Best practices for securing and monitoring AWS environments with IBM Security QRadar

IBM Security

Extend visibility and insights into AWS for better security posture

Agenda

- Intro
- Common challenges
- Best practices
- Use cases
- Next steps

Common challenges with establishing cloud security

Growing threats, tools, and data inhibit security operations across environments

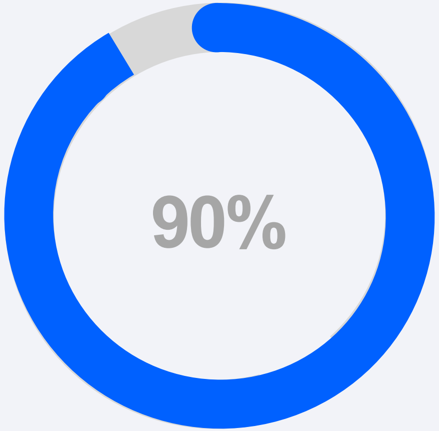
Expanding environments with multiple security tools creates a disjointed security posture

Lack of visibility across the threat landscape can impede threat investigation and response times

Establishing a unified approach to security across all environments and teams can be difficult

Meeting regulatory and compliance requirements on the cloud is fundamentally different than on-premises

As organizations accelerate their journey to AWS, more security capabilities will be delivered exclusively through the cloud



of SIEM solutions will have capabilities like log storage, analytics, or incident management that are only delivered through the cloud, a leap from the current **20%**

Source:
1. Gartner

Best practices for securing AWS deployments

Establish Visibility

Understand who is using what, and why. Have a unified view of cloud access and usage, with the proper controls in place to grant and deny access.

Integrate and align your security tools

Every cloud vendor will have native tooling that you can glue together but evolving your security practices with hybrid cloud often requires a single pane of glass view.

IBM Security QRadar with AWS

Centralized visibility and insights into the most critical threats across AWS environments

Single pane-of-glass

Gain centralized visibility across AWS and hybrid cloud environments via a single pane of glass

Comprehensive insights

Leverage deep integrations with AWS native services to ingest a broad spectrum of AWS logs and flows into QRadar for rapid and accurate threat detection

Real-time security analytics

Correlate data across users, networks, and AWS native services to gain deep insights into key threats including cloud misconfigs, policy changes and suspicious user activity

Prioritize threats

Connect related events to ensure steams only receive a single alert for an incident (ex. Suspicious AWS login to multiple EC2 instances to data exfiltration from S3 bucket)

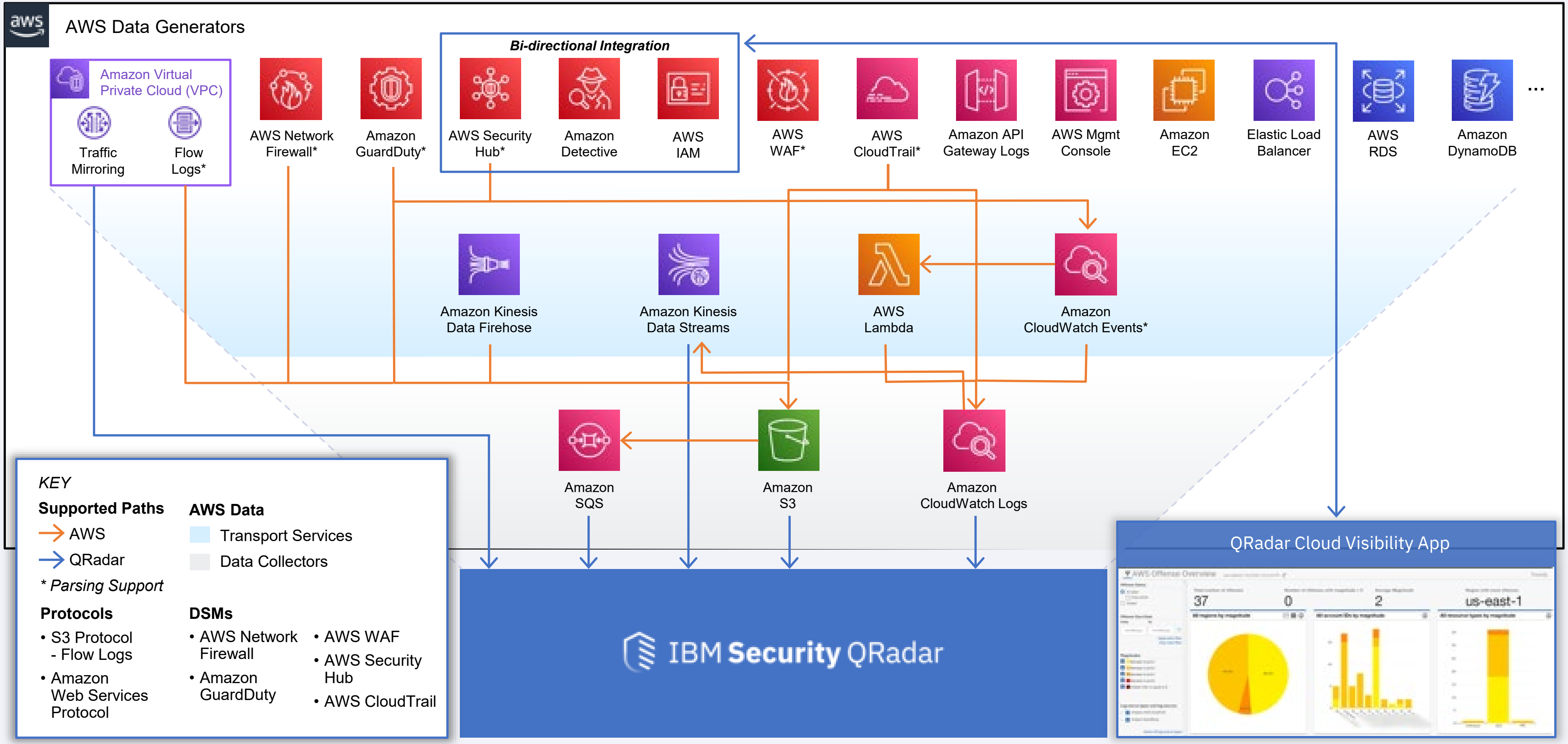
Incorporates AWS native security sources including: Amazon GuardDuty, AWS CloudTrail, AWS Network Firewall, AWS Security Hub and more.

Best practice #1 – Establish Visibility

Understand who is using what, and why. Have a unified view of cloud access and usage, with the proper controls in place to grant and deny access.

Embrace AWS native security services

IBM Security QRadar visibility into AWS



AWS Data Generators

Amazon Virtual Private Cloud (VPC)

Traffic Mirroring

Flow Logs*

AWS Network Firewall*

Amazon GuardDuty*

Bi-directional Integration

AWS Security Hub*

Amazon Detective

AWS IAM

AWS WAF*

AWS CloudTrail*

Amazon API Gateway Logs

AWS Mgmt Console

Amazon EC2

Elastic Load Balancer

AWS RDS

Amazon DynamoDB

...

