trengo

Trengo's vision on security

September 2024

trengo.com

Trengo's vision on security

At Trengo, we prioritise security, recognising that it is a fundamental aspect of our commitment to delivering reliable and trustworthy services. Security is a technical requirement and a core principle that underpins everything we do.

We understand that safeguarding data and protecting against threats requires a multifaceted approach in today's digital landscape. This is why we view security through a comprehensive quadrant model that covers every angle, from the systems we operate to the people involved.

Our security quadrant has four essential areas: systems, people, customers, and company. This model reflects our belief that effective security is a collaborative effort. Trengo's responsibility to secure our environment is not solely its; it's a partnership with our customers. We provide the tools, technologies, and practices necessary for robust protection, but we also rely on our customers to actively maintain their security.

Adopting this quadrant approach ensures that every security aspect is noticed. We work with our customers to address potential risks and implement best practices. This shared responsibility helps us build a secure, resilient platform that meets and exceeds industry standards. Through continuous communication and mutual effort, we aim to create a safe environment where Trengo and our customers can thrive.

Find below a holistic view of security:

Your Employees

At Trengo, we recognise that human actions on the customer side play a crucial role in overall security. We are committed to providing our customers with accessible tools, clear guidance, and informative resources to empower their employees to practise good security habits. By offering user-friendly tools and comprehensive support materials, we aim to make it easier for customers to implement effective security measures and reduce potential risks.

While we provide these resources and recommendations, ongoing training and awareness are essential. We encourage our customers to actively educate their employees about security best practices, which are vital to creating a secure environment. Trengo views this as a collaborative effort, where our proactive support and the customer's internal training contribute to a robust security posture.

You can access our public product documentation at our Help Centre. We also have an invite-only customer Academy, including video courses detailing our product setup for Trengo users.

System Configuration on your side

Our platform provides customers robust security features that enhance system protection and control. We offer customisable roles and permissions, allowing you to set precise access levels for different users to manage access tightly. Additionally, integrating Two-Factor Authentication (2FA) adds a crucial layer of security for user accounts, with the flexibility to enforce mandatory 2FA for all employees, fortifying your defence against unauthorised access.

To maintain secure communications, we use TLS encryption, which protects data during transmission between your systems and our platform. We also employ OAuth2, a standardised method for safe authentication, for secure and efficient third-party integrations. These features safeguard you against potential threats and empower you to configure your systems confidently.

Trengo's Employees

Cultivating a strong security culture is integral to our operations. Active discussions on security practices and emerging threats are a regular part of our internal dialogue. This ongoing engagement ensures that every Trengoat remains informed about the latest security protocols and best practices, reinforcing our collective commitment to protecting our systems and customer data.

New hires undergo rigorous security training during their onboarding, which equips them with the essential knowledge to uphold our high-security standards from the outset. Additionally, customer-facing teams participate in regular awareness training, preparing them to manage security-related inquiries and incidents with expertise. This comprehensive approach ensures that every team member plays a vital role in maintaining a secure and resilient environment, demonstrating our dedication to internal and external security.

Trengo's SaaS Service offering

Our service is built on the fundamental principle of "secure by design," ensuring that security is integrated into every aspect of our platform from the ground up. This approach involves making strategic design choices to minimise human factors that could compromise security, thereby reducing potential vulnerabilities. By embedding security into the very fabric of our systems, we create a robust foundation that upholds the highest standards of protection.

To enhance our security posture further, we implement rigid procedures such as regular access reviews and the principle of least privilege. These practices help to limit the attack surface by ensuring that users and systems have only the access necessary for their roles, mitigating the risk of unauthorised access. Additionally, secure backups and data encryption are integral components of our service, ensuring that data is protected, private, and fully compliant with GDPR in Europe.

