HARDENING GUIDE

Virtual Desktop Infrastructure Workflows

Microsoft Azure

Revision 1

July 2020

Executive Summary

Microsoft has engaged Independent Security Evaluators (ISE) to review Virtual Desktop Infrastructure (VDI) architectures using the Microsoft Azure cloud computing environment and to establish an Azure-specific hardening guide for the media and entertainment (M&E) industry.

The M&E industry wishes to use Azure with both its internal and vendors' software systems to increase the throughput, security, scalability, and cost-efficiency of its film production activities while improving the deployment's security posture. This document is intended for administrators who may be deploying VDI systems and describes hardening steps specific to that workflow as well as general guidance that can be applied to any Azure deployment.

These security controls were developed after hands-on evaluations of relevant Azure services and access to all publicly available documentation. This guide is current as of July 2020. Changes to Azure after this date may invalidate certain recommendations or introduce new concerns. Furthermore, users are responsible for understanding their cloud deployments and associated security risks.

Overall, ISE recommends that studios consider the security controls described in this document and perform independent deployment assessments of individual asset management systems in the future.

Revision	Date	Description
1	July 2020	Initial hardening guide.

Table of Contents

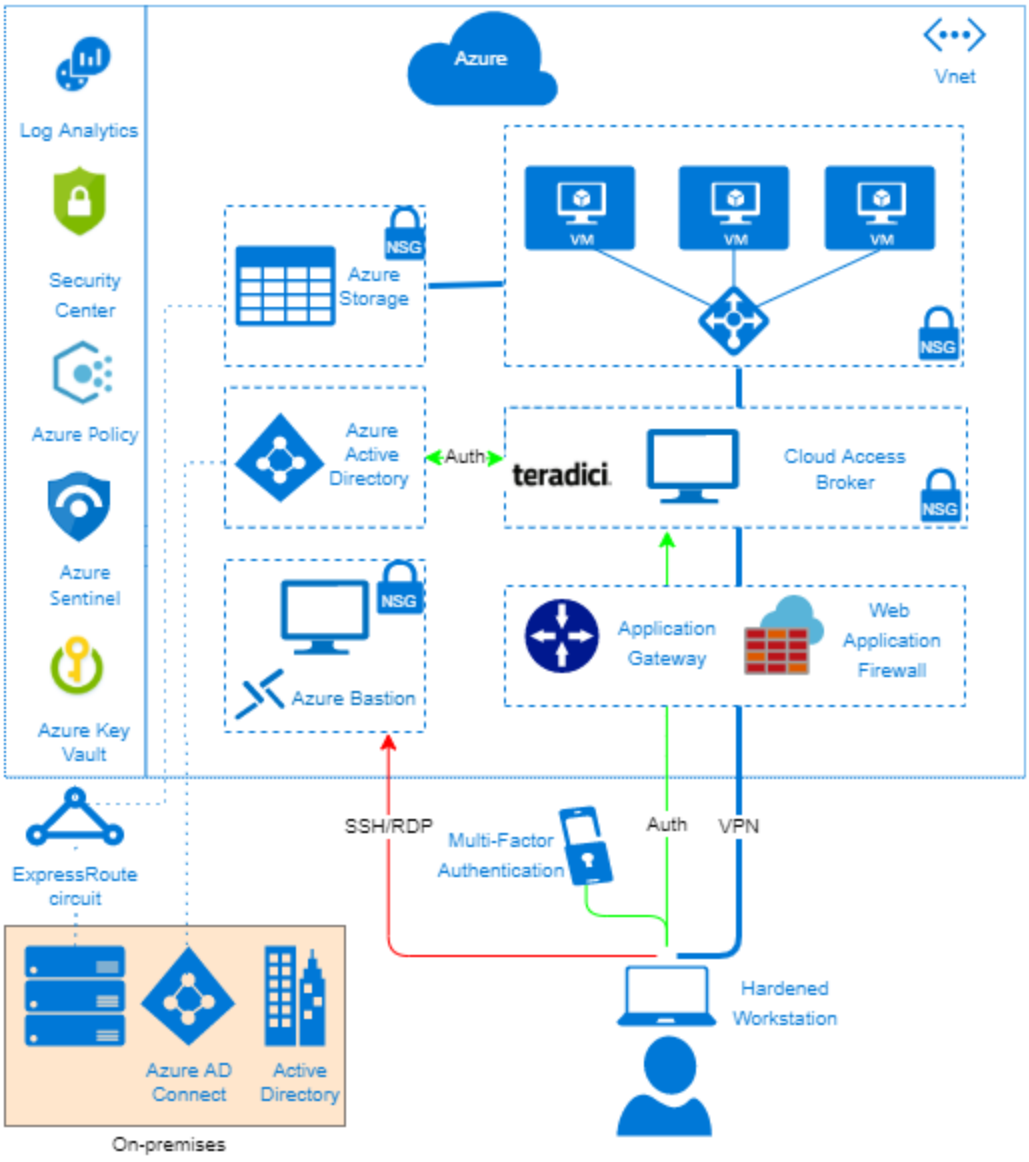
Introduction

Cloud virtual desktop infrastructure (VDI) uses virtual machines hosted in a cloud computing environment, such as Microsoft Azure, to provide and manage virtual desktops. VDI hosts desktop environments on a centralized server and deploys them to end-users on request. In VDI, hypervisors segment servers into virtual machines that, in turn, host virtual desktops. End users remotely access these desktops from their devices, and all processing is done on the host server. Users connect to their desktop instances through a connection broker, which is a software-based gateway that acts as an intermediary between the user and the server. Workflows that may benefit from VDI include a rendering of three-dimensional graphics, asset management, content post-production, and secure digital asset management.

Virtual desktop infrastructure offers several advantages, such as user mobility, ease of access, flexibility, and greater security. In the past, its high-performance requirements made it costly and challenging to deploy on legacy systems. However, the rise of hyper-converged infrastructure (HCI), particularly using cloud computing resources, offers a solution that provides scalability and high performance at a lower cost. Furthermore, with respect to media and entertainment workflows, data resides on the server rather than the end client device, a significant feature. This helps to protect data if an endpoint device is ever stolen or compromised.

