
Microsoft

Secure VFX in the Cloud

Burst rendering, storage, and key management

Microsoft Azure

Joel Sloss, Microsoft
Board of Directors, CDSA

Agenda

No premise for On-Premises

Is it safe?

On Being “Internet-connected”

Architectures, Workloads, & Workflows

Deployment and Configuration

Security Controls

And then, in real life …

HD, 2K, 4K, 6K, 8K, HDR, 3D, VR, …

So … you want to touch (big) studio content …

How will you handle the next-generation of content?

What is your infrastructure costing you today? Tomorrow?

What happens when you run out of capacity? Or bandwidth? Or time?

Can you compete? (Do you have the talent but not the infrastructure?)

Is your security up to the task? Can you prove it?

No One Can Hear You Scream

You want collaborative workflows with people anywhere in the world

You're not 100% safe, regardless

It's about understanding and remediating your risks, planning for recovery

Move your risk to someplace better equipped to handle it

- How big is your security staff? Budget?
- Compare that to your cloud vendor

Mind the Gap

An air-gap != security

Policies < zero without enforcement

Encryption is useless if you have a simple password

Having a firewall doesn't help if it is misconfigured

Eventually, you'll be forced to use hosted services—what then?

Treat the cloud as an extension of your work environment

- PCoIP
- Or start fresh as cloud-native

Key to Scaling

Hybrid is okay … you don't have to abandon ship

"Bursting" to the cloud gives you scale and control

Tools exist to manage deployment / provisioning / de-provisioning

Orchestration engines help simplify and automate

Pay-as-you go, zero capital expenses—dump it all when you're done

Cloud-ported tools for front-end, PCoIP, …

Do It Securely

How to protect studio content

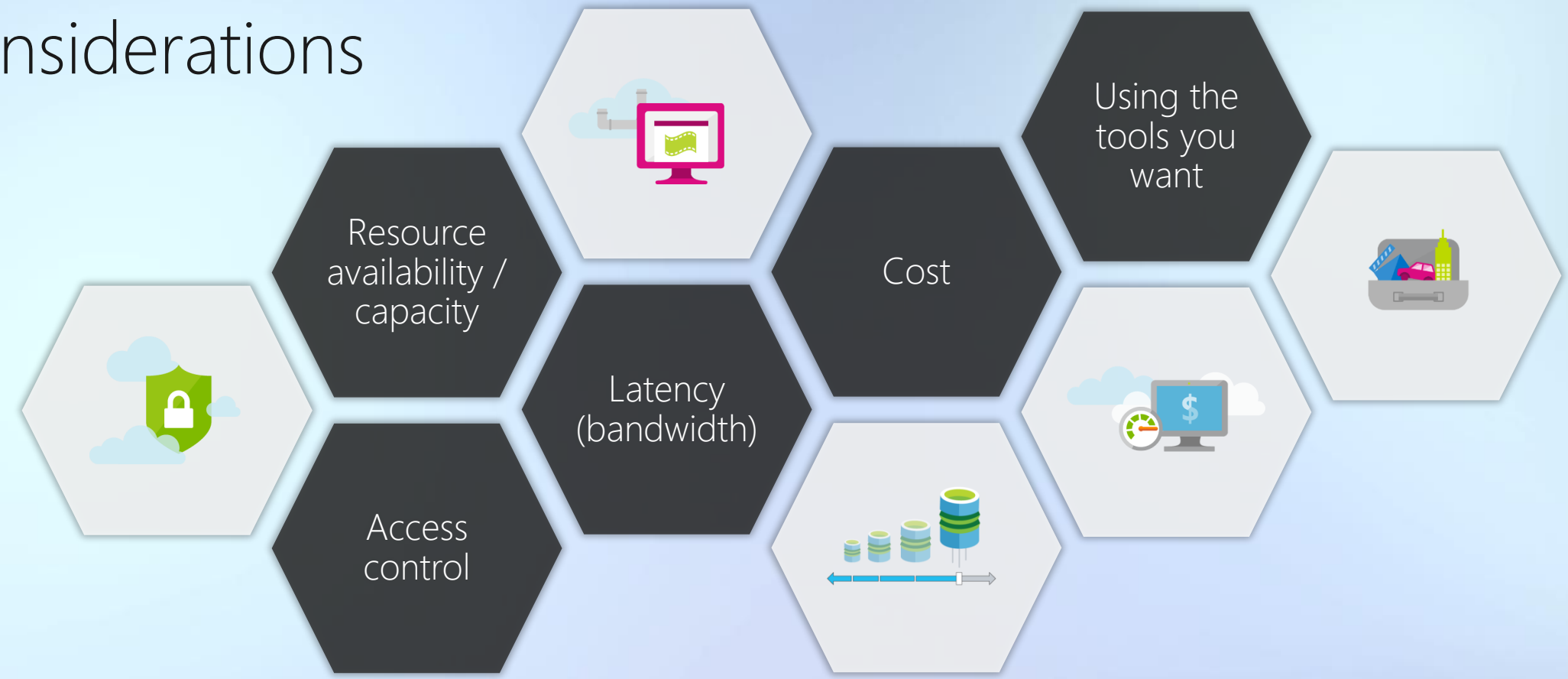
Prove it: monitoring, logging, auditing—big part of complying with standards

