trengo

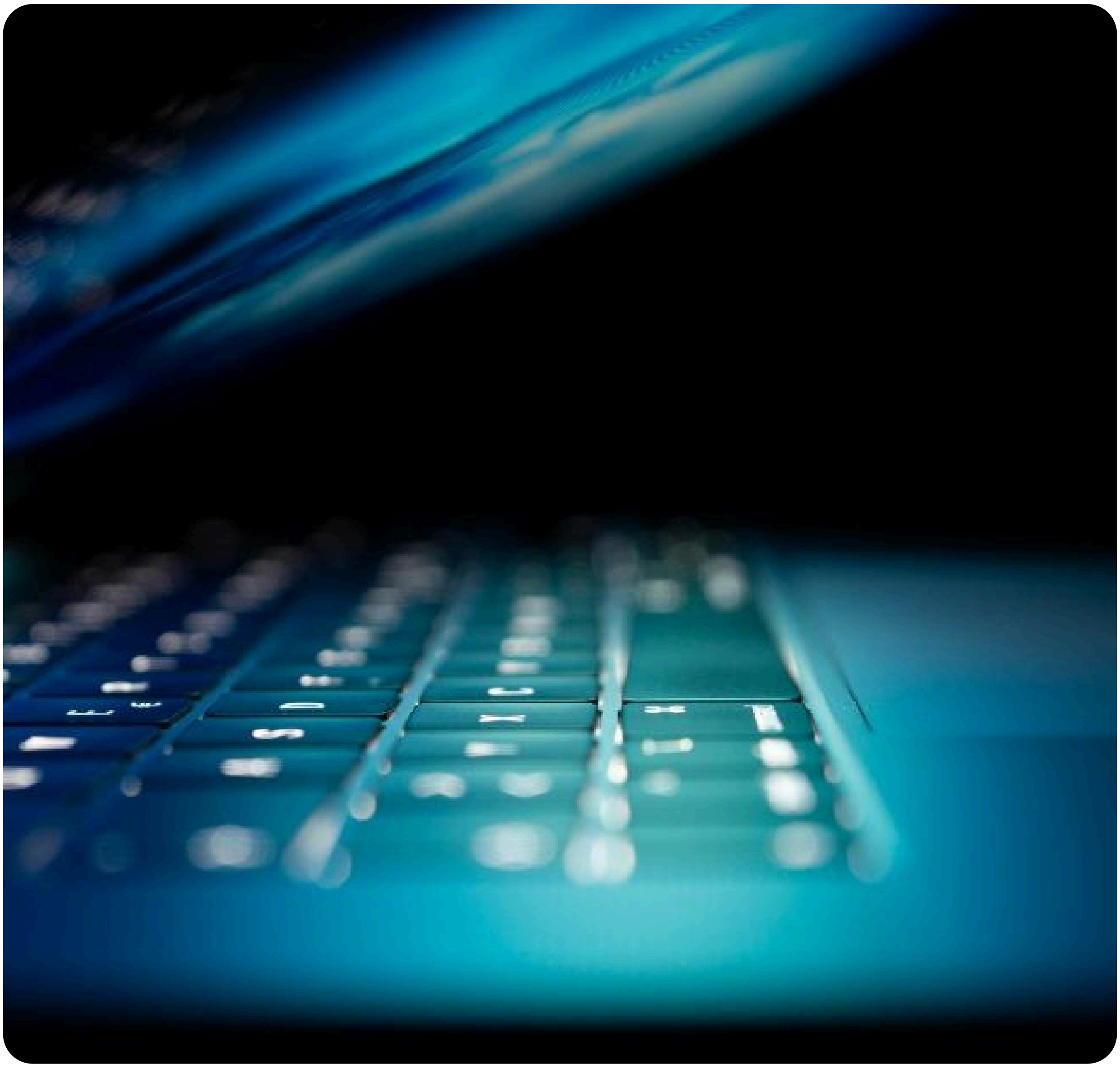
Trengo's vision on security

trengo.com

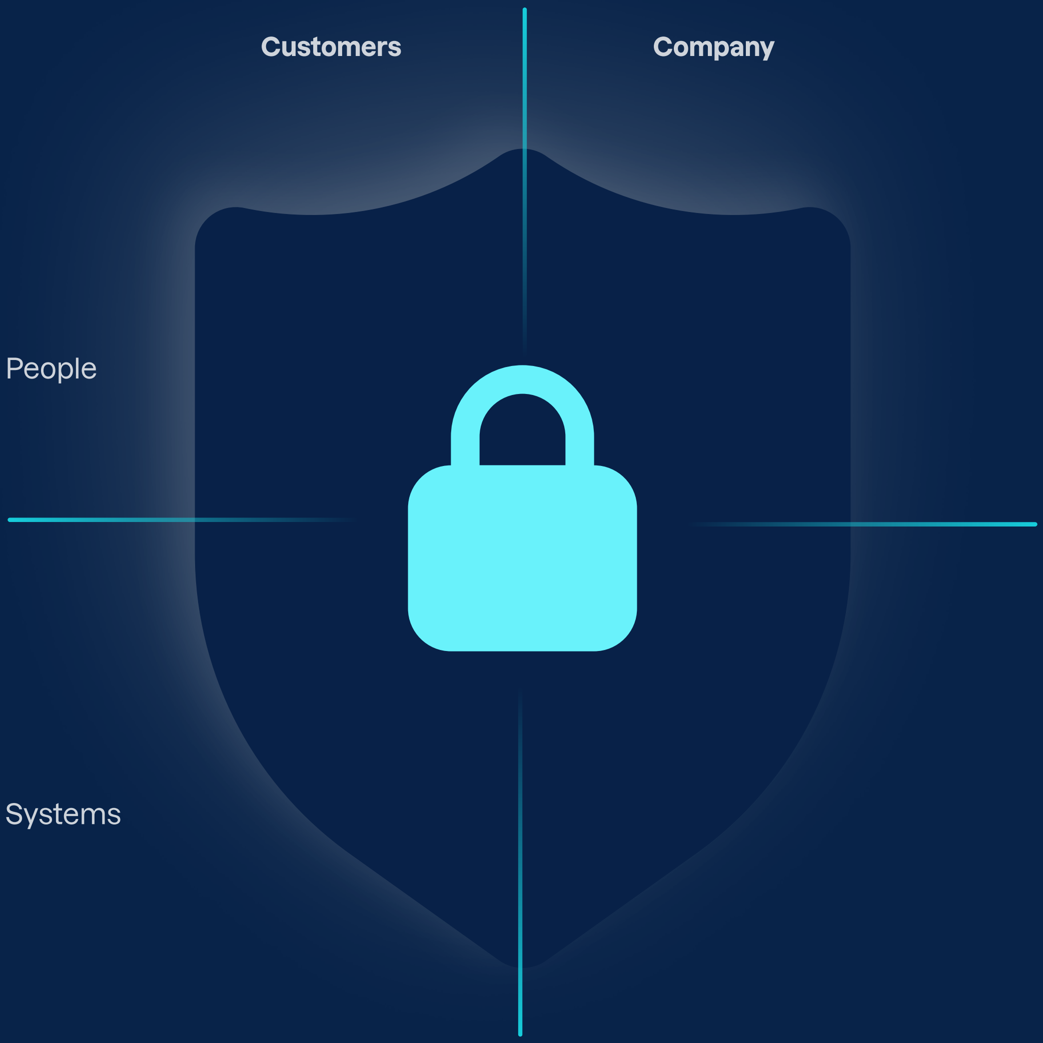
Trengo's vision on security

At Trengo, we prioritise security as a fundamental part of delivering reliable and trustworthy services. It is both a technical requirement and a core principle underpinning everything we do.

We recognise that safeguarding data and protecting against threats requires a multifaceted approach. That's why we view security through a comprehensive quadrant model, covering every dimension—from the systems we operate to the people involved.



Our security model includes four essential areas:



This model reflects our belief that effective security is a collaborative effort. Trengo ensures robust protection through tools, technologies, and best practices, but also counts on customers to maintain secure usage of their environment.

This shared responsibility model ensures that every aspect of security is covered. Through continuous communication and mutual effort, we create a safe, resilient platform that meets—and exceeds—industry standards.

1. Customer-Side Security

Your Employees

We recognise that human behaviour plays a crucial role in maintaining security. Trengo provides:

- Accessible tools and configuration options
- Clear guidance and best-practice resources
- Customer Academy access with detailed product setup courses

We encourage ongoing training and awareness within customer teams to supplement our own tools and materials.