Media and entertainment workflows utilize both persistent and nonpersistent VDI instantiations. Each type offers different benefits:

- With persistent VDI, a user connects to the same desktop each time, allowing users to personalize the desktop for their needs since changes are saved even after the connection is reset. Desktops in a persistent VDI environment act similarly to a dedicated personal computing device.
- Nonpersistent VDI, in which users connect to generic desktops and no changes are saved, is usually simpler and cheaper since there is no need to maintain customized desktops between sessions. Nonpersistent VDI is often used in organizations with a lot of task workers, or employees who perform a limited set of repetitive tasks and do not need a customized desktop.



Securing Azure VDI Workflows

For this hardening guide, Microsoft partnered with a VFX studio that uses Teradici, a virtual desktop platform, to provide ISE with a reference implementation of virtual desktop infrastructure. While the reference architecture uses the Teradici PCoIP solution for running a graphics intensive workflow, ISE provides security recommendations in this guide for a generic VDI deployment that may be used for workflows such as editorial and digital asset management. Teradici products were outside the scope of the evaluation; however, since they were used in the reference, they will be used as a baseline for discussion here. Alternatives to Teradici include Azure Windows Virtual Desktop, which provides secure, managed access to Windows desktops.

While out of the scope of this document, Microsoft provides their own security best practices for that service in their Azure documentation[1].

The Teradici PCoIP protocol is a lossless pixel transfer between the client and the agent. Pixels are transferred over the Internet as a compressed and encrypted stream. There is no local storage or caching of either the session or the login credentials.

The Teradici PCoIP system consists of two parts: an agent running on the Azure virtual machine host which encodes the PCoIP stream, and a client entity which renders the stream for interactive remote machine experience for the end-user. There are hardware and software-based agents available. The hardware based remote station agent card sends data to the user. The software-based agent runs on Windows or Linux Azure VMs and encodes then sends the PCoIP stream. In this evaluation, ISE evaluated the software-based agents.

Strategic Recommendations

Preparation and Planning using Azure Tools

When planning for VDI deployment, studios and media producers should consider using an HCI environment as HCI's scalability, and high performance are a natural fit for VDI's resource needs. In addition to infrastructure considerations, follow the best practices listed below when implementing VDI:

Configure environment using a secure workstation: When creating an Azure environment, use a hardened client device to access the Azure Portal and CLI.

Build network templates using Azure Template: Since VDI performance is so closely linked to network performance, it's important to know peak usage times and anticipate demand spikes to ensure sufficient network capacity.

Utilize Azure logging and monitoring to detect performance issues: Perform capacity planning in advance using a performance monitoring tool to understand the resources each virtual desktop consumes and to calculate overall resource consumption needs.

Utilize Azure Cloud resources to pilot test: Windows Virtual Desktop and Teradici offer testing tools that allow customers to run a test VDI deployment beforehand. This testing can be used to ensure resources have been configured correctly.

Consider using acceleration and caching services: In order to improve the performance of certain VDI workflows, consider using services such as Avere vFXT. Consider the following recommendations when using Avere vFXT:

- All Avere vFXT resources should be deployed in their own resource group.
- The Avere vFXT cluster and the cluster controller VM nodes should have a separate administration user account outside of the scope of any workflow.
- The Avere vFXT cluster and the cluster controller VM nodes should only be accessible through a Bastion host. Do not use Avere vFXT controller node as the jump host; instead, use a dedicated bastion host.
- Avere vFXT cluster nodes should not be assigned a public IP address.

[1] https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide

- Use a point-to-site or site-to-site VPN from a private network to Azure vFXT nodes for all data communication unless using dedicated lease line connection such as ExpressRoute.
- Use a separate Blob Storage account for Avere vFXT deployment.
- Configure Network Security Groups (NSGs) for the Service Endpoint for backend storage — the NSGs should be configured to deny all outbound internet traffic by default unless needed. It should be noted that default NSGs allow outbound Internet traffic, so this default configuration should be examined and reviewed prior to deployment.
- If needed use service tags in the NSG to allow only traffic to specific Azure services. Use a separate Blob Storage account for Avere vFXT deployment.
- Log and monitor all resource activity associated with Avere vFXT resource group including monitoring Avere service level run-time issues, Avere VM nodes, Avere subnet traffic logs, and Avere storage account.
- Always manually check the Avere deployment configuration after installing Avere vFXT from the Azure Marketplace. Check the deployment logs, created resources and security center for any associated security risks.
- For Avere node authentication, use SSH public key authentication for connecting to the controller.
- The Avere controller password should be created as per local administrator policy or as recommended by NIST 800-63. Do not reuse any other password for the Avere controller password.

Secure Authentication

Use valid certificates: When a connection is first made to a GPU Virtual Machine as launched with these instructions, whether it be a Windows or CentOS cloud virtual machine, if a self-signed certificate is used, a warning is returned, which may result in an error message. To implement secure authentication, utilize Microsoft Azure Vault or certificate management.

Utilize multi-factor authentication (MFA): Authentication in the Teradici software client app uses password authentication and leverages the authentication provided by the host system – Windows or Linux. Passwords alone are widely recognized to be a relatively weak form of authentication. Authentication based on multiple factors – something you know (password), something you are (biometrics), or something possessed (key, device, etc.) – results in stronger authentication. ISE recommends that at least two-factor authentication be used with any remote workflow.

Configure password policies: ISE recommends that user-supplied password policies be created and enforced from a central management system, perhaps the Teradici Management Console. We recommend using the password policies in the NIST SP800-63 (section 5.1.1 of 63b[2]) document as a baseline.

Management of Client Software

Restrict access by client software: Teradici provides the PCoIP Management Console to manage a variety of settings, however this only works for hardware-based solutions. Anyone with login credentials to the virtual workstation can use the client software to connect to the VM. In general, administrators should be able to specific restrictions such as by whom, how, where, and when the VM may be used, and these policies should be enforceable by the connection solution.

