# Controls to safeguard the confidentiality, integrity and availability of data

## Authentication and access management

Industry-leading external service Auth0 is used for customer authentication.

We support (and recommend) Single Sign-On for customer login.

All authentication events are logged and continuously monitored.

## Monitoring and response

All security events are monitored using best-in-class monitoring and analytics tools.

We use multiple vulnerability detection technologies to scan our infrastructure and applications.

Annual penetration tests are carried out by external experts to ensure our resilience against cyber attacks.

## Data storage and usage

All customer data is stored in AWS managed databases hosted in EU (Ireland).

Each customer's data is segregated through database schemas.

Anonymized data is used on an aggregated level to enhance the product and generate value for all customers.

No Personal Identifiable Information (PII) is needed nor persisted in the ZeroNorth platform.

## Availability and Scaling

AWS CloudFront and Load balancer ensures low latency and high availability

AWS allows us to horizontally scale web servers within minutes

## Encryption and backup

Data is encrypted with industry standard AES-256 encryption algorithm in both transit and at rest.

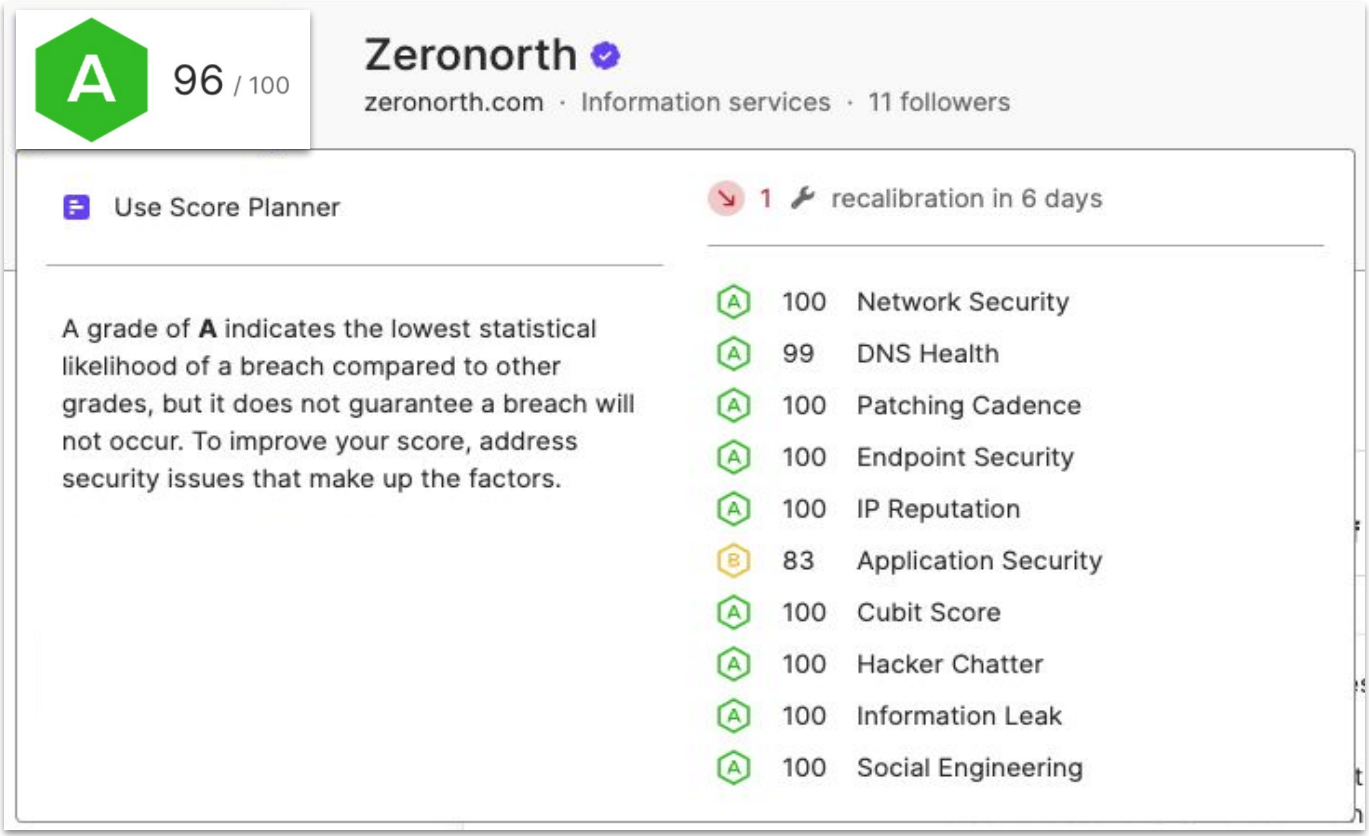
Data integrations are done either through our secure REST API (3rd party authentication with M2M-tokens per customer), SFTP server or our ISAE 3402 Type II audited integration partner Youredi Oy.

