Trust the security and privacy of IBM Watson Workspace and IBM Work Services

IBM Watson Workspace and IBM Work Services is secure by design, features around-the-clock monitoring and is aligned with key standards.

Organizations like yours, large and small, are relying on cloud services that are designed to be secure, protected and aligned with key standards. IBM Watson Workspace and IBM Work Services is built leveraging IBM's security leadership and culture of security being everyone's responsibility so your data is yours and is protected by IBM.

Security leadership

Security is embedded throughout our offering lifecycle.

- Deliver security by design, achieved through our Agile security embedded methodologies and culture.
- Focus on enforced standards, tested processes and dedicated tools to protect your data.
- Ensure annual security education and certification by employees.
- Provide operational security enforced by scanning and intrusion detection, continuously updated to keep ahead of new attack vectors.
- Perform regular audits to verify that operational security meets controls.
- Monitor a global security incident process 24x7 with trained personnel ready to strike in the event of a security incident.
- Minimize exposure to outside threats with multiple distinct and redundant architectures.

Data ownership

IBM Watson Workspace and IBM Work Services aligns with IBM commitment to data ownership in a Cognitive world. Following are key points as taken from the IBM blog on data responsibility (https://www.ibm.com/blogs/policy/dataresponsibility-at-ibm/):

- Clients are not required to relinquish rights to their data to have the benefits of IBM's Watson solutions and services.
- We believe the unique insights derived from clients' data are their competitive advantage, and we will not share them without their agreement.
- IBM client agreements are transparent. We will not use client data unless they agree to such use and we will limit that use to the specific purposes clearly described in the agreement.
- IBM employs industry-leading security practices to safeguard data. This includes use of encryption, access control methodologies, and proprietary consent management modules which allow us to restrict access to authorized users and to de-identify data in accordance with applicable permissions.

