

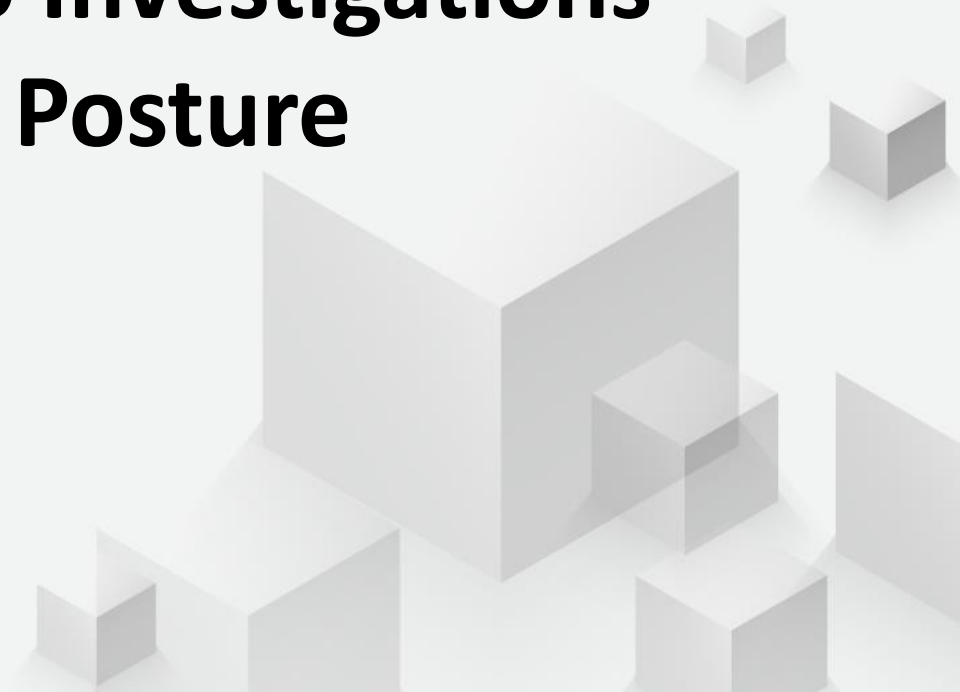


in conjunction with Barracuda




JumpStart Guide to Investigations and Cloud Security Posture Management

Monthly Webinar Series



JumpStart Guide to Investigations and Cloud Security Posture Management

Sponsored by
 aws marketplace

Today's Speakers

- Kyle Dickinson – SANS Instructor, Author and Analyst; Cloud Security Architect at Koch Industries
- Tim Jefferson – Senior Vice President for Barracuda's security solutions across Data, Networking and Application (DNA)
- David Aiken – Solutions Architect Manager, AWS Marketplace

Today's Agenda

What is Cloud Security Posture Management (CSPM)?

Benefits of CSPM and how it can aid in investigations

Advice for cyber investigations and CSPM working together

AWS integration and solutions available in AWS Marketplace

What is Cloud Security Posture Management?



Continuous
Compliance



Asset Inventory



Monitoring/Analytics



Configuration
Management

Benefits of CSPM

- Visibility in all regions
 - AWS China and AWS GovCloud excluded
- Risk management
- Compliance reporting
- Custom signatures/queries
- Software-as-a-Service platform

How Can a CSPM Aid in Investigations?

- Query all AWS accounts owned by organization
- Asset inventory (CIS Critical Control)
- Contextualize VPC Flow Log data
- Visualize user administrative activity

Investigation Considerations

- Authorization to environment
- How the investigation will differ in AWS
- Technologies for acquiring evidence
 - CSPM, AWS CloudTrail, EC2 Snapshot
- Investigation Simulations a/k/a Game Days

Implementation Considerations



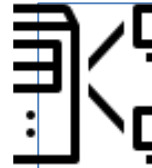
How will the implementation scale?



Can signatures be customized?



Data retention



Can alerts workflow be customized?



What about third-party integrations?



Licensing model?

Summary

- Lots of CSPMs offer similar functionality plus niche capabilities.
- Deployment and deployment validation should be done
- Signature review should be considered
- Alerts be extended to DevOps teams as a feedback loop

Making Cloud Security More Actionable

CSPM Enhancing Cyber Investigations



Fast Pace of Innovation

179

Native services within
AWS today

000's

Number of new features
added to services in 2019
that impact configurations

0?