Heed the lessons of the past (Sony, Larson, …)

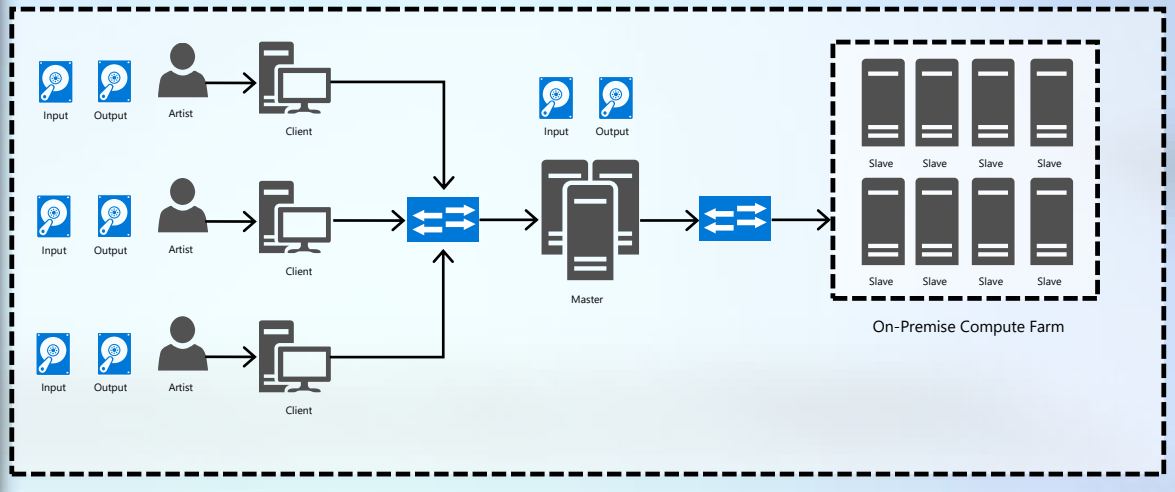
Risk-based approach

http://aka.ms/azurehardeningguide

Considerations



In Brief: On-Premises Security



Typically relies on "air-gap" isolation (w.r.t. Internet) to prevent access

- Increasingly seen as insufficient and impractical given the range of threats
- E.g., mobile devices / USB, lack of scalability, obfuscation!= security

Network

- Separate (V)Nets / segmentation per production
- Firewalls / router ACLs to control traffic; whitelisting inbound/outbound IPs
- Close ports to the Internet (administrative, RDP, SSH); VPN for any remote connection
- Centralized update service (e.g., WSUS) for secure distribution

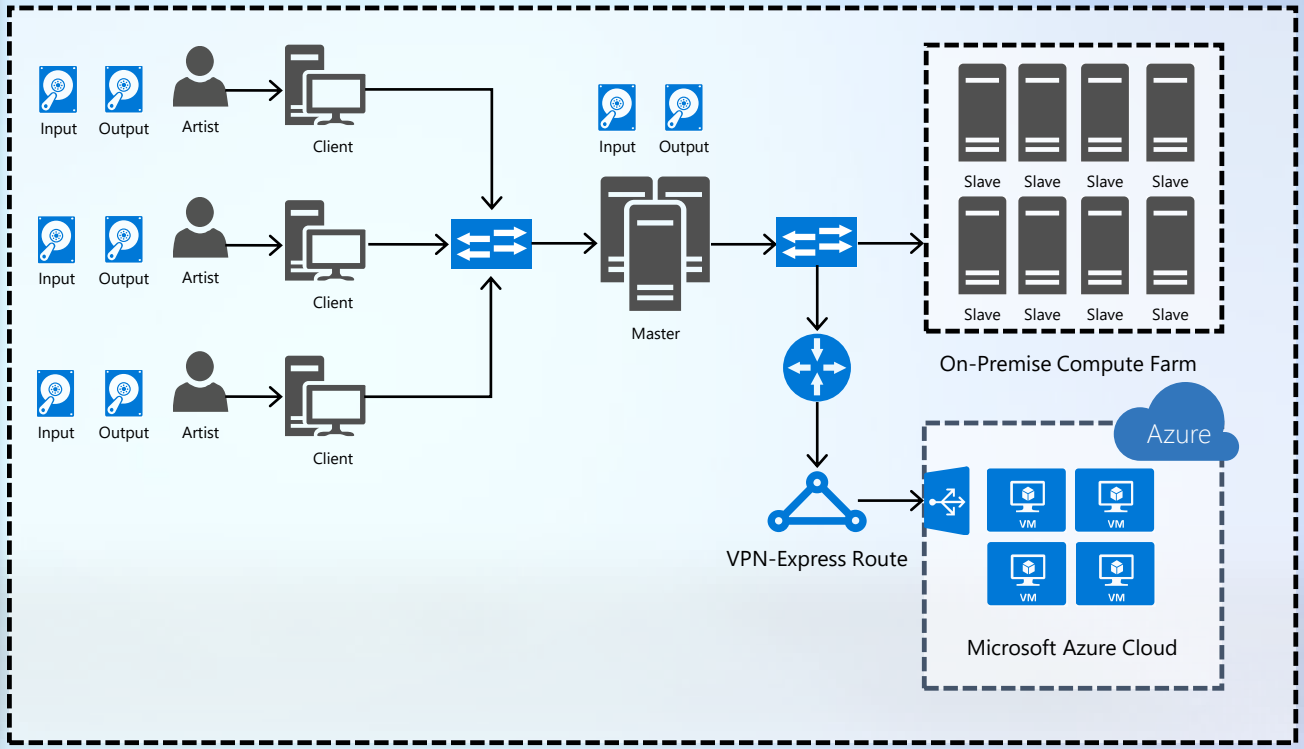
Identity

- Active Directory (or LDAP+Kerberos) with centralized provisioning
- Group Policies or automated configuration management (Chef, Puppet, …)

Monitoring / alerting

- Log all system activities—especially administrative (success and failure)
- Monitor nodes for activity (usage, etc.)—indicates potential problems

Hybrid Security



You still need to control your on-prem environment

What changes?

- Greater flexibility
- Assumption of Internet connection
- Increased focus on system hardening
- Can use cloud-based security resources

Controls

Use a hardened image for render nodes

Cloud Resource Groups simplify render pool management

Group storage, VMs, Vnet, virtual appliances, and IAM as a single resource per-production

Master and slave nodes should be a uniform Network Security Group

Segment master and slave nodes into front-end and back-end subnets

Secure connections between on-premises nodes and the cloud

Use a P2P data link (e.g., ExpressRoute) and VPN

Deploy an application layer firewall for any externally-facing subnets

Bridge network segments with a firewall (virtual) appliance

File transfer protocols should use TLS v1.2 and above (i.e. SFTP)

