Navy Enterprise Networks (NEN)

Orchestrated Repository for Enterprise (ORE)

1.x

**Version:** 2023.01



**Prepared By:**

ORE Team

241 18th St S

Arlington, VA 22202

Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Author** | **Change Description** |
| 2023.01 | ORE team | 1. Initial Document created |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# System Enterprise Architecture

## Introduction

The addition of the Orchestrated Repository for Enterprise (ORE) solution provides oversight and enable good governance over the entire process of transforming and modernizing its legacy network.

The ORE is a strategic platform designed to provide governance, risk and compliance through an orchestrated repository ecosystem. The NDP ORE provides highly secure content management, archival platform, and data orchestration system gateway to the modern data repository ecosystem. The zero trust design ensures both the insider and external threats cannot view, manipulate, or download any unauthorized data: a true “insider threat” prevention system. It seamlessly integrates all data platforms needed for modern application and network development and operations, providing a unified, secure portal. It provides access to source code, documents, key management, image repo’s securely and smoothly.

## System Concept of Operations (CONOPS)

The PEO Digital Orchestrated Repository for the Enterprise (ORE) is a strategic platform designed to provide governance, risk, and compliance through an orchestrated repository ecosystem. The ORE provides a highly secure multimedia Content Management System that provides archival with extremely robust index-able search capabilities – with the ability to index, organize, search and retrieve video, audio, and various image and text documents - and also provides a data orchestration system gateway to the modern data repository ecosystem.

The zero trust design ensures both the insider and external threats cannot view, manipulate, or download any unauthorized data: a true “insider threat” prevention system. It seamlessly integrates all data platforms needed for modern application and network development and operations, providing a unified, secure portal. It provides access to source code, video, documents, secrets management, and image repositories securely and seamlessly. The secure orchestration of these repositories will allow the Navy to obtain visibility into hybrid multi-cloud environments to support DON's operational ability to control and maneuver critical environments and support the DON's zero-trust digital transformation.

The platform is designed to provide governance, risk and compliance through an orchestrated repository ecosystem and has the ability to integrate with all data platforms needed for modern application and network development and operations, providing a unified, secure portal. It provides access to source code, video, documents, secrets management, and image repositories securely and seamlessly which enables visibility into the Navy hybrid multi-cloud environments to support DON's operational ability to control and maneuver critical environments and support the DON's zero-trust digital transformation.

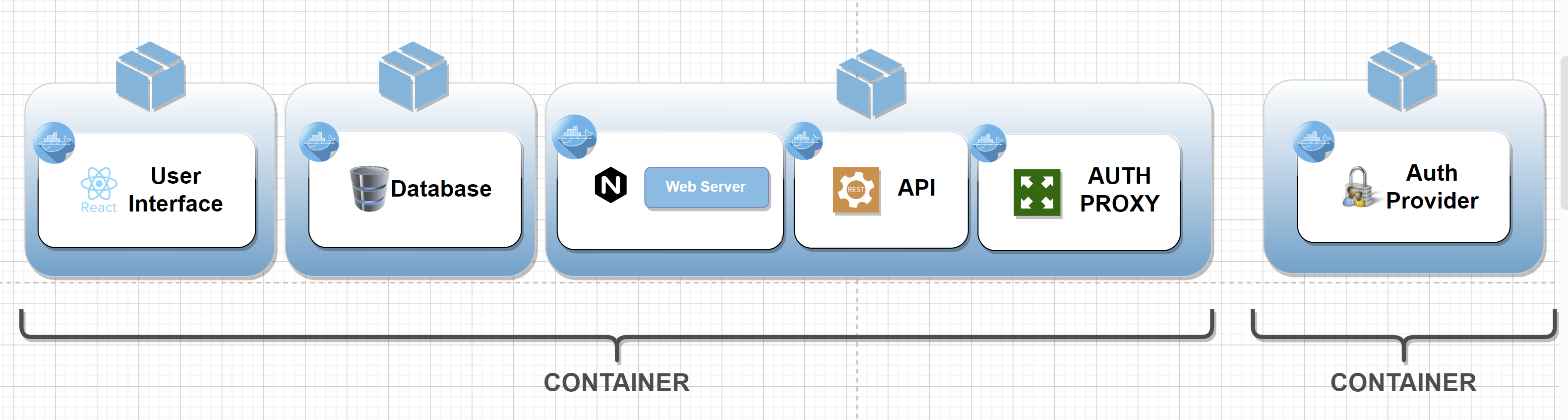


Figure 2: DRAFT ORE Architecture Diagram

As an example workflow, the Navy engineering team will leverage the ORE to adopt modern software delivery practice and to transform current manual/stovepiped engineering design and operations. These services must be underpinned with agile development processes: devops, gitops, and leverage secure secrets (user to machine and machine to machine) that enable secure automation. This is a paradigm shift that requires embracing a world where machine to machine communication through automation becomes the majority of datacenter and network traffic.

