TransLinguist.

TRANSLINGUIST SECURITY WHITE PAPER 2023

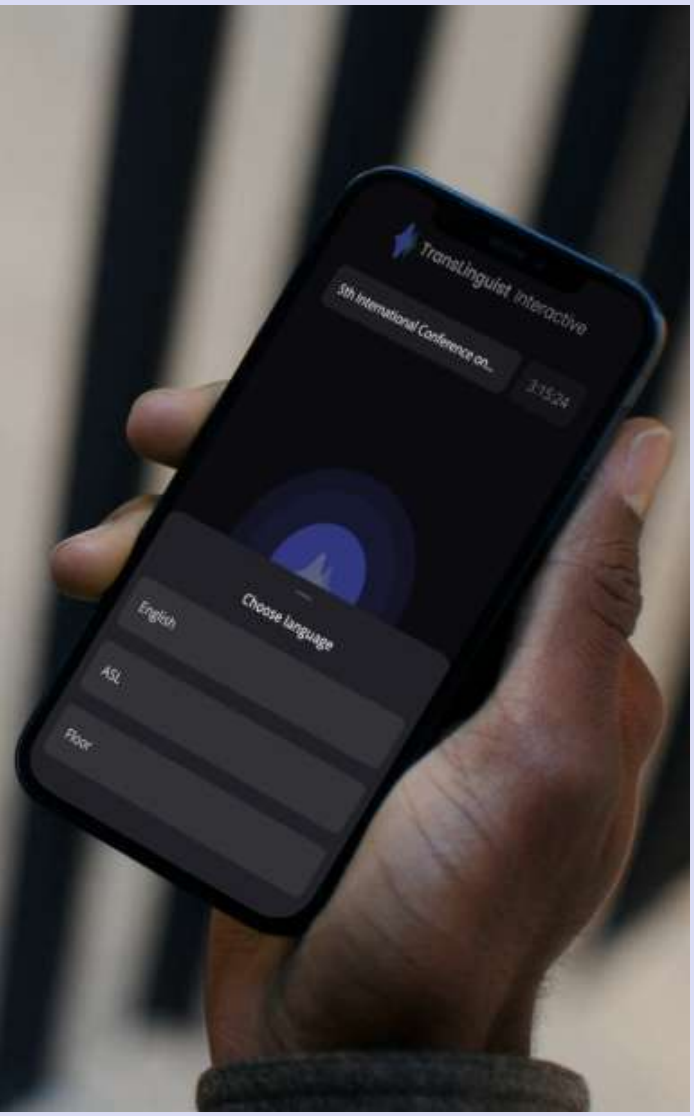
https://translinguist.com/

Introduction

What is TransLinguist Interactive?

At TransLinguist, our values center around innovation, diversity, and inclusion. Therefore, we have crafted an all-in-one multilingual platform that connects people worldwide. TransLinguist Interactive is a Video Remote Interpretation and Remote Simultaneous Interpretation platform designed to eliminate language barriers and promote inclusion. Our platform supports online, on-site, and hybrid meetings, guiding businesses toward a more sustainable future.

TransLinguist Interactive is a perfect blend of human interpretation combined with AI technology to deliver high-quality real-time interpretations in over 50+ languages globally. Our cost-effective, state-of-the-art product not only eliminates the multiple costs associated with multilingual communication through legacy methods but also enables clients to organize and structure their events hassle-free.