System Configuration on your side

Trengo empowers customers with built-in features for control and safety:

- Custom roles and permissions for granular access
- Multi-Factor Authentication (MFA) with enforceable policies
- TLS encryption to secure communications
- OAuth2 authentication for safe and standardised integrations

These tools enable customers to confidently configure secure systems resistant to unauthorised access.

2. Security at Trengo

Our People

Security is part of our company culture. We maintain continuous discussion, awareness, and education across teams:

- Mandatory onboarding security training for all employees
- Ongoing awareness sessions for customer-facing teams
- Proactive communication on new threats and best practices

Every team member plays a role in maintaining a secure environment and protecting customer data.

Secure-By-Design SaaS Platform

Trengo's platform is built on a "secure by design" foundation. This means:

- Security is embedded in every stage of product development.
- We apply access reviews and least privilege principles.
- Data is fully encrypted and backed up for GDPR compliance.

Even our carrier and third-party connections follow strict encryption and security protocols, ensuring customer data safety across the ecosystem.

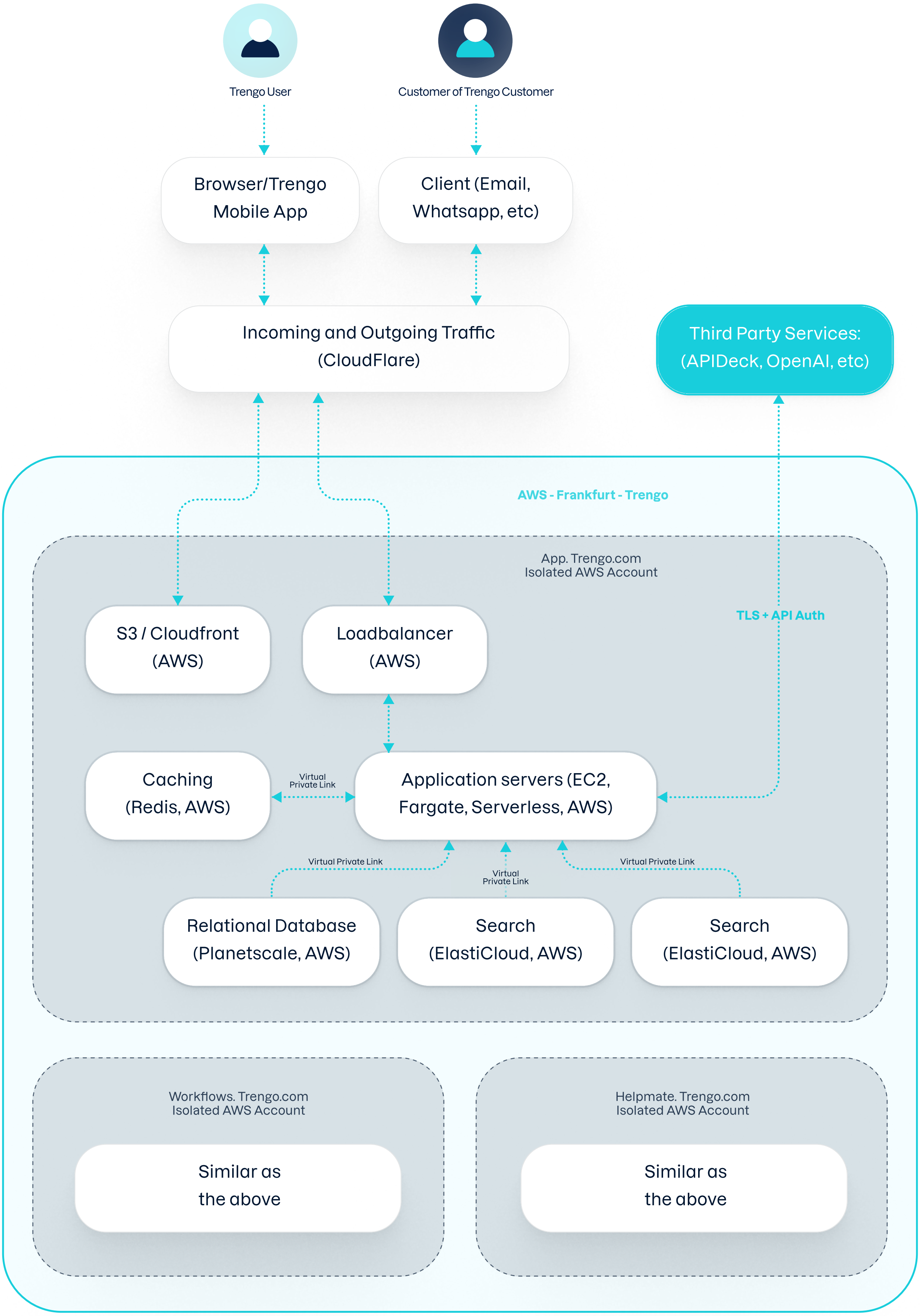
3. Trengo Cloud Architecture

Trengo operates within a PaaS-oriented cloud architecture, optimised for performance, security, and scalability.

Key Features

- **Virtual Private Links (VPLs) reduce exposure to open networks.**
- **Standard architectural framework minimises human error.**
- **Edge connectivity via Cloudflare enhances global performance, security, and DDoS protection.**

This architecture ensures our infrastructure remains both efficient and secure across 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

4. Frequently Asked Questions

What's the Difference Between SaaS and On-Premise?

- On-premise: Hosted internally within a specific location.
- SaaS (Trengo): Hosted externally in the cloud—secure, scalable, and accessible globally.

How Is Data Encrypted?

- At Rest: AES-256 encryption, managed with a secure KMS, restricted access, and auditing.
- In Transit: TLS (1.3 or higher) encryption and HTTPS-secured APIs.

What Security Standards Do You Meet?

Our solution aligns with:

- NIST Cybersecurity Framework
- GDPR standards for data protection and privacy compliance
- ISO 27001 best practices

How Are Backups Managed?

- Automated daily incremental and weekly full backups
- Redundant storage across regions
- AES-256 encryption for all backups in transit and at rest
- Defined retention and deletion policies

4. Frequently Asked Questions

What's Your Incident Response Plan?

1. Detection and identification
