Controls to safeguard the confidentiality, integrity and availability of data

Authentication and Access Management

We support (and recommend) Single Sign-On via SAML through Azure Active Directory

Duo security is used for Multi-Factor Authentication

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 US East-1 (N. Virginia) with a cold site contingency environment in US East-2 (Ohio)

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

Web servers and databases are striped across multiple availability zones

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

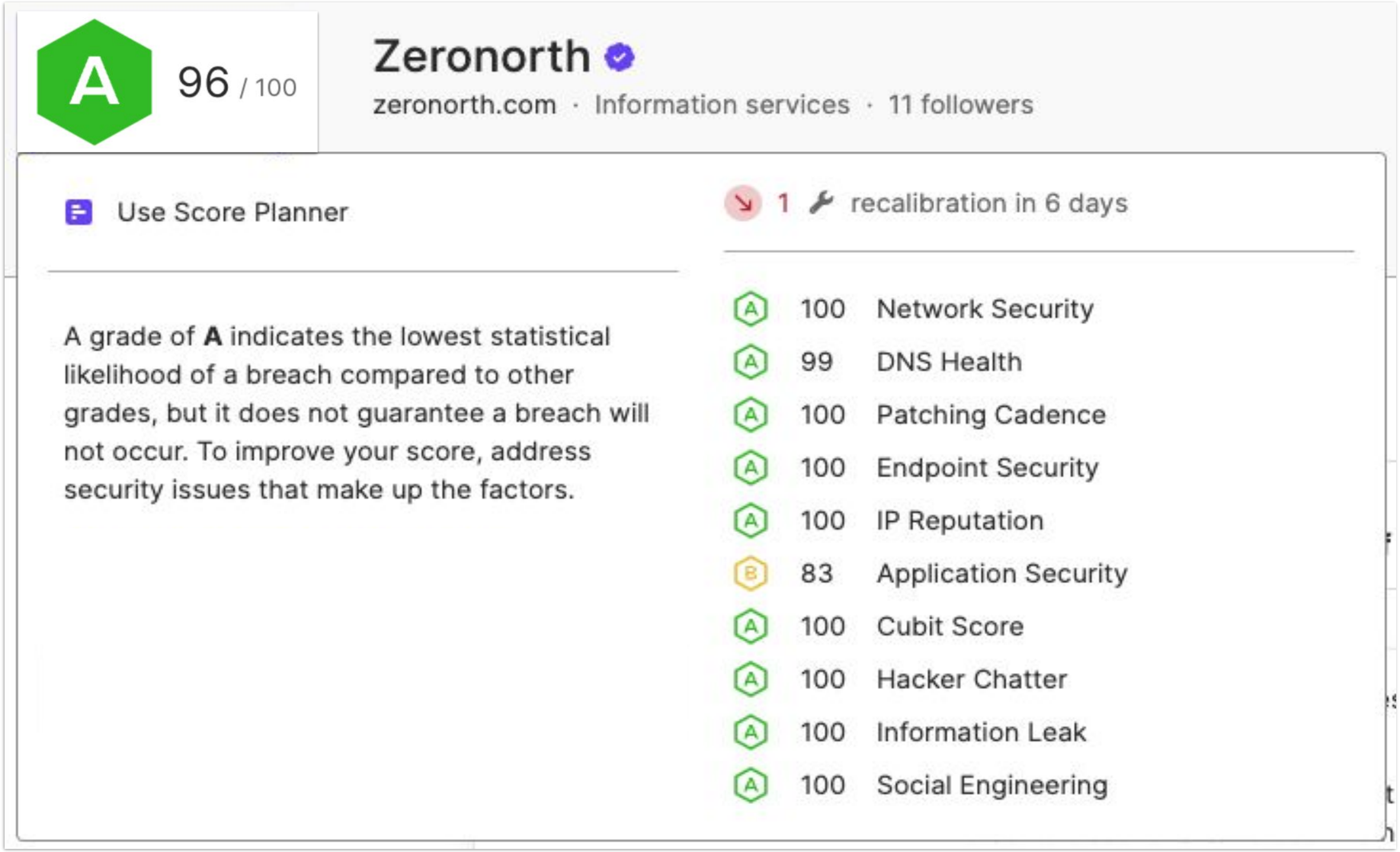
VMS Integrations are performed via an API where an XML file using an authentication token is sent to ZN Bunker via whitelisted servers