Security at TransLinguist

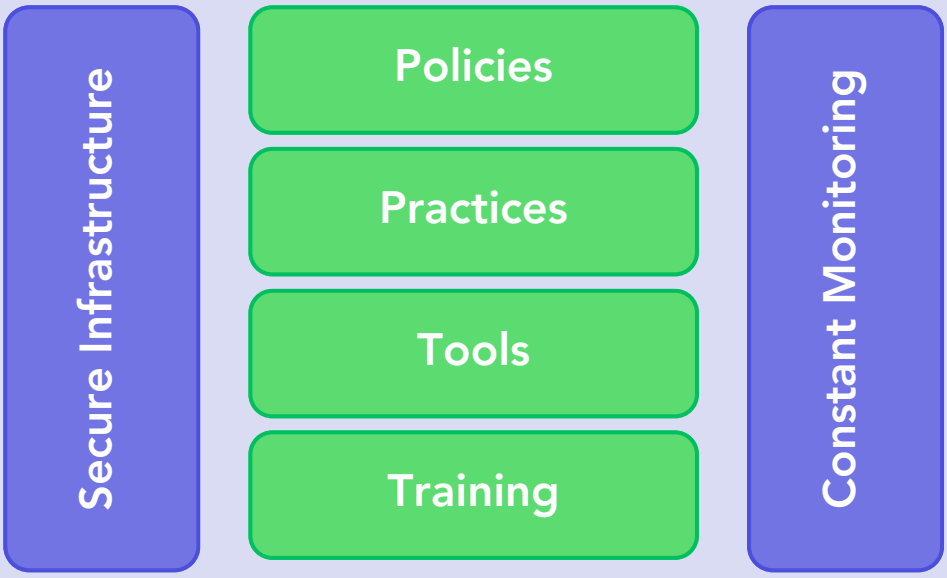
Ensuring the security and protection of our client's data is a top priority at TransLinguist. We recognize that trust is essential to satisfying our clients, which is why we have meticulously developed our product with all necessary security measures. Our employees undergo training to guarantee the protection and security of our clients' data. Meeting our clients' expectations for the best multilingual collaboration experience on a secure, robust, and compliant platform is paramount, and TransLinguist Interactive is committed to consistently meeting and exceeding these evolving expectations.

This whitepaper provides an overview of TransLinguist's current security practices and compliance specifics, offering assurance that your meetings are safe with TransLinguist.

Our Security Model

TransLinguist Security Model

The TransLinguist security model relies on two key factors. Firstly, we prioritize ensuring the initial security of our design to establish a robust infrastructure. Additionally, our dedicated team monitors security 24/7 for any breaches or necessary improvements. Regular check-ins are conducted to ensure the incorporation of new technology and innovation, guaranteeing that clients benefit from the best security industry practices.



Our security practices are in alignment to the ISO best practices. In order to ensure a smooth and secure client experience we follow some security measures as follows:

- We adopt an approach that prioritizes building a solid foundation, and to achieve this, we concentrate on ensuring our product is inherently secure by design.
- Consistent with our core approach, we guarantee that all our practices, tools, policies, and employee training adhere to the principle of being designed without any loopholes, as they form the fundamental basis of a secure product.
- Consistent monitoring and reporting is a core part of our day to day practices
- The model serves as a comprehensive framework for shaping both high-level Secure by Design concepts and their implementation at a more detailed, pillar-level. It also facilitates regular monitoring enforcement.

TransLinguist teams are intentionally organized to prioritize knowledge sharing, mitigating the risks of misunderstandings that could escalate and cause delays during a security incident. Furthermore, our ongoing monitoring and alerting process, in collaboration with the DevSecOps (Development, Security, and Operations) team, remains a central aspect of our solution.

