neysa

neysa velocis

Security Shared Responsibility Model

Version 1.0

Dated: 15th November 2024

Created by: Cyber Sec Team – Neysa

Table of Contents

1. Introduction

Neysa Velocis is a high-performance computing platform designed to accelerate generative AI and machine learning models' deployment, training, and inference. It allows enterprises to access GPU-powered cloud infrastructure on demand, which is ideal for AI workloads. The platform simplifies AI adoption by providing tools and services specifically built to manage AI-native applications at scale.

This document highlights the essential details regarding the Security Shared Responsibility Model between Neysa and its Customers.

2. Neysa Velocis – Tenets

The Velocis AI Acceleration Cloud System is designed with a highly scalable and secure architecture to meet the demanding needs of AI workloads. There are two tenets to the Velocis environment, namely Velocis infrastructure platform and Customer instance within the same.

- **Velocis Infrastructure Platform –** It is the foundation of the system, providing a fully managed and highly scalable environment that enables rapid deployment and efficient management of AI workloads. This platform is hosted and operated by Neysa, ensuring high levels of reliability, security, and performance.

- **Customer (Tenant) Instance –** Neysa enables each customer to provision and manage their own isolated Tenant Instances, which are designed to run AI workloads independently of other customers. These instances are built on top of the Velocis Infrastructure Platform, providing flexibility and customization while benefiting from the security and reliability of the underlying system.

The Security responsibility is different for each tenet details of which are laid out below.

3. Shared Responsibility Model

The **Shared Responsibility Model** establishes a secure environment by defining the security tasks Neysa manages and those that are the responsibility of the customer.

Necessity of the Shared Responsibility Model

As AI and data-intensive applications grow, so too do the security requirements for managing sensitive data and ensuring reliable performance. A Shared Responsibility Model helps Neysa and customers collaboratively address these requirements, ensuring a secure environment for GPU-accelerated and non-GPU workloads alike.

The Shared Responsibility Model is essential for several reasons:

- **Defined Accountability:** Clarifying security roles allows both Neysa and the customer to manage their specific responsibilities, reducing the chance of security oversights and enabling faster response to potential issues.
- **Flexible Security:** While Neysa provides a secure infrastructure platform layer for both GPU and non-GPU workloads, customers have control within their own environments, enabling tailored business-driven security services and configurations that align with workload needs.
- **Enhanced Risk Mitigation:** With Neysa focused on platform-level protections and customers on tenant & application-level security, risks are managed across the entire environment, helping prevent vulnerabilities at multiple layers.
- **Regulatory Alignment:** By clearly outlining security responsibilities, customers can better understand and meet regulatory requirements relevant to their data and applications within their tenant-managed environments.

Within this model, Neysa secures the core infrastructure platform (Security of the Cloud), including data centre, physical hardware, networking, Infrastructure Security and essential platform services necessary for both GPU and non-GPU

capabilities. Neysa is also responsible for ensuring strict isolation between each customer's tenants.

Customers, in turn, are responsible for securing their tenant environment (Security in the Cloud), including advanced security controls, application-level settings, data, and access controls configured within their instances. By clarifying these roles, Neysa and the customer can work in tandem to safeguard all aspects of their workloads.

Neysa's Responsibilities

As the cloud service provider, Neysa is responsible for securing and managing the core Velocis Infrastructure Platform (Security of the Cloud), which serves as the foundation for all customer workloads. Below are the key areas of responsibility for Neysa:

- **Datacenter and Physical Layer Security**

  Neysa secures the physical infrastructure of the Velocis Infrastructure Platform. This includes controlling access to data centers, and surveillance systems, and ensuring the protection of hardware components from unauthorized physical access.
- **Infrastructure Security (Core Platform)**

  Neysa is responsible for securing the Core Platform by implementing robust protections across network, compute, and storage resources. This includes defence-in-depth protection for the core infrastructure that Neysa manages covering perimeter, network, application, authentication & authorization, secure connectivity & uninterrupted platform availability, privileged access, workload protection and so on for core Infrastructure and its management.
- **Cloud Management Portal**

  Neysa is responsible for the end-to-end availability and security aspects of the Velocis Cloud Management Portal.
- **Monitoring the Infrastructure**

  Neysa continuously monitors the platform's infrastructure, including infrastructure network traffic, server health, performance metrics and security anomalies. This proactive monitoring allows for quick identification of issues and potential security threats in core infrastructure.

- **Vulnerability Management and Patching**

  Vulnerability Detection: Neysa identifies and manages security vulnerabilities within the Velocis Infrastructure Platform. Regular assessments ensure that security weaknesses are addressed and mitigated.

  Patch Management: Critical security patches and updates are applied to the platform and infrastructure components to ensure the environment remains secure and up-to-date.

- **System Hardening**

  Neysa performs essential hardening of the systems and applications used within the Velocis Infrastructure Platform, applying security best practices to minimize the attack surface.

- **Management of the Velocis Infrastructure Platform**

  Neysa is responsible for the management, maintenance, and operation of the Velocis Infrastructure Platform, ensuring its availability, scalability, and security. Customers provision their Tenant Instances for running AI workloads, benefiting from a secure and reliable underlying infrastructure.

Customer's Responsibilities

Customers are responsible for securing and managing their own Tenant Instances (Security in the Cloud). This includes configurations related to the operating system, network, and application layers within their dedicated environment. Below are the key responsibilities of the customer:

- **Network Security**

  Customers are responsible for configuring and securing their internal network within their Tenant Instances and hosting the resources to access the Internet. This includes setting up firewalls, VPNs, network segmentation, and monitoring tenant network traffic for unauthorized access or anomalies.

- **Data Protection**

  Customers must manage encryption for data within their Tenant Instances, ensuring compliance with data protection standards and safeguarding sensitive information from unauthorized access. Also, ensure encryption for data in transit and apply additional data protection measures as needed. The methods by which any data is collected from or about end users is the Client's responsibility.

- **Tenant Instance Configuration**

  Customers are responsible for provisioning and configuring their own Tenant Instances on the Velocis Infrastructure Platform. This includes selecting appropriate operating systems, configuring networking, and setting up the environment to run their specific workloads.

  For specific cases where a dedicated environment is preferred by the customer, Neysa will support the initial configuration as per Customer requirement however the Security responsibility of the environment lies with the customer.

- **Operating System and Application Security**

  Neysa provides secure, hardened Linux OS images for select distributions, offering customers a reliable and secure base for their Tenant Instances. Customers can further secure and customize these images as needed.

  However, the Customer is still responsible for the security of the Operating System and their Applications. This includes further hardening, applying security patches, deploying & configuring the system firewall & Antivirus and implementing necessary application-level security measures to safeguard against threats.

- **Authentication & Authorization**

  Initial access credentials for workloads will be autogenerated during the provisioning. It is the Customer's responsibility to further provision additional accounts and perform the lifecycle management of the accounts and any additional integration.

It also includes the handling of Customer access accounts that are provisioned for the Velocis Cloud Management portal.

- **Logging and Security Monitoring**

  Customers are responsible for implementing their own monitoring, logging, and SIEM (Security Information and Event Management) solutions within their Tenant Instances. This ensures continuous monitoring of workloads and timely detection of any security events or anomalies. Also establish their own incident response procedures which include identifying, responding to, and mitigating potential security incidents or breaches within their Tenant Instances.

The image below visually represents the **Security Shared Responsibility Model** for Neysa Velocis: