erNavigator

Data Security

Enterprise-Grade Security

Enterprises across the globe trust the erNavigator to manage their labor & employee relations processes, data, and collaboration in the cloud.

Security overview

1. Collaborate in a secure environment

Thousands of users, trust erNavigator for managing their labor & employee relations processes through collaboration in the cloud. Security of personal data, case-related information, files, and interactions within our system is our top priority. Which is why we are constantly focusing our efforts on maintaining the reliability of our product, infrastructure, technologies, and procedures. As we provide you with an easy-to-use, flexible, and scalable process management application, it is vital for us to ensure a trustworthy and reliable service, with comprehensive security at all levels. Below, you can read an overview of erNavigator's security model — physical, network, system, application, and people. For our European customers, with EU Data Privacy mandates, erNavigator is compliant with GDPR including an EU data center location that retains customer sensitive data within the EU.

2. Physical security

World-Class datacenters in US and EU:

erNavigator hosts their services within the Microsoft AZURE cloud platform environment located in the U.S and EU:

More certifications than any other cloud provider.

Microsoft leads the industry in establishing clear security and privacy requirements and then consistently meeting these requirements. Azure meets a broad set of international and industry-specific compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate.

All server and network components are monitored by internal erNavigator support staff. erNavigator's Disaster Recovery infrastructure also resides in the Microsoft Cloud Platform for both US and EU regions, having great scalability and security. Access to each system, network device, and application is limited to authorized personnel, and login details within the event logs are reviewed on a regular basis.

- AZURE Data Centers in the U.S.

- AZURE European Data is hosted in Ireland and this data center retains EU customer data within EU only.

Uptime over 99.9%

Over years of continuous service, erNavigator has consistently met or exceeded 99.9% uptime outside of scheduled maintenance periods, ensuring customers can access their processes and data when needed without interruption.

Continuous data backup

erNavigator is running real-time database replication, to ensure that customer data is both backed up and available on redundant and geographically dispersed servers, physically separated from the primary erNavigator application servers, aiming to ensure fault tolerance.

3. Network and System Security

Tenable Network Security Infrastructure

erNavigator uses industry-standard network protection procedures, and secure connectivity, this allows us to prevent, detect, and promptly remediate impacts of malicious traffic and network attacks.

Regular Updates and Patch Management

Internal network security audits and scanning gives us an overview for quick identification of outdated systems and services. According to the in-house patch management policy: operating systems, software, frameworks, and libraries used in erNavigator infrastructure are updated to the latest versions on a regular basis. Whenever a vulnerability is reported, prompt actions are taken to mitigate any potential risks for our customers — we apply patches promptly upon availability.

4. Application security

Application Security Process

- An in-depth Application Security Life Cycle process is fully integrated into erNavigator's Software Development Life Cycle (SDLC), including:
- Defined in-house security requirements and policies, and well-known security best practices applied in every stage of the lifecycle.
- Security review of architectures, design of features, and solutions.
- Iterative manual and automated (using static code analyzers) source code review for security weaknesses, vulnerabilities, and code quality, and providing of sufficient advice and guidance to the development team.
- Regular manual assessment and dynamic scanning of pre-production environment.

- Security trainings conducted for IT teams according to their respective job roles.

Authentication and Access Control

Each user in erNavigator has a unique account with a verified email address, and protected with a password, which are validated against password policies and stored securely using a strong hashing algorithm with unique salt for every password. 2-Factor Authentication is available as an additional security measure to protect erNavigator accounts. erNavigator also supports multiple methods of federated authentication, including Google Open ID, Azure, Office 365, ADFS and SAML V2, to conveniently and securely gain access to erNavigator account leveraging corporate credentials. An erNavigator account administrator manages and controls individual user rights by granting specific types of user licenses. Customer data can only be accessed by other users within your erNavigator account if access were specifically shared with them. Otherwise, your data is not accessible by other erNavigator users.

Monitoring user activities

erNavigator offers the possibility to get a report with up-to-date account activity information.

Data Encryption

erNavigator uses Transport Layer Security (TLS) TLS 1.2 with a preferred AES 256 bit algorithm in CBC mode and 2048-bit server key length with most modern browsers. When you access erNavigator via a web browser, mobile applications, email add-in, or browser extension, TLS technology protects your information using both server authentication and data encryption. This is equivalent to network security methods used in banking and leading e-commerce sites. All users of erNavigator get the same encryption reliability, regardless of their subscription type, so that your passwords, cookies, and sensitive information is reliably protected from all eavesdropping. User files uploaded to erNavigator servers are automatically encrypted with AES 256 using per file keys. If someone were to gain physical access to the file storage, this data would be encrypted and impossible to read directly. These encryption keys are stored in a secure key vault, which is a separate database decoupled from the file storage layer.

5. Organizational Security

Processes

We have a disciplined approach to processes. This includes policies about escalation, management, knowledge sharing, risk management, as well as the day-to-day operations. erNavigator's operations team have years of experience and we continually improve our processes over time. All these elements are essential parts of our culture.

Need-to-Know and Least Privilege

Only a limited set of employees have access the data stored in our databases: there are strict security policies for employee access, all security events are logged and monitored, and our authentication methods and data are strictly regulated. We limit access to customer data to employees with a job-related need and require all those staff members to sign and agree to be bound by a confidentiality agreement. Accessing customer data, is only done on an as-needed basis.

6. Enterprise Grade Security

If you have any security concerns, please contact our support line and they will provide you with additional information regarding our security maturity.

erNavigator

www.ernavigator.com

North America

Contact Person: Grant Skinner
Telephone: +1 (416) 300 9194
E-mail: grant@ernavigator.com

EMEA (Europe, Middle East, Africa)

Contact Person: Michael Fisher
Telephone: +27 (11) 656 4950
E-mail: sales@ernavigator.com

DISCLAIMER: This document is and shall at all times be subject to erNavigator terms and conditions.

CONFIDENTIAL INFORMATION. This document contains confidential information, which is proprietary to erNavigator. No part of its contents may be used, copied, disclosed, or conveyed to any other party in any manner whatsoever without prior written permission from erNavigator and at all times will be subject to erNavigator terms and conditions.