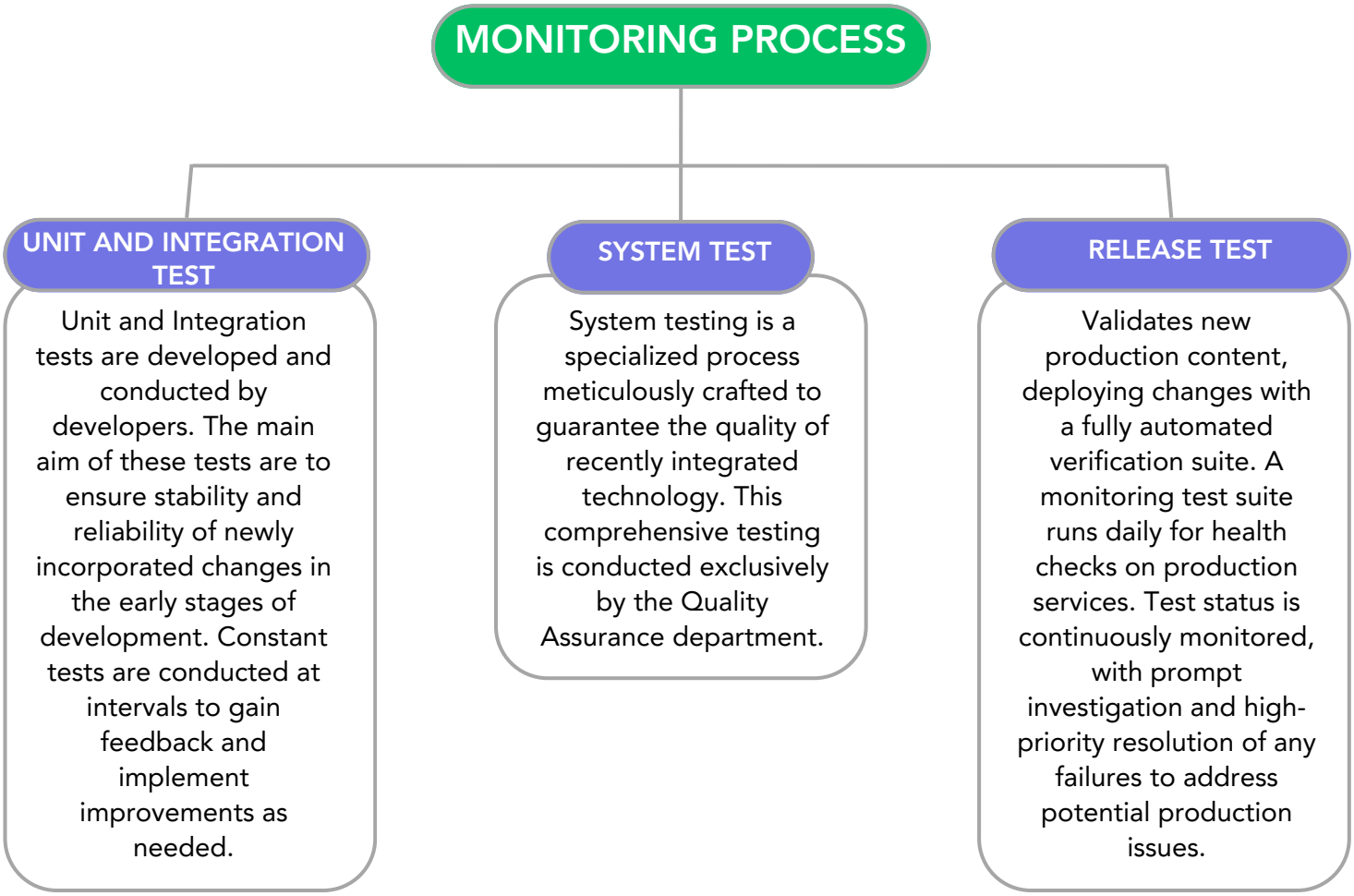
Adhering to Industry Best Practices

TransLinguist adheres to the highest industry standards to guarantee optimal security and data protection for our clients. The following outlines the security practices we follow, with details on their implementation available throughout this white paper.

- **Data encryption:** Encryption of sensitive data to prevent unauthorized access.
- **Access controls:** Managing access to sensitive data.
- **Recognize risk:** Understanding the type of data handled and relevant regulations.
- **Regular data backups:** Preventing data loss from cyberattacks, natural disasters, and system failures.
- **Use cloud security solutions:** we use cloud computing for data security.
- **Monitor data performance:** Using a data warehouse or lake to store and organize data

Monitoring Process

Constant monitoring and testing is done to mitigate risks and monitor performance when changes are introduced to the platform.



Stages Of System Testing

1

SMOKE TESTING

Involves the automated execution of critical path tests exclusively. The objective of these tests is to detect any critical issues that may arise following code changes. Conducted frequently throughout the day for each code alteration, these tests are compact and deliver prompt feedback.

2

FEATURE TESTING

A stage where multiple versions of the same features are tested in order to determine the best user experience. Quality assurance experts are focused on elements of the newly developed features. A log is kept of all the tests and a decision is made according to the findings.

3

PERFORMANCE TESTING

Conducted when implementing significant changes to the platform. The objective of this testing is to stress the system, ensuring it remains robust, stable, and accessible.

4

REGRESSION TESTING

Regression testing re-executes both functional and non-functional tests post-code changes, reporting identified issues to developers for resolution.

DevSecOps

At TransLinguist, we do not treat security as a separate component of the product. To seamlessly integrate security requirements into the development process, we ensure collaboration between our security experts and the development team. This collaboration ensures the incorporation of necessary security measures into the product. The practice of DevSecOps is a continual endeavor to align infrastructure, tools, and knowledge with the most recent security practices while also disseminating knowledge across all engineering teams.

Given the dynamic nature of the cybersecurity landscape, TransLinguist places special emphasis on the upskilling process to remain current on the latest developments and effectively address new cybersecurity threats through adaptation to modern practices.

