IBM® Watson® on the IBM® Cloud

Security Overview

Introduction

IBM Watson on the IBM Cloud helps to transform businesses, enhancing competitive advantage and disrupting industries by unlocking the potential within unstructured data. Fundamental to providing a strong foundation for companies wanting to leverage Watson Services, IBM uses best-in-class security and compliance processes that allow for successful execution of challenging workloads.

Deployment Models

Watson services can be deployed in a variety of ways to satisfy a broad set of security and compliance requirements. Three deployment models are available: IBM Watson public cloud, premium plans which provides additional data isolation within the public cloud, or a dedicated cloud environment for when clients need infrastructure dedicated only for their use (see Figure 1, below). In each case, the functionality of the service remains the same and the security architecture remains consistent.

Figure 1. Watson Deployment Options

Watson Developer Cloud can be deployed in 3 ways...

(1) Standard (Public)

Tenant (You)  Tenant (other Customer)

Cognitive Services
Database
Tooling
Service Hardware
IBM Cloud

(2) Premium

Tenant (You)  Tenant (other Customer)

Cognitive Services
Database
Tooling
Service Hardware
IBM Cloud

(3) Dedicated

Tenant (you)
Cognitive Services
Database
Tooling
Service Hardware
IBM Cloud

Lower Operating Expense
Greater Security through Resource, Network & Compute Isolation
Faster Deployment / Time to Value
Increased Infrastructure Footprint
All IBM deployments reside within hardened enterprise class IBM Cloud data centers that are ISO27001 and SOC2 certified. For additional information see: https://www.ibm.com/cloud/compliance.

Public

The Public Cloud is the most cost effective and provides a shared tenancy model which allows users to embrace the power of IBM Watson services while sharing the infrastructure cost needed to run IBM Watson. Each service provides unique credentials, API Opt-out capability (should users not want to share their data with Watson for service improvement), encryption of data in motion and at rest, and all of the enterprise security controls you expect from IBM. Public plans are a great option for companies looking to get started with Watson Services.

Premium

Provide all of the features above with the added benefits of data isolation and Service Level Agreements (SLAs) or Service Level Objectives (SLOs). Premium plans provide customers a unique instance of a Watson service that is dedicated for their use leveraging containers and dedicated database instances to isolate client data. Customers can also have the ability to implement mutual authentication and whitelisting to ensure users are accessing the service from a trusted location. Additionally, transaction logging for service improvement is disabled by default in our premium plans. This option still has the advantage of shared hardware within the Watson IBM Cloud environment. Premium plans are suggested for customers looking to use Watson services with non-regulated PII data or have other data isolation requirements.

Dedicated Deployments

Allow customers full data isolation by implementing a dedicated instance for each customer within IBM Cloud and Watson services, which allows for integration with most enterprise single sign on solutions, tenant unique encryption keys, and added logging and monitoring capabilities, including detailed access logs. This not only allows customers to see who accessed their environment and when it was accessed, but it also provides the added benefit of knowing the complete solution is running on hardware dedicated for them. Dedicated deployments are appealing to enterprises with workloads that include sensitive data and have a need for additional transparency into where and how their data is managed.

Designing the right transformation to the Cloud

Being aware of the features and benefits of Public, Premium, and Dedicated Cloud is key to designing the right transformation to the Cloud. The added transparency provided by extended security controls in Dedicated Cloud deployments can boost Cloud initiatives. It is important to uncover security and compliance requirements up front and to tackle the hard questions early by including all internal stakeholders into Cloud initiatives. Making sure to include the security and compliance and risk teams early in the process will help ensure that the Cloud adoption program remains on track.
Base Security

The IBM Security Policy requires that all services include network and storage encryption, circuit and application level firewalls, security information and event management, intrusion detection, application source code scanning, 3rd party penetration testing, and regular vulnerability scanning. Figure 2 shows how these standards are used together.