Amazon Kinesis Data Firehose

Amazon Kinesis Data Streams

AWS Lambda

Amazon CloudWatch Events*

Amazon SQS

Amazon S3

Amazon CloudWatch Logs

IBM Security QRadar

QRadar Cloud Visibility App

KEY

Supported Paths

→ AWS

→ QRadar

** Parsing Support*

AWS Data

🟦 Transport Services

⬜ Data Collectors

Protocols

- S3 Protocol
  - Flow Logs
- Amazon Web Services Protocol

DSMs

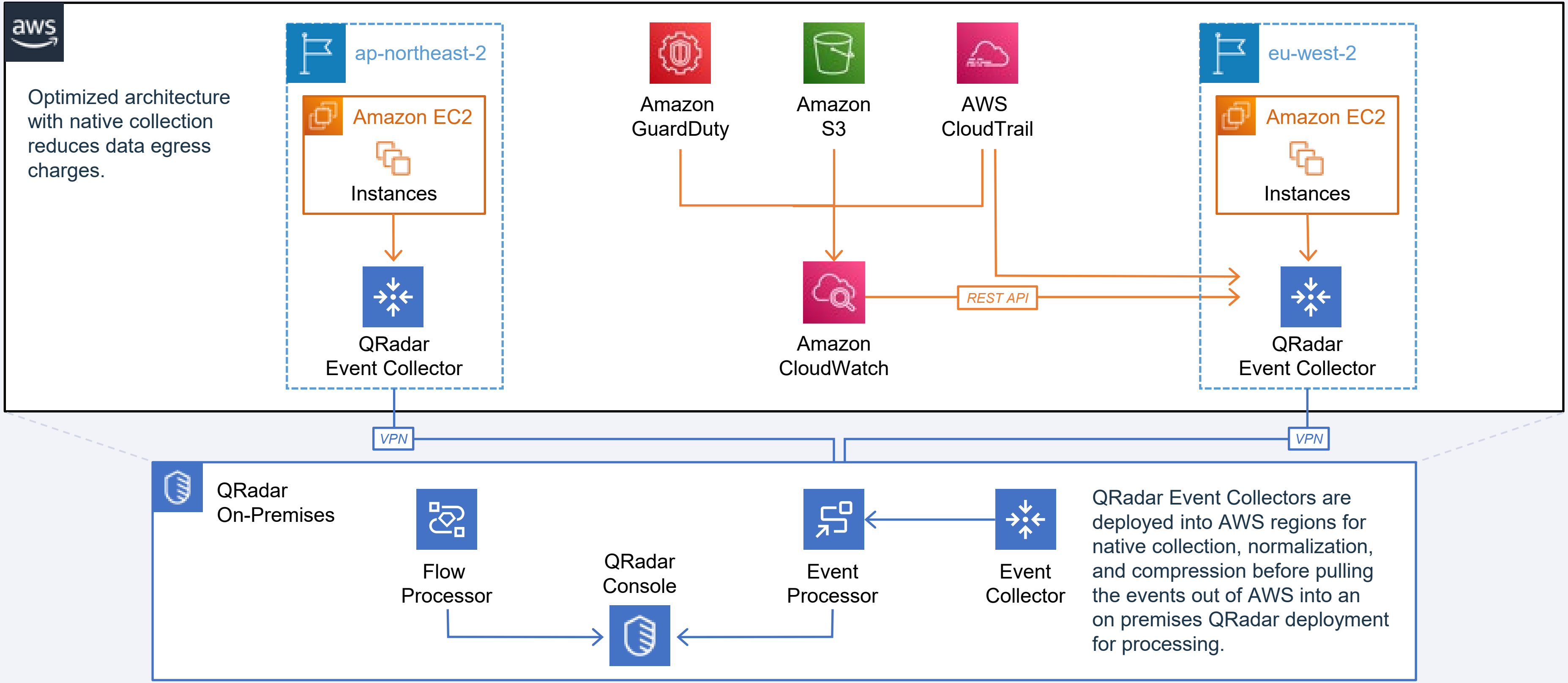
- AWS Network Firewall
- Amazon GuardDuty
- AWS WAF
- AWS Security Hub
- AWS CloudTrail

IBM Security QRadar with AWS integrations

Log Source	Description	AWS Security Use Cases
CloudTrail	Records API calls made on your AWS account and delivers log files to S3 buckets providing visibility into user activity	**Preventing Misconfigurations** • Detecting configuration and policy changes to VPCs, EC2, Security Groups, IAM Roles, S3 Buckets, NACLs, Network Gateways, Key Pair Management, Encryption Certificates **Controlling and Monitoring Access** • Multiple Failed Read Attempts from same Source IP/different geographies, Root User Activity **Protecting Resource Integrity** • Monitoring for terminations/deletions of S3 buckets, EC2 instances, VPCs, CloudTrail Logs **Anomalous User and Account Behavior** • Non-Standard VPC or EC2 instances, Non-Standard users accessing resources
CloudWatch	Real-time monitoring of resources and applications to collect and track metrics in AWS environment	**Monitoring Critical Data Applications and Resources** • Set automatic alerts on significant changes to resource or application usage indicating anomalous behavior
VPC Flows	Log monitoring feature that enables user to capture information about IP traffic going to and from network interfaces in VPC	**Enhanced Analysis of Flow Traffic** • Visualizing VPC Flow traffic to gain further insight into cloud subnet activity
S3 Bucket	Simple Storage Solution buckets are used to store objects, which consist of data and metadata that describes the data	**Securing SaaS Cloud Applications** • Ingesting SaaS operations logs into QRadar for visibility into cloud application security/usage
GuardDuty	Amazon GuardDuty is a basic threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads.	**AWS Native Security Intelligence Feed** • Integrate AWS Security Findings and native use cases into QRadar improving visibility into AWS environment and services
Kinesis	Kinesis delivers real-time analytics capabilities to streaming data from a variety of AWS native services like S3, EC2, CloudTrail and VPC Flows.	**Real-Time Security Analytics** • Enables near real-time Ingestion of AWS network flows and events aggregated into Kinesis • Continuous Security Analytics, Multi-Account/Multi-Region Support, Multi-Account simplification for active threat security monitoring

Hybrid - Deploy IBM Security QRadar Event Collectors in AWS

AWS Multi-Region Example



Optimized architecture with native collection reduces data egress charges.

QRadar Event Collectors are deployed into AWS regions for native collection, normalization, and compression before pulling the events out of AWS into an on premises QRadar deployment for processing.

Best practice #2 – Integrate and align your security tools

Every cloud vendor will have native tooling that you can glue together but evolving your security practices with hybrid cloud often requires a single pane of glass view.

Prioritize threats across AWS telemetry

Use cases

IBM delivers repeatable, security-driven outcomes for AWS environments

Detect cloud misconfigurations

Protect against human error and potential threats by detecting and resolving misconfiguration and policy changes across users and cloud resources

