

05/05/2025



## Securing Live Cloud Production

Content: Bryan Samis, Principal SA

As Voiced By: Thomas Edwards, Sr. Mgr. SA  
AWS Media & Entertainment, Games + Sports



## Security is top priority

“Protecting your customers should always be your number one priority, and it certainly has been for AWS...

from both an operational perspective as well as tools and mechanisms; it will forever be our number one investment area.”

*- Dr. Werner Vogels, CTO Amazon*



# Shared responsibility model

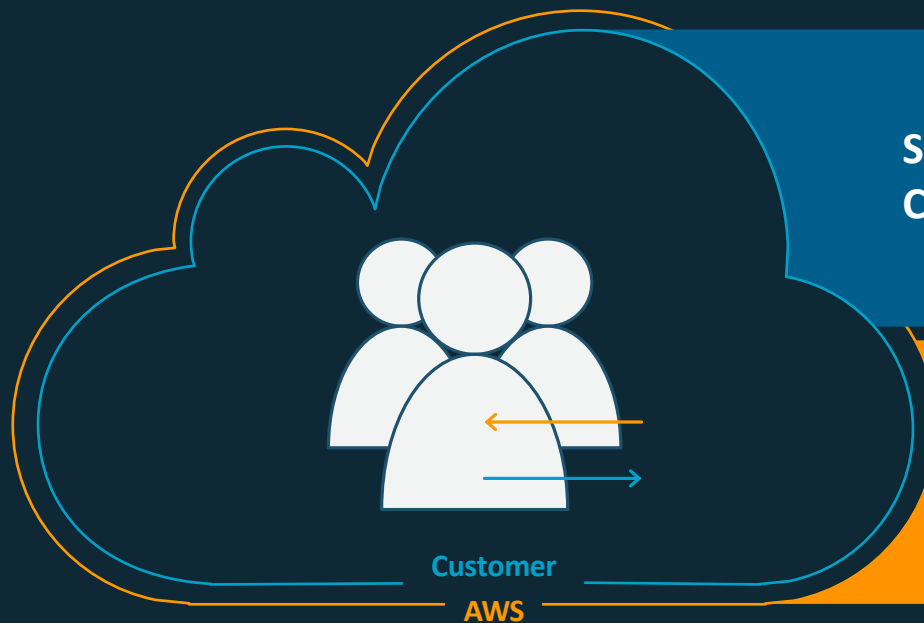


## Security IN the Cloud

Customer responsibility will be determined by the AWS Cloud services that a customer selects

## Security OF the Cloud

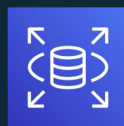
AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud



# The line **varies** ...



Amazon EC2

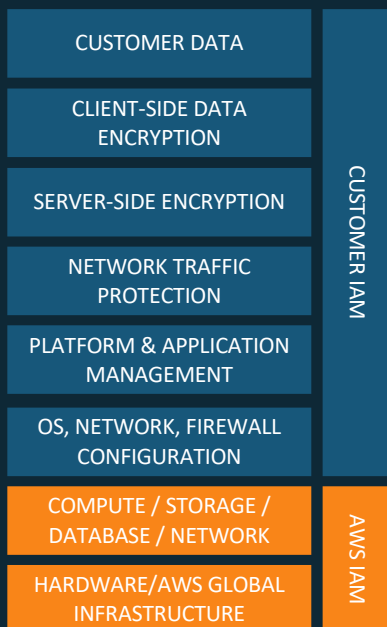


Amazon RDS

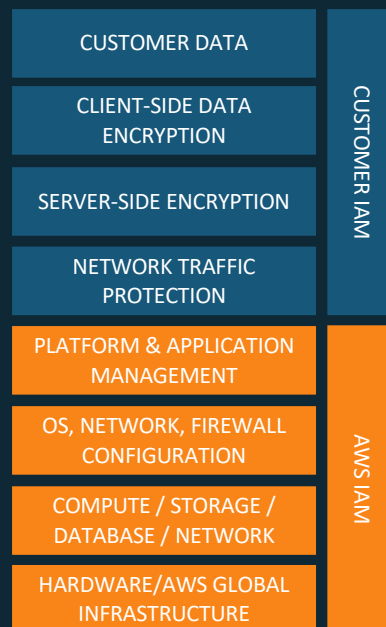


S3

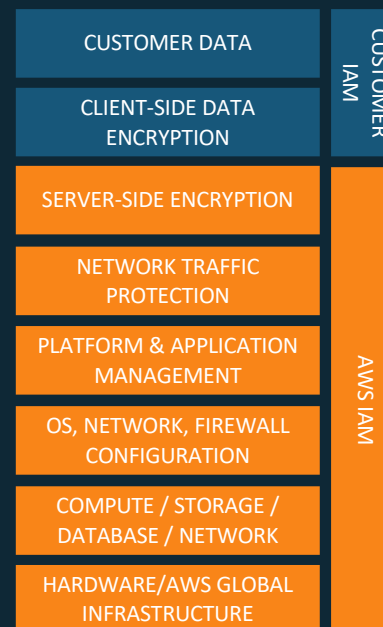
More Customizable  
+  
More Customer  
responsibility



Infrastructure  
Services



Container  
Services



Abstracted  
Services

Less customizable  
+  
Less Customer  
responsibility  
+  
More best practices  
built-in



# AWS security, identity, and compliance solutions



## Identity & access management

- AWS Identity & Access Management (IAM)
- AWS IAM Identity Center
- Amazon Cognito
- AWS Verified Permissions (preview)
- AWS Directory Service
- AWS Resource Access Manager
- AWS Organizations



## Detection

- AWS Security Inspector
- Amazon GuardDuty
- Amazon Macie
- Amazon GuardDuty (preview)
- AWS CloudTrail
- AWS CloudWatch
- IoT Device Defender

aws  
certified

Security

SPECIALTY



## Data protection

- Amazon Macie
- Amazon Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Secrets Manager
- AWS Private Certificate Authority
- AWS Artifact
- AWS Audit Manager



## Incident response

- Amazon Detective
- AWS Elastic Disaster Recovery
- CloudEndure DR



# State of Live Cloud Production

- Live Production in the cloud is growing in popularity – as is the complexity of deployed workloads
- Tier 1 productions have multiple components, from multiple vendors, running the same environment
- How to secure it all in the cloud?

