SYMETRI
PART OF ADDNODE GROUP

NAVIATE

NEBULA

Security Whitepaper

Version 1.4 27 April 2026

CONTENTS

1. EXECUTIVE OVERVIEW

Symetri is committed to developing secure web applications to deliver our digital services, interact with customers, and maintain operational continuity. As digital transformation accelerates, so does the scale, sophistication, and frequency of cyber threats. Security breaches can result in significant business implications—including operational disruption, regulatory penalties, reputational and financial loss—making web application security a strategic imperative.

This whitepaper presents a comprehensive security framework overview for Naviate Nebula, built on the foundational principles of OWASP, the governance structure of ISO/IEC 27001, the regulatory requirements of the NIS 2 Directive, and modern automated security testing practices (SAST and DAST). Together, these elements enable a secure-by-design approach, spanning the full software development lifecycle and reinforcing Symetri's commitment to providing customers with secure, reliable, and resilient digital capabilities.

---

2. INTRODUCTION TO NAVIATE NEBULA

Naviate Nebula is a cloud-based platform designed to provide easy-to-use data management solutions. It facilitates the transfer of data between cloud storage applications such as Autodesk BIM360 and Autodesk Construction Cloud (ACC). Nebula does not store any user data other than connection information to third party cloud storage and other non-critical metadata such as transfer schedules, log files and temporary data such as project names, file names & paths.

Naviate Nebula's architecture leverages modern cloud-native services, emphasizing scalability, resilience, and defence-in-depth. This whitepaper outlines the security measures and principles that guide the design, development, deployment, and operation of the platform.

---

3. SECURITY OBJECTIVES

The primary security objectives for Naviate Nebula are to ensure:

3.1. Confidentiality
Ensuring that sensitive information is accessible only to authorized users.

3.2. Integrity
Protecting data from unauthorized alterations.

3.3. Availability
Ensuring that the application is available and operational when needed.

3.4. Accountability
Ensuring that actions can be traced to the responsible party.

---

4. ARCHITECTURE OVERVIEW

Naviate Nebula is built using a multi-tier architecture comprising:

4.1. Frontend

The user interface developed using modern web technologies including React with Typescript.

4.2. Backend

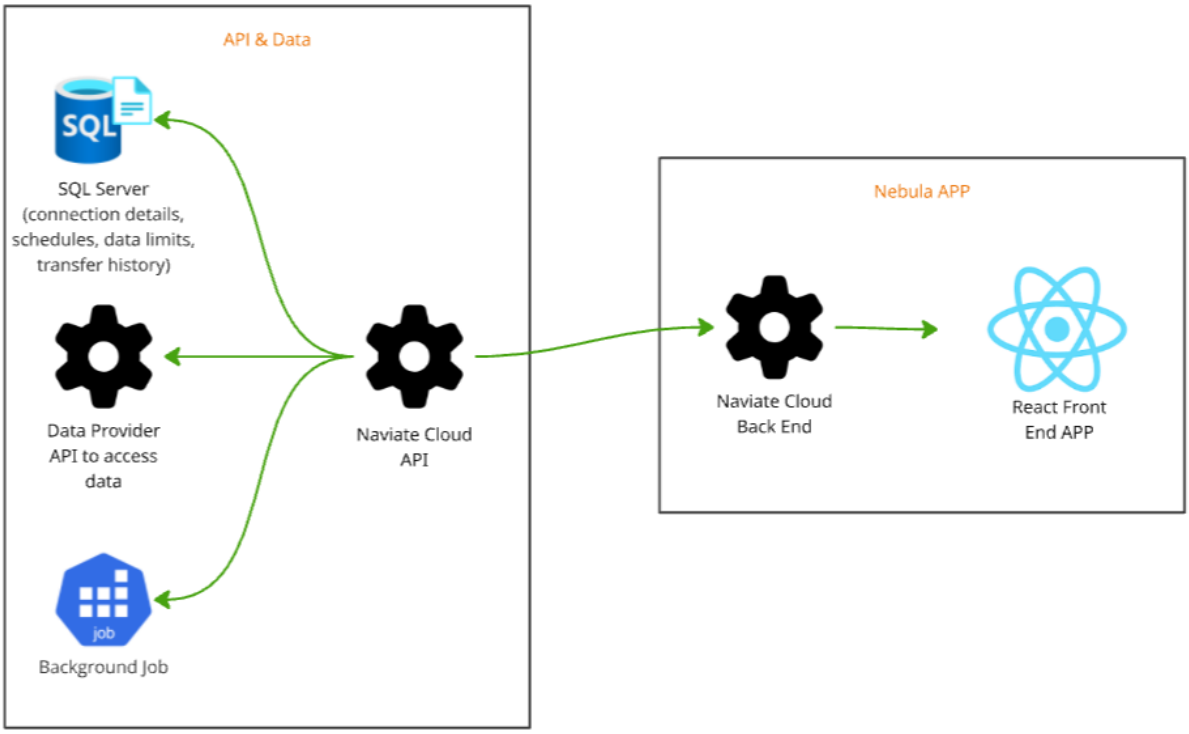
The server-side logic implemented using a robust C# framework.

