Shape

Description automatically generated with low confidence

Colonial First State

RISE - Migration Landing Zone and Decrypt Extension

Apr 2023

Document title

|  |  |
| --- | --- |
| **Project Title** | CFS Core IT |
| **Author** | Avanade:  Abaigail Rose Artagame |
| **Reviewer** | <Insert> |
| **Approver** | <Insert> |
| **Current Version** | 1.0 |
| **File Name** | RISE - Migration Landing Zone and Decrypt Extension |
| **Publication Date** |  |

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Changes |
| 1.0 | 18/4/2023 | Abaigail Artagame | Initial Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 1](#_Toc132716643)

[1.1 Purpose 1](#_Toc132716644)

[1.2 Project Description 1](#_Toc132716645)

# Introduction

## Purpose

The purpose of this document is to provide proof of security controls followed while implementing the new functional requirements for DMT project.

*\*Due to FortiGate issues screenshots are taken from non-production. Production environment also uses same code base. Deployment happens through IAC; same security controls will be applicable.*

## Threat Scenarios

### T01

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Attack Surface | Threat Actor Category | Threat Scenario |
| T01 | Migration Virtual Machine | External | An attacker delivers a malicious payload to  the migration VM SFTP in attempt to gain a  foothold within the CFS network |

**Control Countermeasures**

* Apply MDE – Azure Defender security extensions for antimalware on VMGraphical user interface, text, application, email

  Description automatically generated
* Make sure Defender definitions are up to date. A screenshot of a computer

  Description automatically generated
* Unzip and scan transferred files for Malware. Graphical user interface, text

  Description automatically generated

### T02

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Attack Surface | Threat Actor Category | Threat Scenario |
| T02 | Azure Storage accounts | Internal / External | An attacker delivers a malicious payload to  the Azure Storage accounts in attempt to gain access to data |

**Control Countermeasures**

* Apply Microsoft Defender for Storage on Storage accounts
* Integration to Microsoft Defender for Cloud
* Real time malware scanning of stored data and files

Graphical user interface, text, application, email

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

### T03

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Attack Surface | Threat Actor Category | Threat Scenario |
| T03 | Azure Virtual Desktops | Internal / External | An attacker exploits a security misconfiguration or vulnerability on the AVD to exfiltrate the data |

**Control Countermeasures**

* Separate Personal Desktop Host Pools
* Authentication - Active Directory Tier 1 identities
* Authorization - AAD groups for AVD assignments
* Intra-subnet traffic blocked by default between nodes in same subnet, hosting AVD instances
* AVDs to have zero internet access except from network access required by baseline apps and specific app endpoints only
* Netskope agent part of AVD deployment, separate AD security group for these identities for Netskope policies.
* Netskope policies can lock down access to key portals by Tenant ID, reducing risk of data exfiltration
* Netskope Data Loss Prevention policies
* Netskope monitoring in place, based around the identity for outbound access granted.
* AVDs in this persona must be excluded from:
* OneDrive for Business folder redirection
* Microsoft 365 apps or user’s ability to sign-in into any of the M365 apps such as Word, Excel, or Teams etc.
* Identity is not permitted to cut, copy to clipboard, or paste function outside of AVDs
* Apply security extensions for antimalware, Defender and CrowdStrike
* Lockdown AVD access to the respective application Storage account Vnet over Azure Firewall and NSG
* Once the AVD is no longer needed, AVD and its associated resources should be deprovisioned.

### T04

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Attack Surface | Threat Actor Category | Threat Scenario |
| T04 | AVD SFTP Client | Internal / External | An attacker steals the SFTP secret and uses it to exfiltrate data |

**Control Countermeasures**

**Full Perimeter Controls**

* IP Whitelisting of Application SFTP Server on the Perimeter firewalls and Netskope for outbound TCP/22 SSH connectivity
* FortiGate's configured to perform IPS
* Encryption in flight over SSH only
* Logs on FortiGate. Azure Firewall and Netskope are monitored by SOC for malicious traffic

**FTP Client Security**

* Segregated dedicated subnet with NSG for DMW AVD
* Intra-subnet traffic blocked by default between nodes in same subnet, hosting AVD instances.
* Dedicated DMW AVD host assigned to an identity per application
* FQDN/IP Whitelisting of Application SFTP Server on client
* Authentication and Authorisation through SSH key value pair (public / private cert)
* Antimalware checks on the transferred data with CrowdStrike and MS Defender
* Managed disks encryption at rest using Microsoft Managed Keys
* Encryption in flight over SSH only
* Key Management: Private key and secrets are secured in key vault
* Secure Logging: Azure Sentinel
* On completion of data migration, deprovision AVD and its resources
* Netskope Data Loss Prevention policies

### T05

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Attack Surface | Threat Actor Category | Threat Scenario |
| T05 | Storage Accounts | External / Third Party | An attacker exfiltrates data from Storage accounts |

**Control Countermeasures**

**Full Perimeter Controls**

* IP Whitelisting of external application IP on the firewalls and F5 WAF
* FortiGate's configured to perform IPS
* DDOS protection on F5 WAAP and Fortinet firewalls
* Encryption in flight over TLSv1.2 or above
* Web application firewall (F5 WAF) for inbound https storage account
* Logs on FortiGate, Azure Firewall and F5 WAF are monitored by SOC for malicious traffic

**Storage Account Security**

* Logical Segregation: Dedicated subnet, each application to have separate storage account
* Intra-subnet traffic blocked by default between nodes in same subnet
* NSG to be configured on subnet level to ensure no access to other containers
* The external application will need to have a new Service Principle created
* Https communication to storage on private endpoint
* Limit access to required containers and set container permissions to "Read Only"
* Antimalware checks on the transferred data
* Encryption at rest Service-side with AES256
* Logging: Azure Sentinel
* Azure Bastion host to be used for administrator access to the platform backend.