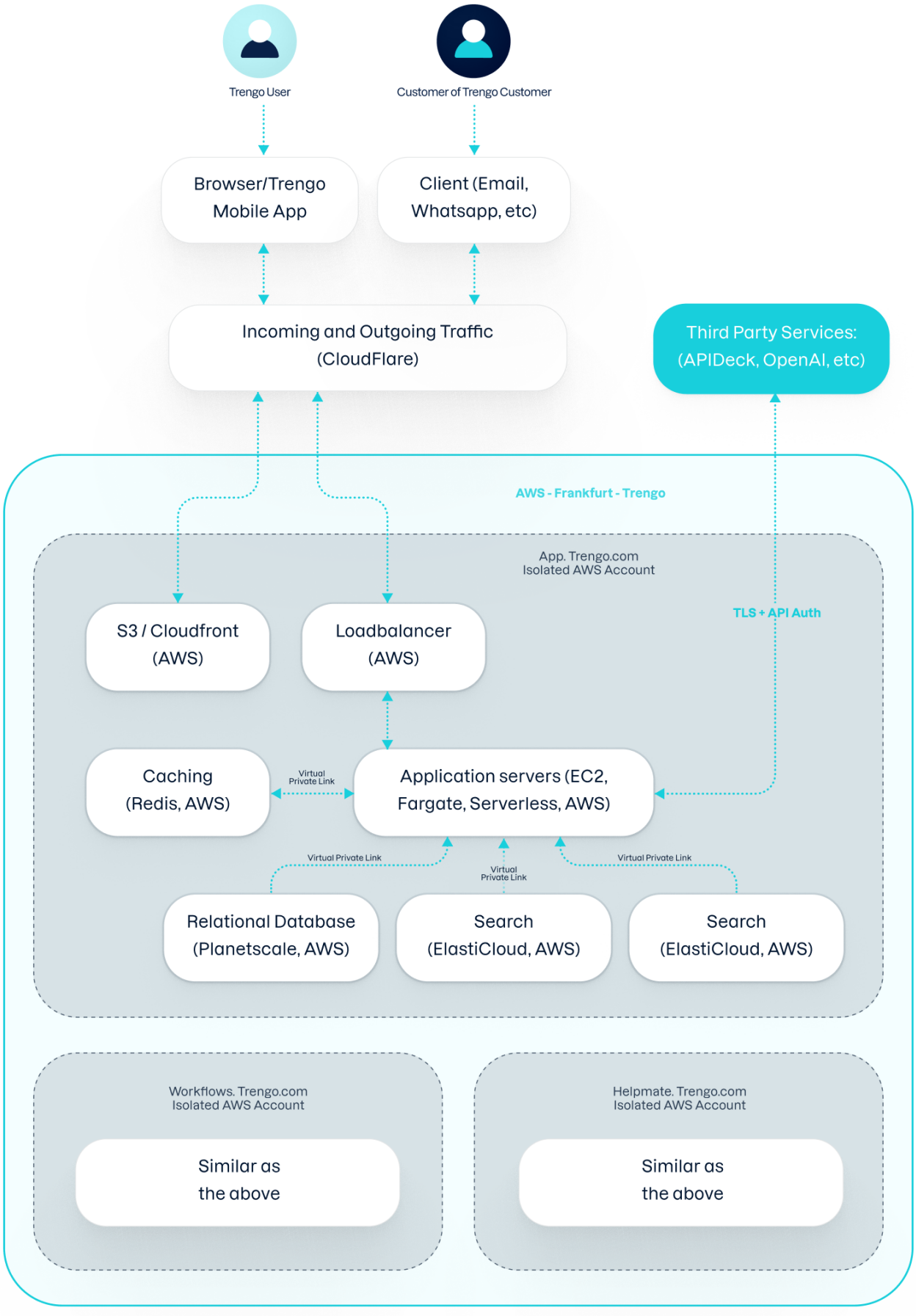
Our commitment to security extends to the connections we maintain with carriers on behalf of our customers. We ensure these connections are as secure as possible, utilising advanced encryption and security measures to safeguard data transmission. This comprehensive approach guarantees that every interaction with our platform is protected, reinforcing our dedication to delivering a secure and reliable service.

