in AWS environments and address security use cases, some of which are mentioned earlier in this presentation.

Where to get Cloud Visibility App

- [IBM Security App Exchange]

ENRICH

Cloud Visibility App - AWS Dashboard

What it does

The app includes the following enhanced AWS capabilities:

- Simplified log source management
- Identity and access management for accounts, users, and IAM roles
- Auto-population of QRadar Network Hierarchy
- Amazon VPC flow log visualization
- Integration with AWS Security Hub and Amazon Detective

Azure integrations

Azure Logs

Azure Activity Logs

Description

These are generated by the Azure control-pane, and essentially describe who did what in your Azure environment

Examples

- Creating a storage account
- Starting a VM
- Deleting a Key Vault

Azure Resource Logs (previously called Diagnostic logs)

Description

Generated by a resource after it's provisioned, and are not enabled by default.

Examples

- Getting a secret from a Key Vault

Azure Active Directory Logs

Description

Where user authentication takes place (Identity and access management).

Examples

- Audit log generated from removing a user
- Sign-in log to track who removed a user

QRadar Integrations with Azure – Resource Roundup

All integrations

Microsoft Azure Platform – QRadar Integrations

- Microsoft Azure Event Hubs Protocol
- Microsoft Azure Platform DSM
- QRadar Content Extension for Azure

Microsoft Azure Active Directory – QRadar Integrations

- Microsoft Azure Event Hubs Protocol
- Microsoft Azure Active Directory DSM
- QRadar Content Extension for Azure

Microsoft Azure Security Center

- Microsoft Graph Security API Protocol
- Microsoft Azure Security Center DSM
- QRadar Content Extension for Azure

Cloud Apps for Microsoft Azure

- QRadar Cloud Visibility App

Microsoft Azure Platform – QRadar Integrations

About

QRadar's integration with Microsoft Azure Platform involves the Azure Event Hubs protocol for collection, and the Azure Platform DSM for parsing/normalization. It should be noted the DSM focuses on Azure Activity logs at the platform-level.

How QRadar integrates with Azure Platform:

- Microsoft Azure Event Hubs Protocol
- Microsoft Azure Platform DSM
- QRadar Content Extension for Azure

INGEST

Azure Event Hubs Protocol

Recorded events
• Azure Activity logs • Linux logs • Syslog

PARSE, NORMALIZE, & MAP

Azure Platform DSM

Parsed events
• Platform level activity logs **ELI5:** This DSM collects high-level information about actions in an Azure environment. **Example:** The DSM would collect logs for creation/deletion of an NSG Flow, but not the NSG Flow logs themselves.

ENRICH

Azure Content Extension

What it does
The QRadar Azure content extensions adds rules, reports, and saved searches to build on the existing QRadar event parsing capabilities for Azure deployments. This content extension is specifically aimed at network security management, Security Rules modification, and Virtual Network management.

Microsoft Azure Active Directory – QRadar Integrations

About

QRadar's integration with Microsoft Azure Active Directory offers the ability to monitor identity, access management and security events from external resources such as Microsoft Office 365 and Microsoft Azure.

How QRadar integrates with Azure Active Directory

- Microsoft Azure Event Hubs Protocol
- Microsoft Azure Active Directory DSM
- QRadar Content Extension for Azure

INGEST

Azure Event Hubs Protocol

Recorded events
• Azure Activity logs • Diagnostic logs • Linux logs • Syslog

PARSE, NORMALIZE, & MAP

Azure Active Directory DSM

Parsed events
• Audit logs • Sign-in logs

ENRICH

Azure Content Extension

What it does
The QRadar Azure content extensions adds rules, reports, and saved searches to build on the existing QRadar event parsing capabilities for Azure deployments. This content extension is specifically aimed at network security management, Security Rules modification, and Virtual Network management.

Microsoft Azure Security Center – QRadar Integrations

About

QRadar's integration with Microsoft Azure Security Center involves the Graph Security API Protocol for ingestion, and the Microsoft Azure Security Center DSM for parsing. This allows you to receive the alerts for high security use cases, such as logons from malicious IP's, when someone uses an encoded executable from the command line, and more. It should be noted you are receiving the alerts, not the contents of the logs themselves.

How QRadar integrates with Azure Active Directory

- Microsoft Graph Security API Protocol
- Microsoft Azure Security Center DSM
- QRadar Content Extension for Azure

INGEST

Graph Security API Protocol

Recorded events
• Graph Security API alerts **ELI5:** This protocol only handles Graph Security API alerts, and doesn't ingest underlying events from Microsoft's end contributing to the alerts.

PARSE, NORMALIZE, & MAP

Microsoft Azure Security Center DSM

Parsed events
• Security alerts See Security Alerts reference here.

ENRICH

Azure Content Extension

What it does
The QRadar Azure content extensions adds rules, reports, and saved searches to build on the existing QRadar event parsing capabilities for Azure deployments. This content extension is specifically aimed at network security management, Security Rules modification, and Virtual Network management.

