Security Operations in the Cloud
Monthly Webinar Series
How to Build a Data Security Strategy in AWS

Sponsored by

aws marketplace
Today’s Speakers

- Dave Shackleford – SANS Analyst
- David Aiken – AWS Marketplace, Solutions Architect
Introduction

• CSA’s Top Threats to Cloud #1 Concern: Data Breaches
  – Is that any different from our in-house concern?
• We’ll need to protect our sensitive data in the cloud.
  – Best practices, regulatory requirements, etc.
• We have more controls and capabilities than ever before.
  – Maturity for data security controls and architecture is growing rapidly.
What We’re Doing in the Cloud

• We’re storing more sensitive data than ever in the cloud:
  – Business intelligence data (48%)
  – Intellectual property (48%)
  – Customer personal data (43%)
  – Financial business records (42%)

• 54% have seen privacy regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) impact existing or planned cloud strategy.

Source: SANS 2019 SANS Cloud Security Survey
Data Security: Data Classification

- Classifying and tracking data is becoming more critical in the cloud than ever.
- Amazon Macie uses machine learning to identify sensitive data:
  - Provides organizations with dashboards and alerting tools that provide visibility and insight into how this data is being accessed or moved
- Amazon Macie can send data to Amazon CloudWatch and AWS Security Hub, too.
Data Security: Encryption

• For data at rest in the cloud, organizations have several major types of encryption to consider:
  – File/folder encryption
  – Full disk encryption for cloud workload storage volumes
  – Specialized encryption (database, email)
  – Cloud-native storage encryption
• Each has pros and cons.
Data Security: Encryption

- Amazon makes site-to-site encryption simple with IPSec VPN connectivity to a virtual private gateway (VPG) object within a customer’s virtual private cloud (VPC).
  - Some organizations may need customized hardware platforms and even acceleration solutions.
  - AWS Direct Connect is a dedicated circuit (not encrypted).
Data Security: Encryption

• The AWS Key Management Service (KMS) is a robust encryption key storage and management service.
  – All major storage types within AWS can be integrated directly with AWS KMS.
  – Heavily audited.

• AWS CloudHSM is a full HSM that you can provision on FIPS 140-2 Level 3 validated hardware.
Data Security: DLP

- Data loss prevention (DLP) has been challenging for many organizations to implement in the cloud.
- In addition to Amazon Macie, numerous network gateway DLP offerings and host-based products can be implemented.
Data Security: Life Cycle Controls

Data can be recovered from AWS physically, too, by using the Amazon Snowball or Amazon Snowmobile services.
Data Security: Monitoring

- The need to monitor user access to data has grown exponentially in recent years as a result of account compromise, insider threats and many more attack vectors.
- Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect customers’ AWS accounts and workloads.
Security Control Changes

- Cloud provider SLAs and data availability/resiliency guarantees are now a part of your shared responsibility strategy.
- Secure transport of data is critical across certain data paths.
- Use of cloud-native data security controls is likely a requirement.
- Emphasis on Bring Your Own Key (BYOK) and better encryption oversight will be paramount.
- Technology needs to work internally and in the cloud in some cases.
Example: S3 Security

• **Data access:**
  – **IAM policies**—User/group/role-based access control to storage buckets
  – **Bucket policies**—Policies applied to a specific S3 bucket and nowhere else
  – **ACLs**—Bucket- and data-specific access controls for users/groups
  – **Query string authentication**—REST-based access key strings that can be passed to AWS for access control

• **Access logs:** All Amazon S3 access and activities can be logged to a separate bucket for collection and analysis.
Example: RDS Access Controls

• **DB Security Groups**—Similar to AWS EC2/VPC Security Groups, these are network ingress controls that allow access only to the database port(s) needed and do not require a restart of the database instances running.

• **IAM permissions**—Can be used to control which Amazon RDS operations each user can call.
Summary

• Securing data in the cloud is easier than ever, largely because of the plethora of cloud-native controls and tools available.

• Encryption, access control and monitoring are all available readily within the AWS Cloud.