Secure SaaS cloud applications

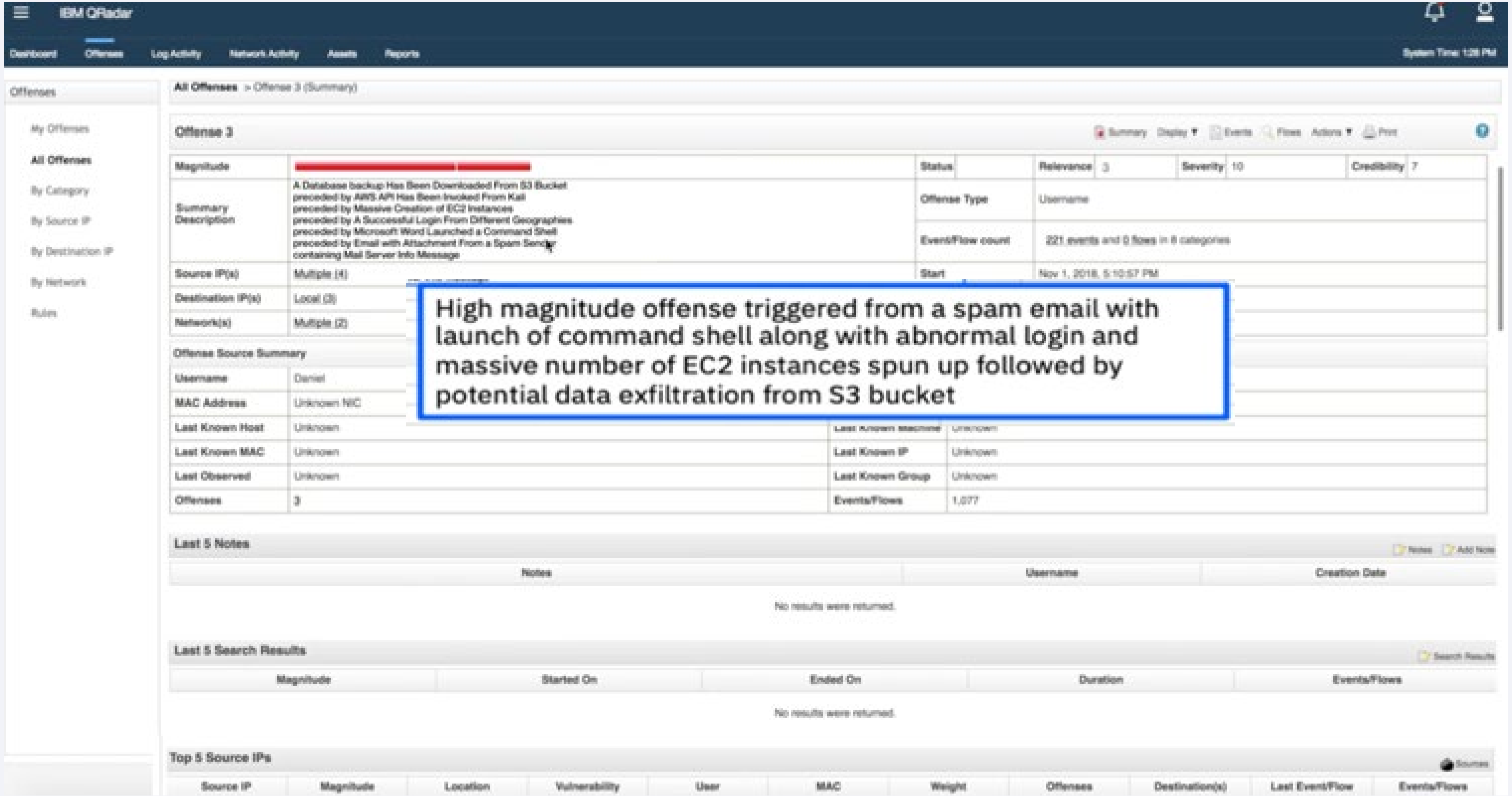
Expand visibility into cloud application security and usage to improve detection of anomalous or suspicious user behavior including shadow IT

Enhance cloud visibility

Enable analysts to monitor, detect, and visualize potential offenses within AWS for the most comprehensive reporting analytics.

IBM Security QRadar content extension with AWS CloudTrail

Extends visibility into suspicious AWS account activity



Offense 3

Magnitude	🟥	Status		Relevance	3	Severity 10	Credibility 7
Summary Description	A Database backup Has Been Downloaded From S3 Bucket preceded by AWS API Has Been Invoked From Kali preceded by Massive Creation of EC2 Instances preceded by A Successful Login From Different Geographies preceded by Microsoft Word Launched a Command Shell preceded by Email with Attachment From a Spam Sender containing Mail Server Info Message	Offense Type	Username				
		Event/Flow count	221 events and 0 flows in 8 categories				
Source IP(s)	Multiple (4)	Start	Nov 1, 2018, 5:10:57 PM				
Destination IP(s)	Local (3)						
Network(s)	Multiple (2)						

Offense Source Summary

Username	Daniel		
MAC Address	Unknown NIC		
Last Known Host	Unknown	Last Known Machine	Unknown
Last Known MAC	Unknown	Last Known IP	Unknown
Last Observed	Unknown	Last Known Group	Unknown
Offenses	3	Events/Flows	1,077

High magnitude offense triggered from a spam email with launch of command shell along with abnormal login and massive number of EC2 instances spun up followed by potential data exfiltration from S3 bucket

Last 5 Notes

Notes	Username	Creation Date

No results were returned.

Last 5 Search Results

Magnitude	Started On	Ended On	Duration	Events/Flows

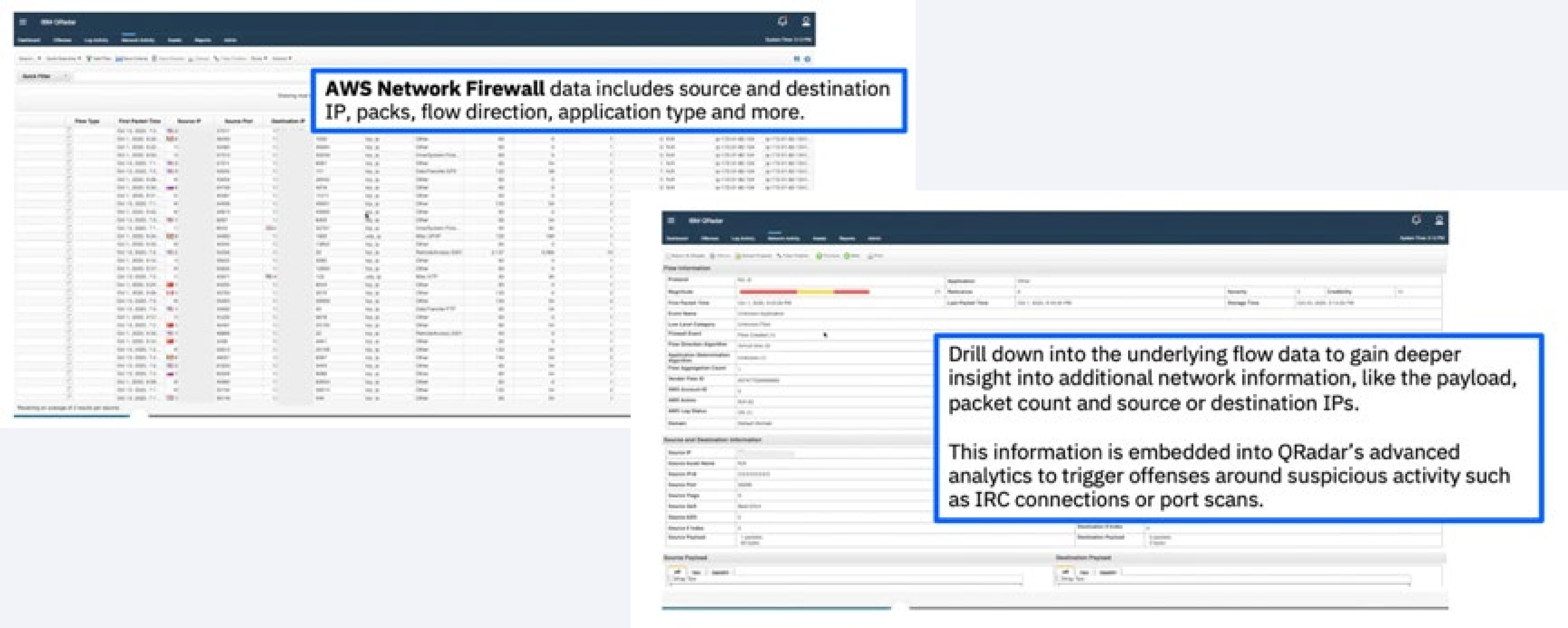
No results were returned.

Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows

IBM Security QRadar integration with AWS Network Firewall Service

Prioritize threats across AWS firewall telemetry



AWS Network Firewall data includes source and destination IP, packs, flow direction, application type and more.

Drill down into the underlying flow data to gain deeper insight into additional network information, like the payload, packet count and source or destination IPs.

This information is embedded into QRadar's advanced analytics to trigger offenses around suspicious activity such as IRC connections or port scans.

Global MSSP offers flexible deployment models to accelerate clients' journey to AWS (ReliaQuest)

RELIAQUEST

Industry:
Cross-industry MSSP

Cloud Environments:
AWS

IBM Solution:

- QRadar SIEM
- AWS CloudTrail
- Amazon GuardDuty
- Amazon CloudWatch
- VPC flow logs
- Amazon CloudFront

Public Reference Link

Client Requirements:

A trusted IBM Security partner for over a decade, ReliaQuest has been at the forefront of providing customers with confidence in their security programs and investments so that they can thrive in the face of uncertainty. With deep expertise in IBM Security QRadar, ReliaQuest helps joint customers accelerate time to value by delivering increased visibility, automated threat detection and faster response.

As more organizations accelerate their move to cloud to drive business innovation and customer success, ReliaQuest continues to drive a unified approach to security for their clients, extending threat management capabilities across on-premise, hybrid and multi-cloud environments. ReliaQuest has seen significant growth in hybrid cloud deployments of QRadar for a wide range of their cross-industry clients.

Solutions:

By helping IBM Security QRadar customers integrate and correlate data from AWS, ReliaQuest delivers industry-leading visibility and robust threat coverage at every phase of the attack Lifecyle. A subset of the repeatable use cases include:

- Misconfigured access policies (Public Access, Security Groups, etc.)
- Large data outflow (S3 bucket, VPC, etc.)
- Deletion of AWS Objects (S3 buckets, configurations, instances, etc.)
- Rapid termination of production EC2 instances

Benefits:

- Flexibility in deployment models to meet their clients' needs
- Deep visibility into the most critical threats across AWS environments with a core set of repeatable use cases
- Combine AWS security event logs with flows to correlate disparate events into a single offense

Partner Quote:

- ***"We're seeing organizations invest a significant amount of resources towards the cloud - whether it's a full cloud, multi-cloud or hybrid environment, the support we provide remains consistent across our customer base because of QRadar's flexible deployment models***" - ReliaQuest

Global MSSP accelerates their clients' journey to AWS with QRadar (Smarttech247)

Industry:
Cross-industry MSSP

Cloud Environments:
AWS

IBM Solution:

- QRadar SIEM
- QRadar Cloud Visibility App
- AWS CloudTrail
- Amazon GuardDuty
- Amazon CloudWatch
- Amazon Detective
- VPC flow logs

Public Reference Link

Client Requirements:

As organizations accelerate their move to cloud to drive business innovation and customer success, Smarttech247 has continued to drive a unified approach to security for their clients, providing threat management across on-premise and hybrid cloud environments.

As more of their clients' workloads migrate to cloud, they have leveraged a broad set of QRadar integrations with cloud native services to secure those environments. There has been an emphasis on AWS to provide a centralized view of risks and threat across networks, users and endpoints.

Solutions:

Today, Smarttech247 leverages QRadar integrations with several AWS security services including AWS CloudTrail, Amazon GuardDuty, CloudWatch, Detective and VPC flow logs to detect cloud misconfigurations. For example, they uses QRadar's integration with AWS CloudTrail to monitor user activity and behavior including:

- Deletions of S3 buckets
- Starting or stopping EC2 instances
- Misconfigured EC2 security group ports and inbound traffic access
- Non-standard users accessing resources, discovery of unused security groups
- Multiple failed read attempts from same source IP/different geographies

Benefits:

- These integrations help their security analysts gain deep visibility into the most critical threats across AWS environments
- Provide a clear view back to their clients on cloud misconfigurations and detect potential blind spots in a client's network
- Combine AWS security event logs with flows to correlate disparate events into a single offense

Why IBM Security:

- IBM Security provided deep security expertise and deep integrations between QRadar and AWS native security services to support and accelerate their migration and their client's migration to cloud

Getting Started

Deploy IBM Security QRadar on AWS Marketplace
Realize enhancements to your security posture within minutes
Visit AWS Marketplace

Additional Resources
QRadar for AWS website
QRadar apps and content extensions for AWS

Who depends on IBM?

IBM Security secures

100%
of the US Fortune 100

95%
of the Global Fortune 500

Finance
49 out of 50 of the world's largest financial services and banking companies

Tech
13 out of 15 of the world's largest technology companies

Healthcare
14 out of 15 of the world's largest healthcare companies

Telecom
The 10 largest telecom companies

Automotive
19 out of 20 of the world's largest motor vehicle and parts companies

Airline
8 out of 10 of the world's largest airline companies

We are invested to be the best

Proven security market leadership across 14 segments

SIEM

Security Analytics

Fraud Reduction Intelligence Platform

Web Fraud Detection

Identity Governance

Access Management

Identity as a Service

Identity Management

Risk-Based Authentication

Data Security and Database Security

Data Center Backup and Recovery

Unified Endpoint Management

Managed Security Services

Cybersecurity Incident Response Services

Questions?

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM

QRadar AWS integrations

Log Sources	Logs	Flows	Use cases
CloudTrail	API calls and user activity		Misconfigurations, Resource Integrity, Access control, User behavior
Network Fire Wall	Firewall Alert and Firewall Flow logs		Suspicious activity such as IRC server connections or port scans
Security Hub	Findings standardized		Cross correlation from Guard Duty, Macie, Inspector
VPC Flows	Flow Logs	IP traffic	Flow traffic analysis and cloud subnet activity
Guard Duty	Threat detection		Patterns of failed login requests, or unblocked port probing from a known bad IP, attempts to disable AWS CloudTrail logging, uand API calls from known malicious IP addresses.
Cloud Watch	Resources and Applications		Anomalous behavior, misconfigurations
Kinesis	Analytics		Mechanism for ingesting data from other services, not an a data generator
S3 buckets (Protocol only)	Data and Metadata		Store and forward other security relevant data.

IBM Security QRadar with AWS integrations

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 buckets

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

IBM Security Threat Management Mission:

Accurate and efficient detection of threats to mitigate the data exposure and business disruption.

