



WHITE PAPER

Cyber Recovery in the Cloud with Rubrik



Table of Contents

INTRODUCTION	3	TESTING	15
Audience.....	3	EXAMPLE USE CASES	16
Objective	3	Use Case: Recovery of a critical workload to a pre-built MVRE running on AWS.....	16
Cyber Recovery in the Cloud	4	Background	17
What is a Minimum Viable Company (MVC)?	4	Scenario	17
What is a Minimum Viable Recovery Environment (MVRE)?	4	Business Impact	17
Why Do We Need an MVRE?	5	Recovery Workflow	17
INTRODUCING RUBRIK SECURITY CLOUD	6	Post Mortem	19
RSC Key Features and Benefits	6	Use Case: Recovery of a critical workload to an on-demand MVRE running on Azure	19
Data Protection	6	Background	20
Data Threat Analytics	6	Scenario	20
Data Security Posture Management (DSPM)	7	Business Impact	20
Cyber Recovery	7	Recovery Workflow	20
APIs and Automation	7	Post Mortem	22
INTEGRATING RUBRIK INTO A MINIMUM VIABLE RECOVERY ENVIRONMENT	7	CONCLUSION	22
High-Level Architecture	8	APPENDIX A	23
Rubrik Security Within an MVRE.....	11	APPENDIX B	27
Immutability	11		
Retention Lock and Quorum Authorization	12		
Access Controls	12		
Data Lifecycle	12		
Data Encryption	12		
Data Protection	13		
PERFORMING A MINIMUM VIABLE RECOVERY WITH RUBRIK	13		
Using an Existing MVRE and Performing a Minimum Viable Recovery	14		
Constructing an MVRE and Performing a Minimum Viable Recovery	14		

INTRODUCTION

Welcome to Cyber Recovery in the Cloud with Rubrik! This document aims to provide a comprehensive overview of the key architectural principles and designs necessary for successful cyber recoveries in the cloud. The primary focus of this document will be on the architecture, security, and workflows required to execute a Minimum Viable Recovery (MVR) using Rubrik Security Cloud (RSC). In comparison to a traditional mass recovery of production, an MVR is intended to rapidly recover only mission-critical core business applications and data.

Rubrik's robust set of features complements an organization's journey in both constructing and recovering to a minimum viable recovery environment. Rubrik Data Threat Analytics removes the guesswork of determining the blast radius and identifying non-anomalous backups. Rubrik's also provides an immutable platform, ensuring that backups are available as an organization's last line of defense. Rubrik's API first approach enables customers to automate and orchestrate nearly every task available within the UI, integrating with many common automation platforms such as Terraform and Ansible. And finally, Rubrik provides a multitude of efficient restore options to solve nearly every recoverability challenge.

By following the proactive steps outlined in this document, customers can enhance their preparedness to respond and recover from cyber incidents. More recently, regulations such as [DORA](#) and [NIS2](#) require periodic recovery testing to validate cyber resilience. Ultimately, the objective is to enable timely recovery of core business functions, minimizing the impact of cyber threats on an organization.

AUDIENCE

This document is designed to cater to a diverse audience, including cloud architects, backup administrators, IT professionals, security teams, and any individuals with a vested interest in cyber recovery within a cloud environment. Cloud architects will benefit from the in-depth exploration of architectural principles and designs for cyber recovery. Backup administrators will gain insights into the workflows and processes required to execute successful recoveries using Rubrik Security Cloud. IT professionals will find valuable information on security measures and best practices for cyber incident response and recovery. Additionally, security teams will discover essential strategies to enhance the resilience of cloud-based cyber recovery operations.

While the document's core is aimed at practitioners, it should be noted that developing and executing preparedness and response plans for cyber and disaster recoveries must include many key stakeholders throughout the organization. Everyone should be involved in safeguarding business continuity and data integrity in the face of cyber threats.

OBJECTIVE

The overall objective of this document is to provide a comprehensive understanding of the key architectural principles, design considerations, and workflows needed to successfully execute a cyber recovery in the cloud using Rubrik Security Cloud. The document emphasizes achieving a successful MVR and highlights the best practices for secure recovery operations. The specific objectives of this document include:

- Outlining the architectural principles and best practices necessary in constructing a Minimum Viable Recovery Environment (MVRE).
- Detailing the deployment and security measures required for secure and resilient cyber recovery operations with Rubrik Security Cloud.

- Describing the workflows and processes necessary to conduct a MVR using Rubrik Security Cloud.
- Providing practical use cases that illustrate the concepts, processes, and best practices that underpin successful cyber recovery operations with Rubrik.

By the end of this document, readers will have a foundational understanding of how to leverage Rubrik Security Cloud to achieve a secure, efficient, and effective cyber recovery of core business applications in the cloud.

CYBER RECOVERY IN THE CLOUD

Cyber Recovery in the cloud is a pivotal aspect of modern cybersecurity strategies, especially in the face of increasingly sophisticated cyber threats targeting cloud infrastructures. [Rubrik Zero Labs](#) reported that nearly all cloud tenants were targeted in 2023, with 94% of cloud tenants targeted every month last year and 62% of targeted cloud tenants being successfully compromised.

When considering the aftermath of a cyber incident in the cloud, organizations may be tempted to recover their entire cloud environment to ensure network integrity and provide all services to their end-users. However, this choice is often impractical both in terms of costs and downtime. And that downtime can be significant following a cyber incident within the cloud, increasing an organization's chance of financial and reputational consequences. This underscores the need to adopt a more strategic approach and prioritize the recovery of critical workloads that are vital to the continued operation of the organization. This concept of prioritization of critical resources and their underlying supporting infrastructure embraces the concept of becoming a Minimum Viable Company (MVC).

What is a Minimum Viable Company (MVC)?

Transforming to become an MVC involves a fundamental shift in both mindset and approach. At its core, an MVC is one that streamlines operations, focuses on essential functions, and maximizes efficiencies to deliver value to its customers and minimize financial loss during an attack by using minimal resources during an outage, be it a cyber attack or other type of disaster.

For example, a financial organization looking to embrace MVC methodologies may prioritize the recovery of their core business: the workloads that support their transactional processing, customer account management, and regulatory compliance. Restoring these services along with any underlying prerequisites as quickly as possible is pivotal to the survival of the organization, while workloads and services dealing with things like employee training and development, non-critical IT projects, and all other non-essential functions can be reprioritized for later recovery.

This concept is known as a Minimum Viable Recovery—and to truly deliver minimum viable recovery, organizations must configure a Minimum Viable Recovery Environment (MVRE).

What is a Minimum Viable Recovery Environment (MVRE)?

An MVRE is a preconfigured or on-demand IT infrastructure environment that organizations can use to quickly restore critical applications and data in the event of an unexpected disruption or cyber incident - similar to the concepts of a "clean room" environment. While both cleanrooms and MVREs are capable of enabling security forensics, an MVRE is typically focussed around recovering core business services to minimize downtime and ensure business continuity by enabling faster recovery with minimum impact on operations while a production environment is quarantined.

Typically, an MVRE is designed to contain the same networking configurations, security configurations, and the organization's most critical production systems, data, and configurations. It also includes all necessary software and connectivity to enable data access and system functionality. Essentially, an MVRE is configured to run core business services at a smaller scale than that of production to ensure expedited readiness and resilience in the event of disruptions.

Why Do We Need an MVRE?

In the critical aftermath of a malicious cyberattack, organizations find themselves grappling with the urgent need to contain the breach and initiate comprehensive forensic investigations and analysis. Often this leads to production environments being quarantined, effectively cutting off external access to contain any further malicious activity. Performing this root-cause analysis within the production environment offers many benefits as opposed to conducting it within an Isolated Recovery Environment (IRE) or a cleanroom such as:

- **Realistic Context:** Analyzing the cyber event within the production environment provides a more realistic context for identifying the root cause. It allows for better understanding of the actual systems, configurations, and interactions that may have contributed to the incident, helping to pinpoint the specific vulnerabilities or weaknesses.
- **Accurate Reproduction:** Analyzing the cyber event accurately in the production environment facilitates a thorough investigation of the incident. It enables the analysis of logs, system behavior, and network traffic in real time, allowing for more accurate reconstruction of the event, identification of the attack vectors, and assessing the extent of the impact.
- **Access to volatile/non-persistent storage:** Having access to volatile/non-persistent storage like memory in the production environment allows for the preservation of critical data and system state during the root cause analysis process. This means that forensic evidence, volatile memory artifacts, and system logs can be retained and analyzed without the risk of data loss or alteration, enhancing the accuracy and depth of the investigation.
- **Availability of security toolsets:** The production environment typically has various security tools and monitoring mechanisms already in place, enabling cybersecurity experts to leverage these tools to identify the root cause of an incident quickly.