QRadar Cloud Visibility App

About

QRadar can detect potential problems in Azure environments and address security use cases, some of which are mentioned earlier in this presentation. Once offenses are created, Cloud Visibility app then helps users manage these offenses in the Azure Offense Overview dashboard

Where to get Cloud Visibility App

- IBM Security App Exchange

ENRICH

Cloud Visibility App - Azure Offense Overview Dashboard

What it does

The Azure Offense Overview dashboard displays active offense data in the following charts:

- All users by magnitude
- All users by related rule
- Most severe offenses
- All users by number of offenses
- Magnitude level indicator

Google Cloud Platform integrations

GCP Logs

Admin Activity Logs

Description

Contain log entries for API calls or other admin actions that modify the configuration or metadata of resources.

Examples

- Creating a VM
- Changing permissions

Data Access audit logs

Description

Contain API calls that read the configuration or metadata of resources, along with user-driven API calls that create, modify, or read user-provided resource data

Examples

- Listing buckets or nodes within a cluster
- Writing data to a bucket

System Event audit logs

Description

Contain log entries for Google Cloud admin actions that modify the configuration of resources. These audit logs are generated by Google Cloud service, and not driven by direct user action.

Examples

- When Google Compute Engine live migrates an instance to another host

QRadar Integrations with GCP – Resource Roundup

All integrations

Google Cloud Audit Logs – QRadar Integrations

- Google Cloud Pub/Sub protocol
- Google Cloud Audit Logs DSM

Google G Suite Activity Reports – QRadar Integrations

- Google G Suite Activity Reports REST API protocol
- Google G Suite Activity Reports DSM

Google Cloud Audit Logs – QRadar Integrations

About

This integration uses the QRadar Google Cloud Pub/Sub protocol to ingest Google Cloud Audit logs. Then, the Google Cloud Audit Logs DSM is used to parse/normalize the data to be brought into the QRadar UI. The Google Cloud services that are supported with this DSM are:

- Google Compute Engine
- Google Cloud Identity and Access Management
- Identity Platform
- Cloud Storage

How QRadar integrates with Azure Platform:

- Google Cloud Pub/Sub protocol
- Google Cloud Audit Logs DSM

INGEST

PARSE, NORMALIZE, & MAP

Google Cloud Pub/Sub protocol

Recorded events
• Google Cloud Platform logs

Google Cloud Audit Logs DSM

Parsed events
• Google Cloud Audit logs

Google G Suite Activity Reports – QRadar Integrations

About

This integrations uses the Google G Suite Activity Reports REST API and DSM to collect and normalize the following event types: Login, User, Account, Google Drive, and Admin that are generated in Google G Suite.

How QRadar integrates with Azure Platform:

- Google G Suite Activity Reports REST API protocol
- Google G Suite Activity Reports DSM

INGEST

Google G Suite Activity Reports REST API

Recorded events
• Login • User • Account • Google Drive • Admin

PARSE, NORMALIZE, & MAP

Google G Suite Activity Reports DSM

Parsed events
• Login • User • Account • Google Drive • Admin

Cloud Security Use Cases

Generic API security use cases

Use cases:

- Successful API Request from different geographies using the same access user
- Successful API Request from unusual countries
- Successful API Request from malicious IP
- Successful API Request from user agents (eg: kali)
- Successful API Request from anon
- Sensitive or Privileged API calls, and to baseline which users can call which APIs
- Multiple forbidden API requests initiated from the same user
- Leaked API token (eg: leaked EC2 instance token)
- to detect password spraying (its like the most common authentication attack)
- Multiple Failed API Requests From Same Source IP / User

Content packs

- **QRadar Content Extension for Amazon AWS**
- **QRadar Content Extension for Azure**

Online File Storage and Sharing services: (AWS, O365, Box, ...)

Use cases:

- File download from a malicious IP
- Permissions for a sensitive file/directory changed to be a publicly available to everyone
- File download or upload from rare on an usual user agent
- File shared with an email hosted on a malicious domain
- File shared with an email hosted on a recently created domain
- File download or upload from rare on an usual user agent
- Confidential or Sensitive File Has Been Accessed or Downloaded From a Foreign Country/Region
- S3 Bucket will be changed to be publicly accessible
- Huge file downloads per IP and per user
- Huge file access per IP and per user
- Huge file deletion per IP and per user
- Unusual user accessing the cloud trail logs in S3

Content packs

- **IBM QRadar Data Exfiltration Content Extension**

Virtual Machine Service, eg: EC2

Use cases:

- Virtual machine communicating to a malicious IPs
- Virtual machine communicating to a crypto-mining IP
- Virtual machine Creating Unusual DNS Queries
- Creation of an unusual virtual machine - VM with large specs
- Creation of an unusual virtual machine - VM with Unusual Image
- Massive creation of virtual machines

Content packs

- QRadar Content Extension for Amazon AWS
- IBM QRadar Virtualized Environment Content Extension

Deployment options

Ways to extend QRadar deployments to the cloud

IBM streamlined deployments: Deployment flexibility aligned to how and where you want to deploy

IBM provides solutions with streamlined architecture for SaaS, on-prem, and cloud-specific deployments.

IBM QRadar on Cloud (QRoC)
Configured with customer specifications and deployed in a dedicated private cloud environment. Hosted by IBM within IBM Cloud datacenters.

