Protecting data while powering global reach.

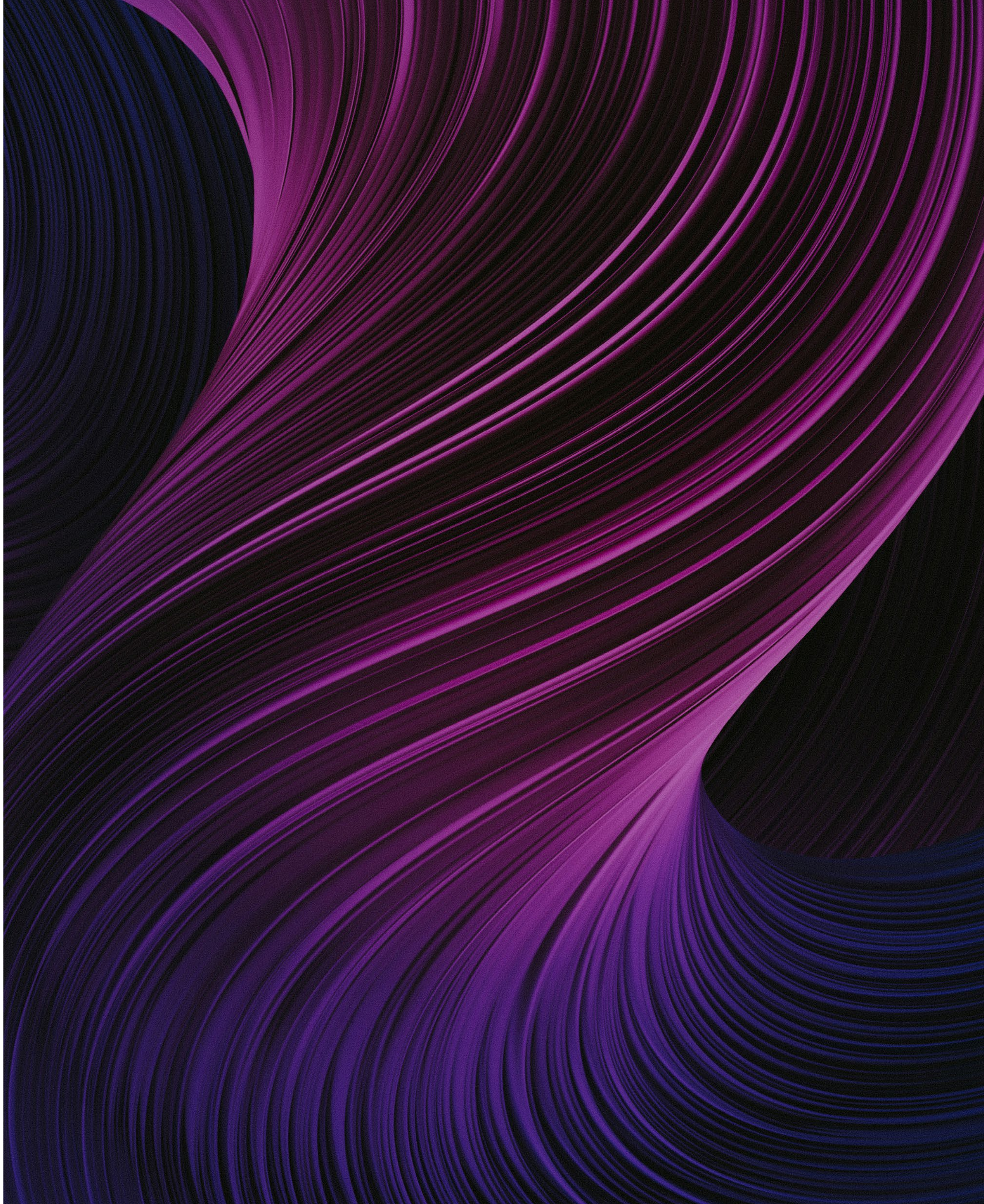
How Language Weaver machine translation enables enterprises to stay compliant, safeguard data and expand globally.

As digital transformation and rapid advances in AI have progressed, translation needs have grown faster than many enterprises and governments can manage.

Accurate, large-scale translation is now essential for communication, collaboration, and global market access. AI-powered machine translation (MT) helps break language barriers, but it also brings serious security risks. Sensitive data, from internal messages to client information, passes through these systems, making breaches a threat to trust, intellectual property, and reputation.

On top of that, organizations must comply with strict regulatory requirements, where non-compliance can lead to heavy fines or loss of certifications. Choosing the right MT solution isn't easy, with options ranging from free public tools to proprietary platforms across on-premises, cloud, or hybrid setups.