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Encryption Between Agent and Client

Encrypt data in transit: Data transferred over the Internet should be protected using robust encryption. Teradici PCoIP specifies 256-bit AES. ISE recommends evaluating any system that transfers graphics. Topics of this evaluation should include key creation, exchange, and use; usage of any involved cryptographic algorithms; and the protocols being used. For example, auditors should ensure systems utilize cryptographically secure algorithms like the aforementioned AES-256 and avoid broken algorithms such as DES.

Audit

Log administrative activity: VDI environments should include auditing capabilities for administrative activity and system events to help respond to outside attacks should they occur.

Log data access events: Data access logs should be enabled for all users. This will help improve auditing against insider threats.

Log VNet traffic: VNet traffic logs should be enabled for virtual desktop servers.

Log VDI software activity: VDI software, such as Teradici, activity should be logged using operating system logging functionality.

Resource Management

Label resources appropriately: The reference implementation addressed resource labeling at the time of compute resource creation but did not highlight the benefits of labeling resources as a cloud deployment is scaled up. As deployment scales up, resource labeling can be useful in tracking cost, usage, management, and logging/monitoring schemas. Resource labeling is a highly effective method to group together with resources that are related to or associated with each other. ISE recommends that Azure VDI deployments label resources as a method to organize and track resources across an account or project.

Template Usage

Utilize templates for deployments: The reference implementation depicts an Azure-based native VDI solution. Unfortunately, the free-form deployment of resources can lead to configuration errors and may result in security vulnerabilities. Resource templates or automation can be used to instantiate new resources or workloads to avoid such issues. For resources that are repeatedly deployed in similar configurations but in disjoint workflows across multiple projects, the resource templates will ensure a consistent and known state. Automated deployment can provide easy configuration and, therefore, security by default. It is recommended the cloud deployment manager or similar automated deployment technologies to deploy resources consistently, securely, and robustly.

Deploy pre-configured environments with Azure Blueprints: Azure Blueprints offers several pre-defined sample configurations that adhere to various compliance and regulatory standards. VDI architects should consider using a secure foundation provided by Azure Blueprints when deploying their environment.

Azure offers a Blueprint designed for Motion Pictures Association (MPA) compliance called “MPAA Audit” that ISE reviewed during the creation of this hardening guide. The MPAA Audit Blueprint has several artifacts that require security-enhancing features of other Azure services to be enabled. Some artifacts are focused on Windows virtual machines and SQL Server databases and customers using other platforms will need to add additional artifacts that correspond to their technology stack. MPAA Audit also features a number of parameterized artifacts that require system administrators to manually configure secure values.

The MPAA Audit Blueprint, and other premade Blueprints, can be found under Azure Policy → Blueprints. System administrators should manually review Blueprint templates before they are used to ensure the artifacts being applied are appropriate for their environment.

Data Sanitization

Sanitize data when shutting down desktops: Sensitive user data should be purged when a machine is no longer needed. Azure Compute supports running shutdown scripts that execute commands right before an instance is terminated or restarted. Shutdown scripts are especially useful for instances in a managed Virtual Desktop Infrastructure (VDI) cluster.

Log sanitization script output: Sanitization scripts should log events to the system log or to a centralized logging system.

Separate Control and Data Users

Assign access by role: Virtual workstation administration and data owners must have mutually exclusive permissions to data stored on the compute and storage resources. Specifically, administrative users should have appropriate access via identity management to perform workstation setup and management but not have access to data stores attached to the device. Conversely, end-users should not be able to manage VDI infrastructure or other resources.

Harden Operating System Images

Configure images before use: Operating system images need to be configured properly before use. Some default configurations of OS images expose sensitive surfaces, have an increased attack surface due to additional running services, or lack other security hardening steps such as their SSL/TLS configurations set up for maximum compatibility, rather than security. Administrators should perform hardening steps, including closing unused ports (e.g., FTP, SSH), uninstalling unnecessary applications, updating software, configuring web servers using current best practices, and setting firewall rules.

Recommendation-TPN-Service Mappings

The following table maps ISE's recommendations to a draft version (current as of June 2020) of the Trusted Partner Network's (TPN) control categories and a suggested Azure service to fulfil that recommendation.

ISE Strategic Recommendation	TPN Category	Azure Service
Use valid certificates	Access Control	Azure Vault
Utilize multi-factor authentication	Access Control	Azure Active Directory
Configure Password Policies	Access Control	Azure Active Directory
Restrict Access by client software	Access Control	Azure Active Directory
Encrypt data in transit	Cryptographic Controls	Multiple
Log Administrative Activity	Auditing & Logging	Azure Active Directory
Log data access events	Auditing & Logging	Azure Storage
Log Vnet Traffic	Auditing & Logging	Azure Virtual Networking

Log VDI software Activity	Auditing & Logging	Multiple
Label resources appropriately	Security Planning	Multiple
Utilize templates for deployments	Change & Config Management	Azure Templates
Sanitize data when shutting down desktops	Data Protection	Azure Compute
Log sanitization script output	Auditing & Logging	Azure Compute
Assign access by role	Access Control	Azure Active Directory
Configure Images before use	Change & Config Management	Azure Virtual Machines