IaaS
Extend deployments to public clouds with images for:

- AWS
- Azure
- Google Cloud Platform (GCP)

QRadar on Cloud

QRadar on Cloud (QRoC)

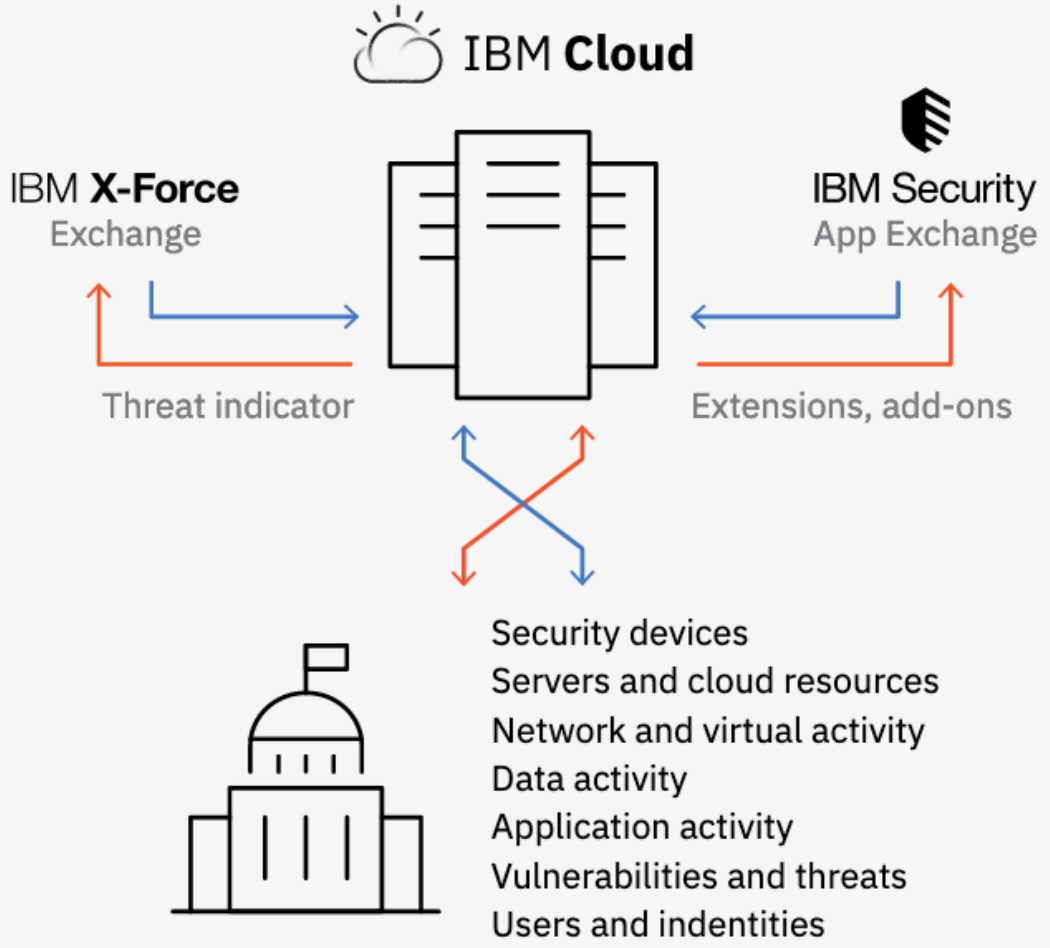
What it is

QRadar on Cloud delivers all the SIEM capabilities of the on-premise product with a single architecture that is hosted and managed in IBM Cloud.

Offering highlights

- Elastic upgrades; rapid time to value
- Dedicated DevOps
- 24x7 health monitoring
- System management: upgrades, patches
- Support for 450+ security and IT integrations
- Advanced threat detection
- Configurable security operations center (SOC) and management dashboards
- Global point-of-presence coverage
- Supports multitenant mode for service providers

IBM QRadar on Cloud deployment model



- Cloud-based offering of #1 Security Intelligence solution
- Collects data from both on-premises and cloud resources
- Leverages real-time threat intelligence from X-Force
- Includes access to value-added features from App Exchange

QRadar on Cloud: A global footprint

- Globally-distributed
- Resiliency and redundancy by default
- Built on security-rich IBM Cloud™ infrastructure

IaaS

IaaS

Public Cloud Marketplace images

With Bring Your Own Licensing (BYOL), customers can extend QRadar deployments to public clouds, as well as ingest log sources from clouds.

QRadar in AWS

- QRadar Console
- QRadar Managed Host
- QRadar App Host

QRadar in Azure

- QRadar Console
- QRadar Managed Host
- QRadar App Host

QRadar in Google Cloud Platform

- QRadar Console
- QRadar Managed Host
- QRadar App Host

Deploying QRadar in AWS

AMIs on the AWS Marketplace

Licensing: Bring Your Own License (BYOL)

Current Version: QRadar v7.3.2

- **QRadar Console.** Can act as an All-in-one appliance or a Console in a distributed deployment.
- **QRadar Managed Host .** Allows you to deploy a new QRadar managed host to extend QRadar systems and gain deeper visibility into Azure.
- **QRadar App Host.** Provides extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your QRadar Console.