# Live Cloud Production Examples

- Sky Sports' Women's Netball



- European League of Football



- Lega Pro Serie C

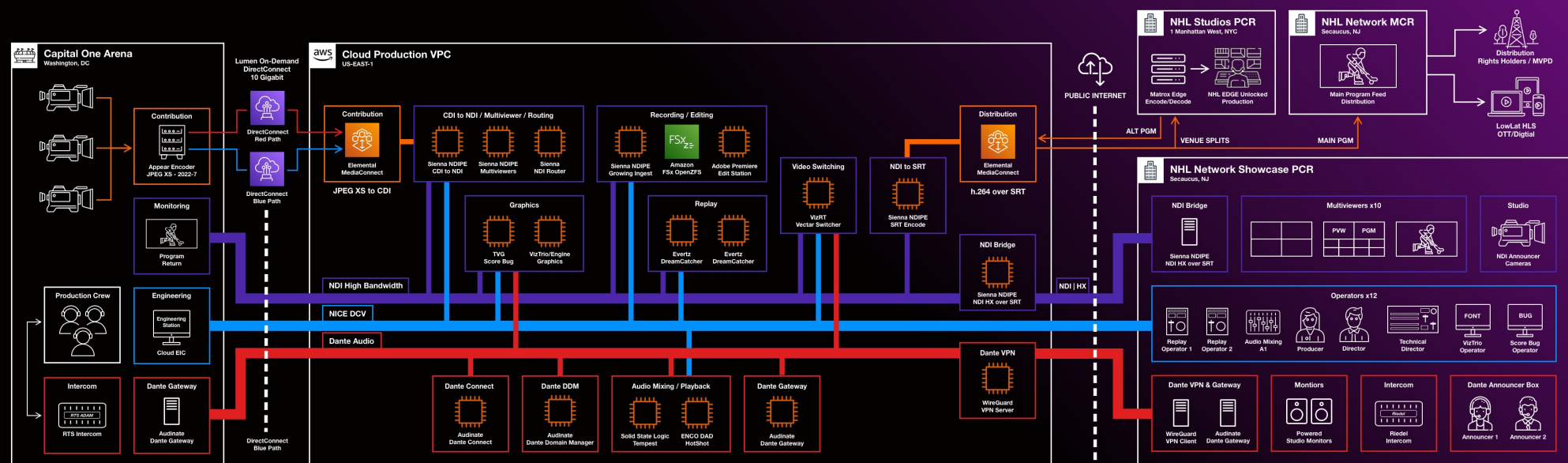




# Multi-vendor, High-tier Sport Live Cloud Production

NHL Network Showcase

## Live Cloud Production on AWS

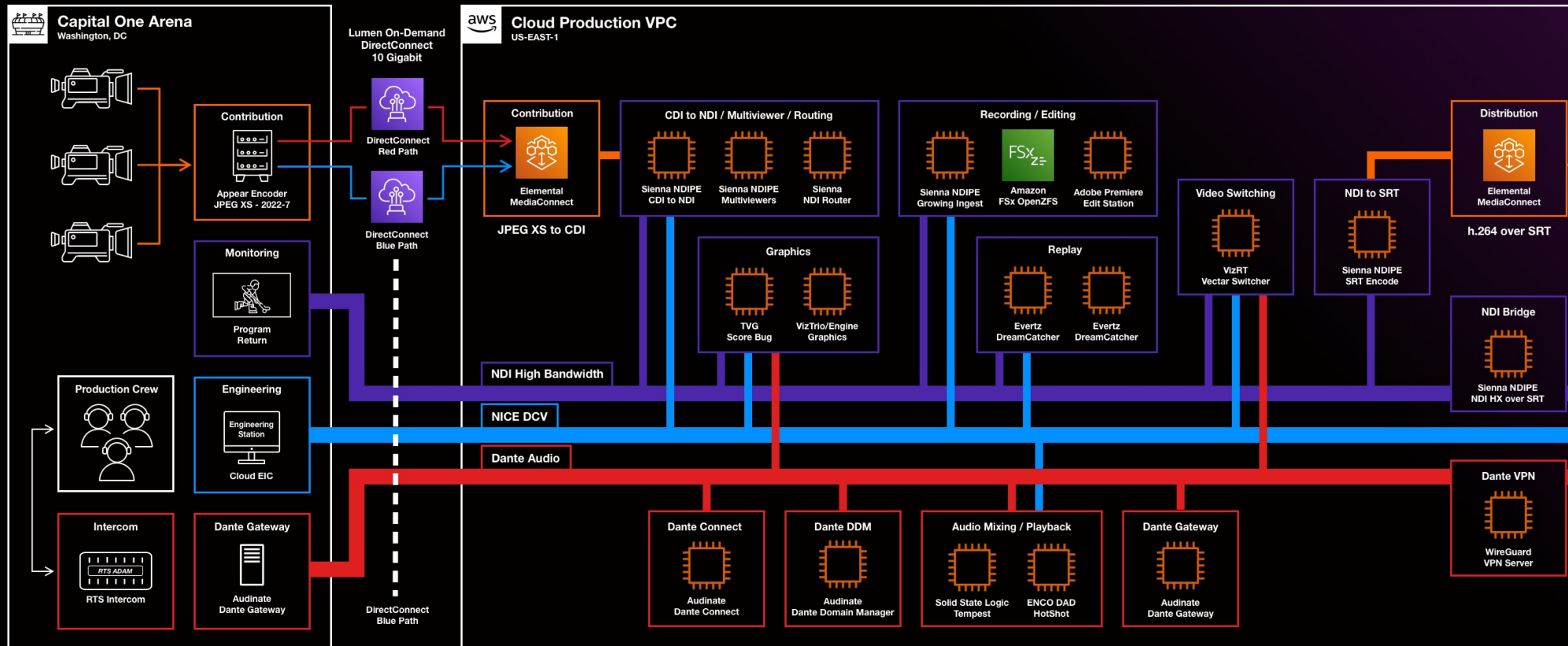


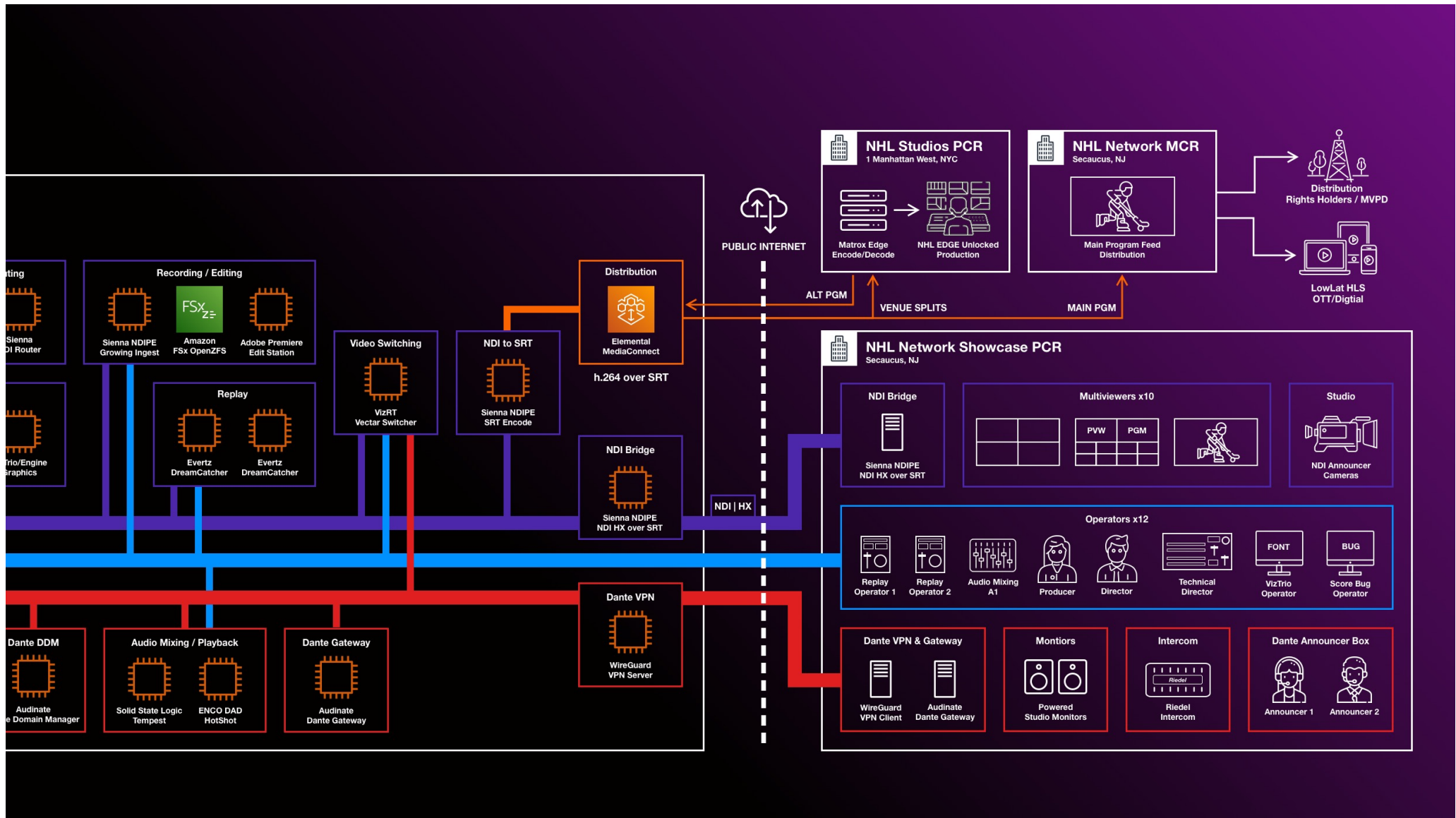
© Copyright VSF 2024  
Confidential



## NHL Network Showcase

# Live Cloud Production on AWS





# AWS Well-Architected Security Pillar

- AWS Well-Architected Framework provides guidance on best practices in architecting AWS workloads.
- The Security Pillar provides a set of design principles & guidance surrounding areas such as:
  - Identity and access management
  - Detection
  - Infrastructure protection
  - Data protection
  - Incident response
  - Application security