All keys are governed in AWS Key Management Service.

Data is backed up per AWS best practices.
Restoration tests are frequently executed.
Recovery Time Objective (RTO) < 6 hours.
Recovery Point Objective (RPO) < 2 hours.

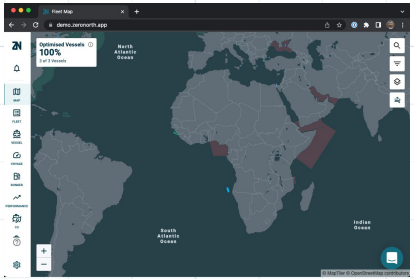
ZERO NORTH

# External security rating by Security Scorecard



# Security stack

aws



## Vulnerability scan

Heyhack

BurpSuite

AWS Inspector

## Penetration test

VANCORD

nccgroup

## Authentication

Auth0

SSO

AWS IAM

## Availability & protection

AWS Cloudfront

AWS Loadbalancer

Firewall & WAF

## Storage & Backup

AWS Encryption KMS

AWS Backup

## Monitoring

AWS Cloudwatch

AWS Cloudtrail

AWS Guardduty

DATADOG

## Orchestration

docker

Terraform

## Code and infra security

GitHub Enterprise

Dependabot

DATADOG

CSPM

## Endpoint protection

macOS

hexnode

XPROTECT

## Governance

NIST National Institute of Standards and Technology

IDENTIFY PROTECT DETECT RESPOND RECOVER

OWASP Open Web Application Security Project

# Data FAQ

## Who can see my information?

Access to the data is available only through the restricted access control layer implemented through the application. We also use various encryption techniques to ensure data residing on the cloud and data transferring over the cloud is protected and accessible only by the authorized users. The following entities or users are covered by this policy:

- Full or part-time employees of ZeroNorth who have access to ZeroNorth or customer data.
- ZeroNorth vendors or processors who have access to ZeroNorth or customer data.
- Other persons, entities, or organizations that have access to ZeroNorth or customer data.

All network, system, and application events must only result from allowable actions through access control mechanisms. Permission may be derived directly from an individual's identity, or from a job classification or administrative privilege based on that individual's identity. The principle of "least privilege" specifies that individuals only be granted permission for actions needed to perform their jobs.

Limiting actions to those properly authorized protects the confidentiality and integrity of data within the ZeroNorth processing environment.

In this context, access control refers to a security service that allows or denies a user request based on privilege, group information, or context. Confidentiality refers to a security service that prevents disclosure of information to unauthorized parties while the information is in use or transit or being stored.

## How much control do I retain over my data?

Clients have complete control as well as ownership of their data. With necessary access credentials, Client users can access data anytime, anywhere in the world.

## Will ZeroNorth use my data?

ZeroNorth will, unless otherwise specified by the client, aggregate any and all data entered the application to formulate anonymized voyage data, trends and insights that would be beneficial to voyage management. ZeroNorth takes the utmost care in anonymizing this aggregated data so anything published or sent externally could not be identified or tied to any one client of the application.

## How is activity in my account monitored and tracked?

Appropriate logging techniques are in place at the AWS, local operating system and database levels to capture valuable metrics and events. At the individual application level, audit control is maintained with clear indication of user, date/time capture on creation and modification of data.