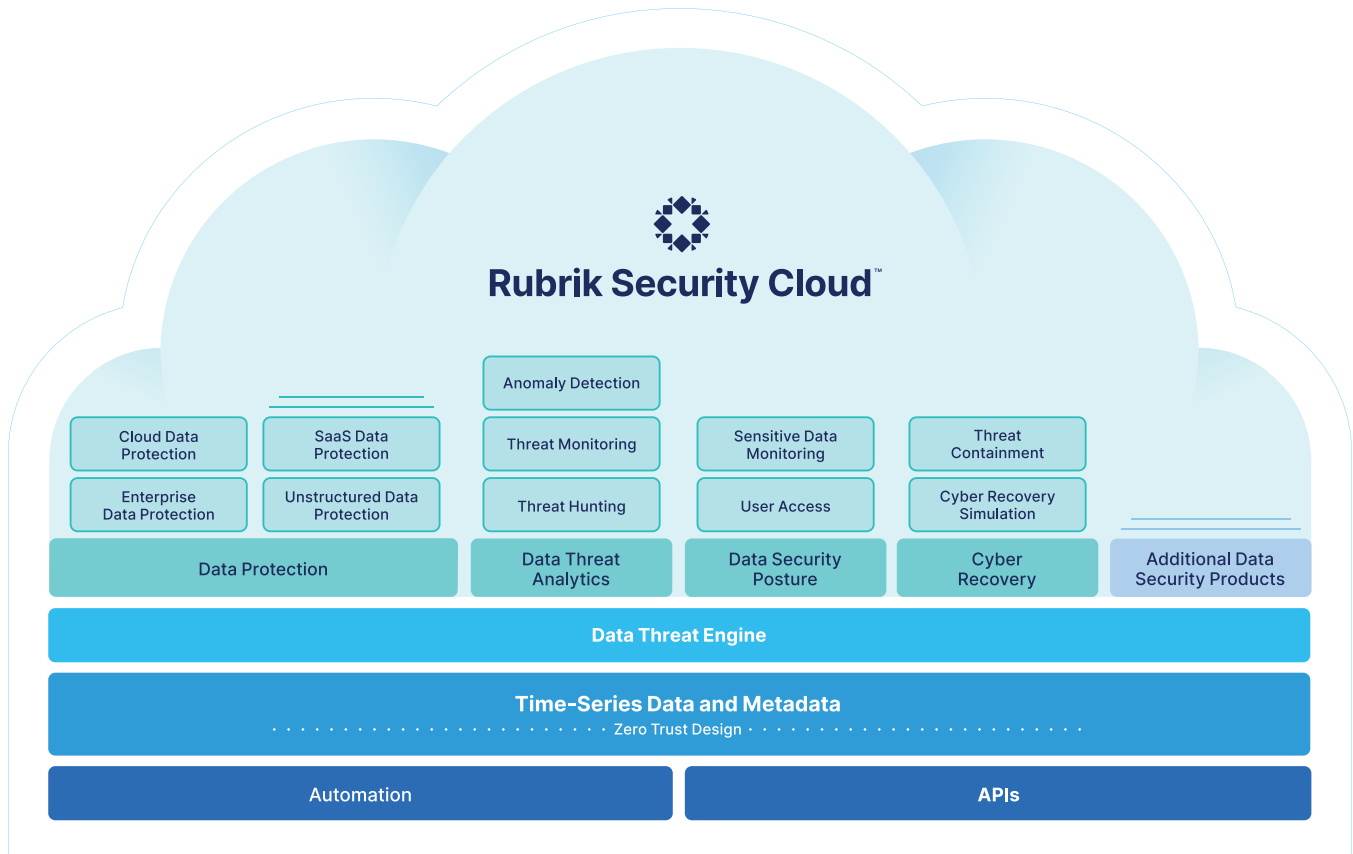
During this crucial analysis phase, security teams assume control of production to dissect the attack, uncovering its intricacies and identifying the root causes that led to the breach. That said, this analysis can often take vast amounts of time, time in which critical services are unavailable. Organizations need to have environments preconfigured or have the resources available to construct them post-attack to support restorations of their core services.

This is where the concept of a MVRE becomes paramount. By distinguishing critical resources and assets that form the backbone of core business operations and having a plan to deliver them in a secondary environment, organizations can streamline their recovery efforts, optimizing the allocation of resources and expediting the restoration process. The MVRE approach enables rapid recovery by focusing on the most vital applications, systems, and data, ensuring minimal disruption and downtime.

By identifying critical workloads and focusing recovery efforts to core services, organizations can minimize downtime, ensure the continuity of business operations, and avoid the prohibitive costs of recovering their entire cloud environment. The remainder of this paper will introduce us to the core features and benefits of RSC, dive deep into some of the design principles, constraints and requirements of architecting an MVRE, and illustrate how RSC can help automate and support these types of recoveries.

INTRODUCING RUBRIK SECURITY CLOUD

Rubrik Security Cloud (RSC) is a robust data security platform designed to deliver cyber resilience across enterprise, cloud, and SaaS environments. By incorporating a zero-trust architecture and cloud design principles, RSC enables organizations to automate data policy management, safeguard sensitive information, and orchestrate swift recovery from cyber incidents and operational disruptions.



RSC KEY FEATURES AND BENEFITS

Rubrik Security Cloud (RSC) offers a comprehensive data security platform that addresses the evolving challenges of cyber threats and helps organizations enhance their cyber resilience. Here are the key platform capabilities of RSC and why they matter:

Data Protection

Data protection ensures the integrity and availability of data through automated, secure, and access-controlled backups. This capability is designed to withstand cyberattacks, malicious insiders, and operational disruptions. By automating data policy management, Data Protection simplifies and streamlines the process of protecting critical data, reducing the risk of data loss and ensuring business continuity.

Data Threat Analytics

Data Threat Analytics continuously monitors for threats to data, including ransomware, data destruction, and indicators of compromise. By leveraging advanced analytics and real-time threat intelligence feeds, organizations can proactively identify and mitigate security risks. The ability to detect and respond to threats in a timely manner helps prevent or minimize the impact of cyber incidents, reducing downtime and potential data breaches.

Data Security Posture Management (DSPM)

DSPM enables organizations to proactively identify and monitor sensitive data exposure. With intelligent insights and analytics, DSPM helps organizations identify areas of vulnerabilities in their data security posture and take appropriate measures to mitigate risks. This capability empowers organizations to enhance their overall security posture and ensure compliance with industry regulations and standards.

Cyber Recovery

Cyber Recovery improves cyber readiness by enabling organizations to easily test and orchestrate recovery workflows. It can expedite the recovery of critical application resources, data, systems, and networks in the event of a major disaster or cyberattack. This capability minimizes downtime, enhances organizational resilience, and reduces the risk of reinfection.

By leveraging these capabilities, RSC helps organizations build cyber resilience, ensuring the integrity, availability, and protection of critical data.

APIs and Automation

The entire Rubrik platform employs an API First approach, ensuring that actions performed within the Rubrik UI simply call underlying APIs. This opens up endless possibilities to automate and orchestrate data management processes, and integrate and automate Rubrik with IT environments. Through these APIs, businesses can automate data protection tasks, streamline workflows, and enhance efficiency, reducing the manual overhead associated with traditional data management processes. Moreover, Rubrik's APIs support a wide range of use cases, from managing backups and recoveries to integrating with third-party applications, thereby providing greater flexibility and scalability. This ensures that IT teams can maintain robust data security and compliance while optimizing resource utilization and improving overall operational agility.

INTEGRATING RUBRIK INTO A MINIMUM VIABLE RECOVERY ENVIRONMENT

Architecting for cyber recovery in the cloud requires a comprehensive understanding of the unique challenges and opportunities presented by the cloud computing paradigm. Unlike traditional on-premises environments, the cloud offers scalability, agility, and elasticity, enabling organizations to flexibly provision resources and rapidly respond to changing business needs. However, this dynamic nature also introduces new complexities as workloads and data are distributed across various cloud services and infrastructure components.

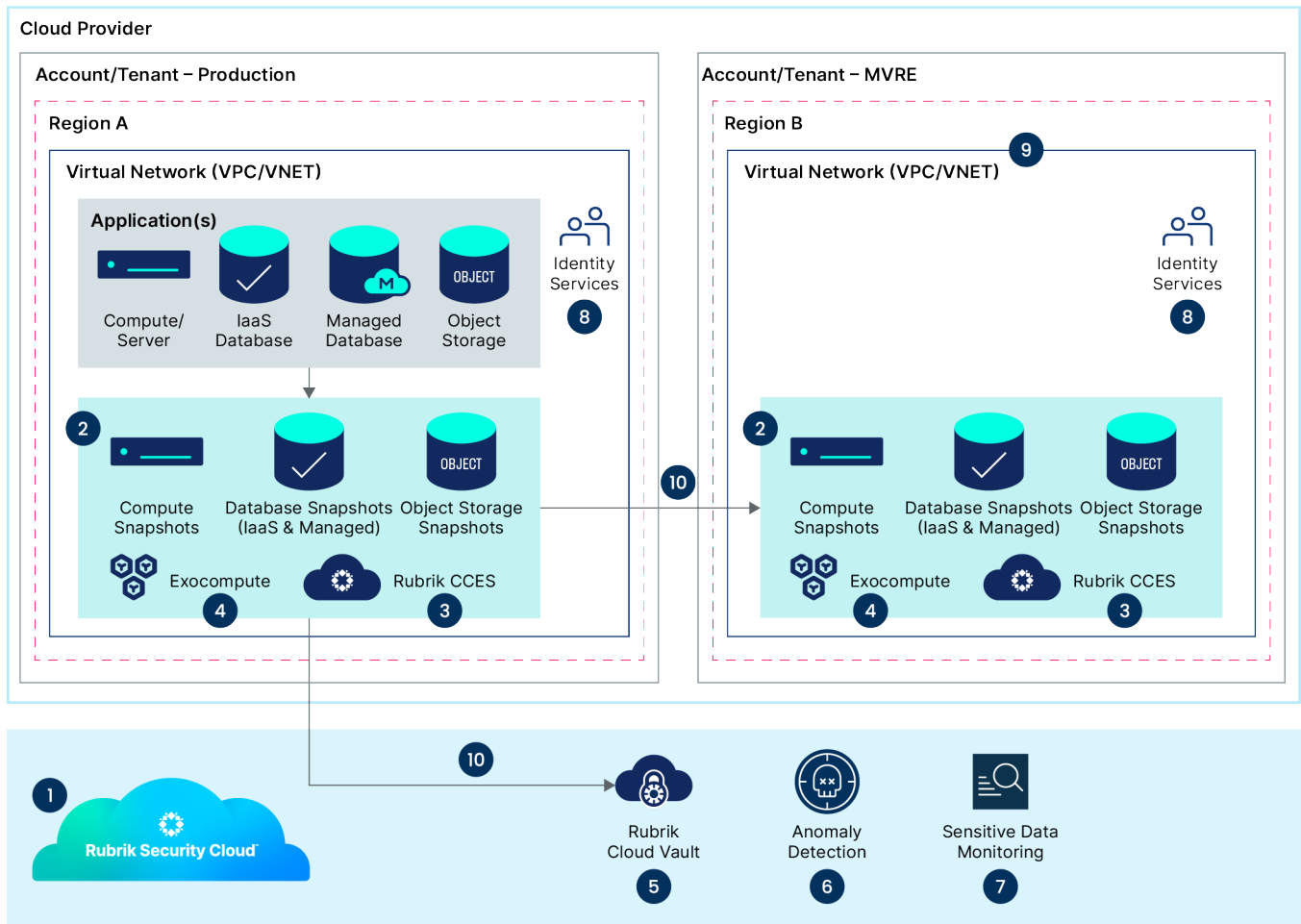
It is within this complex landscape that the concept of an MVRE assumes critical relevance. By carefully integrating the MVRE into their architectural framework, organizations can ensure a segregated and controlled environment, ready to host their core services should production environments be quarantined or lost. With the deployment of robust architectural strategies tailored to the nuanced nature of cloud environments and the invaluable inclusion of the MVRE, organizations can forge ahead in their quest for cyber resilience, fortified against the relentless threats that permeate the digital landscape.