<https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html>

# Security Challenges in Live Cloud Production

- Securing infrastructure
  - Securing application access
  - Securing audio/video protocols
- 
- Satisfying corporate IT



# Challenges: Infrastructure

- Security best practices are to frequently update systems with security patches
  - Can we update critical on-air systems? How often? When?
  - What testing is required?
  - Need vendors to provide & bless updates
  - Balancing good security posture with 24x7 seamless operations
- Common security agents (antivirus, endpoint security & management, logging and monitoring) can interfere with real-time operation
- Vendors sometimes ship software as machine images running outdated operating systems
- Vendors sometimes do not allow modifications or access to underlying operating system





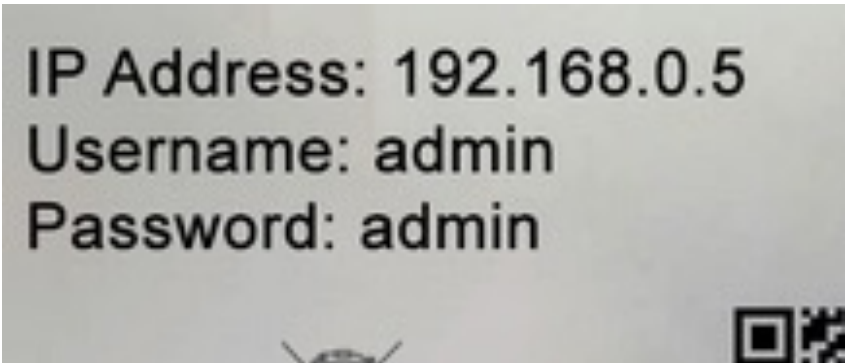
## Challenge: Application Access

- How many times have you seen this in our industry?



## Challenge: Application Access

➤ Or this?



IP Address: 192.168.0.5  
Username: admin  
Password: admin



## Challenges: Application Access

- Many broadcast applications do not follow IT best practices for securing access
  - Unencrypted protocol for logins
  - Do not support Single Sign On / MFA
  - Do not enforce credential complexity or rotation
- Workflows often involve credential sharing or reuse
- Balance right authentication for purpose:
  - 24 x 7 monitoring consoles vs. authenticated logins that can break things



# Challenges: Audio/Video Protocols

- Many audio/video transport protocols used in LCP designed to be used on flat, isolated AV networks
- NDI network ports... “5960 **and up**”
  - That's 59,575 ports that need to be opened between machines