Images & Appliances

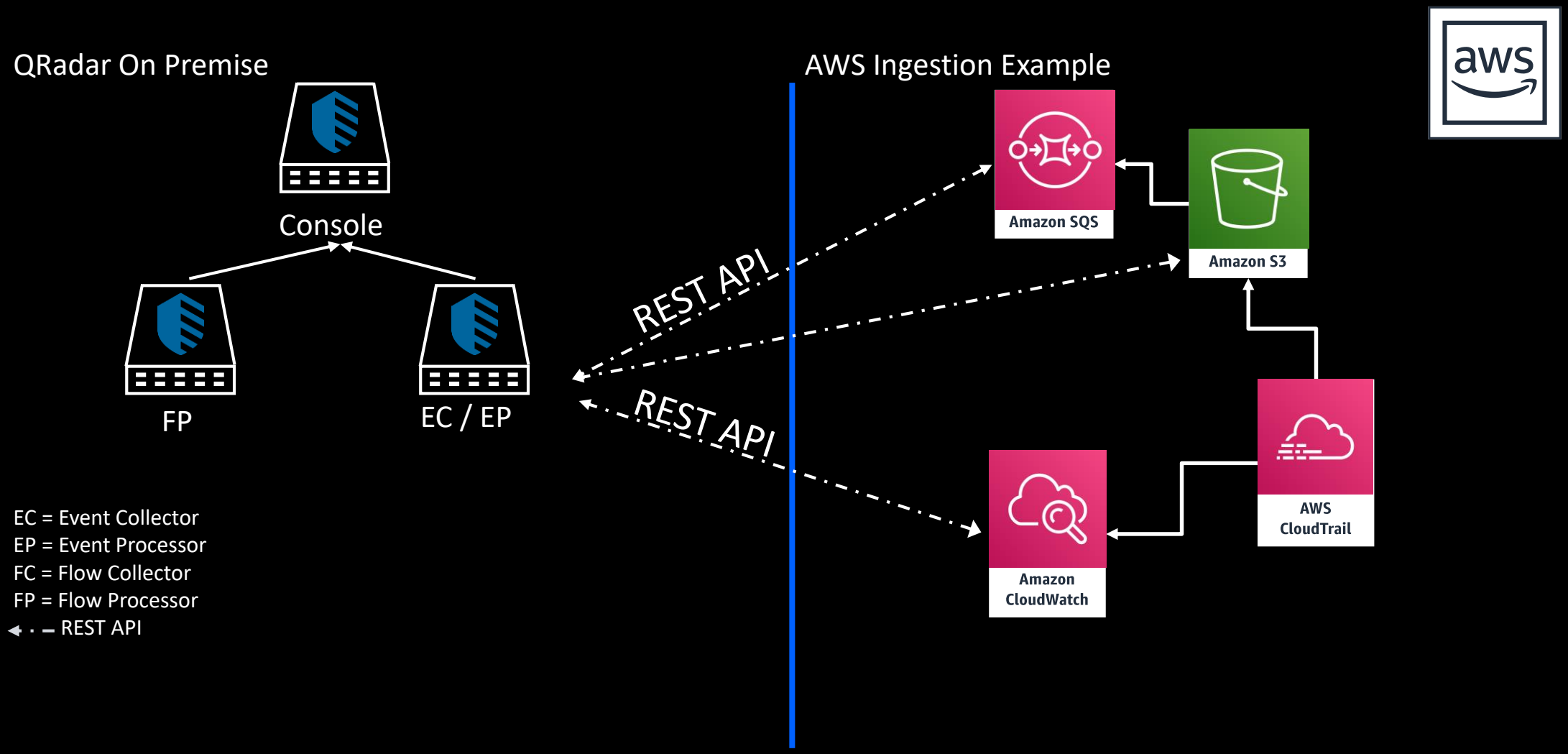
The QRadar AMIs can be configured into multiple QRadar appliances, and deployed in all major AWS regions.

Console
- Distributed deployment
- All-in-one

Managed Host
- Event Collector
- Event Processor
- Combination Processor
- Data Node
- Flow Collector
- Flow Processor
- Data Gateway