Throughout this section, we will explore the key considerations of how to integrate RSC into an MVRE and explain the vital components involved. Our aim is not only to provide you with the necessary knowledge to architect a minimum viable recovery environment but also to equip you with the expertise to effectively leverage Rubrik's capabilities to protect your network and help ensure the uninterrupted availability of critical business systems.

HIGH-LEVEL ARCHITECTURE

Architecting a MVRE requires thoughtful consideration of the key components, application interdependencies, and the integration of robust data protection solutions like Rubrik. Integrating intelligent data management tools like Rubrik brings automation, centralized control, and granular recovery options to the MVRE, ensuring effective data protection and rapid restoration. By carefully evaluating the following considerations and key components, organizations can construct a MVRE that addresses their unique requirements and forms a solid foundation for business continuity in the face of potential disruptions.

The following diagram illustrates a high-level architecture for an MVRE running in the cloud integrating with Rubrik Security Cloud:



As illustrated, there are many moving pieces in terms of operating an MVRE. Let's explore some of the labeled processes and their functions.

1. Rubrik Security Cloud

Rubrik Security Cloud provides the unified interface to manage both the production and recovery environments. Management is performed completely out-of-band, allowing organizations to recover faster by eliminating the need of having data protection management stacks deployed within environments before a restoration can take place.

2. Rubrik Cloud Native Protection (CNP)

Rubrik Cloud Native Protection (CNP) is a service running within RSC that provides native, agentless backup of cloud environments. Backups can be stored locally (within the production environment) and archived in an alternate location such as storage within another cloud account or to Rubrik Cloud Vault. Cloud Native Protection can be leveraged to protect the following cloud-provided services:

- **Cloud Compute Instances:** Agentless backups of compute services such as Azure VMs, AWS EC2, and GCP Compute.
- **Cloud Database PaaS Services:** Agentless backups of cloud database PaaS services such as AWS RDS and Azure SQL
- **Cloud Kubernetes:** Backups of cloud-based services providing fully managed Kubernetes solutions such as AWS EKS and Azure AKS.
- **Object Storage:** Backups of object storage such as AWS S3, Azure Blob, and Azure DataLake.
- **Cloud Based Identity Services:** Active Directory running within a cloud compute instance as well as cloud native identity solutions such as Entra ID can be protected with Rubrik.

3. Rubrik Cloud Cluster Elastic Storage (CCES)

Rubrik CCES is a solution offered by Rubrik that allows organizations to create a virtual Rubrik cluster within their private cloud. CCES leverages object storage and various native cloud technologies to securely store backup data. CCES can be run as a single node or with multiple nodes to provide flexibility and scalability to meet business needs in terms of backup and recovery performance.

Rubrik CCES is cluster-aware, meaning organizations can easily replicate data from one CCES instance to another CCES instance located within the MVRE.

There are many use cases for deploying CCES instances, including:

- **Granular Level Backups of IaaS instances:** For organizations that may be running databases within IaaS compute instances, CCES can provide a more granular level of backup and restore than CNP can, including the ability to restore individual databases.
- **Backup of native file services** providing an NFS or SMB interface.
- **Rubrik's Managed Volumes** can be leveraged from within CCES to host nearly any data that is able to be exported to a mountable volume. This allows for network configurations, infrastructure configurations, or any data that can be generated via a script to be secured within the Rubrik platform.

4. Rubrik Exocompute

Exocompute is software that is executed to perform various tasks such as snapshot indexing, file recovery, storage tiering, and application-consistent protection within cloud environments. Exocompute leverages cloud-native compute frameworks such as Azure Kubernetes Service and AWS Elastic Kubernetes service to perform these tasks.

Exocompute is managed by Rubrik Security Cloud and automatically launches short-lived, transient compute instances to perform necessary operations, sending metadata back to Rubrik Security Cloud and then terminating. The lightweight nature of exocompute allows Rubrik to ensure processes are completed successfully while optimizing resource utilization and the subsequent cost.

5. Rubrik Cloud Vault

Rubrik Cloud Vault (RCV) is a secure and fully managed cloud archival service provided by Rubrik. It enables organizations to securely store archived backups in the cloud within an account that is logically air-gapped from the production environment and fully managed by Rubrik.

Leveraging RCV within an MVRE architecture ensures that there is no dependency on data within a customer's production environment, ensuring that backups are available, even if the production environment is not.

6. Anomaly Detection

Anomaly Detection, part of Rubrik's Data Threat Analytics service leverages a machine learning model running within RSC to detect and report on anomalies as they are found within backup data. Anomaly Detection enables organizations to quickly identify the blast radius after an attack occurs, pinpointing the exact workloads and services an attack has affected. Furthermore, Anomaly Detection saves precious time when recovering workloads by identifying the last known non-anomalous point in time backup that can be leveraged for restoration.

7. Sensitive Data Discovery

Sensitive Data Discovery, part of Rubrik Data Security Posture services allows organizations to automatically identify and classify sensitive data contained within their workloads. Understanding where your sensitive data lives, and who has access to that data, better prepares organizations to respond to cyber attacks and aids in improving an organization's overall data security posture and risk.

8. Identity and Authentication

An MVRE is of very little significance if end users and services have no way of authenticating into the environment itself. Identity and Authentication play key roles in performing a successful recovery. Some organizations chose to employ a mechanism that keeps identity services between production and the MVRE completely separate, by leveraging different users and groups belonging to completely separate domains for the purpose of authentication and authorization. Other organizations chose to ensure they are able to duplicate any directory services that have deployed within production to their MVRE, either through the use of scripts and/or native services provided by the cloud provider.

9. Network Configuration

Network configurations are a critical aspect of designing a successful MVRE. To increase the likelihood of a successful recovery, it is ideal to replicate the networking setup of the production environment in the MVRE. This includes duplicating the production networks and ensuring the IP addresses of workloads remain unchanged during restoration.

Depending on the timing of MVRE creation, different strategies can be employed. Prior to any attack, organizations should invest time in configuring the networking within the MVRE. This allows them to reference and duplicate the networking configurations from the production environment, which will

ultimately set them up for success during the recovery process. Infrastructure as Code (IaC) tools can also be leveraged to define production environments, making it easier to replicate networking infrastructure in the MVRE with simple modifications to the account the IaC plan is applied to.

In the event of an attack where access to the production environment is lost and an MVRE hasn't been previously built, Rubrik can assist in obtaining the necessary networking configurations for deployment. Rubrik's inventory of workloads within the cloud environment includes crucial networking information such as AWS VPCs and Subnets or Azure VNets and Subnets. This information can be extracted using the Rubrik Security Cloud GraphQL API. After retrieving this information, organizations can manually recreate the respective networking configuration within their MVRE using the acquired details. Examples of how to leverage the RSC GraphQL API to extract cloud networking information can be found in [Appendix A for AWS](#) and [Appendix B for Azure](#). After obtaining the networking information from RSC, organizations can then use the details to manually reconstruct VPCS, VNETs, and Subnets inside of an MVRE.

10. Backup Data Locality

In order to successfully recover data into an MVRE the environment needs to have access to the backup data. Rubrik enables organizations to place data in a variety of different locations. Choosing a location depends on the types of workloads that are being protected, the cloud provider that is utilized to host the MVRE, and whether or not the MVRE is constructed before an attack occurs.

For those leveraging Azure as a cloud provider, the MVRE can be either built ahead of time (before the attack), or after the attack has taken place. Building an MVRE before the attack takes place offers the fastest RTOs as production backup data can be copied into the MVRE using Rubrik's archiving capabilities. If building out the MVRE pre-attack is not an option, customers should archive data to Rubrik Cloud Vault, as data can be restored from RCV to a newly built MVRE, however this process will add to the overall time to recover.

For those leveraging AWS the MVRE must be provisioned before an attack takes place. Rubrik's replication capabilities can then be utilized to replicate snapshots from the production account to the MVRE account. This provides the fastest restore times as the data already exists within the MVRE. Rubrik Cloud Vault is currently not supported within AWS.

RUBRIK SECURITY WITHIN AN MVRE

In an ideal scenario, any service with access to both the production and MVRE is placed out of band. This ensures that should an attack occur, artifacts cannot be compromised to gain access to the MVRE. In addition to out of band management, Rubrik Security Cloud employs several security related mechanisms to ensure that backups can be leveraged as an organization's last line of defense, and can be successfully recovered into the MVRE.

Immutability

At its core, Rubrik is a platform to store immutable data. This ensures that backups ingested and stored on the Rubrik platform cannot be modified or deleted. A custom file-system ensures immutability when storing data on-premises, while cloud technologies such as S3 Object Lock and Azure WORM are implemented to ensure data integrity within the cloud. This prevents rogue attackers from being able to modify or delete your backups.

Retention Lock and Quorum Authorization

While immutability protects against rogue attacks, Retention Lock prevents accidental or rogue administrators changing a Rubrik SLA Domain in such a way that results in backups being expired and/or deleted via Rubrik's lifecycle management processes. In the event that an organization desires to reduce the retention of an SLA Domain that would result in expired backups, Quorum Authorization ensures that these changes need to be approved by two designated employees within the organization.

Access Controls

Access controls are vital in ensuring that only authorized individuals or systems have legitimate access to the recovery resources. By implementing appropriate access controls, organizations can enforce the principle of least privilege and minimize the risk of unauthorized access or data breaches.