ISE Recommendation for Azure Security Controls	TPN Category	Azure Control
Utilize Secure Workstations to Access Azure	Access Control	Azure Active Directory
Extend Federated Identity Management for Access Control	Identity & Authentication	Azure Active Directory
Utilize the Custom Banned Password List	Access Control	Azure Active Directory
Restrict Access to Bastion Hosts	Access Control	Azure Bastion
Utilize Logging features	Auditing & Logging	Azure Bastion
Ensure Updated Node Agents are Used	System Integrity	Azure Batch
Isolate Jobs in Separate Batch Pools	Production Specific Controls	Azure Batch
Restrict Access to Azure Container Registries	Access Control	Azure Container Registry
Scan Images for Security Vulnerabilities	System Integrity	Azure Container Registry
Avoid Transferring Sensitive Data over the Public Internet	Data Protection	Azure Express Route
Use Separate Azure Storage Accounts for Media Service Accounts	Access Control	Azure Media Services
Define Policies that Ensure Compliance	Network Security	Azure Policy
Define a Security Response Plan	Security Awareness	Azure Security Center
Limit Security Center Data Collection	Data Protection	Azure Security Center
Enable Advanced Threat Protection	System Integrity	Azure Storage
Enable Encryption at Rest	Cryptographic Controls	Azure Storage
Periodically Rotate Access Keys	Access Control	Azure Storage
Protect Assets with Digital Rights Management (DRM)	Data Protection	Azure Storage
Require Secure Transfers	Data Protection	Azure Storage
Use Shared Access Signatures to Access Storage Account Resources	Access Control	Azure Storage
Ensure Disk Storage is Encrypted at Rest	Cryptographic Controls	Azure Virtual Machines
Ensure Virtual Machines are Patched Regularly	System Integrity	Azure Virtual Machines
Apply a Multi-tiered Architecture for VNets	Network Security	Azure Virtual Networking
Avoid Deprecated Cryptography for IPSec VPNs	Cryptographic Controls	Azure Virtual Networking

Configure Network Watcher-Configure Connection Monitor	System Integrity	Azure Virtual Networking
Configure Network Watcher-Configure Flow logs	Auditing & Logging	Azure Virtual Networking
Create Separate Virtual Networks for Productions	Production Specific Controls	Azure Virtual Networking
Enable DDos Protection	System Integrity	Azure Virtual Networking
Isolate Virtual Appliances Using Individual Subnets	Network Security	Azure Virtual Networking
Secure Connections to Azure Networks	Network Security	Azure Virtual Networking
Use Azure Application Gateway	Network Security	Azure Virtual Networking
Use Network Security Groups (NSG)	Network Security	Azure Virtual Networking

Azure Security Controls

Security controls, as outlined in the executive summary, are presented here for virtual desktop infrastructure systems running within Azure. They are grouped according to each specific Azure component and apply to both VDI and general Azure workflows.

These Azure-specific security controls consider the high-level architecture of the system within its operational context and offer recommendations for the hardening of that system. A description of each security control, recommendation, and where to find further documentation for each follows in this section.

Azure Active Directory

Extend Federated Identity Management for Access Control

Managing identity is as essential in Azure as it is on-premises. Studios use on-premises Active Directory (AD) systems to store directory data and manage communication between users and resources, including user logon processes, authentication, and directory searches. When scaling out virtual desktop infrastructure workflows to Azure in a hybrid deployment, the cloud resources are being used as an extension of the on-premises datacenter—in this scenario. Some applications require a domain controller to handle authentication and authorization.

Recommendation: Use the Azure Active Directory Service

Use an Active Directory service in the cloud. The Windows Server AD is running in VMs created using Azure Virtual Machines, and the AD VMs should be grouped into a virtual network connected to an on-premises datacenter using the Azure Virtual Network.

The virtual network carves out a group of cloud virtual machines that interact with the on-premises network via a virtual private network (VPN) connection, which allows the AD Azure virtual machines to look like just another subnet to the on-premises datacenter.

Documentation: Information about Azure Active Directory is described here: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-whatis.

Utilize the Custom Banned Password List

Compromised user accounts are a common cause of breaches and security incidents. Often, the source can be traced to an account using a weak password. To help mitigate this risk, administrators can set password policies and restrictions that prevent the usage of insecure passwords. Azure supports two forms of banned password lists that can aid this goal: a global banned password list that uses a Microsoft-curated compilation of exposed passwords, and a custom banned password feature. The custom list allows administrators to ban passwords containing words and phrases that may be easy to guess, such as the company's name.

Recommendation: Use the Custom Banned Password list

Azure administrators should configure a custom banned password list that blacklists easily guessable words or phrases. Consider the following suggestions:

- Company name and/or initials
- City, state/province, and country where the company is located
- Product and project names
- Names of software used in Azure environment

Documentation: Information about banned password lists is available in Azure's documentation: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad.

Utilize Secure Workstations to Access Azure

Secure workstations are hardened computers that are used for a single purpose, such as accessing Azure resources. These workstations should not be used to perform any other tasks such as general web browsing. Azure facilitates the creation and management of secure workstations using services provided by Azure Active Directory.

Recommendation: Configure Secure Workstations

Managed workstations dedicated to accessing Azure resources or VDI instances should be used by administrators and employees as possible. These machines should be restricted as much as possible to prevent using them for non-authorized purposes. Training should be given to employees on the use of these secure workstations.

Documentation: Azure provides detailed guidance on the enrollment and configuration of managed secure workstations here: https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-azure-managed-workstation.

Azure Bastion

Restrict Access to Bastion Hosts

Bastion hosts provide an entry point into a network and are typically used to connect to resources that have restricted access from public networks. As these machines have a critical role in network security, access to bastion hosts must be secured.

Recommendation: Limit Access to Bastion Hosts

Access to Azure Bastion hosts should be restricted to only users who require this access. Furthermore, firewall restrictions can be used to limit access to certain known IP addresses, such as the IP addresses for employee offices.

Utilize Logging Features

Proper logging can enable administrators to track who accessed what systems and are a vital piece of any audit strategy. Azure Bastion supports a feature called Diagnostic Logging that stores information about the users who accessed the service.

Recommendation: Enable Diagnostic Logging

Diagnostic logging should be enabled, and suitable retention policy for the logs should be configured. Diagnostic logging may allow administrators to investigate a security incident better if the attacker uses the Azure Bastion service during the attack.

Documentation: Information about Azure Bastion's logging capabilities can be found at https://docs.microsoft.com/en-us/azure/bastion/diagnostic-logs.

Azure Batch

Isolate Jobs in Separate Batch Pools

Azure Batch jobs within different pools are unable to view or communicate with one another. This may be useful if processing must occur in a manner that requires isolation.

Recommendation: Place Jobs Requiring Isolation in Separate Pools

Jobs performing processing that could benefit from isolation should be placed in separate batch jobs. For example, processing on media assets can be separated by production.

Ensure Updated Node Agents are Used

The Batch node agent is a software installed on virtual machines used in Batch jobs that provides an interface for controlling the virtual machine. Periodically, new releases of the node agent are released that contain new features and bugfixes.