4.3. Database

Secure SQL storage for application metadata.

4.4. APIs

Interfaces for communication between different components.



Naviate Nebula application runs on cloud infrastructure (using Microsoft Azure VM servers). Nothing is installed in the user's infrastructure, and the application is accessed using standard web browsers. Nebula functions as a streaming service, transferring data from the Source Accounts (Hubs) to the Destination Account (Hub). Data is not stored on Symetri systems, it is streamed from the Source to the Destination via the Symetri server. Only metadata related to the transfer is stored on the Symetri server e.g. connection details, transfer schedules, user data limits and transfer history.

Access to the Source and Destination Accounts (Hubs) is controlled by the vendor application (e.g. Autodesk Construction Cloud) security features. A valid user account is required, and the user must be granted permission to the Hubs / Projects / data in the vendor application. In addition, the Nebula / Cloud Manager App Integration must be added to all Accounts (Hubs) in the vendor application by the Account Administrator.

Access to metadata stored in the SQL Server is limited to the application server and cannot be accessed from any other source.

All API's are secured to prevent unauthorised access.

---

5. THREAT LANDSCAPE FOR MODERN WEB APPLICATIONS

Web applications today face a broad range of threats, including:

- Injection and input manipulation attacks
- Credential stuffing and brute-force attacks
- Misconfigurations in cloud infrastructure
- Malicious API traffic
- Supply chain vulnerabilities in open-source components
- Zero-day attacks targeting frameworks or libraries

These risk categories align with data from major threat intelligence sources and are directly reflected in the OWASP Top 10, making this framework an essential guide for Naviate Nebula's security approach.

---

6. OWASP SECURITY PRINCIPLES

Our development team are trained in OWASP principles and apply it's principles throughout the security architecture and Software Development Life Cycle.

6.1. OWASP Top 10 Alignment

Below is a summary of how Naviate Nebula addresses key OWASP categories:

A01: Broken Access Control

- Role-based access controls (RBAC)
- Principle of least privilege
- Multi-layered API authorization

A02: Cryptographic Failures

- TLS 1.2+/1.3 enforced encryption
- Encrypted data at rest using cloud-native KMS

A03: Injection

- Parameterized queries
- Strict input validation and sanitization frameworks

A04: Insecure Design

- Systematic threat modelling as part of SDLC
- Secure coding standards for all development teams

A05: Security Misconfiguration

- Automated configuration validation
- Baseline hardened templates for cloud deployments

A07: Identification and Authentication Failures

- Single sign-on (SSO) and MFA options
- Secure session management

A09: Security Logging and Monitoring Failures

- Centralized SIEM integration capability
- Anomaly detection for suspicious activity

6.2.3. OWASP ASVS (Application Security Verification Standard)

Naviate Nebula aligns to ASVS Level 2, applicable to enterprise-grade web applications.

---

7. ISO 27001 CERTIFICATION

Symetri Europe (including our technical division responsible for product development) are certified under ISO 27001:2022 as of March 2026. A copy of our certificate is available on request.