Number of qualified Cloud
Security Architects working
for you



Each service has its own configuration impacts



- DeleteBucket
- DeleteBucketPolicy
- DeleteObject
- DeleteObjectTagging
- DeleteObjectVersion
- GetBucketAcl
- GetBucketLogging
- GetBucketPolicy
- GetEncryptionConfiguration
- GetObject
- GetObjectAcl
- GetObjectVersionAcl
- GetObjectVersion
- ListAllMyBuckets
- ListBucket
- PutBucketAcl
- PutBucketPolicy
- PutBucketVersioning
- PutEncryptionConfiguration
- PutInventoryConfiguration
- PutObject
- PutObjectAcl
- ...

 **CIS Benchmarks™**



permissions



AWS CloudTrail: Actionable Telemetry

```
Records": [{
  "eventVersion": "1.0",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam:123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-03-06T21:01:59Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "StopInstances",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "205.251.233.176",
  "userAgent": "ec2-api-tools 1.6.12.2",
  "requestParameters": {
    "instancesSet": { "items": [{"instanceId": "i-ebeaf9e2"}] },
    "force": false
  },
  "responseElements": { "instancesSet": { "items": [
    {
      "instanceId": "i-ebeaf9e2",
      "currentState": {
        "code": 64,
        "name": "stopping"
      },
      "previousState": {
        "code": 16,
        "name": "running"
      }
    }
  ] }
  }
}
```

} who and what made this call

} What did they try to do and when

} Requested action and response



CSPM Making AWS CloudTrail Telemetry Actionable

TIME	ACCOUNT - REGION	EVENT NAME	EVENT SOURCE	DETAILS
	aws cuda-se-public-clouddev	AuthorizeSecurityGroupIngress	ec2.amazonaws.com	<pre>Identity: userName: vshastrj@barracuda.com principalId: AIDAJN3VPS2YSUBSINKAY accessKeyId: ASIAW27PQA27WR3ZPXWW invokedBy: signin.amazonaws.com sessionContext: { sessionIssuer: { object Object }, attributes: { object Object }, webIdFederationData: { object Object } } type: IAMUser arn: arn:aws:iam:470264317631:user/vshastrj@barracuda.com accountId: 470264317631</pre>

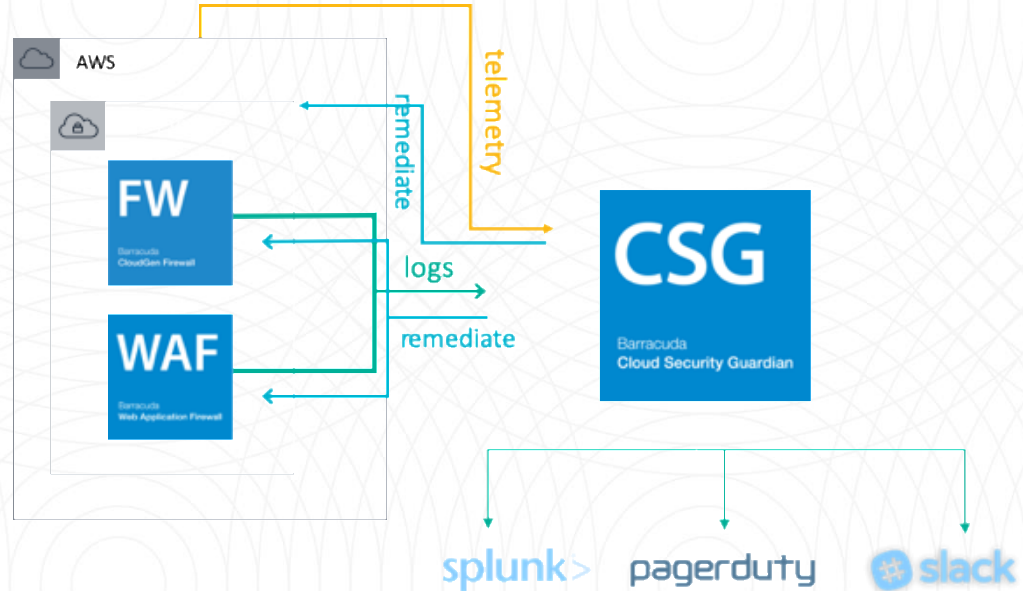
- What did they try to do and when
- who and what made this call
- Were there any security alerts as a part of the event?