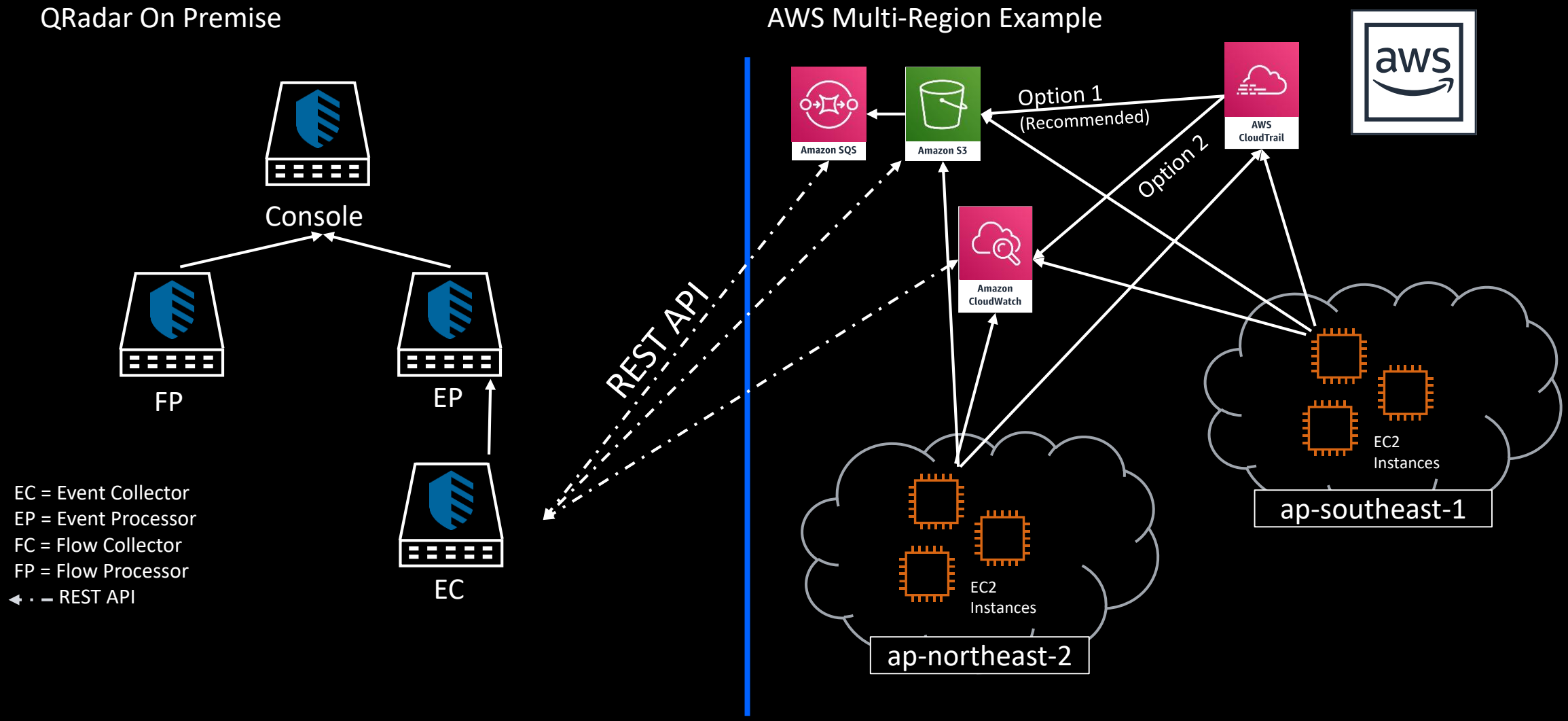
App Host
- App host

Collect from the Cloud – AWS Infrastructure Logging



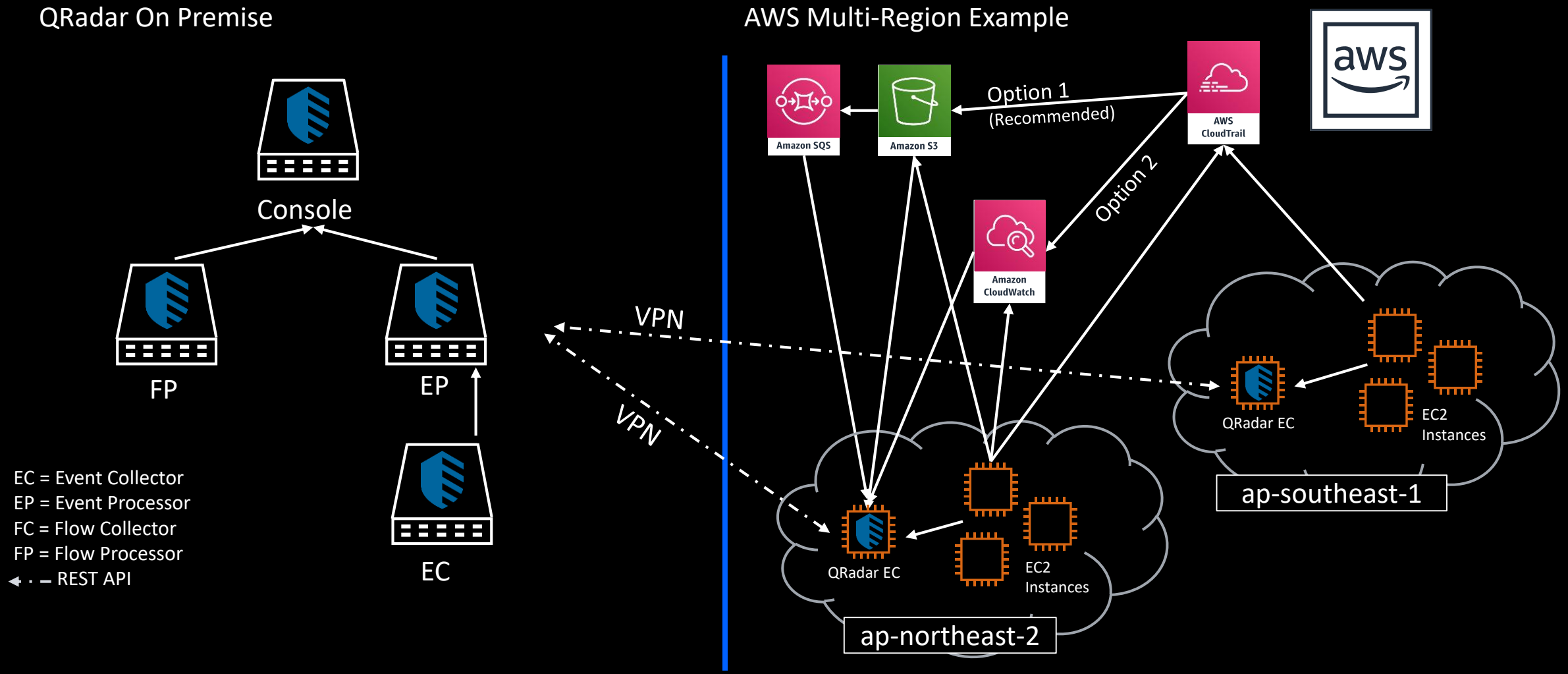
This diagram outlines how event collection works for most users today. Data is collected by the QRadar On Premise appliances.