That's why we focus on the critical security standards an enterprise-grade AI platform must meet. In this guide, we'll outline best practices, architecture, and features behind Language Weaver, helping organizations choose secure, scalable MT solutions with confidence.



The unique security imperatives

Machine translation (MT) brings unique security challenges. It handles huge volumes of sensitive data, everything from internal messages and financial records to customer details and proprietary research. Protecting this content is critical.

Because MT relies on advanced algorithms and complex systems, it becomes a target for cyberattacks. Any breach could lead to data leaks, regulatory penalties, loss of trust, and lasting damage to the business.

Selecting a security-centric machine translation solution.

As organizations navigate these risks, a standard off-the-shelf public cloud MT system and its underlying security options may not suffice. The nature of enterprise MT use cases calls for a robust, comprehensive and tailored security approach—an MT system that not only provides flexible translation capabilities but also incorporates security as a core fundamental principle of its design and function at all levels.

Such an MT solution should embody a **secure-by-design** approach, where security parameters are woven into every facet of its build and operation, rather than being an added feature or an afterthought. This approach ensures that security is deeply and natively embedded within the system's architecture, offering a secure foundation for all other functionalities.

In the following sections, we will explore the critical security features deployed by Language Weaver, illustrating the role of each in ensuring a secure and dependable system. We will highlight the security measures and capabilities that need to be considered to ensure that your chosen MT solution not only meets its functional requirements but also aligns with your security policies to safeguard valuable data assets and retain stakeholder trust.

Secure architecture design and secure development lifecycle

Language Weaver Cloud and Language Weaver Edge has been designed with a fundamental emphasis on security:

- Data protection and privacy preservation have been primary considerations throughout their infrastructure development and operational procedures.
- The architecture of both solutions includes stringent controls for secure data management, access and storage.
- They adhere to a thorough secure software development lifecycle (SSDLC) process, integrating security measures from the inception of the software development process. This process incorporates routine code reviews, vulnerability evaluations and penetration tests.

Language Weaver: secure by design.

Language Weaver offers three flexible deployment options:

Cloud

The cloud-based architecture of Language Weaver has been designed to embody strength and reliability, reflecting a robust foundation of industry-leading infrastructure principles. The system is hosted on Amazon Web Services (AWS), a platform renowned for its security, scalability and flexibility.

The adoption of AWS allows Language Weaver not only to inherit the platform's inherent resilience, but also its exhaustive measures across physical, infrastructure and service-level security – all meticulously designed to safeguard data, protect against potential threats and secure application interfaces.

By capitalizing on the strengths of AWS, Language Weaver is able to provide a secure, dependable and powerful solution that meets the highest industry standards and expectations.

Cloud data residency

Language Weaver maintains two fully separated and segregated instances of its cloud infrastructure: one in Europe and one in the US. This allows clients to choose where their data will reside, safe in the knowledge that there is no data transfer between the two instances. This is particularly important for organizations for whom data must remain within designated geographical boundaries – for example, within the European Union – to meet certain regulatory requirements.