Rubrik's Role-Based Access Control (RBAC) allows organizations to enforce the principle of least-privileged access within their environment. This implementation of least-privileged access aligns with the best practice of limiting access rights to only what is necessary for users to perform their job functions. By leveraging RBAC and enforcing least privilege, Rubrik emphasizes security and access control as integral components of its data management solution.

Furthermore, when protecting cloud environments Rubrik does not require standing write access to customers data. Instead, organizations grant Rubrik read access to the resources they protect. When it comes time for restoration, privileges can be escalated on-demand in order to grant Rubrik temporary access to perform recoveries within the cloud environment. In the case of an MVRE, Rubrik would only maintain read access to the recovery environment until the recovery needs to take place.

Data Lifecycle

When deploying an MVRE, careful consideration should be given to data lifecycle processes. Without proper data hygiene, organizations run the risk of escalated cloud bills within their MVRE environment, and perhaps more importantly, run the risk of data exfiltration. Data lifecycle processes ensure the integrity and compliance of customers' data.

Rubrik's data lifecycle management is a fully automated process driven by its intelligent SLA Domain policy engine. As data is marked for expiration, Rubrik ensures data is purged in a timely manner. Without a proper and automated process to handle data lifecycle management, organizations run the risk of higher cloud bills and an increased overall TCO.

Data Encryption

Many cloud providers offer key management services to support the encryption of data and disks. Quite often, organizations leverage services such as AWS KMS and Azure KeyVault to create, manage, and rotate keys in order to ensure that data is encrypted.

Depending on the type of cloud encryption utilized, along with what the cloud providers support, Rubrik may be able to allow organizations to re-encrypt exported data using different keys within the MVRE in the event the original keys are quarantined within the production environment. Careful consideration should be taken when dealing with encryption mechanisms within an MVRE and automated testing of workload restorations should be performed to ensure deployed encryption mechanisms are valid.

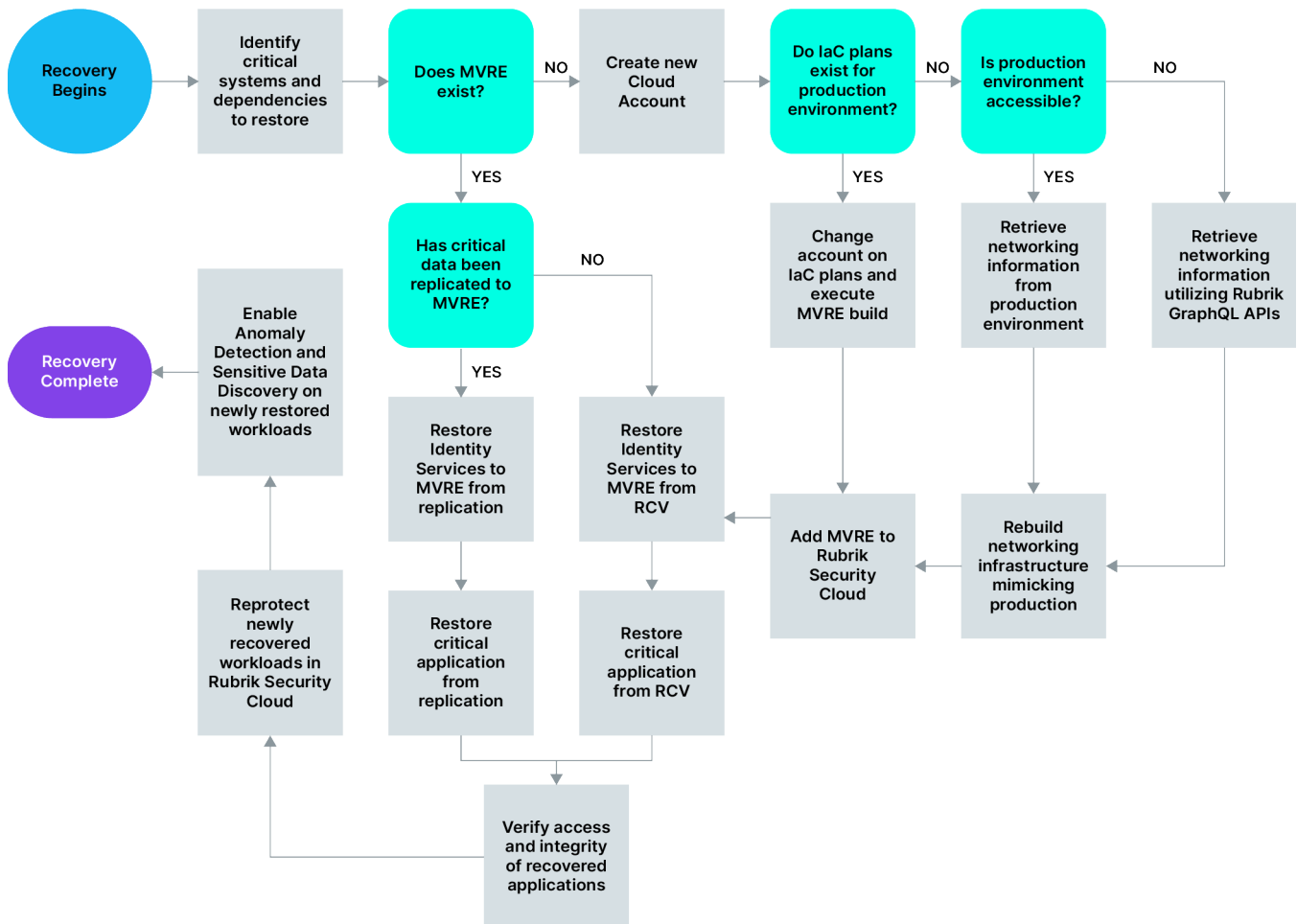
Data Protection

Data protection within an MVRE is essential to safeguard critical data during recovery and continuity scenarios. It's important to note that once data is recovered to the MVRE, it takes the place of your production data, and that data will require reprotection by the data protection solution to defend against day-to-day recovery scenarios and cyber threats.

Rubrik provides the ability to automatically protect data within cloud accounts by assigning an SLA Domain to the entire account. This results in any existing workloads, along with any newly created workloads inheriting the SLA Domain, allowing backups to begin automatically without any user intervention. Another method of automatic protection is to restore the workloads with the same tag assignments they had when they were backed up. SLA Domains can then be assigned to workloads based on tag rules, which will assign any workloads with a specified key-value tag pair to the SLA Domain, automatically protecting the workload.

PERFORMING A MINIMUM VIABLE RECOVERY WITH RUBRIK

In this section, we will explore the key steps and considerations for performing a minimum viable recovery using Rubrik's robust data security platform. From identifying critical systems to building out the MVRE and restoring data, we will dive into the essential processes and best practices to ensure a successful recovery strategy. The following outlines at a high level the process of performing a minimum viable recovery with Rubrik.



The process of performing a minimum viable recovery differs slightly based on whether or not an organization already has an MVRE built. Let's explore each option in more detail below.

USING AN EXISTING MVRE AND PERFORMING A MINIMUM VIABLE RECOVERY

As highlighted earlier, ensuring you have an MVRE before you actually need it provides a faster time to recover than that of having to build one during the cyber event. The following outlines the process of performing a minimum viable recovery to an existing MVRE.

1. Leverage Rubrik Anomaly Detection service to quickly and easily determine the latest non-anomalous backup to recover.
2. Restore Identity, Authentication, Authorization, and any other services to the MVRE in the event they don't already exist. Depending on your configuration, these services may be restored directly from within the MVRE if leveraging Rubrik's Cross-Account replication or copied from an RCV instance hosting the backups.
3. Restore all layers of the desired critical application. This could involve running restorations from both Rubrik Cloud Native Protection and Rubrik Cloud Cluster Elastic Storage. All restores can be completed through the Rubrik Security Cloud UI.
4. Verify the connectivity and integrity of the recovered applications, ensuring they are functioning as desired.
5. Leverage RSC to reprotect the restored applications to ensure day-to-day restores can be performed while running within the MVRE.
6. Optionally, Rubrik Data Threat Analytics and Data Security Posture services can run against the restored workloads, ensuring anomalies and sensitive data are detected.

CONSTRUCTING AN MVRE AND PERFORMING A MINIMUM VIABLE RECOVERY

Having to construct the MVRE and perform the recovery post-attack is a bit more complicated as it does contain some extra steps that need to be manually run. The following outlines the process of constructing the MVRE on demand and performing a minimum viable recovery.

1. Create a new cloud account to host the MVRE. This should be created within the same cloud provider as the production.
2. Configure the networking components within the MVRE to mimic that of production. Networking component creation can be accomplished in a variety of ways, depending on the organization's deployment strategies. If the production environment is still accessible, it's recommended to reference it to retrieve the networking configuration. If the production environment is quarantined, which is a common practice, networking configurations can be retrieved from the following:
 - a. If you have leveraged IaC toolsets to create the production networking components, the account ID on the plans can be swapped and the plans run against the MVRE to create copies of these.
 - b. If you have no documentation whatsoever around your production networking, the RSC GraphQL APIs can be queried in order to return metadata about your production environment. See [Appendix A](#) for AWS and [Appendix B](#) for Azure.

3. Add the MVRE Cloud Account to Rubrik Security Cloud.
4. Leverage Rubrik's Anomaly Detection service to determine the latest non-anomalous restore point to recover to.
5. Restore Identity, Authentication, Authorization, and any other services to the MVRE in the event they don't already exist. These backups can be restored from the Rubrik Cloud Vault instance they were archived to.
6. Restore all layers of the desired critical application. This could involve running restorations from both Rubrik Cloud Native Protection and Rubrik Cloud Cluster Elastic Storage. All restores can be completed through the Rubrik Security Cloud UI.
7. Verify the connectivity and integrity of the recovered applications, ensuring they are functioning as desired.
8. Leverage RSC to reprotect the restored applications to ensure day-to-day restores can be performed while running within the MVRE.
9. Optionally, Rubrik's Data Threat Analytics and Data Security Posture services can be enabled to scan the data within the MVRE, ensuring organizations are aware of any security events that may arise while running workloads within the MVRE.

TESTING

Regular testing of the restoration of data is not only a requirement within many regulations such as DORA and NIS2, but it also provides peace of mind and confidence that a recovery will work as expected during an outage.