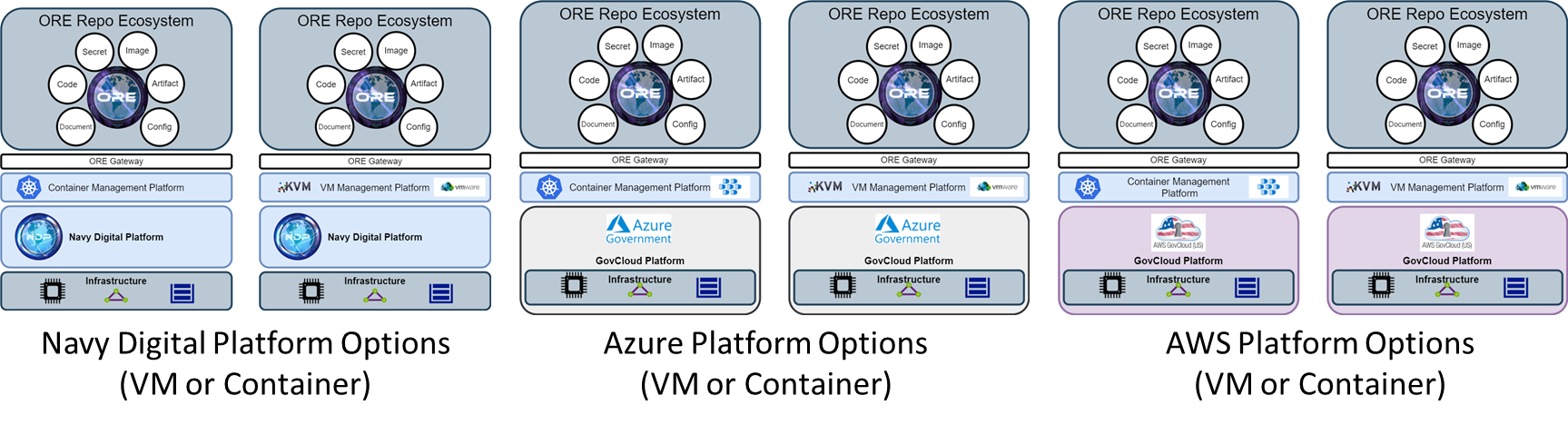
### Security Information and Event Management (SIEM)

The main components of the ORE:

1. UI
2. API & Video API
3. Database
4. Authentication Provider

Components of the ORE are API driven and are leveraging the latest cloud native technologies to secure the API connections. The ORE can be hosted in any cloud platform and call to any storage system that has API tokens. The servers are virtual machine instances – as well as containers and Kubernetes - that operate on top of AZURE and AWS physical infrastructure located in AZURE East, Google Cloud Platform, and AWS East region (Washington D.C Metro area).  The users of the system are currently located in the Eastern US although the plan is to scale to West Coast.

The image below shows where the application has been deployed to date, highlighting the flexibility of the ORE application. The ORE will inherit the controls from the platforms.



ORE implements a combination of services to provide **daily (within 24 hours) full backups** and long-term, offline storage in accordance with DON infosec policy.

Full backups are either accomplished in code, or through regularly scheduled push to the Simple Storage Service (S3). Spot backups that occur during change request events are done through automated snapshots invocations for the respective service or component that require its data to be recovered.

