aws marketplace

SECURITY

Understanding and Analyzing Emerging Cloud Security Trends

Dave Shackleford
Senior Instructor and Analyst, SANS Technology Institute
and Owner/Principal Consultant, Voodoo Security

In collaboration with

SANS

Today's Speaker

Dave Shackleford – SANS Analyst

Today's Agenda

Analyst Program

- Introduction
- Trends in Core Cloud Infrastructure and Architecture
- Identity and Access Management
- Cloud Threat and Vulnerability Management
- Looking Ahead

Introduction

- Over the course of the past several years, we've seen a number of major shifts in the realm of cloud security
  - Major cloud providers are improving security controls available to consumers
  - There's also been a significant increase in focus from the security community on cloud security
  - Sadly, most cloud security incidents relate to lack of oversight or poor configuration of cloud assets and services

Trends in Core Cloud Infrastructure and Architecture

Analyst Program

- As PaaS and IaaS deployments grow, consumers have a number of new security requirements and responsibilities
- These include:
  - Cloud network detection and response
  - Tuning workload detection and response
  - Cloud infrastructure for “zero trust”

Cloud Network Detection and Response (NDR)

Analyst Program

- NDR in the cloud has evolved significantly
  - Traffic monitoring and visualization
  - Risk scoring and reporting
  - Forensics and response + automation
  - Threat hunting
- Cloud native options for monitoring include VPC flow logs and traffic mirroring
- Numerous mature 3rd-party solutions today, as well

Cloud Endpoint Detection and Response (EDR)

Analyst Program

- Many EDR vendors have adapted their agents to be very lightweight and supported in all cloud platforms
- Core capabilities should include:
  - Continuous threat monitoring and incident detection
  - Incident response
  - Threat intelligence collection/dissemination
  - Forensic evidence acquisition
  - Threat hunting
- PaaS will usually require different models of deployment
  - Provider integration is integral

Detection & Response

Planning for Cloud Workload Security

Analyst Program

1. Ensure that periodic reviews of the overall risk posture within cloud environments are performed
2. Keep system instances in the cloud as locked down as you can
3. Pay careful attention to privilege allocation and user, group, and role management associated with workloads
4. Commit to a culture of continuous monitoring
5. Discuss vulnerabilities detected in cloud deployments with all team members
6. Discuss the changing threat landscape with DevOps teams

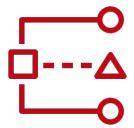
The Cloud and "Zero Trust"

- More like "trust minimization" in two areas:
  - Brokered access **to** cloud services (SASE/SSE)
  - Privilege and network access controls within the cloud
- Workloads can enforce some types of microsegmentation
  - Security groups, service mesh, agent-based solutions
- Plan for service and asset alignment to better facilitate cloud-based zero trust policy creation and enforcement

Identity and Access Management

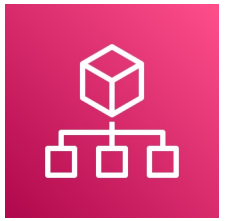
- One of the most important aspects of cloud security is identity and access management (IAM)
  - A core tenet of the AWS Well Architected Security pillar
- Defining roles, enabling strict access models and limiting the resources available to users and systems is a critical step in enabling a sound cloud security strategy overall
- Centralization of IAM both **to** the cloud and **within** the cloud is ideal

IAM Relationship Mapping



- Organizations need to successfully map cloud user and service relationships to create the most restrictive privilege models needed
  - One tool that can help is AWS Access Advisor, which shows AWS services allowed by the assigned IAM policy, policies assigned that grant specific permissions and last access times
  - AWS IAM Access Analyzer, a feature within AWS Identity and Access Management (IAM), performs a more thorough analysis of privilege models in use

Least Privilege: AWS Accounts



- As an isolation and segmentation technique, each account is a completely isolated set of resources that can be configured to access resources in other accounts
- AWS Organizations is a service that organizations can use to define policies and guardrails to apply across multiple AWS accounts
  - With AWS Organizations, you can create service control policies (SCPs) that really govern the use of other IAM policies

Multi-Account Architecture

- Setting up and configuring multi-account architecture has long been considered challenging and complicated, especially for large organizations
- A sample multi-account framework to start from called a "Landing Zone" has been in place for years
- Control Tower can automatically deploy a multi-account starting architecture.
  - Create and implement defensive guardrails like AWS Config monitoring rules, infrastructure-as-code definitions in AWS CloudFormation, strict identity policies that restrict permissions and privileges across accounts, etc.