Automated backup and recovery testing with Rubrik into an MVRE is further empowered by Rubrik's API-first approach and robust APIs, which provide the flexibility to automate nearly all processes achievable within the user interface. Leveraging Rubrik's extensive APIs, organizations can seamlessly integrate backup and recovery testing into the MVRE, enabling the automation of complex tasks and the orchestration of end-to-end testing workflows. This API-first design not only streamlines the configuration and management of backup and recovery processes but also allows for the creation of customized, automated testing scenarios tailored to the organization's specific requirements.

Moreover, the flexibility and extensibility of Rubrik's APIs empower organizations to extend their backup and recovery testing capabilities beyond traditional boundaries. By leveraging Rubrik's APIs, organizations can automate the provisioning and scaling of the MVRE, ensuring that it accurately mirrors the production environment. Furthermore, the API-first design allows for automated validation of individual data protection policies, recovery plans, and system configurations within the MVRE, ensuring that every aspect of the recovery process is thoroughly tested and validated.

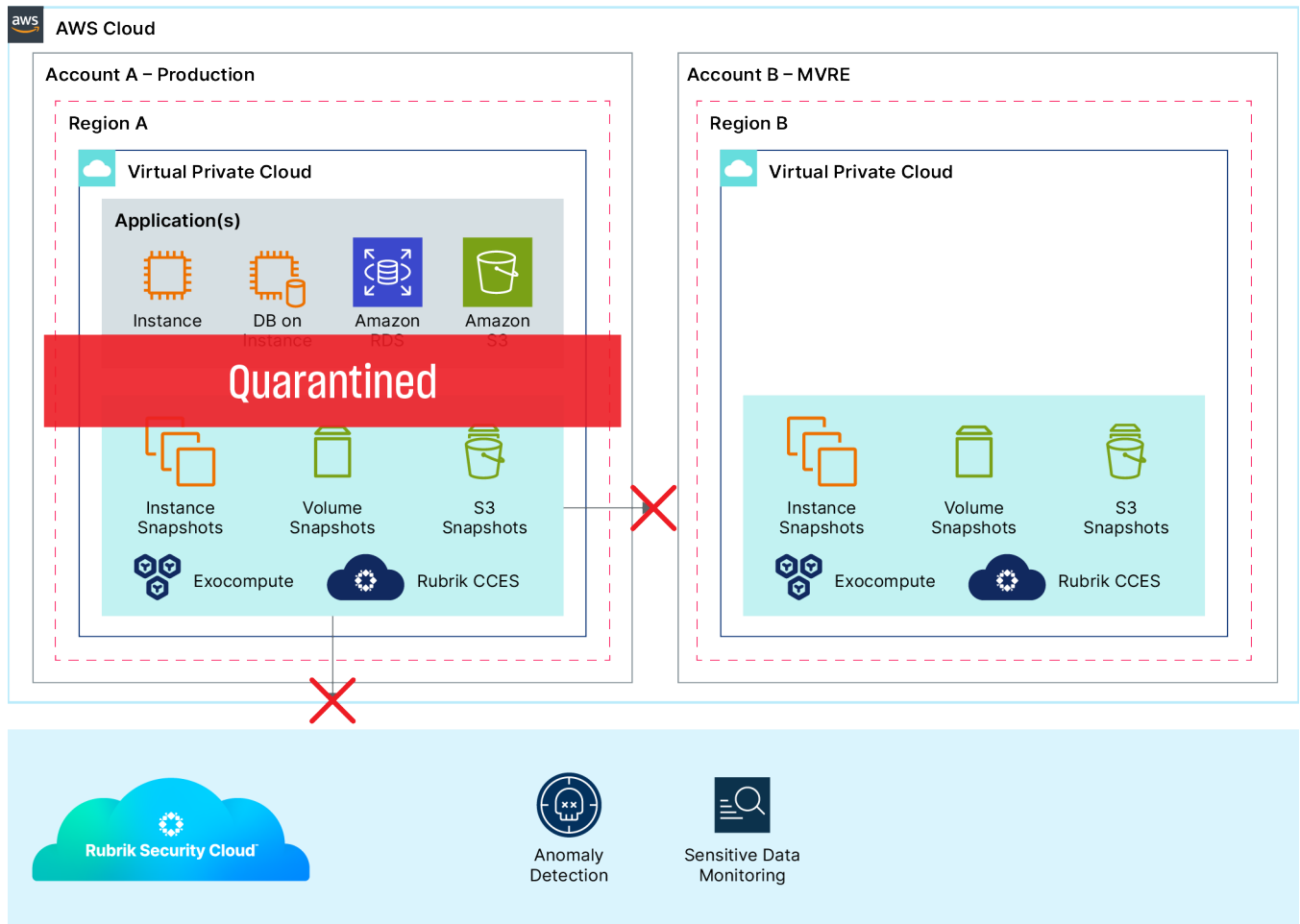
Integrating Rubrik's API-first architecture with backup and recovery testing into an MVRE not only enhances the efficiency and agility of the testing processes but also enables organizations to innovate and expand their recovery capabilities. With the ability to automate virtually any operation within the Rubrik environment, organizations can continually optimize and fine-tune their backup and recovery testing workflows, driving ongoing improvements in resiliency and operational readiness. This flexibility and automation provided by Rubrik's APIs enable organizations to adapt their recovery strategies to evolving business needs and technology landscapes, reinforcing their ability to effectively recover critical data and applications in the face of adversity.

EXAMPLE USE CASES

The following section will outline some of the most common use cases for performing a minimum viable recovery with Rubrik.

USE CASE: RECOVERY OF A CRITICAL WORKLOAD TO A PRE-BUILT MVRE RUNNING ON AWS

In this example, we will walk through the process of recovering a critical cloud workload running on AWS to an MVRE that has been pre-configured on AWS.



Note: The company and scenarios described in this section are for reference only and do not reflect any Rubrik customers.



Background

FinBank, a prominent financial institution, relies on a robust infrastructure hosted in Amazon Web Services (AWS) to deliver critical banking services to its customers. Recognizing the significance of uninterrupted operations, FinBank has proactively prepared a minimum viable recovery environment (MVRE) to minimize downtime and swiftly restore their systems in the event of an unexpected disruption. The MVRE contains an exact replica of their production networking configuration, including VPC, Subnets, and Security Groups. FinBank has been leveraging Rubrik to protect both their on-premises and cloud applications, along with their M365 data.

FinBank has one core application dubbed TransactOne that handles key transactions for their customers that is in scope for a minimum viable recovery. This application utilizes several EC2 instances to run front-end services. Back-end data services are provided by both an MSSQL RDS deployment and another EC2 instance running MSSQL. The application also leverages an S3 bucket to host copies of transactional receipts.

To protect TransactOne, FinBank has configured Rubrik cross-account replication to replicate snapshots of the front-end EC2 instances to their MVRE after each and every backup. As a result, FinBank ensures that they maintain 14 days of restore points within the MVRE while still leaving local backups within their production environment for day-to-day data management operations. FinBank is also leveraging cross-account replication to ensure that data from the MSSQL RDS instance is available within the MVRE. In addition to this, FinBank has also deployed a Cloud Cluster instance in both the production environment and the MVRE. Cloud Cluster is utilized to take database-level backups of the MSSQL database within the production environment and replicate that data to the Cloud Cluster instance within the MVRE. An EC2 instance running Microsoft Active Directory is also being protected by this Cloud Cluster instance. FinBank is also leveraging Rubrik S3 protection to back up their object store data from the production environment to the MVRE.



Scenario

One day, as a result of a cyberattack, FinBank encounters a critical system failure in their production environment. This attack appears to be widespread and has affected a number of workloads including TransactOne. As a result, FinBank's SecOps teams have removed all access to the production environment, essentially quarantining it off from the public as well as its employees, including the IT and backup teams.