TIME	ACCOUNT	RESULT	SEVERITY	SOURCE	VIOLATION	DETAILS
2019-09-26 15:05:09	aws cuda-se-public-clouddev	Failed	Critical	Barracuda: Compliance	CIS 4.1: Ensure no security groups allow ingress from 0.0.0.0/0 to port 22	Found Security Group with SSH port TCP:22 open to the world (0.0.0.0/0) Additional Details FIX IT
2019-09-26 15:05:09	aws cuda-se-public-clouddev	Failed	Critical	Barracuda: Compliance	HIPAA 4.1: Ensure no security groups allow ingress from 0.0.0.0/0 to port 22	Found Security Group with SSH port TCP:22 open to the world (0.0.0.0/0) Additional Details FIX IT
2019-09-26 15:05:09	aws cuda-se-public-clouddev	Failed	Critical	Barracuda: Compliance	NIST 4.1: Ensure no security groups allow ingress from 0.0.0.0/0 to port 22	Found Security Group with SSH port TCP:22 open to the world (0.0.0.0/0) Additional Details FIX IT
2019-09-26 15:05:09	aws cuda-se-public-clouddev	Failed	Critical	Barracuda: Compliance	PCI_DSS 1.2.1: Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic	Scan result does not meet rule requirement Additional Details FIX IT



Barracuda Cloud Security Guardian

- Cloud Security Posture Management SaaS
- Integration with native tools – AWS Security Hub , Amazon GuardDuty
- Integration with Barracuda CloudGen Firewall and Barracuda WAF



CSPM Providing Unique Visibility

CISO/CIO/Security Operations team concerned about visibility into ephemeral usage

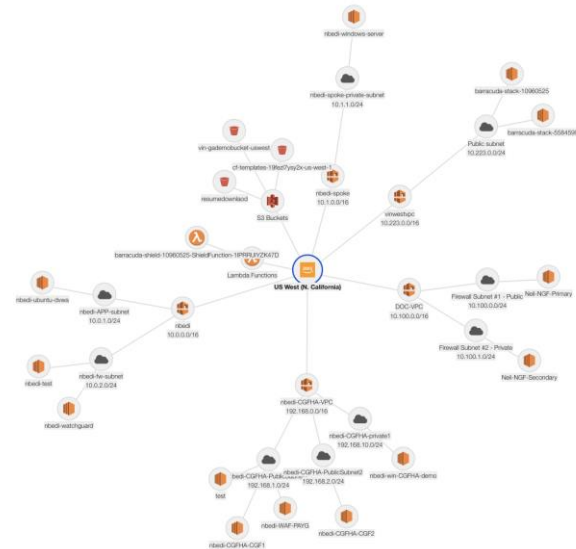
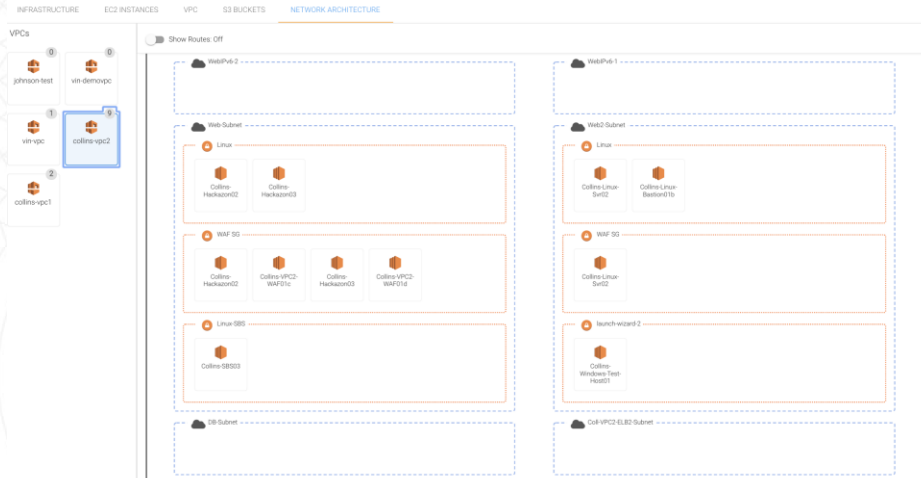
cuda-se-public-clouddev: US West (N. California) (us-west-1)