Collect from the Cloud – AWS Collection Example 1



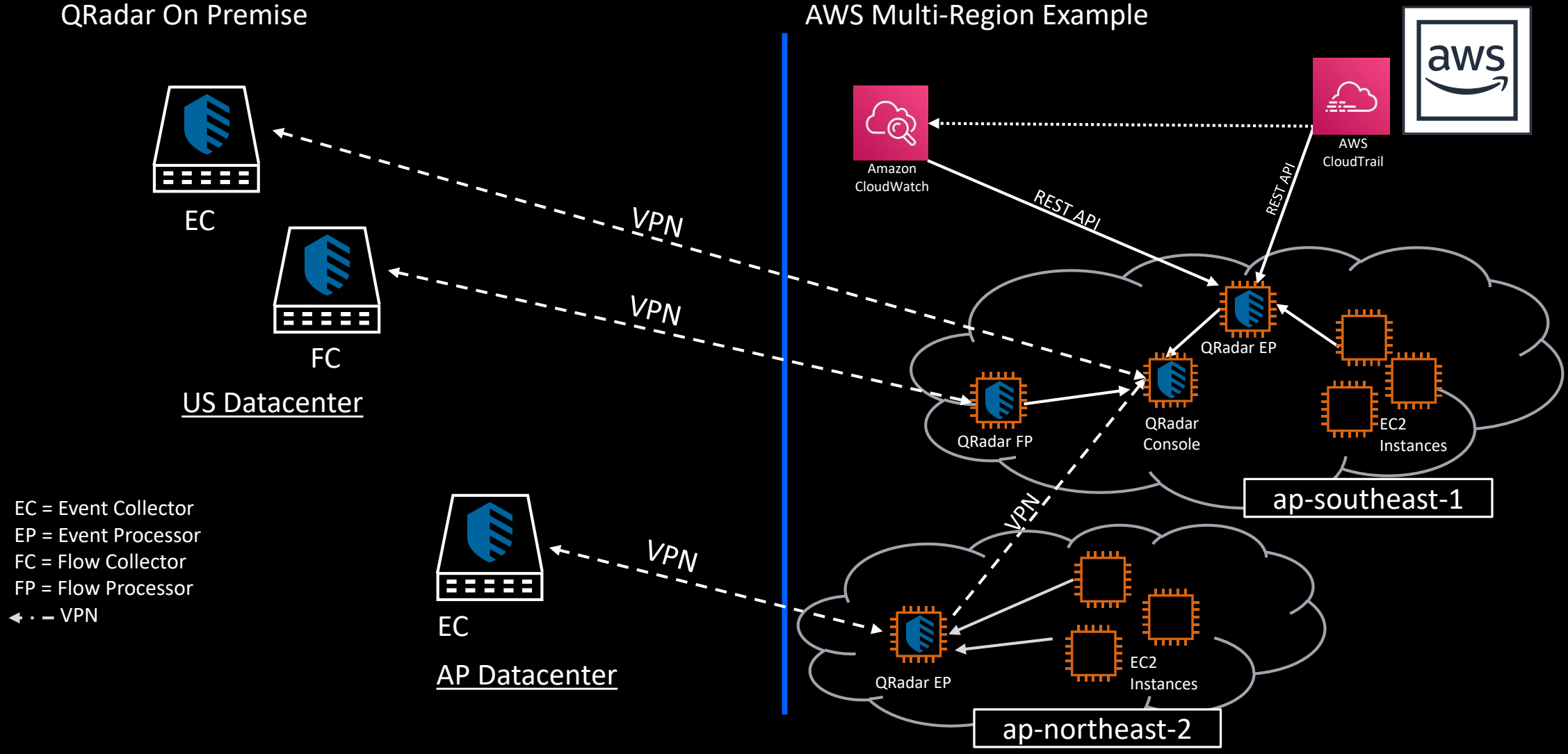
In this architecture outline various data from different AWS Services (CloudTrail, VPC Flow logs, and others) are stored either in S3 or CloudWatch Logs. The QRadar Amazon S3 REST API or AmazonWeb Services Protocols collect this data from the on premise EC or EC/EP combo.

Collect from the Cloud – AWS Collection Example 2



In this architecture outline various data from different AWS Services (CloudTrail, VPC Flow logs, and others) are stored either in S3 or CloudWatch Logs. The QRadar Amazon S3 REST API or Amazon Web Services Protocols collects this data from the CLOUD EC and sends it to an on premise EP**. A benefit is that you save on bandwidth as the event pipeline compresses EC to EP connections. Searches are completed with the on premise appliances.**

Collect from On Premise and Forward to Cloud



This example outlines on premise Event Collector and Flow Collector appliances that VPN data to the QRadar Cloud deployment. A benefit here is it limits the requirement for HA due to Cloud resiliency.