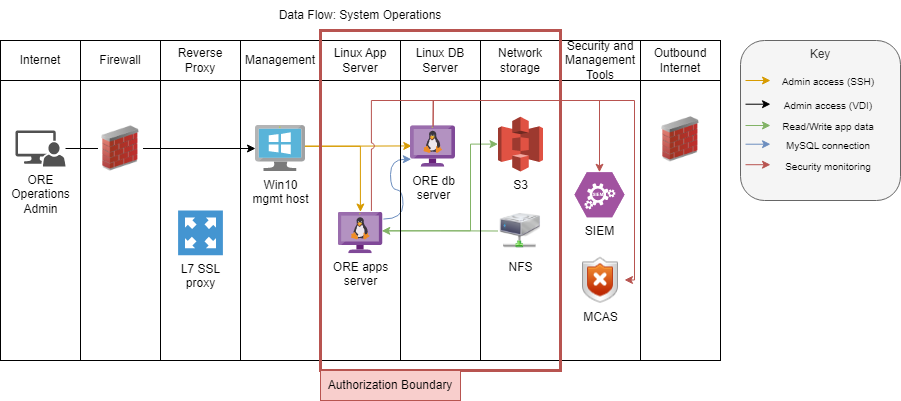
* Cloud-native services
* Blob Snapshot service
* Storage snapshot service
* Server-based services
* Cronjob
* Application-specific solution

#### BAN/LAN Interface Requirements

The BAN/LAN requirements are highly dependent on the Navy’s NDP engineered, tested and consumable platform (IaaS and PaaS).

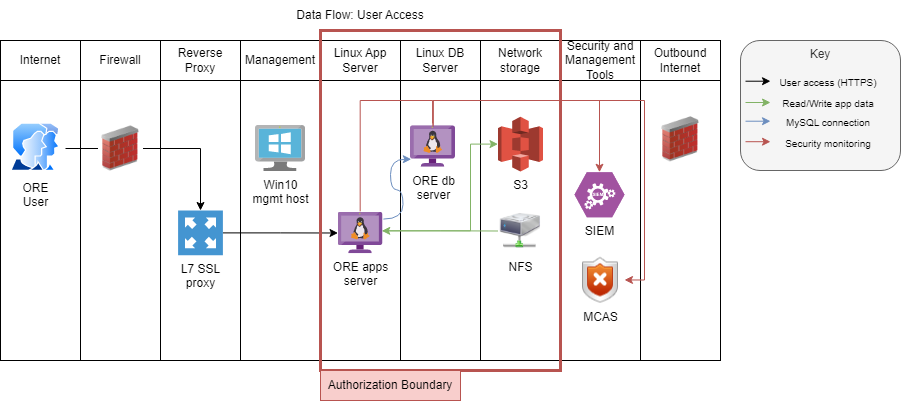
The dataflow examples below highlight the Operations and User Access dataflows. The currently deployed version of the ORE leverages a multi-cloud approach with provided services residing on a combination of the public Azure and AWS clouds, and on-premise cloud residing in 2 Twelve Solutions data-center facility located in Reston, VA. Although the cloud native ORE application is cloud agnostic and can live in any cloud native platform or cloud infrastructure, to include the hyperscaler platforms from AWS, Azure, and Google, or on-premise cloud such as VMware, or bare metal.

Figure 2: Admin Dataflow Diagram



.

Figure 3: User Dataflow Diagram



# Information Security Architecture

## SIEM

### Authentication and Authorization

The currently deployed solution of the ORE supports the existing DoD common access card (CAC and PIV) and Alternate Token (Alt-Token) Public Key Infrastructure (PKI) mechanisms for authentication. It is a pre-production system without the ability to host CUI data. And in-order to facilitate testing and demoing of capabilities to PEO Digital staff, it has been configured to allow single sign-on using username/password and 2FA token. Authorization is handled via group membership within the ORE authorization system.

It is expected that the production ORE deployment will be running on a PEO Digital managed on premise environment called the NDP Core Nodes. Authentication for ORE users will be done via the Naval Identity Service (NIS) which will enforce PKI authentication that meets the security requirements of the Navy.

#### Administrator Authentication and Authorization

ORE administrators are authenticated using MFA. Authorization is based on their group membership within AD/LDAP. Groups are mapped to internal authorization groups.

#### User Authentication and Authorization / Access Management

Internal groups will be mapped to ORE Identity system and Policy enforcement points. The user’s authentication is dependent on the IDP provider(s) that are configured for the ORE and allowed for use by ORE users.

#### Services Authentication and Authorization

ORE services are implemented as individually distinct microservices that exchange data over HTTPS API. All API requests are verified to have valid JWT cryptographic tokens. This serves to be able to scale the ORE services as needed and to implement separation of duties for the respective services and servers that comprises the ORE system.

The system accounts and internal user credentials are created in the application database under the user\_ tables. Each user credential has its own UUID and password values are not stored but is instead hashed using the bcrypt hashing algorithm. Bcrypt hashes are one way hashing functions that are designed to operate too slowly to brute force.