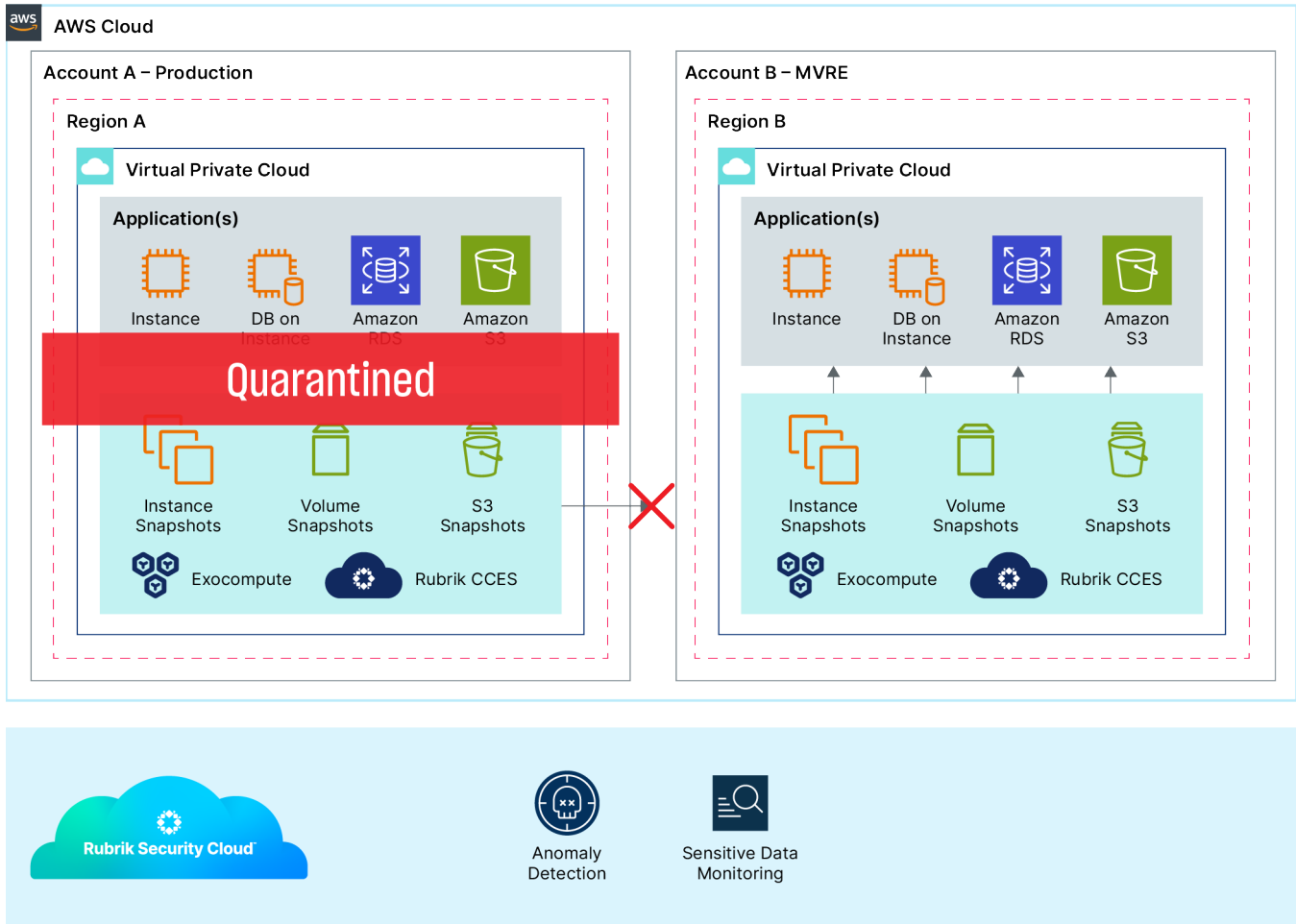
Business Impact

The cyberattack poses significant risks to FinBank, including reputational damage, financial loss, regulatory fines, and legal liabilities. The institution's ability to respond effectively to the attack and restore operations within minimal downtime is crucial for preserving customer trust, maintaining regulatory compliance, and safeguarding its long-term viability in the market. Initial investigations reveal that the environment could be inaccessible for at least a week and executives are pressuring IT teams to ensure that TransactOne is back up and running as soon as possible. FinBank engages in a plan to move forward with the recovery of TransactOne to their MVRE.



Recovery Workflow

Since FinBank has already created the MVRE, they are able to quickly move into the restoration phase of the recovery.



After leveraging Rubrik Security Cloud's historical Data Threat Analytics data, specifically Anomaly Detection, FinBank is able to pinpoint the exact time that the attack occurred against TransactOne, identifying the last known good restore point to recover.

FinBank begins by creating a new EC2 instance using the same AMI that was used to create the image within the production hosting Active Directory. Once complete, RSC is leveraged to restore the Active Directory domain services to the newly built EC2 instance. Authentication and authorization services are tested, verified, and are now up and running within the MVRE.

FinBank then creates a new MSSQL server running on an EC2 instance. After installing the Rubrik Backup Service, RSC is leveraged to restore the back-end database for TransactOne to the EC2 instance. In addition, FinBank leverages RSC to restore the RDS MSSQL databases that also provide backend services for TransactOne. The data layers are tested, verified, and are now up and running within the MVRE.

FinBank then creates a new S3 bucket to host the transactional receipts and leverages RSC to restore the data from the S3 bucket that has been placed in the MVRE.

Finally, FinBank leverages RSC Cloud Native Protection to restore the various front-end EC2 instances within the MVRE. FinBank then re-configures the application to point to the newly created ARNs for the

various resources within the MVRE to ensure service communication. Once complete, the front-end services are tested and verified.

FinBank has now successfully recovered their core business application, TransactOne, into their MVRE. Customers are now able to process transactions with FinBank again.

Lastly, FinBank configures RSC to ensure that at the very least, local backups are being taken of TransactOne within the MVRE.

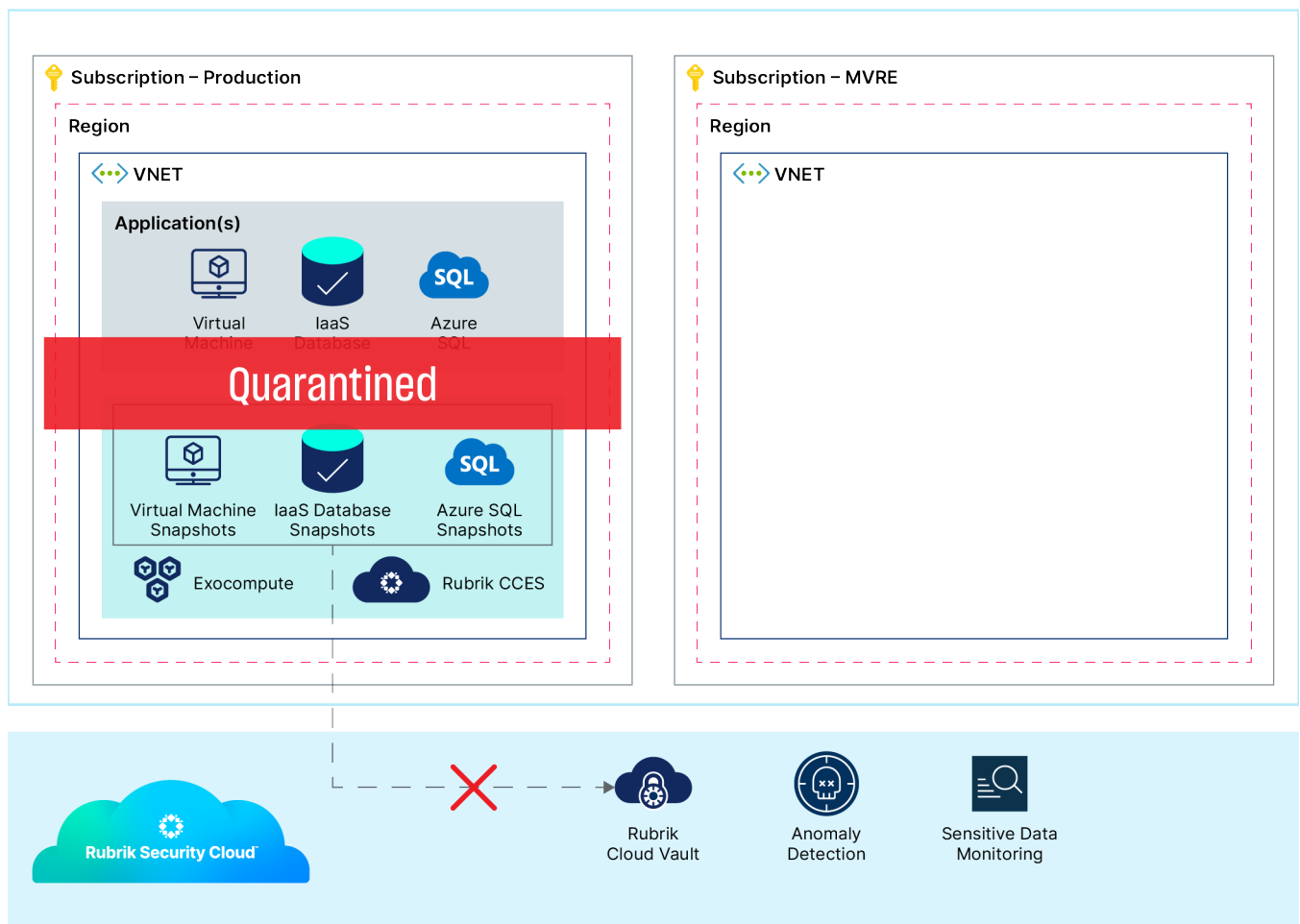


Post Mortem

FinBank concludes that by doing the work upfront to build and configure the MVRE, they have saved hours of work and greatly minimized the amount of downtime for their business. They were able to seamlessly recover their most critical workload with Rubrik Security Cloud.

USE CASE: RECOVERY OF A CRITICAL WORKLOAD TO AN ON-DEMAND MVRE RUNNING ON AZURE

In this example, we will walk through the process of creating the MVRE on demand post-attack and recovering a critical cloud workload. Both the production environment and the MVRE are hosted on Azure within separate tenants.



Note: The company and scenarios described in this section are for reference only and do not reflect any Rubrik customers.



Background

Zaffre Fashion Group (ZFG) is a global fashion retailer that focuses on online sales of their products through a number of solutions that have been built on Microsoft Azure. While ZFG's IT teams would love to have a warm MVRE running all the time, they simply don't have the budget to make this feasible.

ZFG has, however, invested the time up front to define what their key critical business applications are. The main application that ZFG relies on for revenue is their online store presence dubbed ZStore. ZStore is a multi-tier application that leverages many different services on Microsoft Azure to provide customers with an easy way to order and ship productions from ZFG.

ZStores main backend that hosts inventory is serviced by a managed Azure SQL instance. The front end providing access to the e-commerce site is load-balanced across multiple Azure VM instances. In addition to these services, ZStore also relies upon an Azure VM running Oracle that provides shipping and warehouse fulfillment services and another Azure VM hosting their Microsoft Active Directory services. Without ZStore, ZFG runs the risk of lost revenue and brand reputation.

While ZFG has not configured an MVRE to replicate ZStore data, they have taken protection measures that they deemed feasible. They have leveraged RSC's Cloud Native Protection to protect both the Azure VMs running the ZStore frontend and the Azure SQL instance backend data. ZFG has also opted to archive these backups to a Rubrik Cloud Vault instance, ensuring that a secondary copy of the data has been placed outside of their production Azure tenant. In addition to this, ZFG has deployed a Cloud Cluster instance into their production environment to achieve granular protection and restore capabilities of the Azure VM hosting Oracle and Active Directory. Again, this data has been archived to the Rubrik Cloud Vault instance.



Scenario

ZFG's security teams have recently detected widespread occurrences of the Lockbit ransomware within their Azure environment. This has resulted in widespread encryption occurring across their primary Azure tenant that hosts the ZStore services, as well as many other business applications ZFG relies upon for various functions. As a result, SecOps has removed all access in and out of the Azure tenant to help stop the spread of the infection and perform various root-cause analysis and forensics activities.