Product Infrastructure

TransLinguist collaborates with Amazon Web Services (AWS), prominent provider of cloud services and global frontrunner in robust and dependable data centers. The adaptability of cloud services empowers TransLinguist to exhibit maximum responsiveness and flexibility.

AWS Architecture

The foundation of TransLinguist's infrastructure is rooted in AWS and Digital Ocean's Well-Architected Framework, emphasizing Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization, and Sustainability. Our approach to infrastructure management revolves around the guiding principle of Infrastructure as Code (IaC). Put simply, all alterations to TransLinguist's infrastructure are tightly regulated, and each release adheres to a meticulously defined process, with an automated pipeline facilitating deployment. While the capability to revert changes exists, the noteworthy aspect lies in our operations driven by Continuous Integration and Continuous Delivery (CI/CD), enabling the simultaneous implementation of modifications across various environments.

Backups and Reliability

TransLinguist establishes and adheres to stringent benchmarks concerning the frequency and retention of backups to safeguard our clients from potential data loss or corruption. At any given moment, there exist multiple backup copies of the fundamental elements of our platform. This implies that, in the event of a security crisis requiring a rollback to a previous TransLinguist platform version, the process can be swiftly and efficiently executed.

Furthermore, apart from our automated backup protocol, we perform manual backups of the essential components of our platform. These backups are subjected to encryption and securely housed within AWS (Amazon Simple Storage Service), guaranteeing continuous high availability.

TransLinguist Interactive- Product Security

Password Protection

The TransLinguist Interactive platform prioritizes security through robust access control measures. The platform is safeguarded by password protection, ensuring that only authorized personnel can access its functionalities. Administrators, in particular, undergo an additional layer of security with the generation of a one-time password (OTP) when logging in. This two-step verification process enhances authentication by requiring a second form of identification beyond the traditional password. Furthermore, administrators have the option to bolster security even further by enabling Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA), providing an added level of defense against unauthorized access and fortifying the overall integrity of the platform.

Cryptography

Industry-standard encryption process is utilized at rest and transit to ensure protection from cybercriminals.

Encryption at Rest

Stored Data encompasses details generated prior to or after the meeting, including meeting names, dates, times, locations, and participants. This information is securely stored and encrypted. In the improbable scenario of a cybercriminal gaining access to the physical files, decoding the encrypted information would be impossible without the requisite keys.

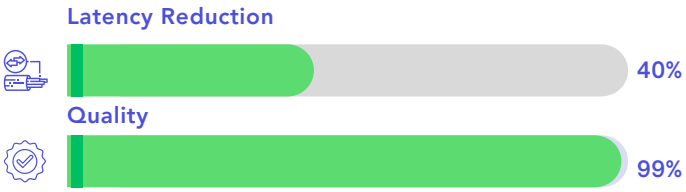
Encryption at Transit

The information actively shared during a meeting, including real-time video streams, constitutes the Data in Transit. Our encryption protocols for Data in Transit serve as a safeguard against potential threats such as Man-in-the-middle attacks, Eavesdropping, Replay, and other forms of cybercriminal interception during data transmission.

As an additional security measure, TransLinguist employs constant bit rate (CBR) encoding for media. This strategic encoding method not only enhances security through encryption but also reduces the chances of attackers deciphering media content details through traffic analysis. In essence, this dual-layered approach fortifies our defense, thwarting any attempts to compromise or steal Data in Transit.

Secure Sockets Layer Protection

SSL protection is a crucial component of the security infrastructure embedded in TransLinguist Interactive, contributing to the safeguarding of sensitive data exchanged within the platform. This advanced security protocol, Secure Sockets Layer (SSL), establishes encrypted connections between the TransLinguist servers and users' browsers. The implementation of SSL ensures that all communication, including real-time interactions, file transfers, and user authentication, remains confidential and secure. Users can easily identify the SSL protection through the "https://" in the URL, signifying a secure and encrypted connection. This robust SSL encryption in TransLinguist Interactive not only enhances the privacy of user data but also fortifies the platform against potential threats, reinforcing trust and reliability in the secure exchange of multilingual communication



Turn/UDP Connectivity

Turn/UDP connectivity in TransLinguist Interactive optimizes real-time communication, addressing network challenges by relaying data through a TURN server. Valuable for low-latency applications like video conferencing, this approach ensures a smooth and uninterrupted experience, enhancing the platform's commitment to high-quality, real-time interpretation services in diverse contexts.