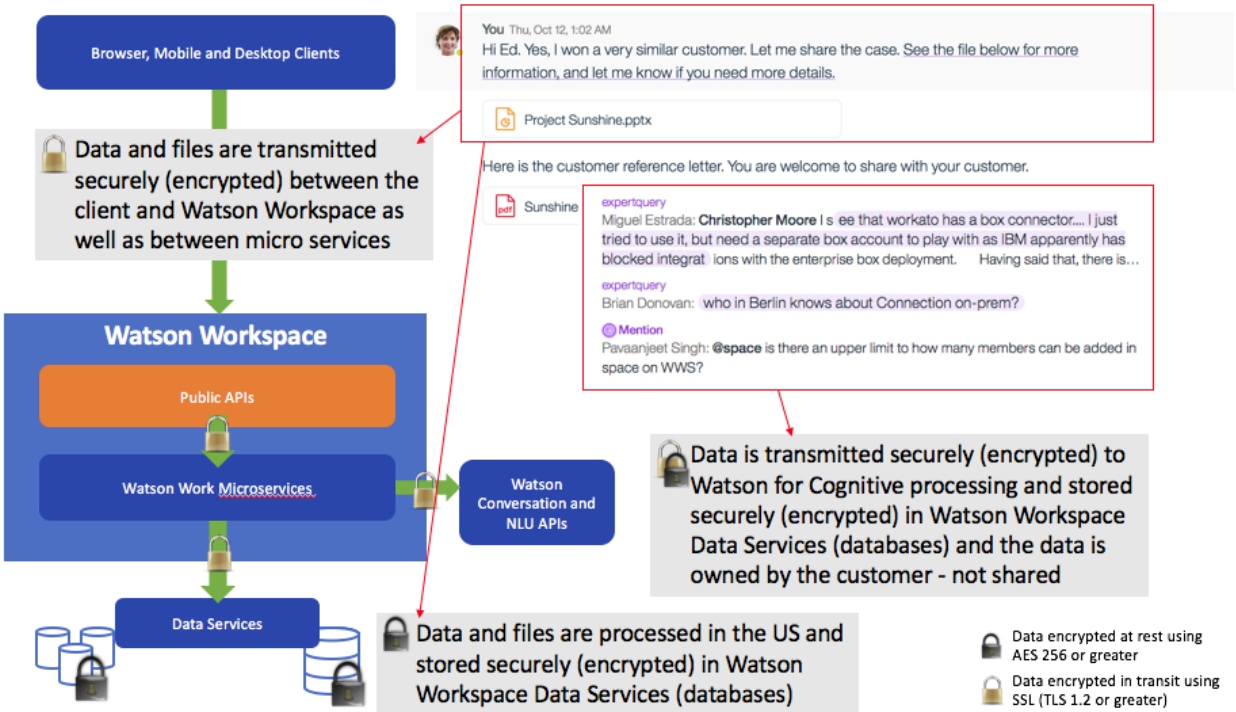
Data Protection

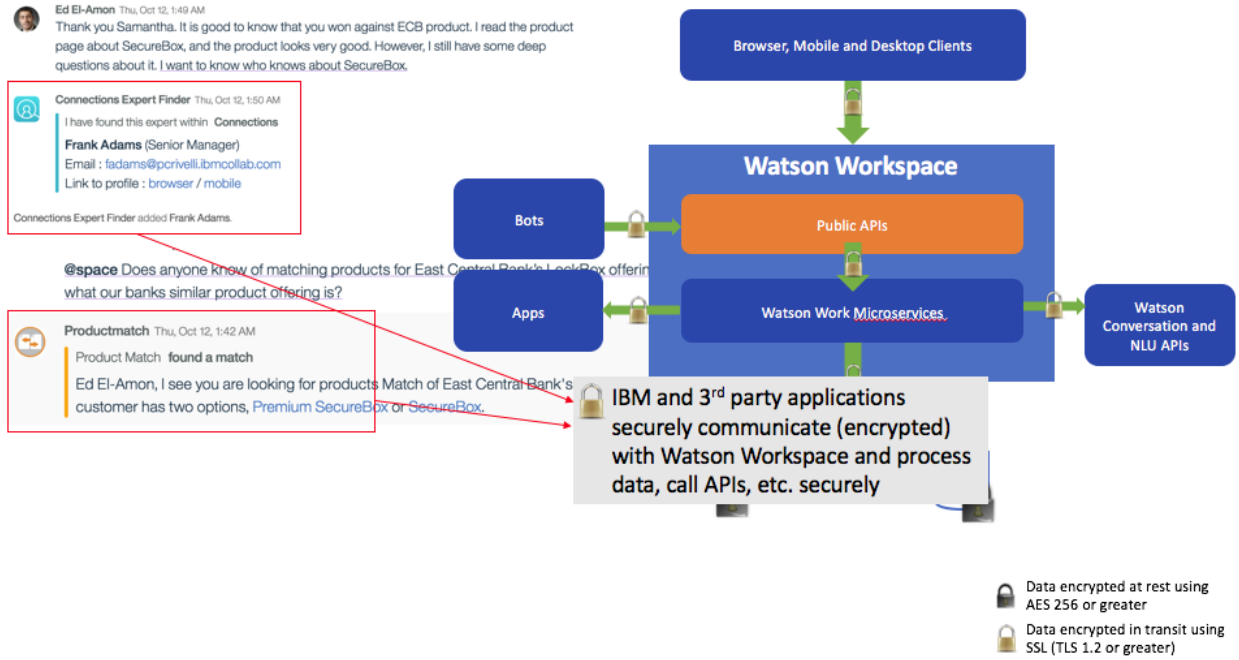
IBM Watson Workspace and IBM Work Services is designed to protect your proprietary content and data.

- Access to client data, including any personal data, is allowed only by authorized personnel in accordance with principles of segregation of duties, strictly controlled under identity and access management policies, and monitored in accordance with IBM's internal privileged user monitoring and auditing program.
- Access to your data is only granted as necessary to deliver services and support to you (that is, least required privilege).
- We are choosing strategically to align with many industry and country requirements, while continuously monitoring regulatory environments for new requirements.
- IBM Watson Workspace and IBM Work Services utilize data centers located in the US.
- IBM Watson Workspace and IBM Work Services is Privacy Shield self-certified and is in the process of external certification.
- IBM will sign EU Model Clauses (EUMC) agreements where required.
- IBM Watson Workspace and IBM Work Services is in the process of GDPR compliance and is aggressively driving to communicate certification well in advance of GDPR taking effect May, 2018.

Watson Workspace utilizes SSO for secure and unified logon through IBM ID.

Your data is encrypted in transit and at rest. While in transit, data is encrypted using TLS 1.2 or greater. When at rest, data is encrypted using AES 256 or greater.





Industry and Global Standard Alignment

IBM has a common set of security standards across the IBM Watson Work portfolio. We regularly review them against commonly accepted industry standards and regulation. IBM Watson Workspace and IBM Work Services is aligned with specific standards and has an aggressive certification road map which includes general, horizontal certifications (e.g., ISO27k, SOC 2, etc.); regional certifications (e.g., GDPR) and industry based certifications (e.g., HIPAA, PCI, etc.).