# TerraSoft Platform Security

## Product Security

TerraSoft's Secure Systems Development Life Cycle (SSDLC) ensures that security is incorporated from the inception of a new project and continued throughout the entire client relationship. The security of services and applications is vital to maintain the reliability and integrity of data under the stewardship of TerraSoft.

This added safeguard has become increasingly important in recent years as applications become more complex, and the cost of remediating a vulnerability after release is often significantly higher than if it had been detected during the early stages of development.

We write secure-by-design software, employing product security engineers to work with engineering from ideation through release.

TerraSoft's SSDLC provides a single comprehensive risk-based process model that governs how engineering projects are planned, implemented, and delivered to ensure the system functions securely and is fit for its intended use.

The scope of the SSDLC includes all system development and integration projects used for and in support of the TerraSoft service. Further, this process is applied to all project efforts associated with the design, execution, migration, and maintenance of new and existing system.

## Security Monitoring (DigitalOcean's)

Terra Translations' has entrusted DigitalOcean to provide cloud-based services.  DigitalOcean's security team monitors and analyzes system components to identify potentially malicious activity within our infrastructure. In addition, user and system behaviors are closely monitored to detect suspicious behavior; in turn, investigations are performed following incident reporting and response procedures.

## Snapshot and Backup Security (DigitalOcean)

Snapshots and backups are stored on an internal, non-publicly visible network on NAS/SAN servers. Customers can directly manage the regions where their snapshots and backups exist. This customization allows customers to control where their data resides within DigitalOcean's datacenters for security and compliance purposes.

## Vulnerability Management

Once software is released, Terra initiates automated vulnerability scanning on a weekly schedule of all our servers and instances.

Daily: All new instances are scanned as they are added to the production environment

Weekly: All content automatically undergoes vulnerability scans

At least every 6-months: We initiate third-party penetration tests

All new features: We perform end-to-end third-party penetration tests

## Access Control

At TerraSoft, we follow the principle of least privilege, including the logical conclusion Zero Trust. The practice of Zero Trust provides employees with the minimal access necessary for their job functions, inclusive of access to software and infrastructure, such that no component of the system has more access than it requires to do the job; this is an important component of how we deliver defense-in-depth. Existing access is audited on a regular basis to ensure that employees only have the permissions necessary to perform their duties.

## Endpoint Protection

TerraSoft employs specific endpoint protection tools depending on system type. In addition, TerraSoft leverages a broader philosophy around 'defense-in-depth' where multiple protections are in place and no single control is relied on to provide adequate protection. This strengthens the holistic approach to security for Terra as a company, as well as client partners.

## Data Encryption At-rest and In-transit

TerraSoft helps you prevent critical identity data from falling into the wrong hands. We never store passwords as clear text — they are always hashed and salted securely using bcrypt.

Certain data-at-rest and in-motion is encrypted — all network communication uses transport layer security (TLS) with at least 128-bit advanced encryption standard (AES) encryption.

The connection uses TLS, and it is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

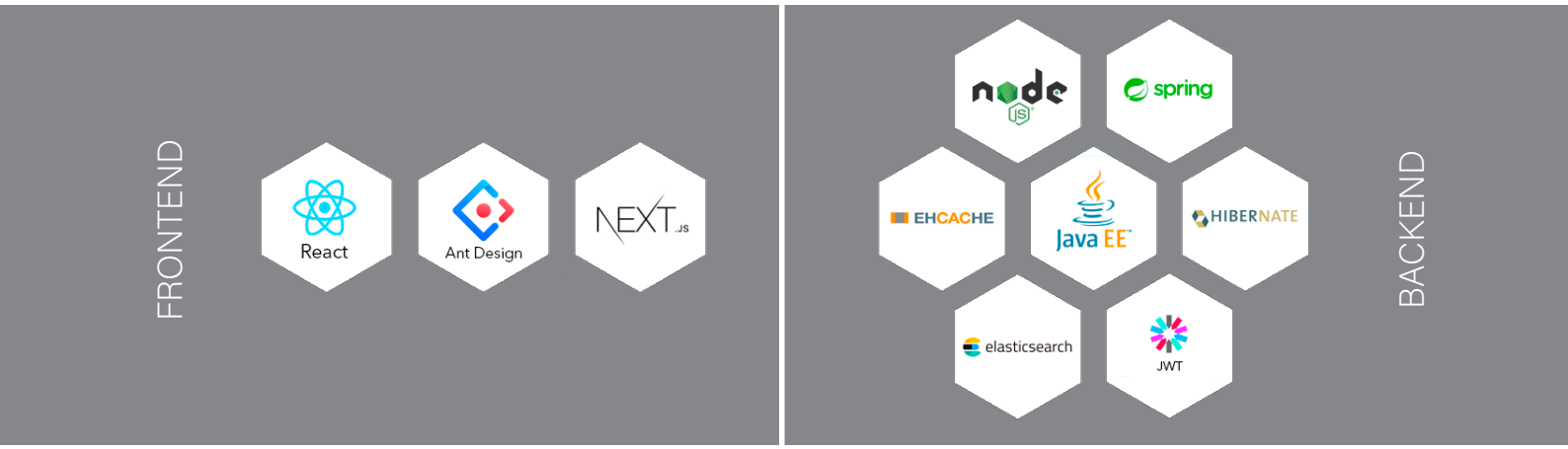
## DDoS protection

All TerraSoft services have built-in rate limiting and automated blocking features to mitigate advanced denial-of-service or authentication attacks.

The TerraSoft network infrastructure is protected against volumetric attacks by their cloud providers, in addition to a dedicated DDoS mitigation service.

To protect the platform, the TerraSoft system imposes rate limits on APIs and database calls.

## Technology used




In its frontend, TerraSoft utilizes the most advanced and innovative technology, allowing for a simple, intuitive, and easy-to-use experience.

At its core, the backend is a JavaEE application with other frameworks and technologies that secure the transaction ease, the security, the speed, and the scalability.

As a result, TerraSoft is not only an attractive and innovative product, it is also secure, user-friendly, and scalable.

## Architecture

TerraSoft's architecture is based on microservices, continuous integration, continuous delivery, and continuous deployment.