Secure Media Stream

Secure media streaming is a cornerstone of our commitment to privacy and data protection during real-time communication. Leveraging advanced security protocols, including Secure Real-Time Transport Protocol (SRTP) and Transport Layer Security (TLS), TransLinguist Interactive ensures that audio and video streams are encrypted, safeguarding against unauthorized access and maintaining the confidentiality of sensitive information. This robust security infrastructure not only protects against potential eavesdropping but also establishes a secure channel from initiation to the transmission of multimedia content. Whether engaging in video conferencing, language interpretation, or collaborative sessions, users can trust TransLinguist Interactive to deliver a secure and private environment for their multilingual communication needs, upholding the highest standards of data integrity and privacy.

Web RTC

In TransLinguist Interactive, WebRTC plays a pivotal role in facilitating seamless and real-time communication experiences within the platform. Leveraging the power of Web Real-Time Communication, TransLinguist Interactive enables users to engage in multilingual meetings, and data sharing directly through their web browsers. The integration of WebRTC eliminates the need for external plugins or applications, providing a streamlined and efficient means of multilingual communication. Through APIs like getUserMedia, TransLinguist Interactive allows users to access their cameras and microphones for audio and video streaming, while the RTCPeerConnection API establishes secure peer-to-peer connections to ensure the privacy and integrity of communication. This implementation of WebRTC not only enhances the platform's collaborative capabilities but also reflects a commitment to delivering a cutting-edge and user-friendly experience for real-time language services.

AES-GCM Authenticated Encryption

Security is paramount, and AES-GCM Authenticated Encryption stands at the forefront of our commitment to safeguarding sensitive information. Employing the Advanced Encryption Standard (AES) with Galois/Counter Mode (GCM), this authenticated encryption methodology ensures a robust combination of confidentiality and authenticity for data transmitted within the platform.

AES-GCM operates as a symmetric encryption algorithm, utilizing keys of varying lengths (256 bits) to encrypt and decrypt data. The incorporation of GCM introduces an efficient mode of operation, providing not only encryption but also authentication through the use of authentication tags. This additional layer of security guarantees that the integrity of the data remains intact, preventing unauthorized tampering during transmission.

Whether facilitating multilingual communication, real-time interpretation, or collaborative sessions, TransLinguist Interactive leverages AES-GCM Authenticated Encryption to create a secure environment. This ensures that users can confidently exchange information, knowing that their data is not only confidential but also protected against any malicious alterations, upholding the platform's commitment to providing a trustworthy and secure language service experience.

Access to the server from set IP

Access to the platform is meticulously managed to ensure security and controlled connectivity. Authorized access to the server is granted through a specified IP address, adding an extra layer of protection to the platform. This approach enhances security by limiting server access to a predefined set of IP addresses, thereby reducing the exposure to potential unauthorized access or security threats.

Users attempting to access the TransLinguist Interactive platform from the set IP undergo a controlled and secure connection process. The platform's authentication mechanisms verify the legitimacy of the incoming connection, ensuring that only authorized users from the designated IP addresses can access and interact with the server. This IP-based access control is an integral part of the platform's security infrastructure, contributing to the overall robustness and reliability of TransLinguist Interactive in safeguarding sensitive language-related data and ensuring the confidentiality and integrity of user interactions.

Certifications

TransLinguist has chosen AWS as its hosting partner for the multilingual communication tool. The AWS platform, holding ISO and CSA certifications, guarantees that our product aligns with and adheres to the stringent standards set by Amazon Web Services. This partnership ensures that TransLinguist Interactive not only leverages the robust AWS infrastructure but also complies with the certifications, reflecting a commitment to security and reliability.

Security of Personal Information
Your data is encrypted, safeguarded, and inaccessible to unauthorized users.

Protection of Confidential Data
Information shared is safeguarded during meetings, including spoken words, shared notes, files, or participation in polls.

Routine System Updates
TransLinguist Interactive conducts regular updates, audits, and modifications.

Data Privacy Guidelines
Your data is exclusively utilized to facilitate your meeting and is not employed for any other purposes.

Essential Data
We operate on the principle of data economy, only the necessary information for successful meeting hosting is collected—no more and no less.