• Tracking sensitive data access is possible at scale with services like Amazon Macie, and monitoring all user behaviors (for data access and more) is easily done with Amazon GuardDuty.
Resources

• SANS Reading Room: www.sans.org/reading-room
• What Works: www.sans.org/critical-security-controls
• NIST CSF: www.nist.gov/cyberframework
• AWS Marketplace: https://aws.amazon.com/mp/security/
• AWS Cloud Compliance: https://aws.amazon.com/compliance/
• Questions: q@sans.org
How to Build a Data Protection Strategy in AWS
AWS services that help secure data in relation to people

Identify → Protect → Detect → Respond → Recover

- **Automate**
  - AWS Lambda
  - Amazon GuardDuty

- **Investigate**
  - AWS Config
  - Amazon Inspector
  - AWS Macie
  - AWS Security Hub

- **Snapshot**
  - Amazon CloudWatch
  - AWS CloudTrail

- **Archive**
  - Amazon S3

- **Recover**
  - AWS Systems Manager
  - AWS Config

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Complete control over people accessing resources in AWS

AWS Identity and Access Management (IAM) can assist with:

- Fine-grained access control to AWS resources
- Multi-factor authentication for highly privileged users
- Managing access control for mobile applications
- Integrating with your corporate directory
Full visibility into people’s access & activities in your AWS environment

- AWS Security Hub is your single pane of glass for all user activities

- Barracuda Cloud Security Guardian will add a security layer at the data plane
Enhance cloud security with user-aware offerings

Cloud Security Guardian (CSG)
Barracuda CloudGen WAF
Barracuda CloudGen Firewall

AWS Module
Barracuda Module
Puppet Agents
Puppet Master
VPC
Auto Scaling group
Internet

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Improve user visibility into the larger picture

Barracuda Cloud Security Guardian provides:

- Protection at the data plane
- Complete visibility
- Continuous compliance and automated security
- Elimination of configuration drift
Secure web apps with dynamic profiling & controls

**Barracuda CloudGen WAF offers:**

- Data loss prevention
- Granular identity and access management
Deep app context & full user identity awareness

**CloudGen firewall enables:**
- Tight integration with cloud platforms
- Budget-friendly consumption models
- Secure, reliable branch-to-cloud connectivity
- Central management of security at the source

![Diagram of CloudGen firewall setup](image-url)
Protection at the application level
Application security through a self-service, cloud-based solution

Business Impact:
Barracuda assisted Club Automation with a safe workload migration to AWS, protecting private subnets from unauthorized access. This has given them the confidence to move their full production environment to AWS.
Protection at the storage level
Scanning, discovery, & alerts keep S3 buckets clean & private

Business Impact:
Symantec helped Snapper reach its S3 storage security goals by automatically scanning all files when they are uploaded, downloaded, or modified.
Protection at the data level
Rapid, highly accurate discovery & classification of sensitive data

Business Impact:
Reduced review and remediation time of heterogeneous, unstructured data by 80%.
Why AWS Marketplace?

Flexible consumption and contract models

Quick and easy deployment

Helpful humans to support you

“If it had not been for AWS Marketplace, it would have taken a couple weeks before I even had the software installed on my side, because I would have to find a vendor, ensure their credibility, obtain quotations, and the proof of concept license.”

Chandrasekaran Hari
Cloud Solutions Architect, MatchMove
How can you get started?

Find and try a variety of free trials

- **Barracuda CloudGen WAF for AWS**
  - Free 30-Day Trial

- **Symantec Protection Engine for Cloud Services**
  - Free 30-Day Trial

- **Data Classification, Protection & Loss Prevention (DLP)**
  - Free 30-Day Trial
Webinar summary

- Securing data in the cloud is easier than ever, it’s a matter of combining the right controls and services to meet business and operating requirements.

- AWS Services can help optimize your data security program.

- Current tools? Check out AWS MP for assurance that what you know works in AWS.

- New tools? Pick vendors that know AWS and offer bleeding-edge capabilities.
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

To our special guest: David Aiken

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