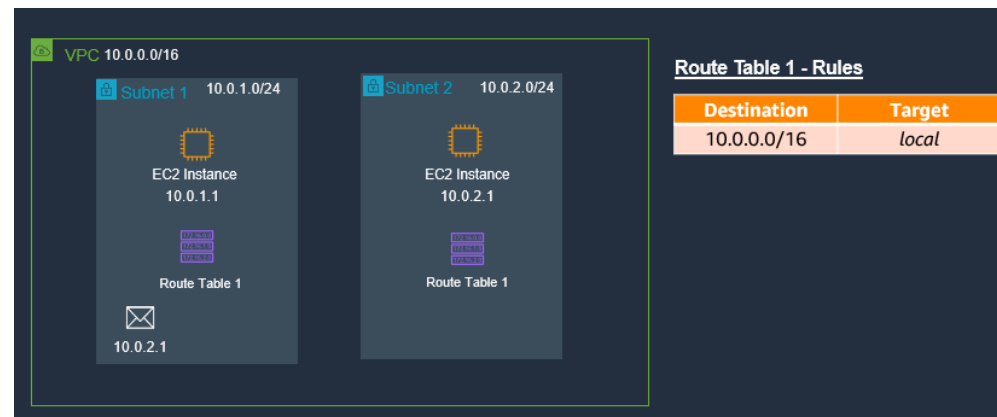
NDI Related Network Ports

Port number	Type	Use
5353	UDP	This is the standard port used for mDNS communication and is always used for multicast sending of the current sources onto the network.
5959	TCP	NDI Discovery Server is an optional method to have NDI devices perform discovery. This can be beneficial in large configurations, when you need to connect NDI devices between subnets or if mDNS is blocked.
5960	TCP	This is a TCP port used for remote sources to query this machine and discover all of the sources running on it. This is used for instance when a machine is added by an IP address in the access manager so that from an IP address alone all of the sources currently running on that machine can be discovered automatically.
5961 and up	TCP	These are the base TCP connections used for each NDI stream. For each current connection, at least one port number will be used in this range.
5960 and up	UDP	In version 5 and above, when using reliable UDP connections it will use a very small number of ports in the range of 5960 for UDP. These port numbers are shared with the TCP connections. Because connection sharing is used in this mode, the number of ports required is very limited and only one port is needed per NDI process running and not one port per NDI connection.
6960 and up	TCP/UDP	When using multi-TCP or UDP receiving, at least one port number in this range will be used for each connection.
7960 and up	TCP/UDP	When using multi-TCP, unicast UDP, or multicast UDP sending, at least one port number in this range will be used for each connection.
Ephemeral	TCP	Legacy to NDI v1 - The current versions (4.6 and later) no longer use any ports in the ephemeral port range.

Source: NDI Networking Best Practices Whitepaper

# Are these challenges unique to the cloud?

- Same threats exist on premises, less scrutiny
  - Broadcast often exists in an “island” that is not subject to IT security audits or compliance
- What about SaaS services?
  - Same issues, but onus on vendor to architect their application securely
- As customers mature in the cloud, many IT departments are enforcing compliance with security best practices, vulnerability scanning, least privileged access, network firewalls, etc.
  - Even though it's possible to build a VPC environment that's just as “isolated” as the on-prem broadcast island!



# The Elephant in the Room: Broadcast Vendors

- Need to do a better job of taking security seriously
- Some vendors shipping software images on old, unsupported operating systems
  - Recently saw a vendor product using Ubuntu 18, which went end of support in 2023
  - Some products still use CentOS 7 which stopped receiving updates in 2024
- When urgent / 0-day security vulnerability patches are released, vendors are often slow to validate and test patches with their software
  - Broadcast vendors typically have slow software release cycles
  - But IT departments might require critical patches to be applied within days or weeks!
  - Maybe vendors could use automated testing techniques to speed up releases?
- Vendors challenged because every customer has their own IT compliance/security requirements which may be different from each other
  - Opportunity to form industry set of best practices that customers can agree to accept?

**EBU** **R 143**  
CYBERSECURITY RECOMMENDATION  
FOR MEDIA VENDORS' SYSTEMS,  
SOFTWARE & SERVICES

**R 160**  
VULNERABILITY MANAGEMENT  
FOR MEDIA COMPANIES AND  
MEDIA SYSTEM VENDORS



## How AWS Handles this Problem

- AWS Elemental Media Services need to be highly available but also compliant with AWS' stringent security requirements, including numerous compliance/audit requirements
- MediaLive and MediaConnect are built with concept of “channel maintenance”
- When OS or application software needs updating, customers sent notice via e-mail or the Personal Health Dashboard that their channel is due for maintenance
- Customer can accept the default maintenance window, or manually schedule their preferred time
- Channel will automatically restart to apply the required updates within that maintenance window
- Two-pipeline MediaLive “standard channels” are restarted one pipeline at a time to avoid outage due to restart (with downstream failover)