Trengo cloud network / architecture diagram

Trengo utilises a Platform-as-a-Service (PaaS) oriented cloud architecture to streamline operations and change management while adhering to industry best practices. By leveraging PaaS services, we ensure that our infrastructure is managed efficiently and follows established standards. We also minimise exposure to open networks by favouring traffic-specific peer-to-peer connections through Virtual Private Links. This approach enhances security by making it challenging for unauthorised access to compromise other services, even if threats target our application servers.

We develop our applications using a consistent architectural framework to promote simplicity and reduce the risk of human error. This uniformity enhances operational efficiency and facilitates seamless transferability and scalability across different systems and environments.

To ensure optimal global availability and enable central monitoring and traffic control—including protection against DDoS attacks—we have chosen to connect to the Edge through Cloudflare. This integration allows us to leverage Cloudflare's extensive network to enhance performance, security, and resilience across all regions.


Trengo User
Customer of Trengo Customer
Browser/Trengo Mobile App
Client (Email, Whatsapp, etc)
Incoming and Outgoing Traffic (CloudFlare)
Third Party Services: (APIDeck, OpenAI, etc)
AWS - Frankfurt - Trengo
App. Trengo.com Isolated AWS Account
TLS + API Auth
S3 / Cloudfront (AWS)
Loadbalancer (AWS)
Caching (Redis, AWS)
Virtual Private Link
Application servers (EC2, Fargate, Serverless, AWS)
Virtual Private Link
Virtual Private Link
Virtual Private Link
Relational Database (Planetscale, AWS)
Search (ElastiCloud, AWS)
Search (ElastiCloud, AWS)
Workflows. Trengo.com Isolated AWS Account
Similar as the above
Helpmate. Trengo.com Isolated AWS Account
Similar as the above

Frequently Asked Questions

What is the difference between SaaS and Self-hosted/On-Premise?

An on-premises solution is a system hosted and managed internally within a specific location, though it may receive support from third-party vendors. In contrast, off-premises solutions, often synonymous with cloud-based solutions, are hosted and supported by external third parties and can serve various locations. While on-premises solutions are confined to a particular physical site, off-premises solutions operate externally and are accessible from multiple venues.

SaaS (Software as a Service) represents a model where the service provider predominantly hosts and maintains the software. This setup allows users to access applications and data remotely, eliminating the need to request information from internal enterprise servers.

How do you ensure data encryption both at rest and in transit?

To protect the confidentiality and integrity of our customers' data, we employ robust encryption protocols for data at rest and in transit.

Data at Rest:

- **Encryption Standards:** We use industry-standard encryption algorithms, such as AES-256, to encrypt all stored data, including databases, file storage, and backups.
- **Key Management, Encryption:** We manage keys securely using a centralised key management system (KMS) that follows best practices, such as regular key rotation and strict access controls.
- **Access Controls:** Access to encrypted data is restricted to authorised personnel only and is monitored and audited regularly to ensure compliance with our security policies.

Data in Transit:

- **Transport Layer Security (TLS):** We use TLS 1.2 or higher to encrypt data transmitted between our servers and client devices. This ensures that data cannot be intercepted or tampered with during transmission.
- **Secure APIs:** All API communications are secured using HTTPS, which employs TLS to protect data exchanges between systems.

Frequently Asked Questions

What security standards does your SaaS solution adhere to?

We designed our SaaS solution to meet stringent security standards and ensure the highest level of protection for our customer's data. Specifically, we adhere to the following security standards:

- **NIST Cybersecurity Framework:** We align our security practices with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This framework provides comprehensive guidelines for improving the resilience and security of our information systems. It includes best practices for identifying, protecting, detecting, responding to, and recovering from cyber threats.
- **GDPR Compliance:** We ensure compliance with the General Data Protection Regulation (GDPR) for our customers in the European Union. This includes stringent data protection measures, transparent data processing practices, and upholding data subjects' rights.

What are your protocols for data backup?

We have implemented comprehensive data backup protocols to ensure the integrity and availability of our customers' data. These protocols are designed to protect against data loss and ensure rapid recovery during a disruption.

- **Regular Backups:** We perform regular automated backups of all critical data. This includes full weekly backups and daily incremental backups to minimise data loss.
- **Redundant Storage:** Backups are stored in geographically diverse, redundant locations to protect against physical disasters. We use highly secure cloud storage solutions with built-in redundancy and high availability.
- **Encryption:** All backup data is encrypted both in transit and at rest using advanced encryption standards (AES-256), which ensures that it is protected against unauthorized access.
- **Retention Policies:** We maintain a structured retention policy to ensure backups are stored for appropriate periods, enabling restoration at various times. Old backups are securely deleted following data retention policies to manage storage and comply with regulations.

Frequently Asked Questions

How do you handle data breaches, and what is your incident response plan?

In the event of a data breach, we follow a structured incident response plan designed to mitigate damage and ensure a swift and effective resolution. Our approach includes the following key steps:

1. **Detection and Identification:** We use advanced monitoring tools and alert systems to detect and identify potential breaches quickly. Any unusual activity is immediately flagged for investigation.
2. **Containment:** Once a breach is confirmed, we immediately contain the incident. This involves isolating affected systems, disabling compromised accounts, and halting unauthorised access to prevent further data loss.
3. **Assessment and Analysis:** Our response team conducts a thorough evaluation to determine the scope and impact of the breach. This includes analyzing how the breach occurred, what data was affected, and identifying exploited vulnerabilities.
4. **Notification:** We promptly notify affected parties under legal and regulatory requirements, including customers and regulatory authorities. Transparency is crucial; we provide clear and timely information about the breach and its implications.
5. **Remediation:** We implement corrective measures to address the root cause of the breach and prevent future occurrences. This includes patching vulnerabilities, enhancing security controls, and updating our policies and procedures.
6. **Recovery:** We work to restore affected systems and services to normal operation while ensuring that no residual threats remain. We also monitor the systems closely to detect any signs of recurring issues.
7. **Post-Incident Review:** After resolving the breach, we conduct a comprehensive review to evaluate our response and identify areas for improvement. This helps refine our incident response plan and strengthen our overall security posture.

Following these steps ensures that data breaches are managed effectively, minimising impact and reinforcing our commitment to protecting customer information.

How do you ensure the physical security of your data centres?

Our SaaS solution is fully hosted in the public cloud, so we do not operate our data centres. Instead, all data is securely stored in the state-of-the-art data centres of trusted third-party providers like AWS. For detailed information on their security policies, please visit their compliance centre.

Frequently Asked Questions

What is your approach to vulnerability management and patching?

As part of our technology strategy, we focus on minimizing the use of hosting components that require frequent vulnerability management and patching. We delegate these responsibilities to specialized providers with deep expertise in these areas whenever possible. Our suppliers are meticulously chosen based on their security certifications, such as ISO 27001 and SOC 2.

For our own software assets, we automate dependency patching whenever feasible. Our source code undergoes rigorous scanning with every check-in, ensuring that any identified vulnerabilities are addressed before the code is deployed to production. Additionally, we run an active security program encouraging white-hat hackers to report any vulnerabilities they discover, further enhancing our security posture.

What authentication mechanisms are in place for customers?

Trengo employs a comprehensive authentication framework to ensure our customers have secure access. We provide a standard username and password combination for initial authentication, complemented by two-factor authentication (2FA) to enhance security. Customers can enforce 2FA as a mandatory requirement for added protection for all users. This multi-layered approach helps safeguard accounts against unauthorized access and ensures that only verified individuals can access sensitive information.

Frequently Asked Questions

How do you ensure data protection regulations (e.g., GDPR) compliance?