INFRASTRUCTURE EC2 INSTANCES VPC S3 BUCKETS NETWORK ARCHITECTURE

Filter: EC2 Instance, VPC or Bucket Name Tag

APPLY

CLEAR



Automate Compliance Monitoring

- Human error is cause of many misconfigurations
 - Misconfigurations often violate security best practices
 - Best practices are inherent aspect of compliance

Dashboard

Last 24 Hours | **AMAZON WEB SERVICES** | MICROSOFT AZURE

License
Status: **Active**
Serial: 1218099

Assets

Asset	Count
S3 Buckets	28
Beamstalk Applications	0
VPCs	61
Security Groups	300
EC2 Instances	12
IAM Users	16
Load Balancers	11
SQL Databases	3
Network Interfaces	141

Compliance Scan Result

Compliance Scan Result (More Details)

Scoring by Compliance Rule

Compliance Rule	Score
CIS	14 / 75
HIPAA	6 / 72
NIST	11 / 65
NIST	12 / 87
PCI DSS	2 / 22

cuda-se-public-clouddev 39 / 251

Passed: 0 | Failed (Critical): 12 | Failed (Medium): 0 | Failed (Low): 0

Storage Shield Statistics

AWS S3 Buckets

Total Buckets:	0
Total Files:	0
Total File Size:	0 B

Storage Shield Detected File Types

No data in this time range

Regions with assets

Alerts

Filter Alerts

Account: 1 of 2 accounts selected | Search for terms in alerts | Preset Time Frame: Today | Start: 2019-09-22 11:30 | End: 2019-09-23 11:30 | APPLY

TIME	ACCOUNT	RESULT	SEVERITY	SOURCE	VIOLATION	DETAILS
2019-09-22 15:44:06	aws cuda-se-public-clouddev	Failed	Critical	Barraouda: Compliance	CIS 4.2: Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389	Found Security Group with RDP port TCP-3389 open to the world (0.0.0.0/0) Additional Details FIX IT
2019-09-22 15:44:06	aws cuda-se-public-clouddev	Failed	Critical	Barraouda: Compliance	HIPAA 4.2: Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389	Found Security Group with RDP port TCP-3389 open to the world (0.0.0.0/0) Additional Details FIX IT
2019-09-22 15:44:06	aws cuda-se-public-clouddev	Failed	Critical	Barraouda: Compliance	NIST 4.2: Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389	Found Security Group with RDP port TCP-3389 open to the world (0.0.0.0/0) Additional Details FIX IT
2019-09-22 15:44:06	aws cuda-se-public-clouddev	Failed	Critical	Barraouda: Compliance	NIST 4.3: Ensure no security groups allow ingress from 0.0.0.0/0 to unencrypted Cassandra client communication port TCP-9042 open to the world (0.0.0.0/0)	Found Security Group with unencrypted Cassandra client communication port TCP-9042 open to the world (0.0.0.0/0) Additional Details FIX IT

Security & Compliance Policies

aws AWS Policies

POLICY NAME	ENABLED RULES	ENABLED CATEGORIES
Default Policy	141 rules	CIS: 46 PCI_DSS: 11 HIPAA: 37 NIST: 47
All	143 rules	CIS: 46 PCI_DSS: 11 HIPAA: 37 NIST: 47 Custom: 2

Remediate Policy Violation Before Breach

Detecting violations is a first step

- Need to understand the “who, what, where, why”
- Quick remediation is key to preventing security breaches

Hackers target misconfigurations as certain mistakes are very common

Remediate Compliance Violation



NIST 1.3: Ensure credentials unused for 90 days or greater are disabled

AUTOMATIC REMEDIATION

RECIPE

Remediation measure will perform the following modifications:

1. By default access key type credential will be set to inactive.
Note: If 'delete_credential' flag is set to true, access key will be deleted.
2. By default password type credential will be ignored.
Note: If 'delete_credential' flag is set to true, password will be deleted.