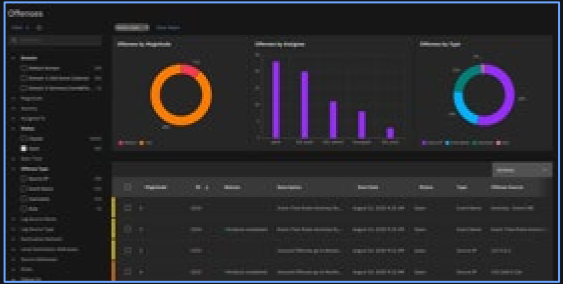
Advanced Analytics
for accurate detection

Streamlined Workflows
for efficient decisions

Comprehensive Integrations
for accurate detection

Modernized Architecture
for efficient deployment

Integrations for a Hybrid Cloud World *Recent Update*



IBM Security QRadar

Google Cloud Audit Logs
Google Cloud Platform Firewall
Google G Suite Activity Reports

Google Cloud Platform

Security Hub
Guard Duty
VPC Flow Logs
Cloud Watch
Web Application Firewall
Elastic Kubernetes Service
Cloud Trail
Network Firewall
Application Load Balancer

aws

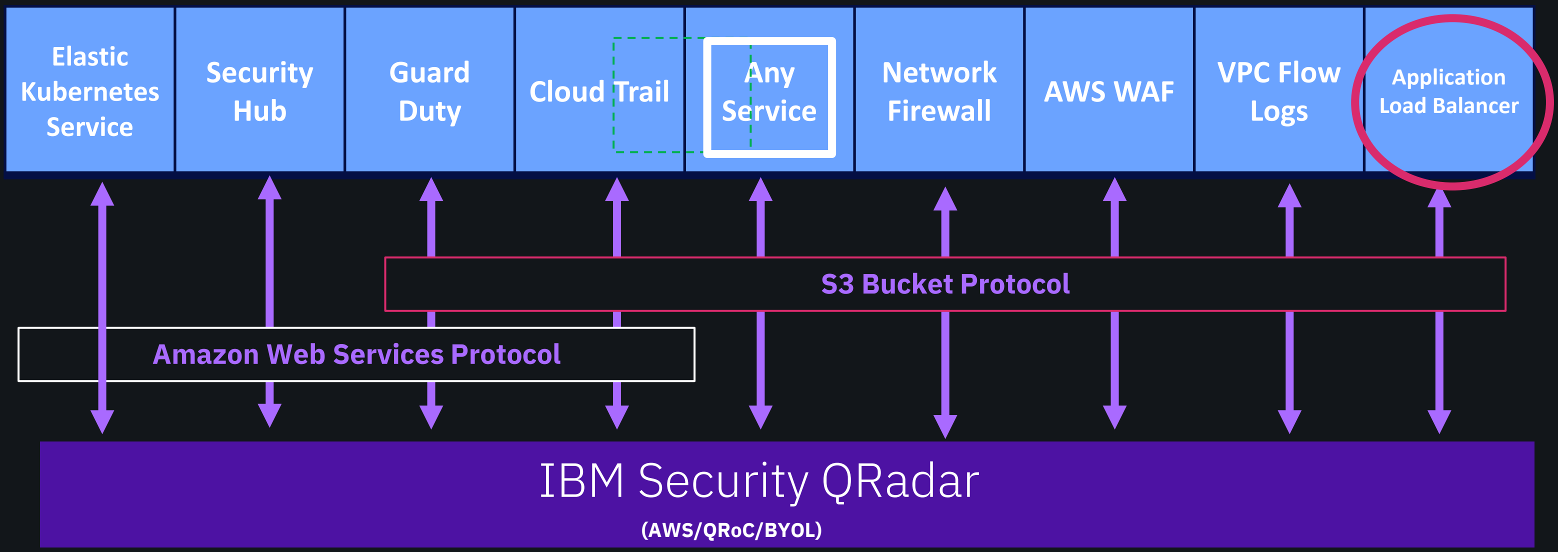
Azure Active Directory
Azure Platform
Azure Security Center
Microsoft O365
Microsoft O365 Message Trace
Windows Defender For Endpoint (ATP)
Microsoft Cloud App Security Workflow

Azure

AWS Integrations for a Hybrid Cloud World

Summary

New!



Elastic Kubernetes Service

Security Hub

Guard Duty

Cloud Trail

Any Service

Network Firewall

AWS WAF

VPC Flow Logs

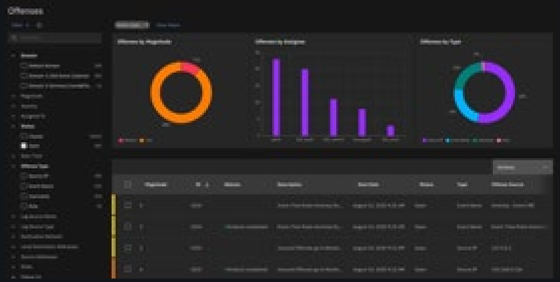
Application Load Balancer

S3 Bucket Protocol

Amazon Web Services Protocol

IBM Security QRadar

(AWS/QRoC/BYOL)



Protocols

S3 Rest API (S3 Bucket)

AWS Protocol (CloudWatch Logs/Kinesis/SQS)

IBM Security Threat Management Mission:

For Amazon Web Services

Comprehensive Integrations:

- ✓ Application Load Balancer
- ✓ Cloud Trail
- ✓ Cloud Watch Events
- ✓ CloudWatch Logs
- ✓ Elastic Kubernetes Service
- ✓ Guard Duty
- ✓ Network Firewall
- ✓ S3
- ✓ Security Hub
- ✓ VPC Flow Logs
- ✓ Web Application FW

Advanced Analytics:

- ✓ Correlation across data sources with out-of-the box use cases
- ✓ User Analytics with Machine Learning
- ✓ Network Traffic Analysis
- ✓ AI for investigation via Watson for Cyber
- ✓ Dashboarding and Reporting capability

Streamlined Workflows:

- ✓ Pre-built content packs with Security Relevant use cases
- ✓ Modernized User Interface
- ✓ Integrations with SOAR and Ticketing Solutions
- ✓ Ability to map rules and use cases to MITRE ATTACK Framework

Efficient Deployment:

- ✓ Instances available in Amazon Marketplace
- ✓ Additional ability to collect data from on-prem, GCP and Azure
- ✓ SaaS Option with QRoC and data gateways deployed in AWS

IBM Security Threat Management : Network Traffic Analysis

For Amazon Web Services

Amazon: VPC Flows

- Supported!

Analyze your network

- Understand what's on your network, and what's normal on your network
- Leverage anomaly detection and real-time visualizations and alerting to detect deviations

Detect threats that are hard to find

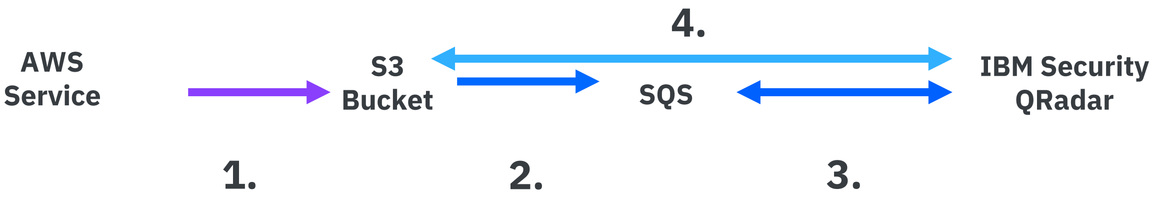
- Identify beaconing and C2 activity to detect attackers who already have a foothold
- Detect staging and low & slow data exfiltration

QRadar AWS Integration Components Available

Amazon Web Services (DSMs)	DSM Guide
AWS Cloud Trail	Here
AWS Network Fire Wall	Here
AWS Security Hub	Here
Guard Duty	Here
VPC Flow Logs	Here