## How AWS Handles this Problem

- Whenever channels start, they start with the latest updates/patches automatically applied
  - So maintenance is not a problem for short-lived channels, only for 24x7 ones
- Customers can opt to manually restart the channel at their convenience to get the latest updates rather than waiting for the maintenance window
- This system is not perfect – it still requires a brief, scheduled interruption
- But it ensures that AWS Media Services resources are always up-to-date with the latest security patches, software updates, drivers, etc.

# Best Practices



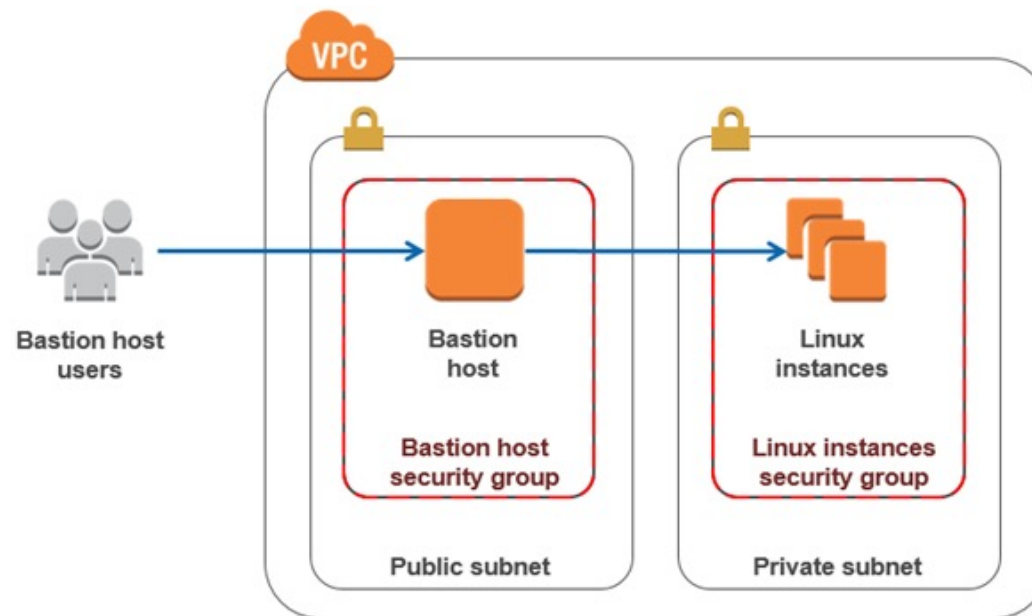
# Some AWS Services to Know About

- AWS Systems Manager
  - Helps you manage EC2 instances & on-premises servers securely at scale
  - Securely connect to node OOB without opening inbound ports, bastion hosts, or manage SSH keys
  - Automate operational commands at scale – like security updates
  - Gives visibility across your entire fleet
  - Parameter store – for passwords, database strings, license codes etc. as plain text or encrypted data. Can be referenced by Systems Manager automation workflows, and can use Secrets Manager for rotation
- AWS Secrets Manager
  - Rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle
  - Accessible via API
- AWS Identity and Access Management (IAM)
  - Fine-grained access control to specific AWS service APIs and resources
  - IAM Users use their sign-in credentials to authenticate with AWS
  - IAM Roles provide short-term credentials for users, workloads, and AWS services to perform actions in your AWS accounts
- Security Groups
  - Virtual firewall that controls inbound and outbound traffic to EC2 instances