Recommendation: Update Node Agents

Node agent updates can be applied by periodically reducing the size of pools to zero compute units. Administrators should back up any log files before performing this operation. Companies should document and implement a policy to perform this action on a regular cadence.

Documentation: Microsoft provides documentation on this procedure and others in their best practices guide for Azure Batch: https://docs.microsoft.com/en-us/azure/batch/best-practices.

Azure Container Registry

Restrict Access to Azure Container Registries

Azure Container Registries (ACR) store container images that can then be deployed using technologies such as Docker. As the Registries may house images containing proprietary or sensitive data, regulating access to ACRs is an important aspect of securing container-based workflows. To support this effort, ACR supports the use of firewall rules to control access to registries.

Recommendation: Use Firewall Rules to Control Access to ACR

Firewall rules should be created to restrict access to Azure Container Registries. When possible, access should be restricted to whitelisted IP addresses or networks.

Documentation: Microsoft provides documentation on ACR firewalls at https://docs.microsoft.com/en-us/azure/container-registry/container-registry-firewall-access-rules and https://docs.microsoft.com/en-us/azure/container-registry/container-registry-vnet.

Scan Images for Security Vulnerabilities

Containers typically bundle an operating system and applications and may contain vulnerabilities from their software and configurations. Using an automated scanner can help detect security flaws before the containers are used in production environments. Azure Security Center supports integration with ACR to scan images as they are uploaded to the registry.

Recommendation: Use the Security Center to Scan Images

Azure Security Center should be configured to scan images stored in Azure Container Registry. This automated testing may be used to detect common vulnerabilities affecting container images. It is important to note that automated scans do not replace manual audits and may not find all security vulnerabilities in an image.

Documentation: Information about scanning ACR images can be found at https://docs.microsoft.com/en-us/azure/security-center/azure-container-registry-integration.

Azure ExpressRoute

Avoid Transferring Sensitive Data over the Public Internet

While modern protocols with transport-layer encryption provide robust security that ensures the confidentiality and integrity of data in transit, for an additional level of security, consider transferring sensitive assets solely over ExpressRoute, a dedicated connection to Azure that does not use the public Internet.

Recommendation: Use ExpressRoute to Transfer Sensitive Data

Instead of using connections to Azure resources that travel over the public Internet and may be exposed to adversaries with privileged network access, utilize an ExpressRoute connection between on-premises data centers and Azure to transfer sensitive data.

Azure Media Services

Use Separate Azure Storage Accounts for Media Service Accounts

When a user creates an Azure Media Services (AMS) account, they either use an existing storage account or create a new storage account.

Recommendation: Use Separate Storage Accounts for Media Accounts

Use separate storage accounts for media accounts to logically different media assets. Assets in the storage account associated with the Media service will likely be shared with an audience or processed for a specific purpose. The content of the storage account associated with the media should only share a limited set of data that the user has explicitly marked for processing or sharing. The storage should be protected with guidance provided earlier in this document.

Documentation: Azure Media account setup is described here: https://docs.microsoft.com/en-us/azure/mediaservices/media-services-portal-create-account.

Azure Policy

Define Policies to Ensure Compliance

Azure Policy allows systems administrators to create compliance checks to ensure resources in their Azure environment follow those rules. To maximize benefits from this service, policies should be designed to provide company and industry guidelines, and best practices are developed.

Recommendation: Create Policies and Audit Compliance

Administrators should configure compliance policies that are tailored to their organization's virtual desktop infrastructure architecture and workflows. In addition, policies should be reviewed regularly to ensure that systems are in compliance with all policies.

Azure Security Center

Define Custom Security Policy

Using Built-in policies, the security center can continuously assess the configuration of the resources to identify security issues and vulnerabilities. The built-in policies cover primary security concerns around resource health, malware, access, and availability –to provide targeted coverage of concerns, custom policies should be defined. These custom security policies should focus on specific VDI systems designs.

Recommendation: Implement Custom Security Policy

Use workflow specific security policy to measure security compliance. General security compliance is a good start in gauging security posture, but it can lead to a false sense of security if not augmented with complete workflow-specific security policies.

Documentation: Information on creating custom Azure security policies is available at https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies.

Limit Security Center Data Collection

Azure Security Center collects and processes security-related data, including configuration information, metadata, event logs, crash dump files, and more to prevent, detect, and respond to threats. Azure security center retrieves data from sources, including other Azure services, network traffic, and resources deployed in Azure. Though the data is kept logically separate from data access controls, there is a large amount of contextual data that can provide sensitive information about the workflow or production or even possibly the content being produced. The user should understand and limit the data being provided security center, continuously remove the data stored by the security center, and validate the security center data location (workspaces).

Recommendation: Define Data Location

Define a separate workspace where the data collected from the Azure virtual machine, including crash dumps and some types of alert data, are stored.

Recommendation: Validate the Diagnostic Data Purge

According to Azure documentation, the Azure Security Center collects ephemeral copies of your crash dump files and analyzes them for evidence of exploit attempts and successful compromises – user and administrator should validate this data is purged periodically and remove.

Documentation: Information on Azure Security Policy can be found at https://docs.microsoft.com/en-us/azure/security-center/security-center-info-protection-policy.

Define a Security Response Plan

The security center provides excellent insight on possible vulnerabilities and threats; however, the data must be reviewed and acted upon proactively. Many organizations define an incident plan after an actual attack has occurred, reducing their preparedness for the initial incident.

Recommendation: Create an Incident Response Plan

Define a custom incident response plan based on the threat model, deployment architecture, and workflow type. The plan should include evidence collection, data process, analysis, assessment, updates, and conclusions.

Documentation: Microsoft has created guidance on creating an incident response plan here: https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-emergency-doc-digital.pdf.

Azure Storage

Use Shared Access Signatures to Access Storage Account Resources

An Azure Storage Account is a logical container used to store and access Azure Storage data objects. Each storage account has two Azure generated 512-bit Storage Access Keys (SAK), which are used for authentication when the storage account is accessed. SAKs are similar to a root password in that users with the key have unfettered access to all the storage account's services. To authenticate access to an Azure Storage Account from a client application, an account access key is required. However, most client applications should not require access to the entire storage environment, which includes all storage services, including Tables, Queues, Files, Blobs, and Azure virtual machine disks.