Amazon Web Services (Protocols)	DSM Guide
AWS S3 Rest API	Here
Amazon Web Services	Here

AWS S3 Integration via SQS Available



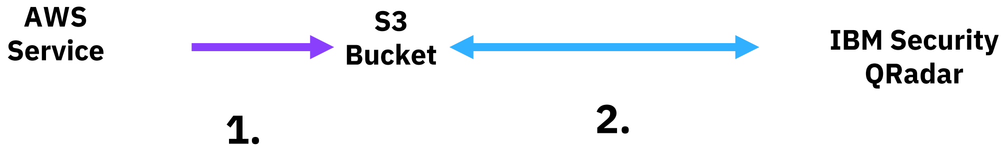
Supported Services

AWS WAF

AWS Network Fire Wall
Guard Duty
VPC Flow Logs
Kinesis Firehose

1. Service publishes data to S3
2. S3 publishes notifications to SQS
3. QRadar pulls notifications from SQS
4. QRadar pulls data from S3

AWS S3 Integration via Directory Prefix Available



Supported Services

AWS WAF

AWS Network Fire Wall

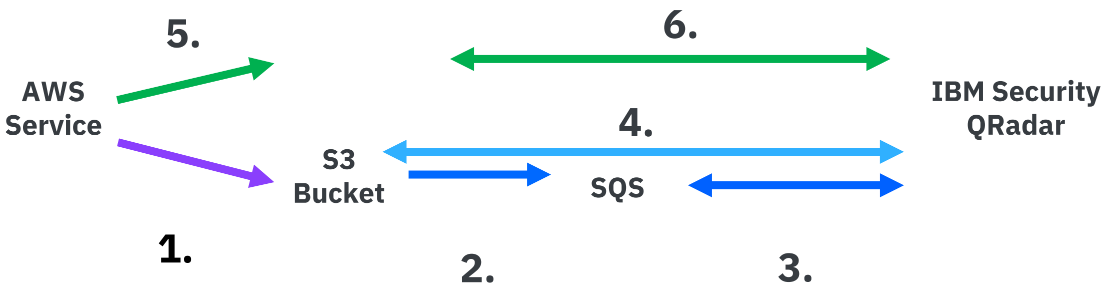
Guard Duty

VPC Flow Logs

Kinesis Firehose

1. Service publishes data to S3
2. QRadar pulls data from S3

AWS S3 Integration Available



<u>Supported Services</u>

AWS WAF

AWS Network Fire Wall
Guard Duty
VPC Flow Logs
Kinesis Firehose

VIA SQS

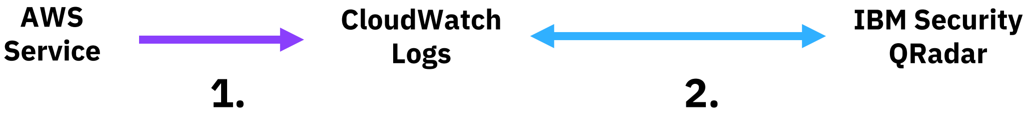
1. Service publishes data to S3
2. S3 publishes notifications to SQS
3. QRadar pulls notifications from SQS
4. QRadar pulls data from S3

VIA Directory Pre-Fix

5. Service publishes data to S3
6. QRadar pulls data from S3

Integrating via CloudWatch Logs Available

Example: AWS CloudTrail



AWS Service

1.

CloudWatch Logs

2.

IBM Security QRadar

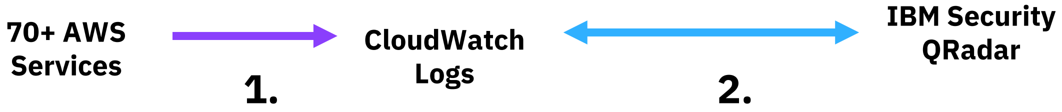
CloudWatch Logs

Monitoring and observability service that collects logs, metrics, and events. Natively integrates with more than 70 AWS services

1. Service publishes logs to CloudWatch Logs
2. QRadar pulls logs from S3 CloudWatch Logs
   - ✓ *Leverages QRadar Amazon Web Services Protocol*

Integrating via CloudWatch Logs Available

Example: AWS CloudTrail



CloudWatch Logs

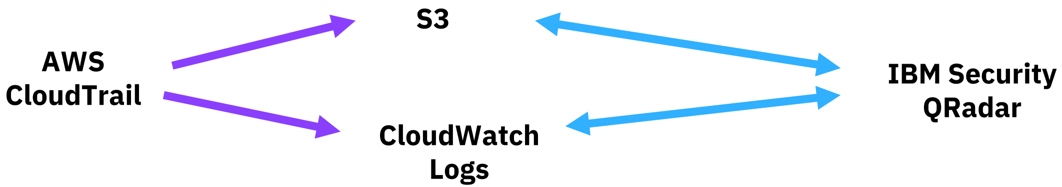
Monitoring and observability service that collects logs, metrics, and events. Natively integrates with more than 70 AWS services

Available DSMs

Guard Duty

1. CloudWatch Events publishes logs to CloudWatch Logs
2. QRadar pulls logs from S3 CloudWatch Logs
   - ✓ *Leverages QRadar Amazon Web Services Protocol*

Integrating CloudTrail Available



CloudTrail Logs

Provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

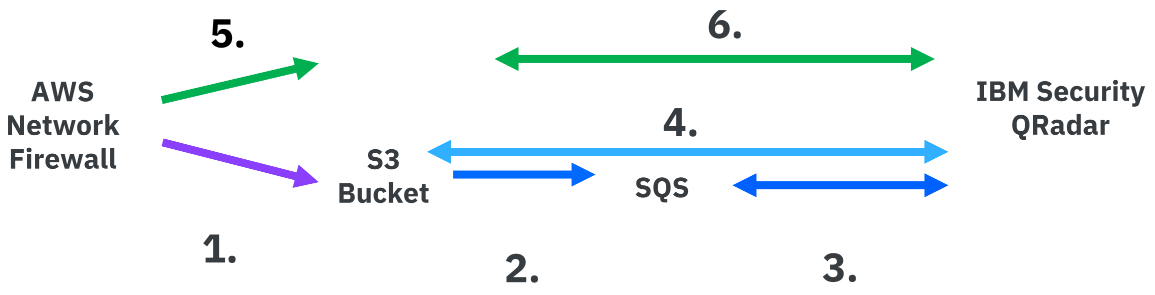
Via S3

1. CloudTrail publishes logs to S3
2. S3 publishes notifications to SQS
3. QRadar pulls notifications from SQS
4. QRadar pulls logs from S3

Via CloudWatch Logs

1. CloudTrail publishes logs to CloudWatch Logs
2. QRadar pulls logs from CloudWatch Logs

Integrating AWS Network Firewall Available



AWS Network Firewall

Service that makes it easy to deploy essential network protections for all of your Amazon Virtual Private Clouds (VPCs)

Define firewall rules that give you fine-grained control over network traffic,

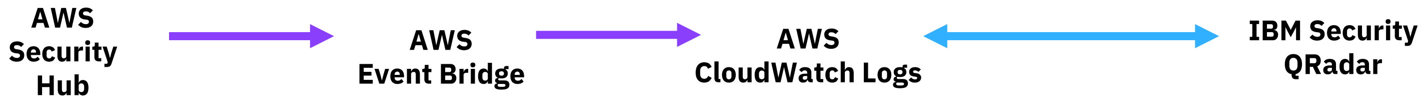
VIA SQS

1. Service publishes data to S3
2. S3 publishes notifications to SQS
3. QRadar pulls notifications from SQS
4. QRadar pulls data from S3