RULE PARAMETERS

SCHEMA

Please fill out the fields below in JSON format:

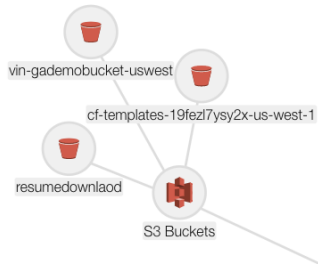
```
{
  "offenders": [
    {
      "offender": "arn:aws:iam::470264317631:user/ncorrea@barracuda.com(violation_details: access_key_type)",
      "offender_params": {
        "delete_credential": false
      }
    },
    {
      "offender": "arn:aws:iam::470264317631:user/mjoffe@barracuda.com(violation_details: password_type)",
      "offender_params": {
        "delete_credential": false
      }
    },
    {
      "offender": "arn:aws:iam::470264317631:user/rhebert@barracuda.com(violation_details: password_type)",
      "offender_params": {
        "delete_credential": false
      }
    }
  ]
}
```

REMEDiate



Protecting AWS S3 Buckets

- Visualize S3 buckets
- Protect your S3 buckets from accidental exposure
- Scan your S3 buckets for malware and advance threats



Page: 1 - 1-3 of 3 < >

ACCOUNT	RESULT	SEVERITY	SOURCE	VIOLATION	DETAILS	
aws cuda-se-public-clouddev	Failed	Critical	Barracuda: Compliance	Custom 2.1: Ensure S3 Buckets are not publicly accessible	Found at least S3 bucket open to public network Additional Details	FIX IT
aws cuda-se-public-clouddev	Failed	Critical	Barracuda: Compliance	HIPAA 2.9: Ensure S3 Buckets are not publicly accessible	Found at least S3 bucket open to public network Additional Details	FIX IT
aws cuda-se-public-clouddev	Failed	Critical	Barracuda: Compliance	NIST 2.7: Ensure S3 Buckets are not publicly accessible	Found at least S3 bucket open to public network Additional Details	FIX IT

Report Filter

Report Name: Cloud Storage Shield Scan Log | Limit Scan Determination: All Files | Preset Time Frame: Last 120 Days | Start: 2019-05-26 00:00 | End: 2019-09-23 15:45 | Account: aws | [RUN REPORT](#)

DETERMINATION	CLOUD ACCOUNT: REGION	S3 BUCKET	FILE INFO
Virus	aws:155517015620: US East (Ohio)	ridademo	malicious-28.pdf (73.1 KB)
Virus	aws:155517015620: US East (Ohio)	ridademo	malicious-28.pdf (73.1 KB)
Virus	aws:155517015620: US East (Ohio)	ridademo	malicious-28.pdf (73.1 KB)
Virus	aws:155517015620: US East (Ohio)	ridademo	malicious-28.pdf (73.1 KB)
Virus	aws:155517015620: US East (Ohio)	ridademo	Fact_No-2SB317021.test123.doc (76.75 KB)
Virus	aws:155517015620: US East (Ohio)	ridademo	malicious-28.pdf (73.1 KB)



Getting Started

30-day free trial on the AWS Marketplace!





Exploring Security Solutions Available in AWS Marketplace



What Barracuda Solutions are Available in AWS Marketplace?



Barracuda Cloud Security Guardian

Provides end-to-end visibility of your security posture

Barracuda CloudGen Firewall

Leverage threat protection, segmentation, and visibility in this enterprise-grade firewall