We ensure compliance with data protection regulations through the following measures:

1. **Data Handling Policies:** We have strict data handling policies and procedures that align with GDPR, and other relevant regulations, ensuring that personal data is collected, processed, and stored lawfully and transparently.
2. **Data Protection Officer (DPO):** We appoint a DPO who is responsible for overseeing compliance with data protection laws, managing data protection activities, and serving as a point of contact for regulatory authorities.
3. **Employee Training:** We regularly train employees on data protection regulations and best practices to ensure they understand their responsibilities and the importance of data privacy.
4. **Data Subject Rights:** We implement processes to facilitate the exercise of data subject rights, such as access, rectification, deletion, and data portability, in compliance with GDPR.
5. **Security Measures:** We deploy robust security measures, including encryption, access controls, and regular security assessments, to protect personal data and ensure confidentiality, integrity, and availability.
6. **Third-Party Compliance:** We conduct due diligence and require third-party vendors and partners to sign data protection agreements to ensure that they comply with relevant data protection regulations.

By adhering to these practices, we maintain a high data protection and regulatory compliance standard.

What employee training programs do you have for cybersecurity awareness?

During onboarding, all employees undergo comprehensive training to build cybersecurity awareness. We schedule several events throughout the year to reinforce this knowledge and ensure ongoing vigilance. These sessions are designed to inform our team about the latest security threats and best practices, ensuring they remain aware of the risks and their role in maintaining our security posture.

Frequently Asked Questions

What measures do you take to ensure the security of APIs and integrations?

To ensure the security of our APIs and integrations, we implement the following measures:

1. **Authentication and authorisation:** We use OAuth 2.0 and API keys to ensure only authorised users and applications can access our APIs.
2. **Encryption:** All data transmitted through our APIs is encrypted using TLS to protect against eavesdropping and tampering.
3. **Rate limiting:** We enforce rate limiting to protect against DDoS attacks and abuse.
4. **Input validation:** We perform strict input validation to prevent common vulnerabilities like SQL injection and XSS attacks.
5. **Regular security audits:** Our APIs undergo regular security audits and penetration testing to identify and mitigate vulnerabilities.
6. **Logging and monitoring:** We maintain comprehensive logging and monitoring of API activity to promptly detect and respond to suspicious behaviour.

These measures ensure that our APIs and integrations are secure, reliable, and resilient against threats.

What controls are in place to manage access permissions and user roles?

For comprehensive details on the latest authorisation features, please refer to this Help Centre article. This resource provides in-depth information and guidance on managing and utilising our authorisation functionalities effectively.

Frequently Asked Questions

What steps do you take to secure software development and deployment pipelines?

Our source code undergoes scanning with every check-in to identify and address any vulnerabilities before the code is released to production. This proactive approach ensures that potential security issues are resolved promptly, maintaining the integrity of our software.

In addition to automated scanning, all source code is subject to peer review. This collaborative process allows our development team to identify and address any issues that may have been overlooked, further enhancing the quality and security of our codebase.

Do you conduct regular security audits and penetration testing?

Yes, we conduct regular security audits and penetration testing to ensure the robustness of our security measures. These activities are carried out annually by a reputable external security partner who brings a fresh perspective and specialised expertise. The external audits thoroughly examine our security posture, including our systems, processes, and controls, to identify potential vulnerabilities and ensure compliance with industry standards.

In addition to our scheduled audits, we also offer our customers the opportunity to perform their penetration tests with prior notice. This is part of our commitment to transparency and collaboration. However, to maintain the integrity of our security infrastructure, we do not compromise or lower our existing security measures during these tests. Consequently, our security protocols could prevent certain testing activities, potentially leading to an initial blockage of the test. This approach ensures that our security remains robust while allowing customers to assess their interactions with our systems.

Start delivering reliable and trustworthy customer service

Trengo is the customer communication platform that centralises all your customer communication, and helps your team automate repetitive tasks. With Trengo, all your customer communication is in one view. It almost sounds too good to be true, right? Luckily it's not. We've helped over 3k companies create unforgettable customer experiences in the last seven years.

Would you like to know more?
Our team is always happy to help.

trengo

Stadsplateau 30, 3521 AZ
Utrecht, Netherlands

trengo.com