Business Impact

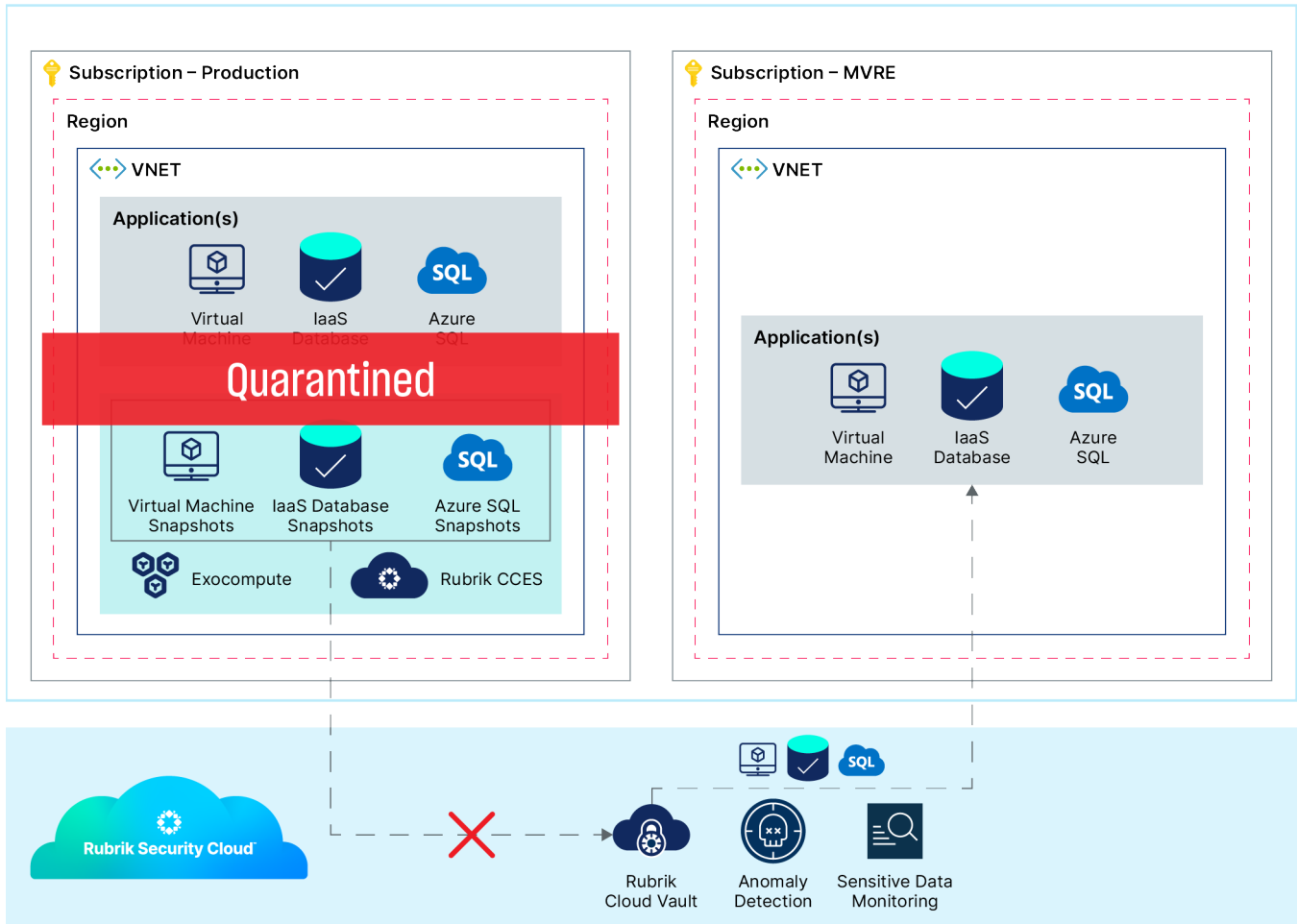
Without a functioning ZStore instance, ZFG is losing potential revenue and suffering from a blemished brand reputation. Because of this, leadership has instructed the relevant IT teams to focus solely on the restoration of the ZStore application into another Azure tenant that they recently provisioned after the attack occurred. Currently, the Azure tenant contains only the default networking configuration and has not been customized to ZFG's network standards. Leadership would like IT teams to use this tenant as an MVRE for the ZStore application. Unfortunately, all of the documentation outlining ZFG's networking configuration for Azure is currently unavailable as it's quarantined within the production Azure environment.



Recovery Workflow

Before ZFG can restore any data, they first need to ensure that the networking configuration within the MVRE has been deployed and tested. With no access to documentation, IT teams are relying on metadata that RSC has collected to rebuild the various required VNets and Subnets within the MVRE.

ZFG begins by following the steps outlined within [Appendix B](#) to retrieve the CIDR IP ranges and VNet names and recreates the configuration within the MVRE.



Next, ZFG leverages Rubrik’s Anomaly Detection features running against the historical data that has been archived to RCV. This allows ZFG to pinpoint when the attack initially occurred and arms them with the point-in-time snapshot that can be recovered to their environment.

With this information, ZFG then deploys a new Rubrik Cloud Cluster instance into the MVRE, attaching it to the RCV instance hosting the data. A new Azure VM is provisioned, and ZFG leverages Rubrik’s Active Directory restoration features to recover a clean copy of their directory services into the MVRE, providing them with the authentication and authorization services required to run ZStore.

ZFG proceeds by utilizing Cloud Native Protection to export the Azure SQL instance from RCV back to the MVRE. The backend services are tested and verified.

ZFG then leverages Cloud Native Protection to restore the various Azure VMs from RCV to the MVRE that provide front-end access to ZStore. After reconfiguring the front end to point to the new Azure SQL instance, the entire ZStore application is tested and verified.

ZFG then re-protects all of the restored items within the MVRE with RSC and redirects DNS to point to the newly restored ZStore instance. ZStore is now available to the public and ZFG’s core business application is now functional.



Post Mortem

ZFG understands that this entire process could have been expedited by having a standby MVRE ready to recover to; however, they deemed that the time to recover during the scenario was sufficient. They have taken measures to ensure that documentation and procedures are stored out of band from their primary Azure environment and are grateful for Rubrik's out-of-band management and the ability to retrieve all the information they need to successfully recover from a cyberattack within the cloud.

CONCLUSION

In conclusion, leveraging Rubrik for cyber recoveries within an MVRE provides a robust and comprehensive solution for ensuring business continuity in the face of cyber threats. By integrating Rubrik's unique architectural design principles, organizations can achieve a high level of resilience and security while simplifying recovery processes.

Rubrik Data Protection is built on principles that ensure stored backup data remains unchanged from the moment it is captured. By combining an immutable file system with a zero-trust security model, it protects against unauthorized changes, encryption, or deletions. This security measure preserves the integrity and reliability of the data, facilitating a straightforward and dependable recovery process. Through this design, organizations are equipped to quickly restore critical operations within the MVRE, effectively minimizing downtime and preserving operational continuity.

Rubrik's extensive APIs provide the flexibility to integrate and automate recovery processes within the MVRE. This API-first approach empowers organizations to orchestrate and customize recovery workflows, facilitating seamless integration with existing cybersecurity tools and processes. Organizations can enforce data threat analytics to detect anomalies and proactively take action to safeguard critical data and applications. This integration allows for continuous monitoring, analysis, and remediation of cyber threats, bolstering the organization's security posture and ensuring a quick and effective recovery in the event of an incident.

Ultimately, leveraging Rubrik within an MVRE enables organizations to establish a resilient foundation for cyber recoveries. The combination of immutability, API extensibility, Data Threat Analytics, and efficient recovery processes enhances the organization's ability to quickly detect, respond to, and recover from cyber threats. By embracing Rubrik's comprehensive solution, organizations can confidently protect their core business functions, mitigate the impact of cyber incidents, and maintain uninterrupted operations, ensuring business continuity and mitigating potential financial and reputational risks.

APPENDIX A

RETRIEVING AWS VPC AND NETWORKING INFORMATION FROM RUBRIK SECURITY CLOUD

The following outlines how gather networking information about an AWS environment from the Rubrik Security Cloud API for purposes of recreating it within an MVRE.

1. Retrieve a list of all AWS accounts configured within RSC.

```
// Example Query

query AllAWSAccounts {
  awsNativeAccounts(awsNativeProtectionFeature: EC2) {
    nodes {
      id
      name
    }
  }
}

// Example response

{
  "data": {
    "awsNativeAccounts": {
      "nodes": [
        {
          "id": "9f6825cd-d01b-4b74-80b1-19596879ce99",
          "name": "rubrik-lab"
        }
      ]
    }
  }
}
```

2. Retrieve a list of all VPCs within those accounts. Use the id returned from the previous query.

```
//Example Query

query VPCs {
  allVpcsFromAws (awsAccountRubrikId: "9f6825cd-d01b-4b74-80b1-19596879ce99" ) {
    id
    name
  }
}
```

```
// Example Response

{
  "data": {
    "allVpcsFromAws": [
      {
        "id": "vpc-b146e8ea",
        "name": "",
        "securityGroups": []
      },
      {
        "id": "vpc-920b05c0",
        "name": "",
        "securityGroups": []
      },
      {
        "id": "vpc-0f443b8efac655964",
        "name": "roxie-vpc-demo-usw2",
        "securityGroups": []
      },
      {
        "id": "vpc-03429a206acde656f7a",
        "name": "orion-vpc-services-usw1",
        "securityGroups": []
      },
      {
        "id": "vpc-72322e0e",
        "name": "",
        "securityGroups": []
      },
      {
        "id": "vpc-0e23b9f335dc13dea",
        "name": "dipper-vpc-demo-usw2",
        "securityGroups": []
      },
      {
        "id": "vpc-0asc931f44a4bb48ae0a",
        "name": "nova-vpc-test-use1",
        "securityGroups": []
      },
      {
        "id": "vpc-3e347a52",
        "name": "",
        "securityGroups": []
      },
      {

```

```

    "id": "vpc-036f49da05fde4870",
    "name": "roxie-vpc-management-usw1",
    "securityGroups": []
  },
  {
    "id": "vpc-0322340d02de28ee2",
    "name": "roxie-vpc-test-use1",
    "securityGroups": []
  },
  {
    "id": "vpc-021f245a2824fb3e",
    "name": "orion-vpc-services-use1",
    "securityGroups": []
  },
  {
    "id": "vpc-00234f3d5c42fef",
    "name": "orion-vpc-services-usw2",
    "securityGroups": []
  }
]
}
}