Cloud Threat and Vulnerability Management

- A trend we see growing in 2023 and beyond is a significant emphasis on cloud vulnerability and threat management. This will largely focus on attack surface management (ASM) and cloud security posture management (CSPM)
- ASM can help organizations discover and track exposed assets
- CSPM tools can assess the actual control plane of the cloud environments in use for compliance assessment, operational monitoring, DevOps integrations, risk identification, and risk visualization

Key Considerations for ASM/CSPM

- When evaluating any sort of ASM/CSPM solution, security teams should look for key features that a mature service offering should provide :
  - Configurable and automatable remediation capabilities
  - Custom policy and rules engine enforceable across a multi-account environment
  - Integration with DevOps tools and provider APIs
  - Detailed and configurable reporting

Looking Ahead

Analyst Program

- In 2023 and beyond, we see a variety of trends that will be likely to grow and continue:
  - Cloud workload detection and response platforms that are more intuitive and tuned to cloud environments and potential attacks/threats
  - Cloud network detection and response that takes advantage of packet mirroring and other strong access controls and monitoring available in large Paas/IaaS environments
  - Major focus on identity and access management, especially centralized monitoring and control of identities and privileged identity control and oversight
  - A trend toward zero trust within the cloud, aligning and focusing assets and workloads/applications based on a principle of least privilege and access minimization
  - Cloud posture assessment tools for analyzing and remediating control plane security configurations and exposed asset vulnerabilities
  - Improvements in privileged user management in and for the cloud

How can you get started?

Find

Strengthen your portfolio, predict risk, accelerate fraud detection, and augment advisory services all from a single destination, AWS Marketplace: https://aws.amazon.com/marketplace/solutions/security/

Learn more about SANS Institute: https://www.sans.org/

Buy

Through flexible purchasing options:

- Free trial
- Pay-as-you-go
- Budget alignment
- Bring Your Own License (BYOL)
- Private Offers
- Billing consolidation
- Enterprise Discount Program
- Private Marketplace

Deploy

With multiple deployment options:

- SaaS
- Amazon Machine Image (AMI)
- CloudFormation Template
- Containers
- Amazon Elastic Kubernetes Service (EKS)
- Amazon Elastic Container Service (Amazon ECS)
- AI/ML models
- AWS Data Exchange

Summary/Key takeaways

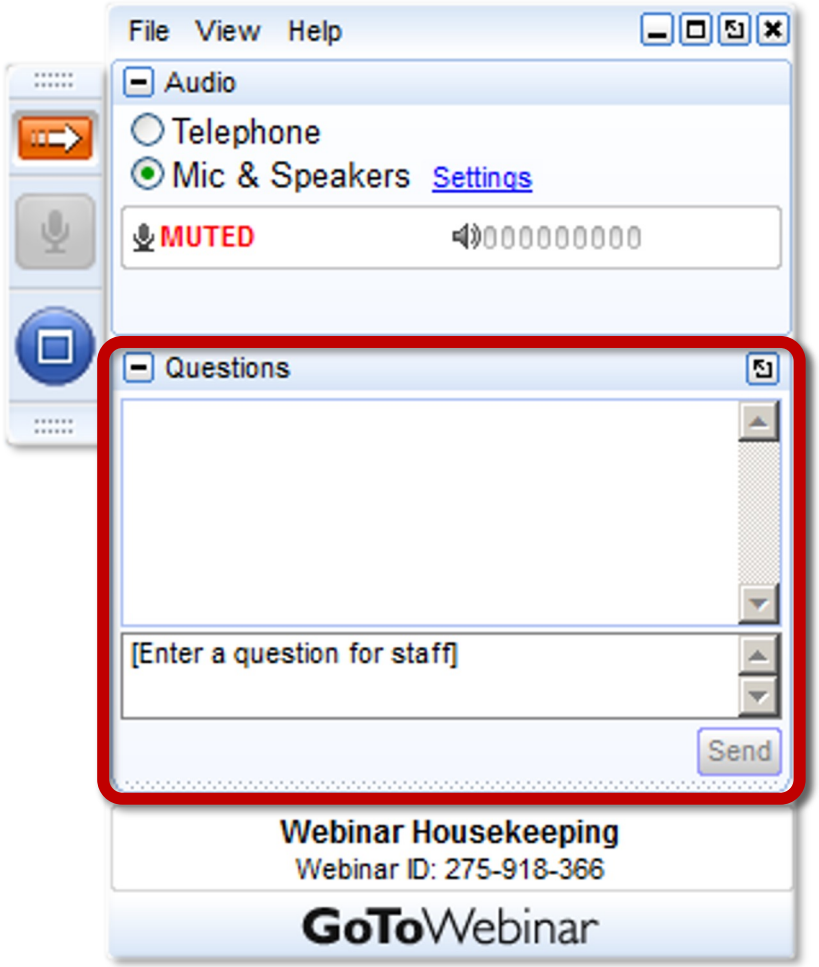
The six emerging security trends for 2023:

- Maturing network detection and response in the cloud
- Tuning endpoint detection and response for cloud workloads
- Cloud infrastructure growing as a critical element of Zero Trust architecture models and controls
- Maturing cloud identity and access strategies
- Improving privileged user management in the cloud
- Increases in focus on cloud attack surface management and posture management

Q&A

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

Send to "Organizers" and tell us if it's for a specific panelist.



aws marketplace

Thank you!

In collaboration with

SANS