This provides a formal structure for managing information security through an Information Security Management System (ISMS).

This alignment ensures Naviate Nebula's processes follow global best practices and support audit readiness.

---

8. SOC 2 COMPLIANCE CONSIDERATIONS

Naviate Nebula aligns with core **SOC 2 (System and Organization Controls 2)** Trust Service Criteria, including:

- **Security** — access controls, change management, and robust monitoring.
- **Availability** — resilient Azure-based infrastructure with multi-zone redundancy.
- **Processing Integrity** — validated deployment processes, regression testing, and CI/CD quality gates.

- **Confidentiality** — encryption at rest and in transit, strict access controls, and secure key management.
- **Privacy** — alignment with GDPR data protection principles and structured data handling workflows.

These controls reinforce Naviate Nebula's commitment to maintaining a secure, available, and trustworthy SaaS environment.

---

9. NIS 2 DIRECTIVE COMPLIANCE CONSIDERATIONS

The **NIS 2 Directive** raises cybersecurity obligations for essential and important entities across the EU.

Naviate Nebula's security model supports compliance with core NIS 2 provisions including:

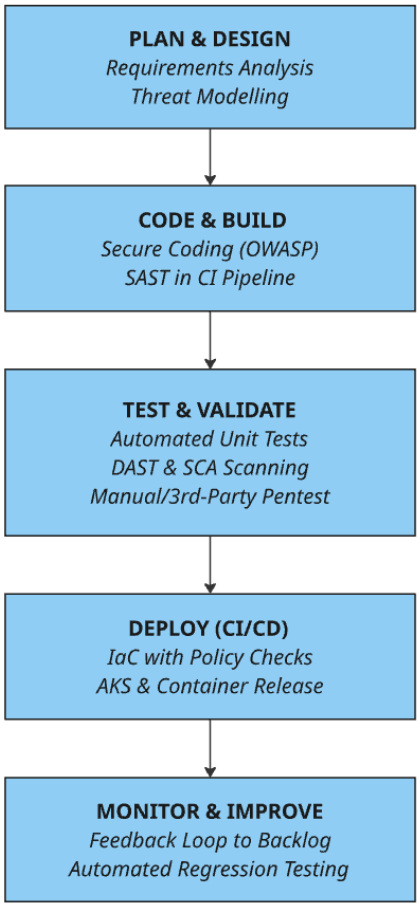
- **Risk management and mitigation**
- **Secure software and system development**
- **Incident detection and reporting procedures**
- **Access control and identity management**
- **Vulnerability management and patching requirements**

NIS 2 emphasizes supply chain security—an area addressed through Nebula's dependency vetting, SBOM tracking, and secure third-party integration processes.

---

10. SECURE SOFTWARE DEVELOPMENT LIFE CYCLE

Security is embedded throughout Naviate Nebula's software development lifecycle. Below is a visual representation of the CI/CD pipeline used in Naviate Nebula's development process:



10.1. Design Phase

- Threat modelling
- Attack surface mapping
- Secure architecture reviews

10.2. Development Phase

- Secure coding guidelines based on OWASP
- Mandatory code reviews
- SAST integrated into CI/CD pipelines

10.3. Testing Phase

- DAST on running services
- Penetration testing by internal and third-party specialists
- Dependency scanning for vulnerabilities (SCA)
- Automated unit & regression testing

10.4. Deployment & Operations

- Infrastructure-as-Code with validated templates
- Automated compliance scanning
- Continuous monitoring via SIEM and dashboards

10.5. Monitor & Improve

- Continuous improvement processes gather feedback from customers, product specialists and developers to help refine and improve the product.
- Automated regression testing helps to deliver improvements faster and with fewer defects

---

11. SAST & DAST INTEGRATION

Naviate Nebula uses automated and manual testing methods to detect vulnerabilities.

11.1. SAST (Static Application Security Testing)

SAST is integrated into the build pipeline to identify code-level vulnerabilities before deployment.