Restrict connections by source-IP ranges

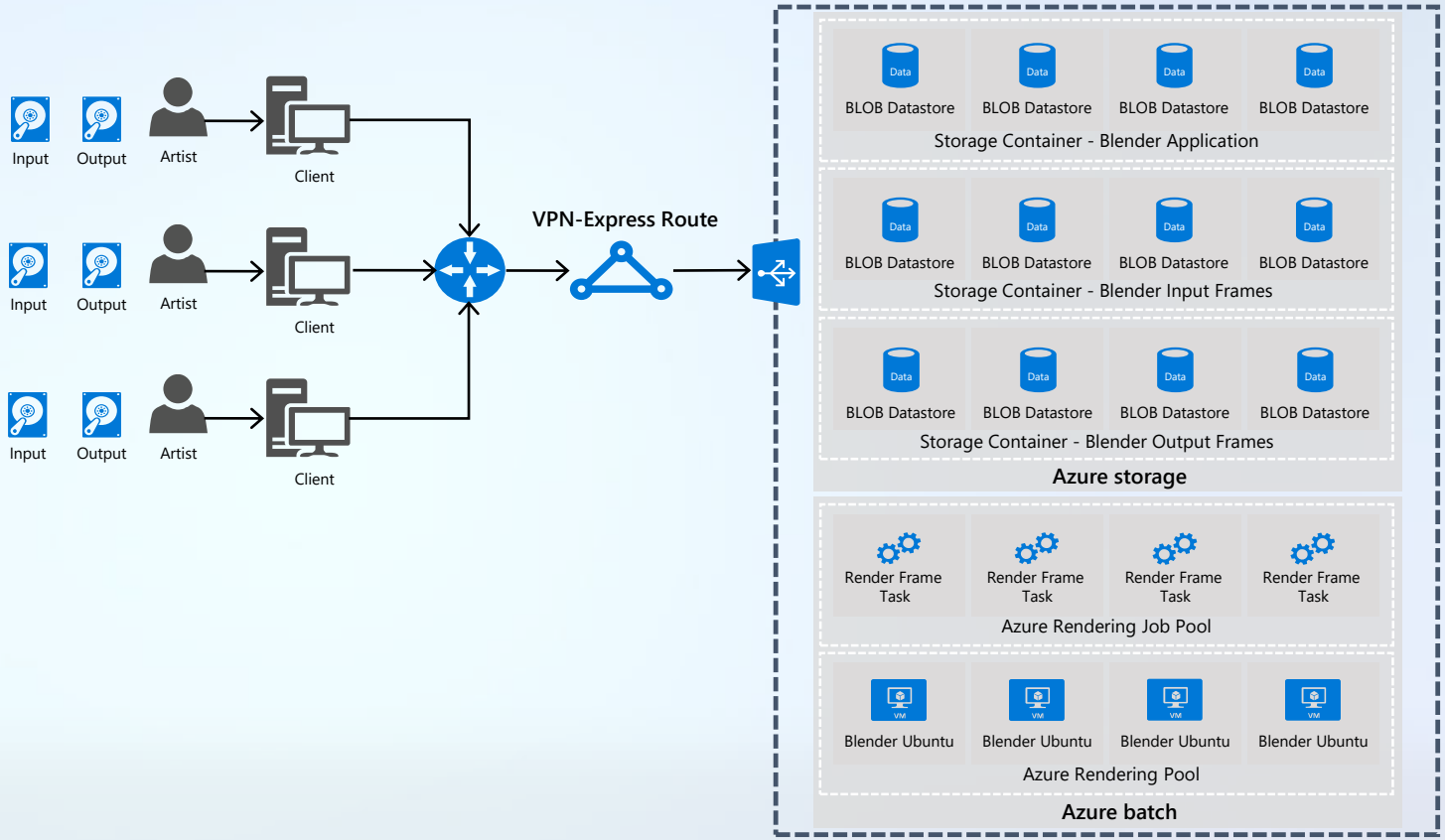
Harden the protocol / product to protect pre-release media assets

Securely distribute SSH host key fingerprints; ensure users verify them

Disable shell access and port forwarding

Use asymmetric key authentication in place of password authentication

Ensure client software effectively verifies server hostname and certificate



Cloud-Native Security

Instantiate separate storage containers for input, output and application files

Instantiate batch application services with a security evaluated trusted software package

- Ensure the application is up to date and patched

Implement a centralized monitoring management scheme for the batch processing

- Monitor application performance, access, users, and data traffic

Restrict data sharing between storage containers

- Use a network security group or resource handler,
- Set up IAM roles to control access to storage from associated rendering nodes

Security Controls

Virtual Networks

Azure Batch

Resources

Key Vault

Virtual Networks

Create separate VNETs for each production

Restrict input-endpoint configurations / VMs

Use Network Security Groups

Limit default communications

Segment networks

Isolate appliances on their own subnet
Apply a multi-tiered architecture
Deploy firewalls between networks

Use TLS / VPN

Do not use deprecated cryptography

Azure Batch

URLs	Use obfuscated URLs for Batch account URLs
Keys	Periodically update access keys
Accounts	Sanitize and destroy old batch accounts when not needed
Storage	Create storage exclusively for specific batch workflows
Applications	Use a security validated application package for batch workflow
Workflows	Use integrity checks on application packages for batch workflow
Monitoring	Hold workflow if Batch applications fail
Logging	Log Batch events for monitoring and diagnostics

Resources

Storage	Use Shared Access Signatures to access object storage account resources Periodically rotate Storage Access Keys
Compute	Configure virtual machines for authentication via public key Use hardened OS images to provision VMs Avoid caching session information in when using Azure command-line Sanitize all cloud and local resources at the completion of production
RBAC	Assign custom roles to manage access to automated users Integrate on-premises IDM to manage access to cloud services

Azure Key Vault

Use	Use permissions to manage access
Segregate	Segregate data and key / secret owners
Manage	Manage access to keys and secrets on a per-key/secret basis
Audit	Periodically rotate keys
Rotate	Audit all key management activities
Restrict	Restrict access to Key Vault using Network Security Groups

The How

Products and services

Microsoft Azure

- Azure ExpressRoute
- Azure Storage
- Azure Virtual Machines
- Azure Virtual Network

Questions?

Thank you!