Deploying QRadar in Azure

VMIs on the Azure Marketplace

Licensing: Bring Your Own License (BYOL)

Current Version: QRadar v7.3.3

- **QRadar Console.** Can act as an All-in-one appliance or a Console in a distributed deployment.
- **QRadar Managed Host.** Allows you to deploy a new QRadar managed host to extend QRadar systems and gain deeper visibility into Azure.
- **QRadar App Host.** Provides extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your QRadar Console.

Images & Appliances

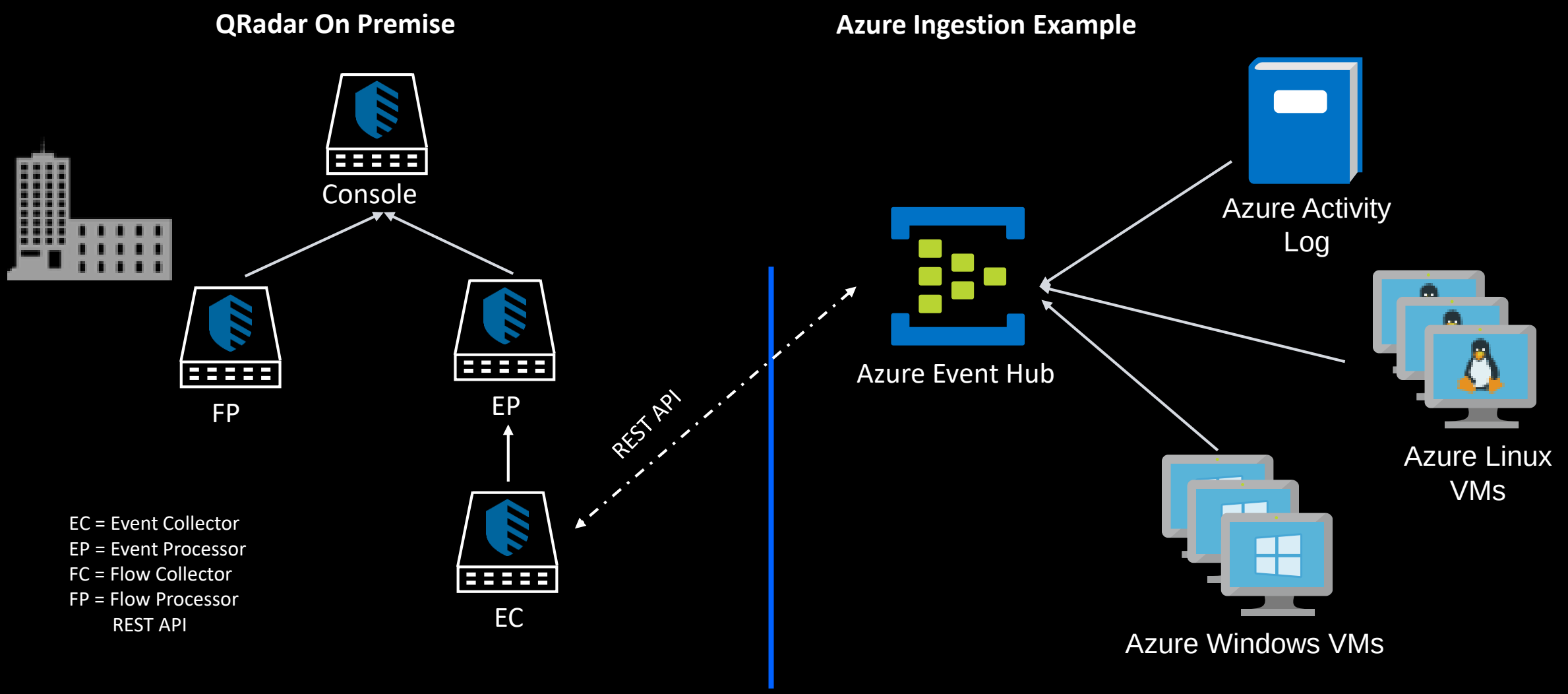
The QRadar VMIs can be configured into multiple QRadar appliances, and deployed in all major Azure regions.

Console
- Distributed deployment
- All-in-one

Managed Host
- Event Collector
- Event Processor
- Combination Processor
- Data Node
- Flow Collector
- Flow Processor
- Data Gateway

App Host
- App host

QRadar On Premises – Azure Event Hubs Integration



This diagram outlines how event collection works for the Azure Event Hub. Data is sent to the Azure Event Hub and queried by the QRadar On Premise appliance using a REST API.

Deploying QRadar in Google Cloud Platform (GCP)

Images on the GCP Marketplace

Licensing: Bring Your Own License (BYOL)

Current Version: QRadar v7.3.2

- **QRadar Console.** Can act as an All-in-one appliance or a Console in a distributed deployment.
- **QRadar Managed Host .** Allows you to deploy a new QRadar managed host to extend QRadar systems and gain deeper visibility into Azure.
- **QRadar App Host.** Provides extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your QRadar Console.

Images & Appliances

The QRadar images can be configured into multiple QRadar appliances, and deployed in all major regions.