Recommendation: Use Shared Access Signatures

A SAS provides granular access to services within a storage account. The goal is to avoid distributing the SAK to other users or applications, hardcoding it, or saving it anywhere in plaintext that is accessible to others. Virtual desktop infrastructure workflows should only require access to a subset of services within a storage account, and access via SAS should be used. Additionally, ISE recommends using a policy to explicitly define controlled SAS expiration times, tokens, and source IP address ranges.

Documentation: Azure SAS has multiple use-cases and deployment models. Our recommendation focuses on the use of Shared Access Signature to control access to services within a storage account. Azure SAS is defined here: https://docs.microsoft.com/en-us/azure/storage/storage-dotnet-shared-access-signature-part-1.

Periodically Rotate Access Keys

To authenticate to an Azure Storage Account from a client application, an account access key is required. Regenerating SAKs can affect associated Azure services (e.g., Batch) that are dependent on the storage account.

Recommendation: Regenerate Storage Access Keys Regularly

Administrators should regenerate storage account access keys periodically according to company or regulatory policies. All storage account client services that use the access keys to access the storage account must be updated to use the regenerated key.

Documentation: Azure compute virtual machines, and Batch computes processes rely on storage accounts. Each storage account has a set of access keys. Storage account keys are 512-bit strings created by Azure that, along with the storage account name, can be used to access the data objects in storage. These storage account keys should be rotated after a pre-defined period (for example, every 90 days) or after completion of production.

Azure storage security processes are defined here:

https://docs.microsoft.com/en-us/azure/storage/storage-securityguide.

Enable Encryption at Rest

All Virtual machines have an operating system disk and possibly multiple attached data disk devices. These devices should be encrypted using a key managed by the Key Vault. Encryption at rest protects data if attackers gain access to the physical storage devices used by an account.

Recommendation: Encrypt Disks

Administrators should enable encryption when virtual machines or data disks are instantiated.

Documentation: Azure compute virtual machines rely on on-disk storage for operations system and user data. In the context of VDI workflows, these storage account disks should be protected at rest using disk encryption since these disks may hold sensitive content, metadata, or personally identifiable information.

Azure Disk encryption is described here: https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq.

Require Secure Transfers

Azure storage accounts can support both HTTP and HTTPS protocols for transfers. The former is a plaintext connection that can expose assets to adversaries in privileged network locations, while the latter uses robust encryption to ensure the confidentiality and integrity of network traffic. Depending on the method used to create a storage account, the secure transfer required property may not be enabled.

Recommendation: Enable Secure Transfer Required Property

Administrators should ensure that the secure transfer required property is enabled on any applicable storage accounts.

Documentation: Information on secure transfer is available at: https://docs.microsoft.com/en-us/azure/storage/common/storage-require-secure-transfer.

Enable Advanced Threat Protection

Advanced Threat Protection attempts to detect anomalous or potentially malicious interactions with a storage account. This automated protection can help detect attacks on storage without human intervention.

Recommendation: Enable Advanced Threat Protection (ATP)

Administrators should ensure that advanced threat protection is enabled on any applicable storage accounts. Alerts should be sent to an email address that can be reviewed in a timely manner. Administrators should also consider integrating ATP with Azure Sentinel to provide a central location for viewing security events.

Documentation: Information on advanced threat protection is available at: https://docs.microsoft.com/en-us/azure/storage/common/storage-advanced-threat-protection.

Documentation: Details on Azure Sentinel are provided at: https://docs.microsoft.com/en-us/azure/sentinel/overview.

Protect Assets with Digital Rights Management (DRM)

Media production workflows rely heavily on ad-hoc and near real-time asset sharing and collaboration. Azure Media service video delivery can be used to deliver video assets within a content production team across the globe. The video assets should be protected when shared in this manner.

Recommendation: Use DRM on Media Assets

Media assets should be delivered using a robust DRM solution designed to prevent unauthorized copying or sharing. Azure Media Services supports popular DRM solutions, including Microsoft PlayReady, Apple FairPlay, and Google Widevine.

Documentation: A guide describing how to enable DRM is located here: https://docs.microsoft.com/en-us/azure/media-services/latest/protect-with-drm.

Azure Virtual Machines

Ensure Virtual Machines are Patched Regularly

The applications and operating systems in virtual machines hosted in Azure must be kept up to date to ensure they are protected against known security issues. To better accomplish this, organizations should develop patch management strategies that ensure all software hosted in Azure is updated frequently.

Recommendation: Implement a Patch Management Policy

Administrators should develop and implement a patch management process that regularly updates operating systems and applications hosted in Azure Virtual Machines. A common update cadence is 30 days; however, updates may need to be applied more frequently depending on the software used and the sensitivity of the machines' workflows. Administrators should also develop a strategy to deploy updates that patch critical vulnerabilities in a timely manner, which may need to occur between regular update cadences.

Ensure Disk Storage is Encrypted at Rest

Encryption at rest protects data stored on the physical medium from unauthorized access if an attacker is able to interact with the storage device. Azure Virtual Machines support encryption at rest via the Azure Disk Encryption feature, which uses BitLocker and dm-crypt on Windows and Linux systems, respectively, to encrypt data.