VIA Directory Pre-Fix

5. Service publishes data to S3
6. QRadar pulls data from S3

Integrating via Security Hub Available



AWS Security Hub

AWS Event Bridge

AWS CloudWatch Logs

IBM Security QRadar

Security Hub Logs

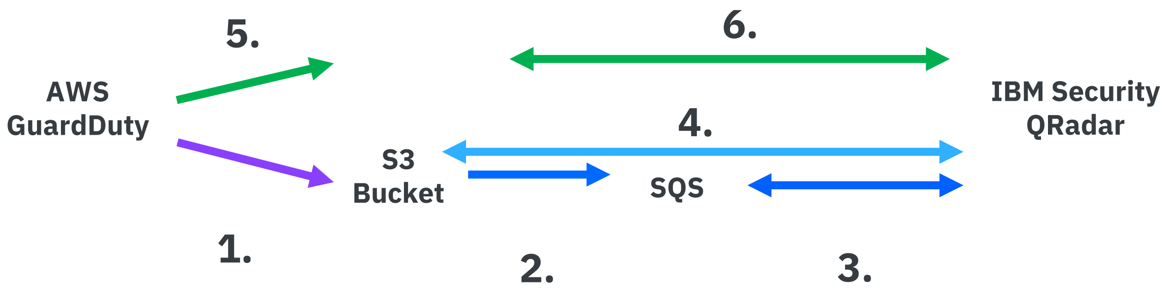
View of your security alerts and security posture across your AWS accounts.

Integrated Services

1. Amazon GuardDuty,
2. Amazon Inspector, A
3. Amazon Macie,
4. AWS (IAM) Access Analyzer,
5. AWS Systems Manager
6. AWS Firewall Manager

1. Security Hub publishes logs to EventBridge
2. EventBridge publishes logs to CloudWatch Logs
3. QRadar pulls logs from S3 CloudWatch Logs
   - ✓ *Leverages QRadar Amazon Web Services Protocol*

Integrating AWS GuardDuty Available



AWS GuardDuty

Continuous Threat Detection Service. Provides identification and prioritization of potential threats.

Data Sources: (1) CloudTrail (2) S3 (3) VPC FlowLogs and DNS

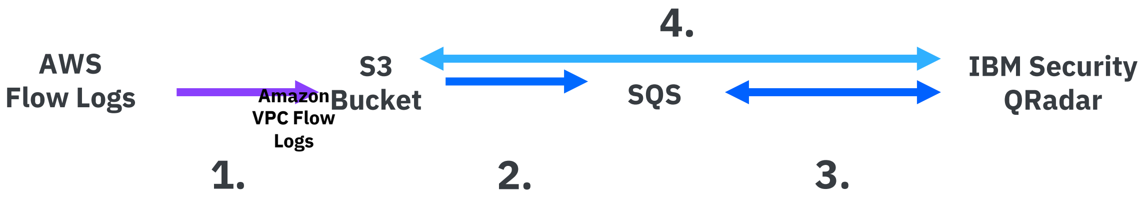
VIA SQS

1. Service publishes data to S3
2. S3 publishes notifications to SQS
3. QRadar pulls notifications from SQS
4. QRadar pulls data from S3

VIA Directory Pre-Fix

5. Service publishes data to S3
6. QRadar pulls data from S3

Integrating AWS Flow Logs Available

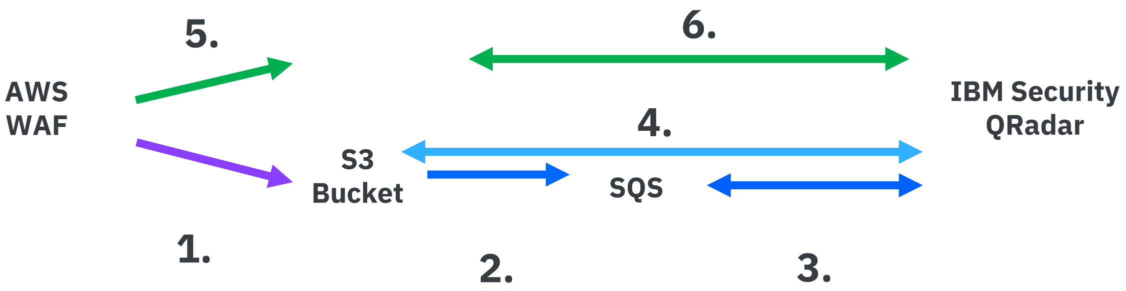


AWS VPC Flow Logs

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC

1. Service publishes data to S3
2. S3 publishes notifications to SQS
3. QRadar pulls notifications from SQS
4. QRadar pulls data from S3

Integrating AWS WAF Coming Soon



AWS WAF

Protects web apps and APIs against common web exploits

Helps to avoid disruptions availability, compromised security, or excessive resource consumption

VIA SQS

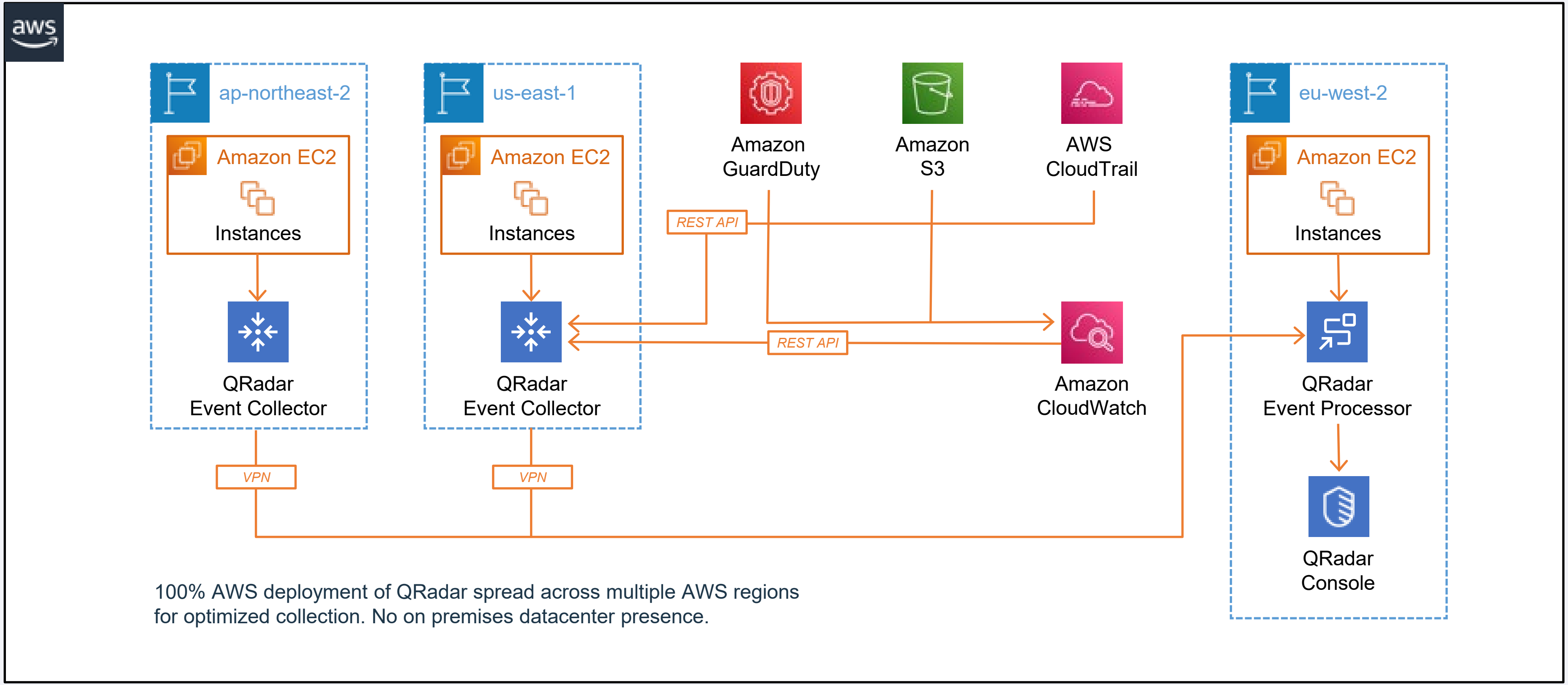
1. Service publishes data to S3
2. S3 publishes notifications to SQS
3. QRadar pulls notifications from SQS
4. QRadar pulls data from S3