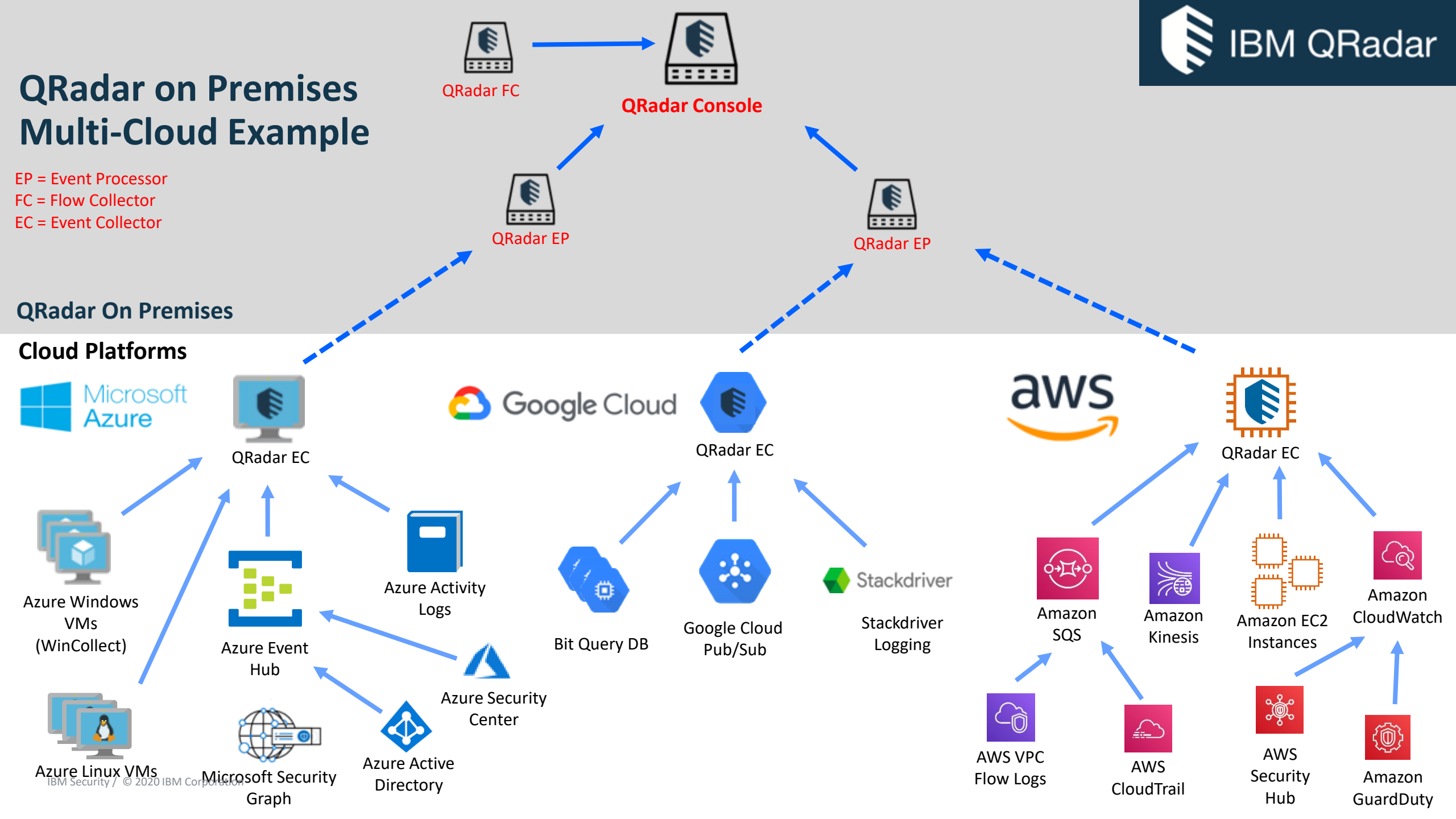
Console
- Distributed deployment
- All-in-one

Managed Host
- Event Collector
- Event Processor
- Combination Processor
- Data Node
- Flow Collector
- Flow Processor
- Data Gateway

App Host
- App host

QRadar on Premises Multi-Cloud Example

EP = Event Processor
FC = Flow Collector
EC = Event Collector



Qradar Cloud Security Resources

General Learning

- Supported DSMs documentation
- Configuring QRadar in a cloud environment
- IBM Security Communities
- Open Mic events and presentations
- IBM Security Learning Academy
- QRadar Blogs
- IBM Security Virtual Master Skills University 2020 - QRadar Advanced Track
- IBM Security Virtual Master Skills University 2020 - QRadar Basic Track

QRadar & AWS Resources

- Jose Bravo Videos
  - All Jose Bravo AWS Videos
- Blogs
  - IBM QRadar and AWS Best Practices - AWS VPC, AWS IAM, and AWS Security Groups
  - QRadar integration with Amazon VPC Flow Logs
  - Ingesting Kubernetes Logs from Amazon Elastic Kubernetes Service (Amazon EKS)

QRadar & Azure Resources

- Jose Bravo Videos
  - All Jose Bravo Azure Videos
- Blogs
  - QRadar Best Practices – Microsoft Azure and Office 365

QRadar & GCP Resources

- Jose Bravo Videos
  - Deploying QRadar in GCP
  - Configuring log sources to collect from Azure Event Hubs

Cloud Visibility App

- Docs
- Jose Bravo Videos
  - Cloud Visibility App