Barracuda Web Application Firewall

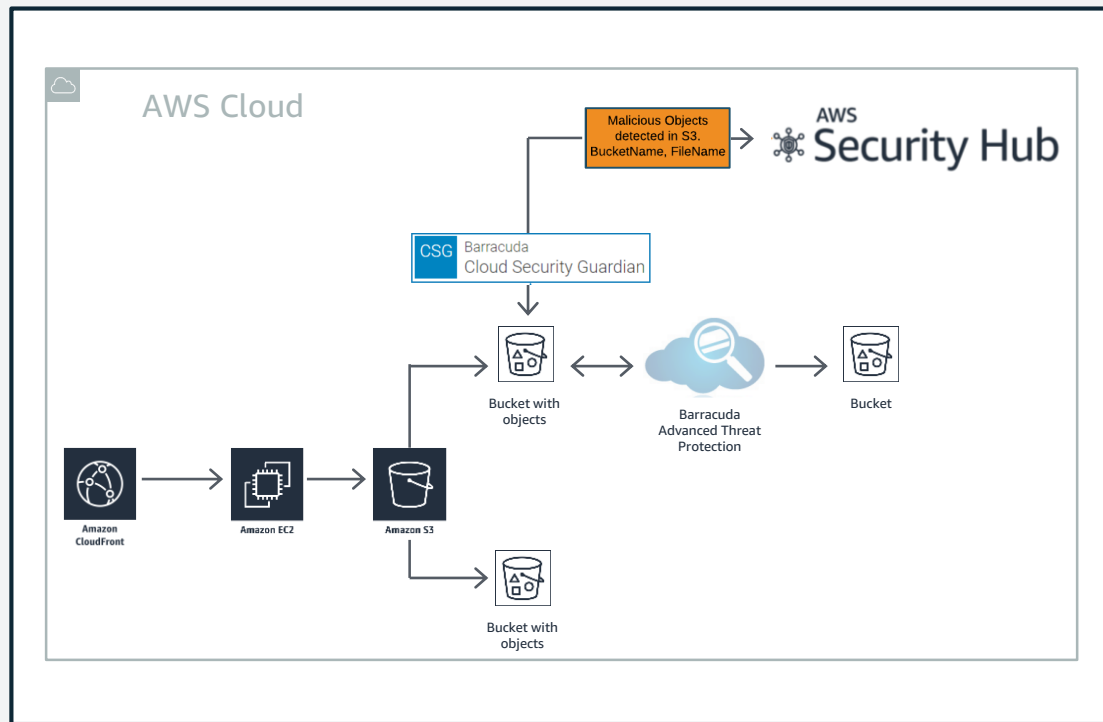
Application security and data loss prevention for your applications

Barracuda Email Security Gateway

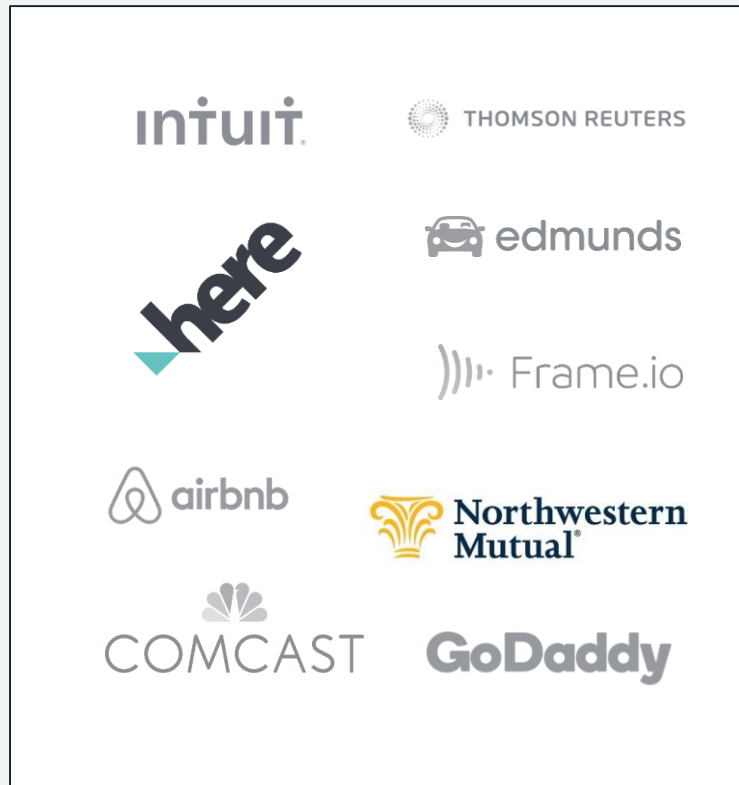
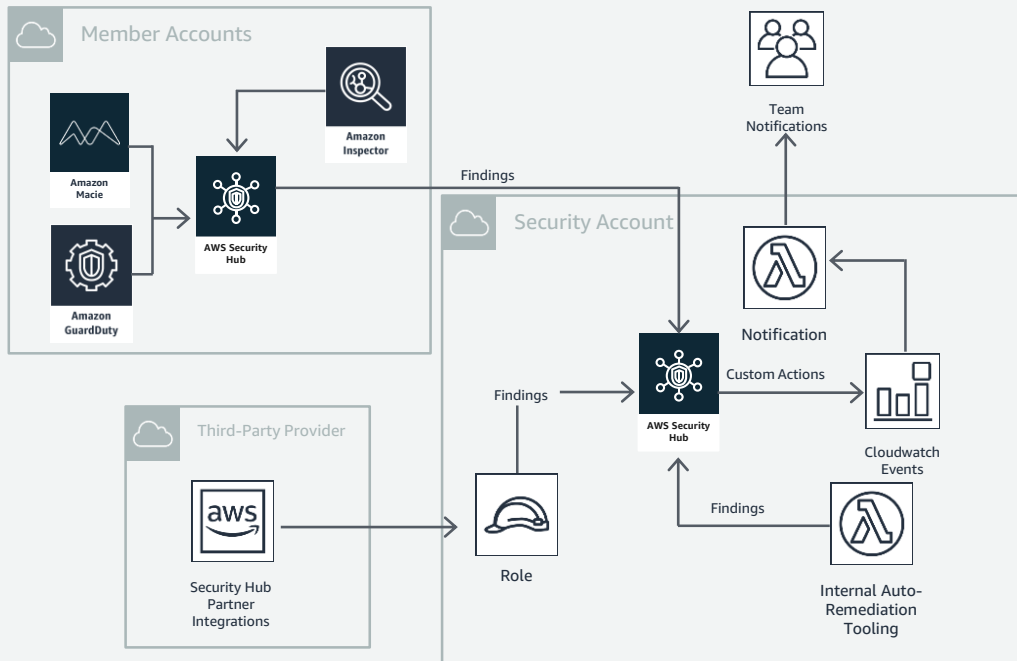
Manages all inbound and outbound email traffic