Edge

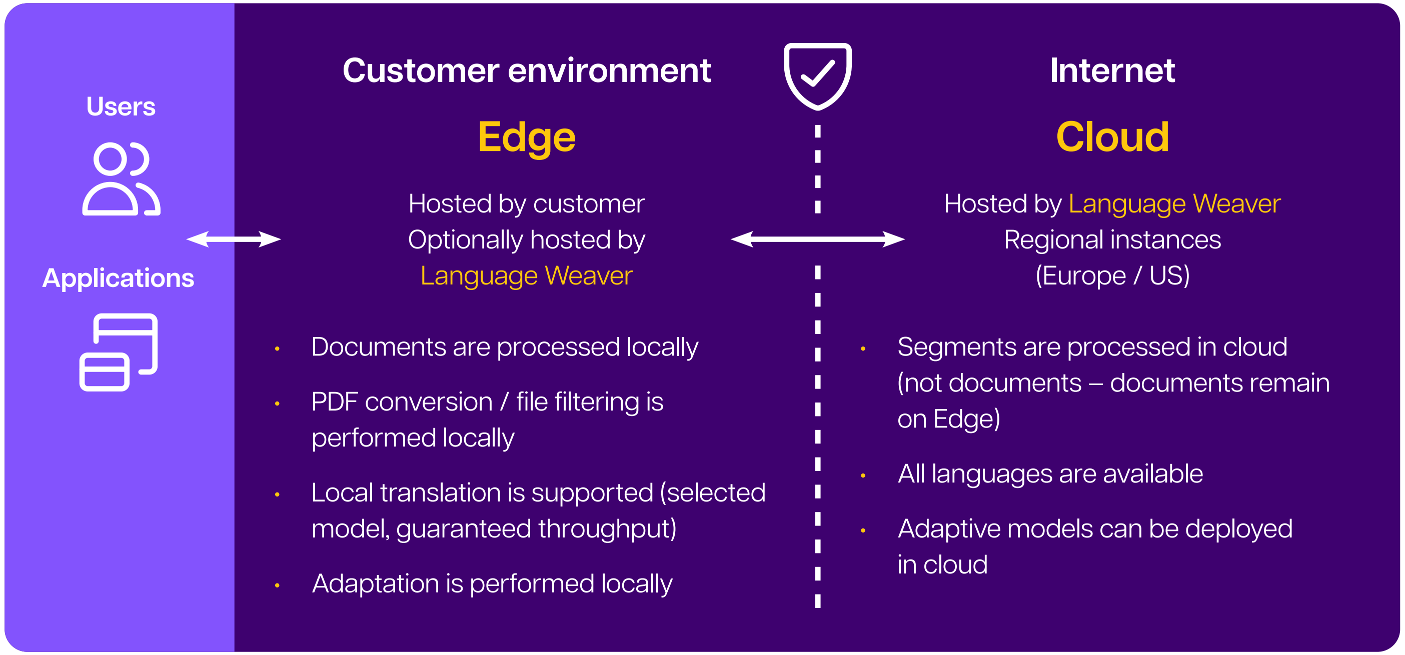
Deployed on-premises or in your private cloud, Edge deployment keeps your content secure by ensuring all translation processing stays within your environment. It offers flexible deployment options, including installation on physical hardware, virtual machines, or within containers, giving you full control over your infrastructure.

A key advantage of this model is its ability to operate in a fully isolated environment, completely disconnected from external networks, which adds an extra layer of security. This deployment approach significantly strengthens your organization's security by ensuring that sensitive data stays within the boundaries of your IT infrastructure. This containment strategy reinforces data control and enhances protection, offering peace of mind for even the most security-conscious enterprises.

Hybrid

Our cloud and Edge hosting models can be seamlessly integrated into a secure hybrid deployment, offering clients enhanced flexibility without compromising their existing security protocols. This hybrid approach allows the on-premises application to connect securely to cloud-based translation engines—for example, to access additional languages available in the cloud. All data is exchanged via an encrypted link, ensuring that original source content and documents remain within the secure on-premises infrastructure.

In today's rapidly evolving AI landscape, global organizations need a security approach that supports innovation while addressing emerging challenges and opportunities. Our solution uniquely combines advanced translation capabilities with robust security and control, enabling enterprises to embrace AI advancements without compromising their data protection standards.



Customer environment

Edge

Hosted by customer
Optionally hosted by
Language Weaver

- Documents are processed locally
- PDF conversion / file filtering is performed locally
- Local translation is supported (selected model, guaranteed throughput)
- Adaptation is performed locally

Internet

Cloud

Hosted by Language Weaver
Regional instances
(Europe / US)

- Segments are processed in cloud (not documents – documents remain on Edge)
- All languages are available
- Adaptive models can be deployed in cloud

Secure communication

Language Weaver uses **HTTPS with TLS 1.2** to ensure secure communication between client and platform. This encrypted communication protocol prevents unauthorized access and interception of data during transmission, safeguarding the confidentiality and integrity of processed content. The platform also employs **AES-256 encryption** and key management best practices to protect sensitive data at rest.

Secure API integration

The API interfaces of Language Weaver solutions use **secure HTTPS** connections and support best-of-breed authentication mechanisms to ensure that data is protected while being transferred between systems.

Data handling and retention

Language Weaver is designed to minimize data retention and ensure that customer content is not stored beyond the time strictly required to perform the translation and return the results. Uploaded files and directly entered text are treated with the same level of sensitivity, and no customer content is used for any purpose other than the requested translation. This approach ensures that customer data is not exposed to unnecessary risks and adheres to strict data minimization principles.

Access control and authentication

Access to Language Weaver solutions is restricted to authorized users with valid Language Weaver machine translation service accounts. The platform verifies user permissions before allowing access to translation services, ensuring that only authorized personnel can utilize the system. Collection of sign-on information is limited to what is necessary to confirm the account of the user.