VIA Directory Pre-Fix

5. Service publishes data to S3
6. QRadar pulls data from S3

Full Cloud Deployment in AWS

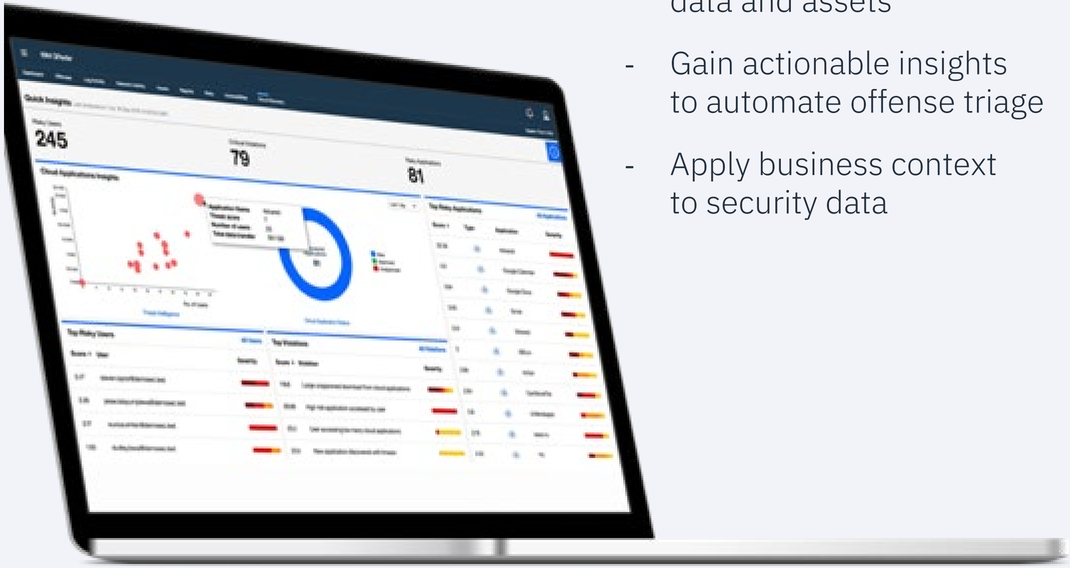
AWS Multi-Region Example



100% AWS deployment of QRadar spread across multiple AWS regions for optimized collection. No on premises datacenter presence.

SaaS cloud applications

Discover cloud application usage across the enterprise

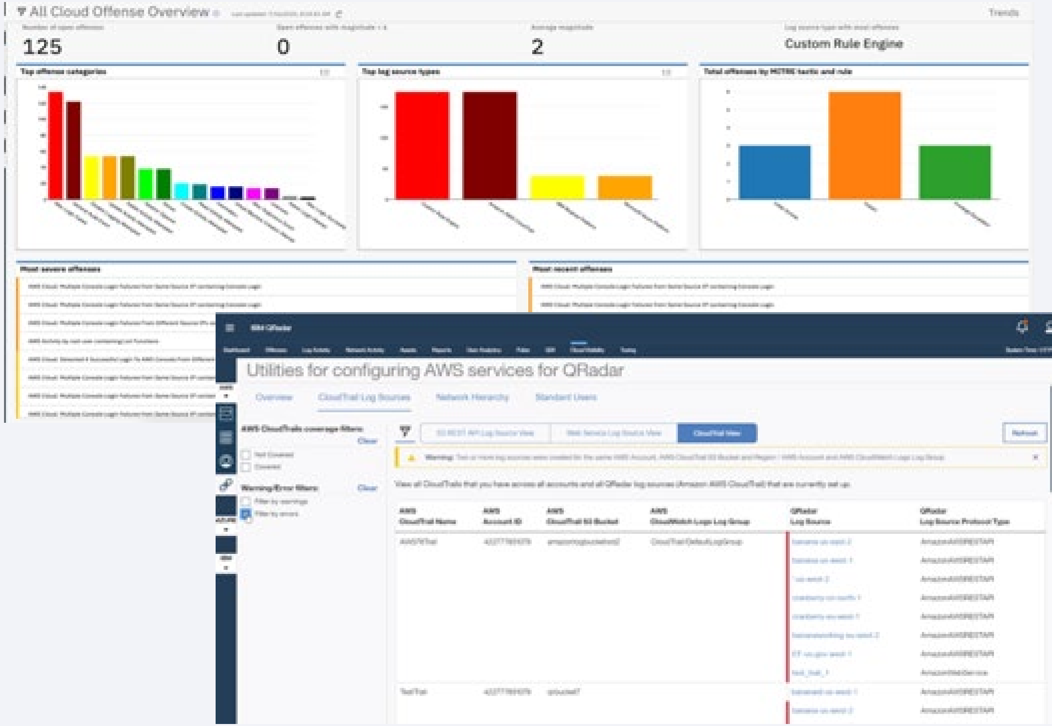


- Uncover and control Shadow IT
- Automatically discover hybrid cloud data and assets
- Gain actionable insights to automate offense triage
- Apply business context to security data
- Enforce security policies leveraging Threat Intelligence
- Safeguard data and intellectual property
- Minimize enterprise risk through real-time classification

IBM Security QRadar Cloud Visibility App

Visualize and prioritize offense across AWS environments

- Centralized dashboard view of all cloud-related offenses across AWS deployments
- Detect and prevent account cloud misconfigurations
- Automated log source creation, detection, and configuration including AWS Security Hub and Amazon Detective
- Visualization into AWS CloudTrail, GuardDuty and VPC flow logs
- Identify and access management for accounts, users and IAM roles including best practices which are not being followed



IBM X-Force Threat Management with IBM Security QRadar

Modernize your enterprise threat management approach on the cloud

Comprehensive security framework

Accelerate and enhance your security posture throughout your AWS journey, regardless of your cloud maturity with IBM’s programmatic approach to cloud security

Full hybrid environment visibility

Gain full visibility across your on-premises and AWS environment to quickly identify and react to known and unknown threats

Accelerated time-to-remediation

Utilize AI-enabled threat investigation, automation and orchestrated response capabilities to accelerate time-to-remediation for security misconfigurations and threats

World-class security expertise

Leverage the expertise of IBM SOC analysts, security testers, and incident responders to ensure your security postures matures as you grow