Benefits:

- Early detection
- Reduced remediation cost
- Enforcement of secure coding standards

11.2. DAST (Dynamic Application Security Testing)

DAST evaluates running services for behavioural and runtime vulnerabilities.

Benefits:

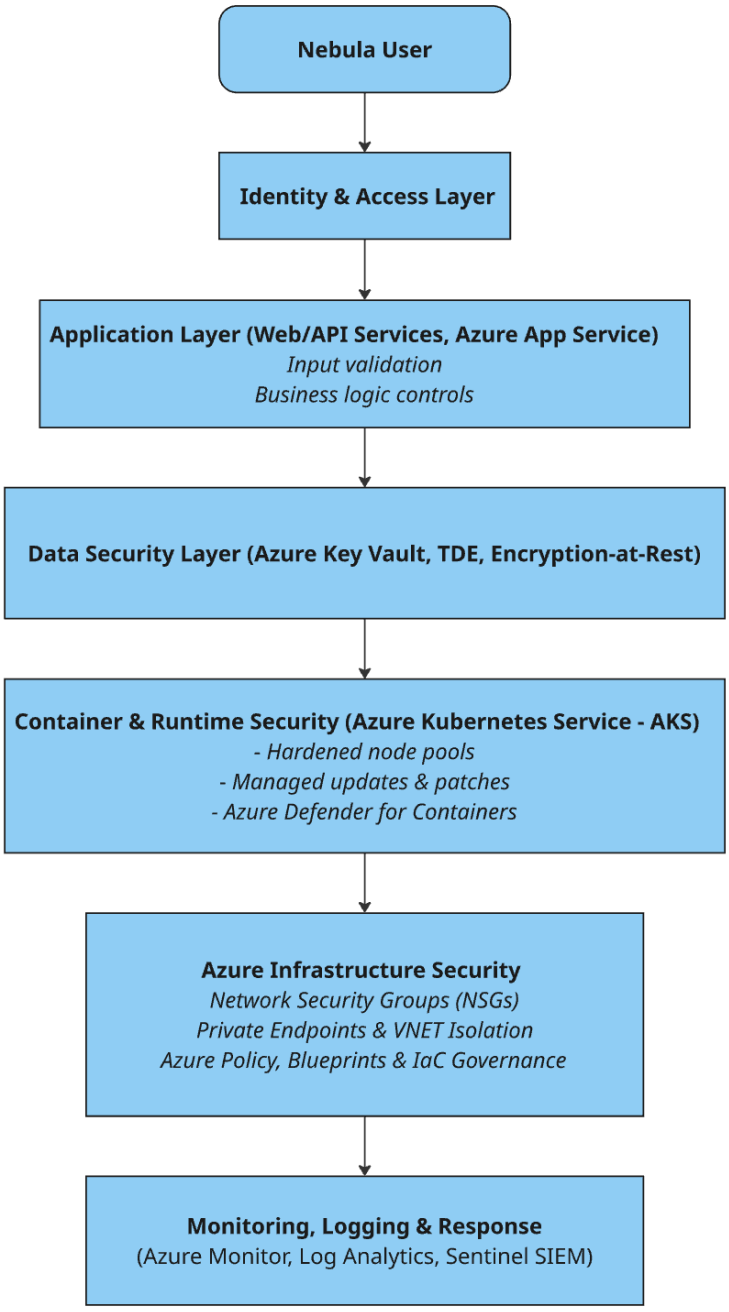
- Detects issues not visible in source code
- Validates configuration and authentication controls

Together, SAST and DAST form a comprehensive testing strategy aligned with modern DevSecOps practices.

---

12. SECURITY ARCHITECTURE OVERVIEW

Below is a conceptual diagram representing Naviate Nebula's layered security model, aligned with **Microsoft Azure's cloud platform**, including Azure-native security capabilities, managed container services, and built-in resilience tooling.



12.1. Azure Infrastructure Security Enhancements

Naviate Nebula leverages Microsoft Azure's cloud-native security framework to ensure a resilient and compliant hosting environment. Key enhancements include:

Network & Perimeter Security

- **Azure Virtual Networks (VNETs)** enabling tenant/data isolation.
- **Network Security Groups (NSGs)** enforcing granular ingress/egress rules.