Our cloud solution also provides federated identity options for single sign-on (SSO), while Edge deployment supports integration with LDAP and SAML for single sign-on (SSO) and centralized access control, further enhancing security and simplifying user management.

User roles and permissions

Language Weaver solutions implement **role-based access control (RBAC)** to manage user permissions and restrict access to sensitive data and functionality. The platform supports the **primary user roles of admin, linguist and translator**. Additional roles are available when opting for Edge deployment for access to reporting information.

By design, each user role has distinct access to defined functionalities and system control features. This separation of roles ensures that users only have access to the features and data necessary for their specific tasks, reducing the risk of unauthorized access or misuse.

Optional feedback mechanism

Language Weaver solutions offer an optional, **real-time feedback mechanism** for end users to contribute to the improvement of the MT models. Users can submit feedback on translation quality and suggest translation improvements for enhanced performance of the platform. By default, collection of feedback data is explicitly triggered by the user. Administrators can automate feedback approval based on the data handling guidelines of their organization. Collected data is used only to improve the specific translation models of the client. It is never reused for any other purposes.

Regulatory compliance and industry standards

Language Weaver adheres to the General Data Protection Regulation (GDPR) and other relevant data protection laws, ensuring that customer data is handled in accordance with legal requirements. OWASP best practices are adhered to, to maintain a secure software development Lifecycle (SSDLC).

Ongoing security assessments and monitoring

Language Weaver solutions undergo regular and rigorous security assessments and monitoring to identify and address potential vulnerabilities:

- Internal security and vulnerability assessments are performed before every release.
- Static code analysis is conducted using best-of-breed applications, and manual code reviews are enforced alongside automated tests (unit and regression tests) for all code committed to the repository.
- External penetration tests are performed at least annually by third-party qualified auditors.

This continual monitoring and assessment process ensures that the platform remains secure and up-to-date with the latest security best practices.

Auditing and logging

Auditing and logging are essential components of a secure platform to ensure continuous assessment of the security, integrity and availability of system resources.

For cloud deployment, full audit and logging is enabled, and logs are stored for one year.

Edge deployment provides enterprises with comprehensive auditing and logging capabilities. It supports log forwarding, full audit for REST API and http calls, and also exposes Prometheus metrics for a native integration with popular monitoring tools.

ISO 27001:2013 Certification

Language Weaver has ISO 27001:2013 certification for information security management systems.

The ISO 27001:2013 certification demonstrates that Language Weaver has:

- Policies to address information security risks through a well-defined assessment and treatment process.
- Appropriate security controls and safeguards to protect sensitive information.
- Rigorous incident response and business continuity planning.
- Employee security awareness and training programme.

The power of adaptability

A key differentiator of Language Weaver is its adaptability. Understanding that every enterprise and organization has unique needs, these platforms offer adaptive models that can be trained by clients themselves to cater to their specific requirements. Notably, this allows clients to create models attuned to their needs, without having to share any data with Language Weaver or any other third-party organization, further enhancing the security and privacy of their sensitive information. The result is an MT system that is not only robust and secure, but also uniquely private to the client organization.

Embracing large language models

Large Language Models (LLMs) are now being integrated into machine translation workflows, enhancing the fluency and contextual accuracy across domains. As these models continue to advance and integrate with enterprise environments, having robust standards for security, scalability, and reliability is essential. As LLMs bring with them complexity, ranging from data privacy concerns to model unpredictability, it requires organizations to take a proactive approach to governance and risk mitigation.

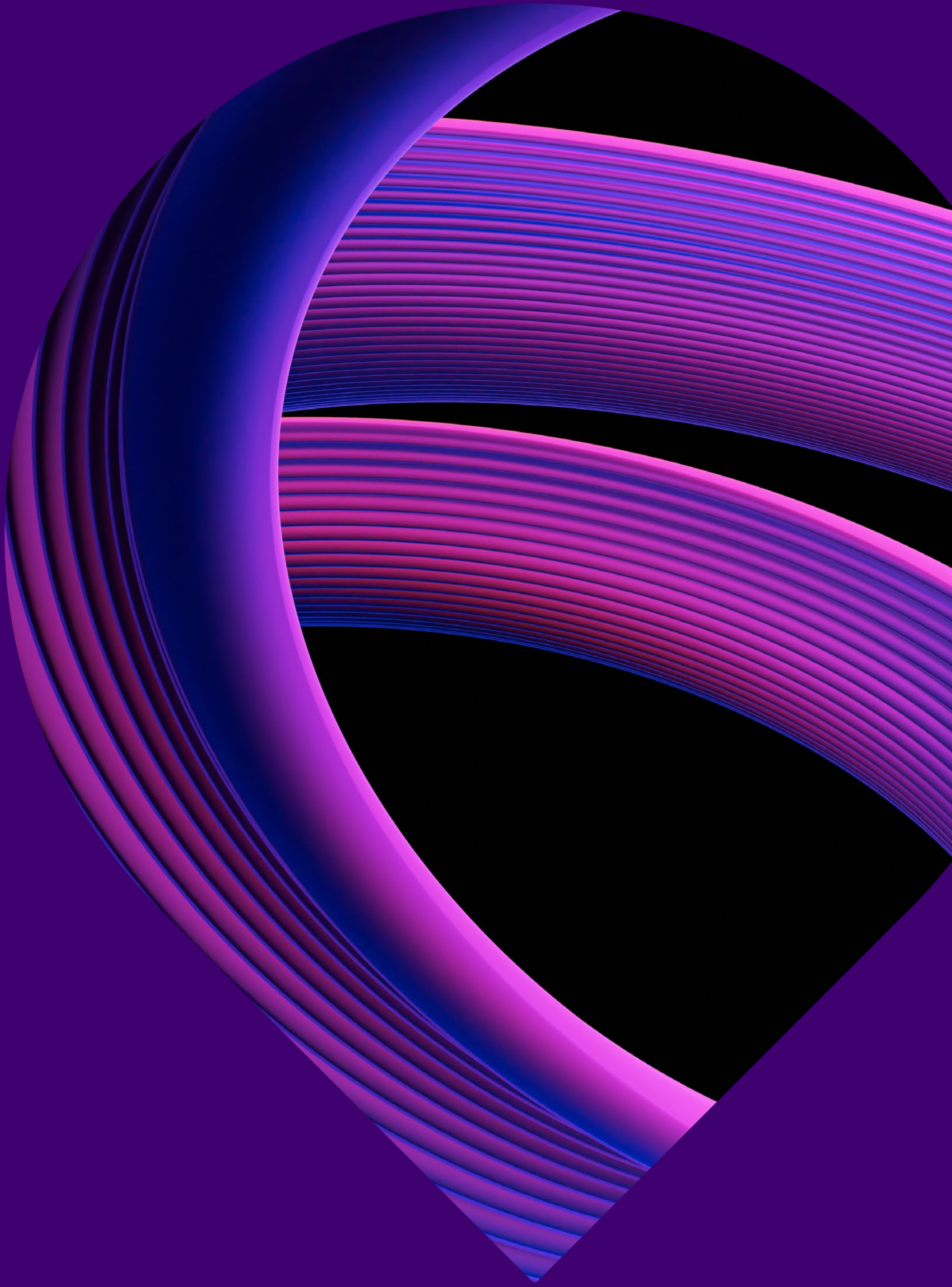
Language Weavers' commitment to secure-by-design principles, architecture, and enterprise-grade deployment model ensures that organizations can confidently leverage AI-powered machine translation while maintaining compliance, protecting sensitive data, and scaling with agility.

Why Language Weaver?

Language Weaver solutions employ a secure-by-design approach and enterprise alignment focus, ensuring that they are prepared to not only to meet the needs of enterprises today but for the future challenges that AI advancements will bring.

These principles, combined with their robust features and proven performance, have made Language Weaver the preferred enterprise solutions across a wide range of sectors. Financial institutions, law firms, life-science companies, high-tech businesses, law enforcement agencies, allied military forces and the intelligence community all rely on Language Weaver for their machine translation needs. Their choice is a testament to the security, scalability and adaptability that these solutions are designed to deliver.

With a proven track record of serving many of the top brands and government organizations across the world, Language Weaver continues to prioritize security and other enterprise-grade requirements in order to deliver best-in-class machine translation.



Start translating securely.

rws.com/language-weaver

About us

RWS is a content solutions company, powered by technology and human expertise. We grow the value of ideas, data and content by making sure organizations are understood. Everywhere.

Our proprietary technology, 45+ AI patents and human experts help organizations bring ideas to market faster, build deeper relationships across borders and cultures, and enter new markets with confidence – growing their business and connecting them to a world of opportunities.

It's why over 80 of the world's top 100 brands trust RWS to drive innovation, inform decisions and shape brand experiences.

With 60+ global locations, across five continents, our teams work with businesses across almost all industries. Innovating since 1958, RWS is headquartered in the UK and publicly listed on AIM, the London Stock Exchange regulated market (RWS.L).

More information: **rws.com**

Hello,
world.