All keys are governed in AWS Key Management Service

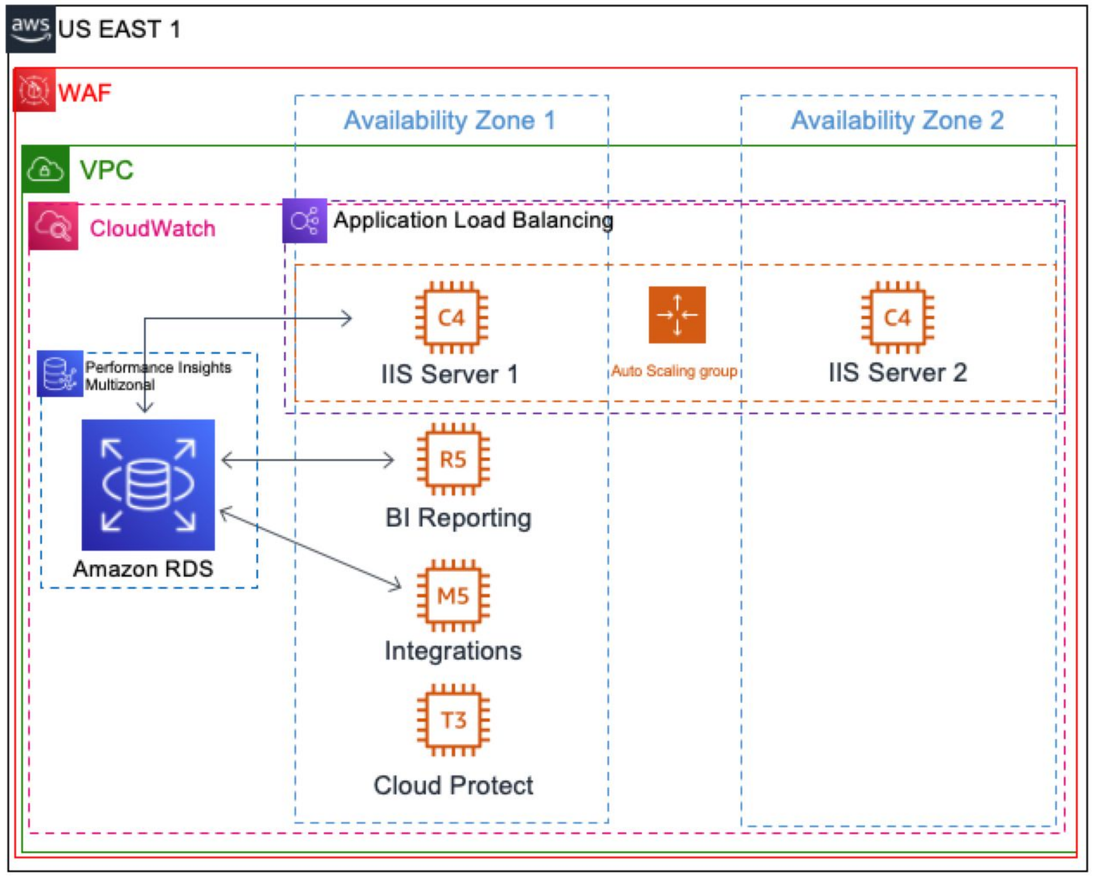
Data is backed up per AWS best practices
Recovery Time Objective (RTO) < 6 hours
Recovery Point Objective (RPO) < 2 hours
Disaster Recovery Plan is tested Bi-Annually

ZERO NORTH

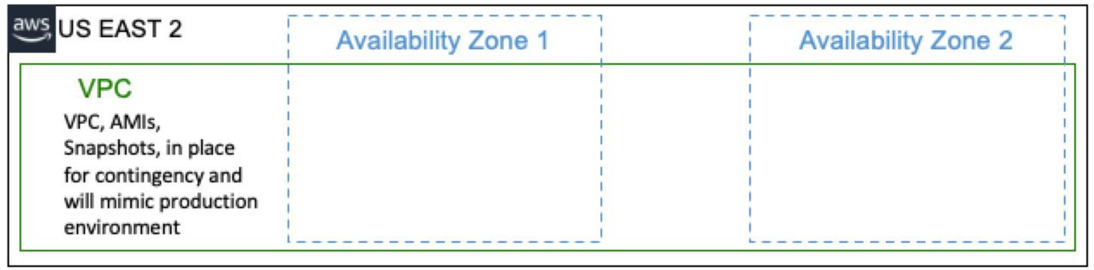
External security rating by Security Scorecard



Hosting



Disaster Recovery Warm Site



Security Stack

SDLC	• GitHub • Jenkins • Annual Source Code Review by Independent Consultant
Infrastructure	• OpenVPN • Encrypted EBS and RDS • Private S3 Buckets • ALB Crypto Protocols • AWS Security Groups / ACL
Alerting and Monitoring	• AWS CloudWatch/AWS Athena (Infrastructure) • DataDog (Application Performance Monitor) • AWS Performance Insights (RDS SQL DB)
Application Security	• AWS Web Application Firewall • AWS Inspector scan and patch management • BurpSuite Web Application Scanning • Vulnerability scans (OpenVAS, Nuclei, Nmap) • Regular reviews of 3rd Party Dependencies • Annual Penetration Test by Independent Consultant
Data Backups and Protection	• N2WS Cloud Protect Manager (Regularly scheduled polices of production and DR region)
Internal Endpoint Protection	• Hexnode Mobile Device Management • SSO/MFA on all Accounts • Credentials stored on 1Password

ZERO NORTH

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 ZN Bunker who have access to ZN Bunker or customer data.
- ZN Bunker vendors or processors who have access to ZN Bunker or customer data.
- Other persons, entities, or organizations that have access to ZN Bunker 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 ZN Bunker 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 ZN Bunker use my data?

ZN Bunker will, unless otherwise specified by the client, aggregate any and all data entered the application to formulate anonymized market data, trends and insights that would be beneficial to the purchasing of bunkers and voyage management. ZN Bunker 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.