Platform Governance & Compliance

- **Azure Policy** and **Azure Blueprints** enforce configuration baselines across all environments.
- **Role-Based Access Control (RBAC)** integrated with Microsoft Entra ID ensures least-privilege access.
- **Managed identities** prevent embedded secrets and strengthen workload identity management.

Secure Infrastructure-as-Code (IaC)

- Environment deployments are governed via **Terraform**, integrated with policy validation.
- Continuous compliance scanning evaluates every deployment for misconfiguration drift.

12.2. Use of Docker Containers on Azure for Resilience & Recovery

Naviate Nebula uses Docker containers to achieve high availability, consistency, and rapid recovery.

Container Resilience Features

- **Immutable container images** ensure predictable, reproducible deployments.
- **Self-healing orchestration** (automatic pod restart, node rescheduling) improves uptime.
- **Auto-scaling** based on real-time workload demands.

Security & Hardening

- **Azure Defender for Containers** scans images for vulnerabilities.
- **Azure Container Registry (ACR)** enforces image signing, scanning, and version governance.
- **Runtime sandboxing and namespace isolation** reduce the impact of potential compromise.

Disaster Recovery & Business Continuity

- **Instant redeployment** of container workloads across Azure regions.
- **Multi-zone AKS node pools** ensuring workloads survive availability zone failures.

These capabilities ensure Naviate Nebula can recover rapidly from infrastructure failures while remaining secure and operational across Azure's global cloud footprint.

---

13. CUSTOMER RESPONSIBILITIES

While Symetri ensures robust security, customers are also responsible for implementing their own robust procedures, for example:

- Managing user access and permissions appropriately on Nebula and connected platforms.
- Defining strong password policies on all platforms.
- Administration of user licences

---

14. CONTACT & SUPPORT

Please raise a support ticket for any security-related inquiries:

Support Portal: https://my.symetri.com/MySupport

---

15. CONCLUSION

Security is foundational to the design, development, and operation of **Naviate Nebula**. By aligning with OWASP guidance, ISO 27001 principles, NIS 2 regulatory requirements, and integrating modern SAST/DAST practices, Naviate Nebula delivers a security posture that is proactive, comprehensive, and continuously improving.

This commitment ensures customers can trust Naviate Nebula to protect their data, intellectual property, and mission-critical workflows across the entire digital lifecycle.

---

16. FAQ'S

1. How is my data protected?

We use industry-standard encryption protocols (such as TLS/SSL) to protect your data in transit and at rest. Our systems are regularly audited and monitored for vulnerabilities.

2. Where is my data stored?

Your data is stored in secure data centres located in the EU or US. These facilities comply with international security standards such as ISO 27001 and SOC 2.

3. Who has access to my data?

Access to customer data is strictly limited to authorized personnel and is managed by the customer on the relevant cloud storage application. Access to metadata stored on Symetri server is limited to those who have a legitimate need to provide support or maintain the system.

4. Do you comply with GDPR or other privacy regulations?

Yes, we are fully compliant with GDPR and other applicable data protection laws. You can read more in our Privacy Policy.

5. What should I do if I suspect unauthorized access to my account?

Immediately reset your password and contact our support team at https://my.symetri.com/MySupport. We'll investigate and help secure your account.

6. Do you offer multi-factor authentication (MFA)?

Yes, we strongly recommend enabling MFA for an added layer of security. You can activate it in your account settings.

7. How often do you perform security audits?

We conduct regular internal and third-party security audits to ensure our systems remain secure and up to date.

8. Can I delete my data permanently?

Yes, you can request permanent deletion of your data by contacting our support team. Once deleted, the data cannot be recovered.

9. How do you handle data breaches?

In the unlikely event of a data breach, we follow a strict incident response plan, notify affected users promptly, and take corrective actions to prevent recurrence.

10. Is my payment information secure?

Nebula does not store any payment information or process any financial data.