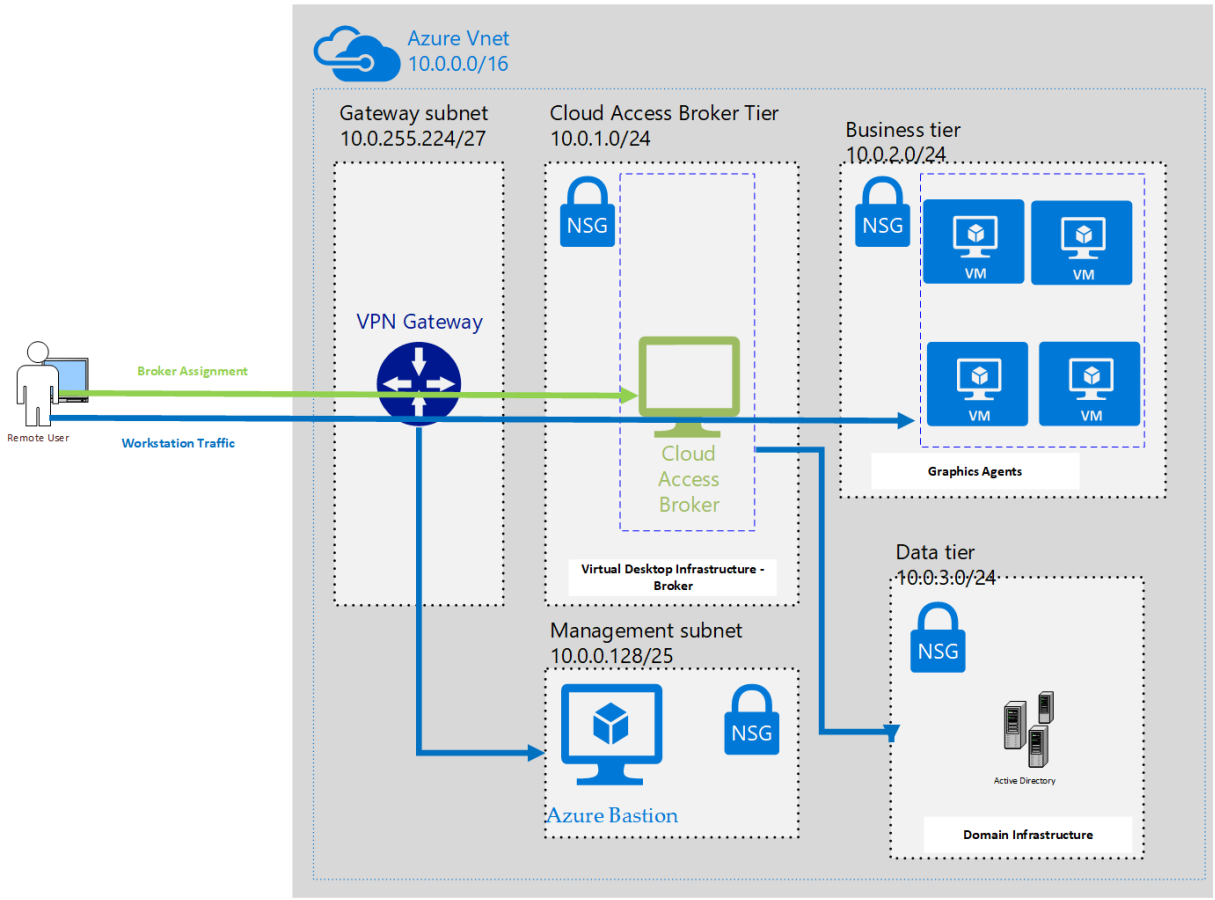
Recommendation: Enable Disk Encryption Features

Azure Disk Encryption should be enabled on all disks used by virtual machines, especially if they store sensitive assets. The additional protection offered by this feature provides a layer of defense-in-depth if attackers are able to compromise the physical storage devices used by the virtual disk.

Documentation: Azure provides additional information about disk encryption here: https://docs.microsoft.com/en-us/azure/security/fundamentals/azure-disk-encryption-vms-vmss.

Azure Virtual Networking

The following diagram depicts a typical VDI setup for media post-production in the cloud.



Use Network Security Groups (NSG)

While Azure completely restricts incoming traffic from the Internet, it is more permissive about internal traffic—essentially allowing open communication between all VM instances within the virtual network (VNet) similar to a physical LAN network. While the default endpoint security features are a useful mechanism for securing Azure VMs, they have limited functionality. Network Security Groups (NSG) secure both inbound and outbound access to both Azure VMs and Azure VNets, similar to a traditional firewall. NSG rules are defined with a standard five-tuple definition (source network, source port, the destination network, destination port, protocol) as well as a name, type, priority, protocol, and access (allow or deny).

Recommendation: Secure Traffic Flow with Azure Network Security Groups

Use network security groups to restrict access to assets to the greatest degree possible.

Documentation: Information about Network Security Groups can be found at: https://docs.microsoft.com/en-us/azure/virtual-network/security-overview.

Use Azure Application Gateway

Azure Application Gateway is a layer-7 load balancer that allows load balancing at the application layer. This type of load balancer allows it to make decisions based on the content of incoming HTTP requests, such as the path of the URL. More importantly, for security concerns, Azure Application Gateway includes a web application firewall (WAF) that can help protect web applications from common types of exploits.

Recommendation: Use the Azure Application Gateway for Web Applications

In order to benefit from the defense-in-depth, Azure Application Gateway provides, configure the load balancer to protect any web applications deployed in Azure.

Documentation: Additional information about Azure Application Gateway can be found at: https://docs.microsoft.com/en-us/azure/application-gateway/overview

Secure Connections to Azure Networks

Azure supports multiple methods for connecting on-premises networks to the cloud. Services like VPN Gateway, ExpressRoute, and Bastion can be used to create secure connections to Azure resources.

Recommendation: Use Dedicated Services to Connect to Azure

Azure's managed services provide hardened and secured methods for joining on-premises networks to Azure. VPN Gateway uses traditional VPN technologies to create private connections, while ExpressRoute uses dedicated physical connections to connect to Azure so that traffic does not travel on the public Internet. Azure Bastion can be used to provide secure access to Azure resources using a managed bastion host.

Documentation:

- VPN Gateway: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways
- ExpressRoute: https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction
- Bastion: https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

Isolate Virtual Appliances Using Individual Subnets

When using virtual appliances, such as a firewall, WAN accelerator, Active directory server, or VPN gateway in Azure, isolate them in their own gateway subnet. Virtual appliances are useful to create routes between Azure resources and on-premises data centers.