2. Containment
3. Assessment
4. Notification of affected parties
5. Remediation and recovery
6. Post-incident review for continuous improvement

How Is Physical Security Ensured?

All hosting is within trusted third-party cloud providers such as AWS, with robust data centre controls.

How Do You Manage Vulnerability and Patching?

- Automated dependency patching and source code scanning
- Engagement with white-hat security researchers
- Partnerships with ISO 27001 / SOC 2–certified suppliers

How Do You Ensure GDPR Compliance?

We employ:

- Defined data handling policies
- A dedicated Data Protection Officer (DPO)
- Regular employee training
- Strong data subject rights processes
- Third-party compliance reviews

4. Frequently Asked Questions

What Authentication Mechanisms Are Used?

To further strengthen our authentication capabilities, Trengo has integrated Stytch as our enterprise authentication provider. This integration introduces Single Sign-On (SSO) functionality, enabling organisations to authenticate seamlessly using their existing identity providers such as Microsoft, Google, and other SAML/OIDC-compliant systems. Stytch's platform also provides advanced security features including passwordless authentication via magic links and one-time passcodes (OTP), passkeys and WebAuthn support for phishing-resistant login, and Time-based One-Time Passcodes (TOTP) for enhanced multi-factor authentication. Session management is secured through JWT-based tokens with configurable session timeouts, and all authentication traffic is encrypted via TLS. This upgrade provides enterprise customers with flexible, modern authentication options while maintaining the robust security standards Trengo is committed to delivering.

How Do You Secure APIs and Integrations?

- OAuth 2.0 and API key authentication
- TLS encryption
- Rate limiting and input validation
- Regular security audits and logging

How Do You Secure Development Pipelines?

- Automated code vulnerability scans on every check-in
- Peer review for all code submissions
- Annual external penetration testing from accredited partners

Conclusion

At Trengo, security is embedded in our DNA—from product design to employee training and customer empowerment. Our collaborative, quadrant-based model ensures that every stakeholder contributes to creating a secure, resilient communication platform.

Start Delivering Reliable Customer Service

Trengo is the customer communication platform that centralises all conversations and automates repetitive tasks. Over 3,000 companies trust us to deliver secure, unforgettable customer experiences.

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

trengo

Trengo HQ
Stadsplateau 30, 3521 AZ
Utrecht, Netherlands

trengo.com