How Are Software Sellers Integrating with AWS Services?

- AWS Security Hub provides comprehensive visibility for all user activities
- Barracuda Cloud Security Guardian will forward additional findings to AWS Security Hub for richer context



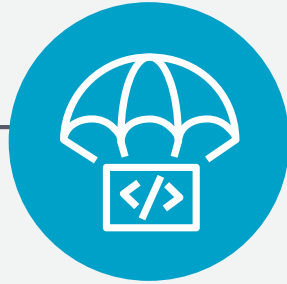
How Are Customers Leveraging AWS Security Hub?



Why AWS Marketplace?



**Flexible consumption
and contract models**



**Quick and
easy deployment**



**Helpful humans
to support you**

How Can You Get Started?

Find



a breadth of security solutions available:



Check Point
SOFTWARE TECHNOLOGIES LTD.



Buy



through flexible pricing options:

Free trials

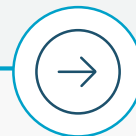
Hourly | Monthly

Bring Your Own License (BYOL)

Seller Private Offers

Channel Partner Private Offers

Deploy



with multiple deployment options:

SaaS

Amazon Machine Image (AMI)

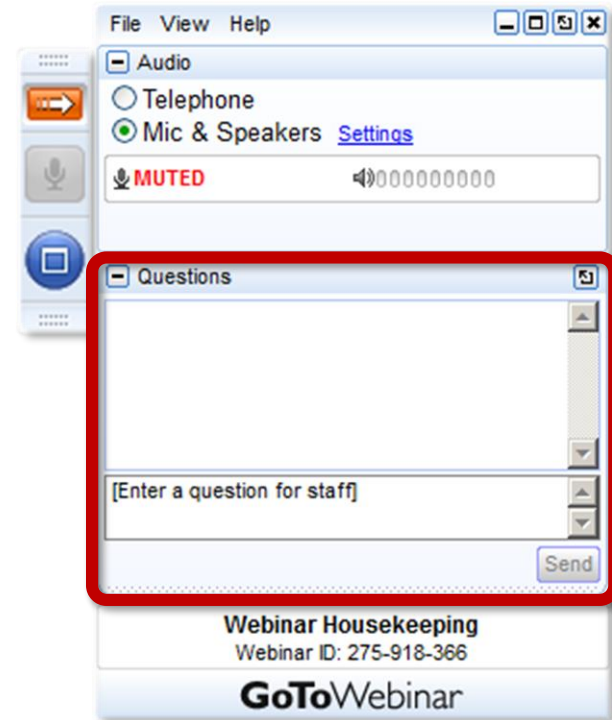
CloudFormation Template

Container

Q&A

Please use **GoToWebinar's** Questions tool to submit questions to our panel.

Send to “Organizers” and tell us if it’s for a specific panelist.



Acknowledgments

Thanks to our sponsor:



aws marketplace



Barracuda®

To our special guest: David Aiken and Tim Jefferson

And to our attendees, thank you for joining us today!