Recommendation: Use Gateway Subnet with User-Defined Routing

Use a gateway subnet with a user-defined routing mechanism to isolate networking appliances in their own dedicated private network subnets. Specifically, to secure these services and appliances, prevent direct internet connectivity by placing them in a separate subnet with an NSG acting as a firewall. Additionally, close all ports on the appliance or service servers except those necessary for authentication, authorization, and server synchronization.

Documentation: Editorial and asset management workflows require implementing a secure hybrid network that extends the on-premises network and datacenter to Azure. The user-defined routing mechanism in the gateway subnet filters or blocks all user requests other than those received from the on-premises network.

The Azure network DMZ architecture is described here: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/secure-vnet-dmz.

Apply a Multi-tiered Architecture for VNets

A three-tiered virtual network has front-, mid- and backend network segments to create isolation between various types of assets. In a virtual desktop infrastructure environment, place compute or data storage resources in the backend while placing authentication and traffic shaping (e.g., load balancing) servers in the front-end.

The front end, which contains web servers in its own subnet, directly faces the Internet. The mid-tier, which contains business logic, does not have direct internet access, either inbound or outbound, and can only be reached from the front-end subnet. The back end, again in its own isolated subnet, contains persistent data such as a database system or storage and can communicate only with the middle-tier.

Recommendation: Use Gateway Subnet with User-Defined Routing

Use a Place workload computes machines in the backend while placing authentication and scheduler software servers in the front-end. Apply different Network Security Groups (NSGs) for each subnet.

Documentation: Azure virtual networks are described here: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview. Furthermore, a reference architecture for deployment of N-tier applications is described here: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/virtual-machines-windows/n-tier.

Create Separate Virtual Networks for Productions

In order to better isolate sensitive content in the event of a network intrusion, separate VNets can be used to logically separate environments that process data belonging to different productions.

Recommendation: Separate Productions using VNets

Separate productions and projects into multiple VNets to better isolate them in the event of a network compromise.

Documentation: Azure virtual networks are described here: https://docs.microsoft.com/enus/azure/virtual-network/virtual-networks-overview; network security concepts and guidance can be found here: https://docs.microsoft.com/en-us/azure/virtual-network/security-overview.

Avoid Deprecated Cryptography for IPSec VPNs

In contrast to SSL/TLS, configuring the set of permitted cipher suites at each end of an IPsec connection can be a manual and time-consuming process. The following concerns affect the configuration of the Cloud IPsec VPN:

- *IKEv1 protocol supported*. The Cloud IPsec VPN, for compatibility, supports both IKE version 1 (introduced in 1998) and IKE version 2 (introduced in 2005). One of the goals of IKEv2 was to improve security over IKEv1, including cryptographic weaknesses[3]. Specifically, the IKEv1 supports 3DES and SHA1 (SHA128) as the encryption and hashing algorithms, respectively.
- *HMAC-MD5, supported (IKEv2).* The Cloud IPsec VPN allows *HMAC-MD5* to be used for integrity checking. HMACMD5 is deprecated due to weaknesses in the underlying MD5 algorithm[4].
- SHA1 *supported (IKEv2).* The Cloud IPsec VPN allows SHA1 to be used for integrity checking. SHA-1 has been practically broken and is considered insecure and ineffective[5].
- *DES, 3_DES, supported (IKEv2)*. The Cloud IPsec VPN allows DES, 3_DES to be used for data encryption. DES is inherently insecure, while Triple-DES has much better security characteristics but is still considered cryptographically flawed.

Recommendation: Configure IPsec to Avoid Deprecated Cryptography

Configure the IPsec VPN to avoid the use of deprecated or inherently insecure protocols and modes of operations. Administrators should configure their IPsec clients in accordance with their security policies and avoid using ciphers and security protocols that have been deemed broken or weak by the industry including

Configure Network Watcher

Azure Network Watcher is a built-in service that can be used to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network. The network watcher service can be used to monitor unstable or inactive endpoints, troubleshoot connections, and review other system-level issues. Though Network Watcher is enabled automatically, it is still necessary to enable NSG flow logs or connection monitor to view traffic flows.

Recommendation: Configure Connection Monitor

Configure connection monitor between VMs or resources where appropriate.

Recommendation: Configure Flow Logs

Network Watcher uses flow logs to view information about ingress and egress through an NSG. Targeted and focused NSG flow definition will capture the right traffic patterns and provide insight into potential anomalies.

[3] RFC 4306 Appendix A, https://tools.ietf.org/html/rfc4306#page-96
[4] http://tools.ietf.org/html/rfc6151
[5] https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

Documentation: Logging and monitoring of network traffic is a security and workflow function. Azure Network Watcher described here: https://docs.microsoft.com/en-us/azure/network-watcher.

Enable DDoS Protection

Azure provides a basic level of protection against distributed denial of service (DDoS) attacks for resources deployed in Azure. In addition to this basic protection, administrators may enable DDoS Protection Standard, which provides an enhanced level of security to Azure resources.

Recommendation: Enable DDoS Protection Standard

Administrators should enable on DDoS Protection Standard on resources that would benefit from this protection, such as externally facing web applications.

Documentation: Information on DDoS Protection can be found at: https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview.

About ISE

ISE is an independent security firm headquartered in Baltimore, Maryland. We are dedicated to providing clients proven scientific strategies for defense. On every assessment, our team of analysts and developers use adversary-centric approaches to protect digital assets, harden existing technologies, secure infrastructures, and work with development teams to improve our clients' overall security.

Assessing the client through the eyes of potential attackers allows us to understand possible threats and how to protect against those attacks. Our security analysts are experienced in information technology and product development, which allows them to understand the security problems the client faces at every level. In addition, we conduct independent security research, which allows us to stay at the forefront of the ever-changing world of information security.

Attacks on information systems cannot be stopped, however with robust security services provided by an experienced team, the effects of these attacks can often be mitigated or even prevented. We appreciate the confidence placed in us as a trusted security advisor. Please don't hesitate to get in touch for additional assistance with your security needs.

Independent Security Evaluators, LLC

4901 Springarden Drive
Suite 200
Baltimore, MD 21209
(443) 270-2296

contact@ise.io

https://ise.io