```

3. Retrieve a list of all subnets within a given VPC. Use the returned VPC ID and Cloud Account IDs from the previous steps.

```

// Example Query

query subs {
  awsCloudAccountListSubnets (cloudAccountUuid:
    "9f6825cd-d01b-4b74-80b1-19596879ce99",region: US_WEST_1, feature:
    CLOUD_NATIVE_PROTECTION, vpcID: "vpc-00234f3d5c42fef") {
    result {
      name
      subnetId
      vpcId
      cidrBlock {
        cidrBlock
      }
    }
  }
}

// Example Response

```

```

{
  "data": {
    "awsCloudAccountListSubnets": {
      "result": [
        {
          "name": "orion-vpc-services-private-01-usw1",
          "subnetId": "subnet-0b2025f126df68771a",
          "vpcId": "vpc-0329a206ac4asdf6a6f7a",
          "cidrBlock": {
            "cidrBlock": "10.61.20.0/24"
          }
        },
        {
          "name": "orion-vpc-services-public-01-usw1",
          "subnetId": "subnet-0e700f482ada03456",
          "vpcId": "vpc-0329a2062349s6f7a",
          "cidrBlock": {
            "cidrBlock": "10.61.21.0/24"
          }
        },
        {
          "name": "orion-vpc-services-private-02-usw1",
          "subnetId": "subnet-04049dxve41cc67",
          "vpcId": "vpc-032fwke2a",
          "cidrBlock": {
            "cidrBlock": "10.61.22.0/24"
          }
        }
      ]
    }
  }
}

```

4. Repeat step 3 for all of the VPCs you wish to create. Don't forget to also change the regions if using multiple regions within the MVRE.
5. Use the CIDR block information returned to rebuild your VPCs and subnets within the MVRE.

APPENDIX B

RETRIEVING AZURE VNET AND NETWORKING INFORMATION RUBRIK SECURITY CLOUD

The following outlines how gather networking information about an Azure environment from the Rubrik Security Cloud API for purposes of recreating it within an MVRE

1. Retrieve a list of all Azure configured within RSC.

```
// Example Query

query AllAzureSubscriptions {
  allAzureCloudAccountTenants(feature: CLOUD_NATIVE_PROTECTION,
includeSubscriptionDetails: true) {
    subscriptions {
      id
      nativeId
      name
    }
  }
}

// Example response

{
  "data": {
    "allAzureCloudAccountTenants": [
      {
        "subscriptions": [
          {
            "id": "eb10ba2f-f985-4b26-b36a-c573eb379ea3",
            "nativeId": "35ecdc82-729a-4022-8049-226061b5e6f3",
            "name": "TM-Lab-EA"
          }
        ]
      }
    ]
  }
}
```

2. Use the id returned from the previous query to retrieve information about the VNets and associated address prefixes.

```

query AllAzureSubnetsByRegion {
  allAzureCloudAccountSubnetsByRegion(cloudAccountId:
"eb10ba2f-f985-4b26-b36a-c573eb379ea3", region: WESTUS) {
    addressPrefixes
    name
    nativeId
    addressPrefixes
    vnet {
      name
      resourceGroupName
    }
  }
}

// Example Response

{
  "data": {
    "allAzureCloudAccountSubnetsByRegion": [
      {
        "addressPrefixes": [
          "10.0.0.0/16"
        ],
        "name": "subnet-orion-o365-usw",
        "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/
resourceGroups/rg-orion-o365/providers/Microsoft.Network/virtualNetworks/vnet-
orion-o365-usw/subnets/subnet-orion-o365-usw",
        "vnet": {
          "name": "vnet-orion-o365-usw",
          "resourceGroupName": "rg-orion-o365"
        }
      },
      {
        "addressPrefixes": [
          "10.61.82.0/24"
        ],
        "name": "snet-public1",
        "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/
resourceGroups/rg-tm-dev-us-west/providers/Microsoft.Network/virtualNetworks/vnet-
tm-dev-us-west/subnets/snet-public1",
        "vnet": {
          "name": "vnet-tm-dev-us-west",
          "resourceGroupName": "rg-tm-dev-us-west"
        }
      },
      {

```

```

    "addressPrefixes": [
      "10.61.80.0/24"
    ],
    "name": "snet-private1",
    "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/
resourceGroups/rg-tm-dev-us-west/providers/Microsoft.Network/virtualNetworks/vnet-
tm-dev-us-west/subnets/snet-private1",
    "vnet": {
      "name": "vnet-tm-dev-us-west",
      "resourceGroupName": "rg-tm-dev-us-west"
    }
  },
  {
    "addressPrefixes": [
      "10.61.83.0/24"
    ],
    "name": "snet-public2",
    "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/
resourceGroups/rg-tm-dev-us-west/providers/Microsoft.Network/virtualNetworks/vnet-
tm-dev-us-west/subnets/snet-public2",
    "vnet": {
      "name": "vnet-tm-dev-us-west",
      "resourceGroupName": "rg-tm-dev-us-west"
    }
  },
  {
    "addressPrefixes": [
      "10.61.81.0/24"
    ],
    "name": "snet-private2",
    "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/
resourceGroups/rg-tm-dev-us-west/providers/Microsoft.Network/virtualNetworks/vnet-
tm-dev-us-west/subnets/snet-private2",
    "vnet": {
      "name": "vnet-tm-dev-us-west",
      "resourceGroupName": "rg-tm-dev-us-west"
    }
  },
  {
    "addressPrefixes": [
      "10.61.84.0/24"
    ],
    "name": "snet-private1",
    "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/
resourceGroups/rg-tm-prod-us-west/providers/Microsoft.Network/virtualNetworks/
vnet-tm-prod-us-west/subnets/snet-private1",
    "vnet": {

```

```

    "name": "vnet-tm-prod-us-west",
    "resourceGroupName": "rg-tm-prod-us-west"
  }
},
{
  "addressPrefixes": [
    "10.61.86.0/24"
  ],
  "name": "snet-public1",
  "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/resourceGroups/rg-tm-prod-us-west/providers/Microsoft.Network/virtualNetworks/vnet-tm-prod-us-west/subnets/snet-public1",
  "vnet": {
    "name": "vnet-tm-prod-us-west",
    "resourceGroupName": "rg-tm-prod-us-west"
  }
},
{
  "addressPrefixes": [
    "10.61.85.0/24"
  ],
  "name": "snet-private2",
  "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/resourceGroups/rg-tm-prod-us-west/providers/Microsoft.Network/virtualNetworks/vnet-tm-prod-us-west/subnets/snet-private2",
  "vnet": {
    "name": "vnet-tm-prod-us-west",
    "resourceGroupName": "rg-tm-prod-us-west"
  }
},
{
  "addressPrefixes": [
    "10.61.87.0/24"
  ],
  "name": "snet-public2",
  "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/resourceGroups/rg-tm-prod-us-west/providers/Microsoft.Network/virtualNetworks/vnet-tm-prod-us-west/subnets/snet-public2",
  "vnet": {
    "name": "vnet-tm-prod-us-west",
    "resourceGroupName": "rg-tm-prod-us-west"
  }
},
{
  "addressPrefixes": [
    "10.1.0.0/24"
  ],

```

```

    "name": "default",
    "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/
resourceGroups/rg-tm-prod-usw/providers/Microsoft.Network/virtualNetworks/rubrik-
tme-rdp-cces-vnet/subnets/default",
    "vnet": {
      "name": "rubrik-tme-rdp-cces-vnet",
      "resourceGroupName": "rg-tm-prod-usw"
    }
  },
  {
    "addressPrefixes": [
      "10.61.89.0/24"
    ],
    "name": "snet-private2",
    "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/
resourceGroups/rg-tm-services-us-west/providers/Microsoft.Network/virtualNetworks/
vnet-tm-services-us-west/subnets/snet-private2",
    "vnet": {
      "name": "vnet-tm-services-us-west",
      "resourceGroupName": "rg-tm-services-us-west"
    }
  },
  {
    "addressPrefixes": [
      "10.61.90.0/24"
    ],
    "name": "snet-public1",
    "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/
resourceGroups/rg-tm-services-us-west/providers/Microsoft.Network/virtualNetworks/
vnet-tm-services-us-west/subnets/snet-public1",
    "vnet": {
      "name": "vnet-tm-services-us-west",
      "resourceGroupName": "rg-tm-services-us-west"
    }
  },
  {
    "addressPrefixes": [
      "10.61.91.0/24"
    ],
    "name": "snet-public2",
    "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/
resourceGroups/rg-tm-services-us-west/providers/Microsoft.Network/virtualNetworks/
vnet-tm-services-us-west/subnets/snet-public2",
    "vnet": {
      "name": "vnet-tm-services-us-west",
      "resourceGroupName": "rg-tm-services-us-west"
    }
  }
}

```

```

    },
    {
      "addressPrefixes": [
        "10.61.88.0/24"
      ],
      "name": "snet-private1",
      "nativeId": "/subscriptions/eb10ba2f-f985-4b26-b36a-c573eb379ea3/resourceGroups/rg-tm-services-us-west/providers/Microsoft.Network/virtualNetworks/vnet-tm-services-us-west/subnets/snet-private1",
      "vnet": {
        "name": "vnet-tm-services-us-west",
        "resourceGroupName": "rg-tm-services-us-west"
      }
    }
  ]
}

```

3. Repeat step 2 for any other regions you wish to retrieve networking information from.
4. Use the CIDR block information returned to rebuild your VNets and Subnets within the MVRE.



Global HQ
 3495 Deer Creek Road
 Palo Alto, CA 94304
 United States

1-844-4RUBRIK
 inquiries@rubrik.com
www.rubrik.com

Rubrik is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit www.rubrik.com and follow [@rubrikinc](https://twitter.com/rubrikinc) on X (formerly Twitter) and [Rubrik](https://www.linkedin.com/company/rubrik) on LinkedIn. Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.

wp-cyber-recovery-in-the-cloud-with-rubrik / 20240620