# Best Practices: Infrastructure

- Run up-to-date operating systems with latest security patches applied
  - Use tools such as AWS Systems Manager to automatically alert you to noncompliant resources
- Use Infrastructure-as-Code (IaC) to have replicable architecture
  - People building and re-building architecture at the Console are likely to make a mistake
  - CloudFormation / AWS CDK / Terraform
- Apply least-privileged access principle
  - Assign EC2 instances the minimum required IAM role permissions needed for their specific function (e.g., if an EC2 only needs to read from one S3 bucket, scope the role to just that bucket/action)
  - Use condition statements in IAM policies to further restrict access by IP range, time of day, or requiring MFA where applicable
  - Place EC2s in private subnets by default unless public internet access is explicitly required
  - Configure security groups and NACLs to allow only necessary ports/protocols from specific source IPs/security groups (e.g., only allow SSH from a bastion host, only allow SRT traffic from a contribution encoder)
- Do not allow direct access to SSH/RDP – utilize Systems Manager or a Bastion/Jumpbox
  - Ideally with SSO access
  - And don't use passwords – SSH keys are much safer!

# Bastion Host



## Best Practices: Infrastructure

- For real-time, complex environments like LCP, software updates and patches might require extensive testing both by your vendor and by your own teams before being used “on-air”
- Establish an update cadence to properly test and be confident in updates before applying them, while still maintaining a reasonable security posture
- Depending on the nature of your business or production schedule, could be monthly, quarterly, biannually, or even annually.
  - Depends on your risk acceptance and compliance requirements
- Don't store credentials directly in software or on your instance – utilize IAM Roles, and tools like AWS Secrets Manager or Parameter Store for securely storing credentials
  - For example, for accessing files in S3, use an IAM role that grants access via temporary credentials vs. storing API keys in your software

# Best Practices: Operator Access

- Change default passwords
  - Each operator should have their own credentials
  - Operators should use an approved password manager to store credentials
  - Use SSO/MFA where possible
- Only allow access to application from trusted networks
  - Use host firewalls, Security Groups to restrict access to admin/user interface or APIs
  - Operators access via corporate network or VPN
- Enable encryption in transit if your application supports it
  - e.g. HTTPS/TLS for web interface
- For VDI access applications, use protocols that support encryption in-transit
  - e.g. NICE DCV (uses HTTPS/TLS), RDP (uses RC4)

## Best Practices: Audio/Video Protocols

- For protocols that require a range of open ports (ie, NDI), use self-referential Security Groups applied to instances that need to send or receive traffic
  - Create a new Security Group called “NDI Traffic”
  - Create an ingress rule to allow traffic on the required range of ports from the same Security Group (“NDI Traffic”)
  - Apply the security group to any instance in your VPC that needs to send or receive NDI traffic
  - Only instances that are part of your NDI network can access the NDI ports on your systems
- For protocols like SRT, create selective Security Groups to only allow traffic only from the expected source on the expected port
  - Utilize SRT Password Encryption if needed

# Detect Security Threats

- AWS CloudTrail
  - Track user activity and API usage
- VPC Flow Logs
  - For network interfaces in VPC, subnet, or individual network interface
  - Publish to S3 bucket – can SQL query with Athena
  - Or publish to CloudWatch



## Best Practices: Satisfying Corporate IT

- Don't be afraid to push back – ask them what the purpose of a particular requirement is, and if there are other ways it can be mitigated
- Negotiate! They might insist that you update systems weekly – you can offer quarterly as a compromise
- Security can follow the principle of **Defense in Depth**
  - Multiple layers of security ensure that a single vulnerability or misconfiguration cannot be exploited
  - Example: New 0-day vulnerability gives attacker root access by sending a command to a specific port
    - Defense #1: Instance in a private subnet – can't be exploited directly from the internet
    - Defense #2: Instance has Security Group/firewall/NACL that blocks exploit port (since not needed for workflow)
    - Defense #3: Instance IAM role only allows the minimum permissions required for task (e.g. read file from S3 bucket)
  - In this scenario, actual risk of this vulnerability to your system is very low because following the other best-practices has mitigated an attacker's ability to use this exploit.
- Work with your IT team to balance updating and patching requirements with workflow & production requirements, while maintaining security

Thanks for your attention!





**Thank you**

vsf.tv