Figure 2. Watson Services Environment Security

Data
IBM Watson services manage data in a variety of ways. Many of the Watson services are designed to be stateless in nature, meaning that while they may process data, they do not store it; the data is only used to complete the transaction and when that call to the service is completed the data is not retained. Some of the services allow customization which enables customers to help bring specific context to the data being submitted for processing. This configuration information when stored is isolated and encrypted. By default, transaction logs for services deployed in premium and dedicated solutions are not captured for service improvement or to develop new services.

**Authentication & Authorization**

The services are instantiated within the IBM Cloud Platform. Once a service has been requested for use, credentials are generated and managed through the IBM Cloud Console. When a call to a Watson service is made by an application, the credentials are transmitted via TLS for authentication and authorization. This allows only authorized users access to their content. Once this step is completed; a temporary token is generated that is good for 60 minutes.

**Encryption and Data Protection**

IBM employs the latest cryptography technologies technically feasible to protect customer data while at rest and in motion, examples include TLS/SSL, IPSEC, Third Party CAs, Encrypted File Systems, Encrypted Storage Systems, Key Management Systems, etc. Watson services only accept and send client data over the Internet using HTTPS via TLS connections with support for TLS version 1.2. Any client data stored at rest is encrypted using AES256 bit encryption.

**Backup & Redundancy**

IBM Watson Services utilizes a highly available infrastructure and architecture design to ensure service resiliency and availability such that traditional backups are not used. Watson services leverages automation, replication and snapshots to support these requirements. Business Continuity Planning (BCP) is tested at least annually and included as part of our regular controls testing program.

**Network Security**

IBM Watson leverages the defense in depth concept throughout its security stack to ensure visibility & control throughout. Within the Network Security stack there are layers of security controls; inspection, detection, isolation, directive, responsive & preventative. At each layer of the Network stack from Physical to Application, logs are captured, consolidated & analyzed. Load-balancing, DNS spoofing, & DDoS solutions are utilized to ensure defense from attacks against availability.

**Visibility and Intelligence**

IBM Watson Services protect client data through the use of Watson for Cybersecurity and threat intelligence feeds. Combined with a state-of-the-art Security Information and Event Management (SIEM) system, the security team is able to proactively monitor, detect, track, and take action on threats
attempting to compromise Watson and maliciously obtain our clients' data on a 24x7x365 basis. We monitor real time activity that occurs on or within firewalls, servers, and application APIs. This end-to-end monitoring solution allows the IBM Watson security team to quickly respond time to potential security violations or potential incidents.

**Application Security**

An important aspect of ensuring customers’ data is secure is the security and integrity of the services that process and manage data. As part of the regular release process our developers follow IBM's Secure Engineering Framework. Key activities that we regularly perform during our development lifecycle include:

- **Threat Modeling** - Each of our services goes through a comprehensive threat modeling approach that inventories where we process and store both customer and internal data, how it flows between these locations and external entities, how it is protected across these flows and how it is protected when stored. Based on this we identify the top threats and ensure that they inform the design, implementation and testing of our services to ensure any risks or threats are appropriately managed, mitigated or eliminated.

- **Static Code Analysis** - As part of our secure DevOps practices, services undergo static analysis (source scanning) to identify where we need to remove potential and latent security vulnerabilities. Static analysis identifies known pattern-based security vulnerabilities as well as tracing external inputs through execution paths to known dangerous outputs to identify where malicious user input poses a danger.

- **Dynamic Analysis** - We use automated tools against our running services to perform a comprehensive and complex battery of tests across all API endpoints and web application interfaces to identify potential security vulnerabilities on a regular basis.

- **Penetration Testing** – Is performed regularly and involves skilled practitioners using a wide array of automated tools and manual methods in an attempt to compromise a system. All services regularly undergo penetration testing. We use both IBM teams and external vendors to accomplish this. Each of our services is tested at least annually by a certified external vendor.

- **Security Vulnerability Management** - Is managed by our Product Security Incident Response Team (PSIRT) for identification and remediation of security vulnerabilities. All IBM Watson services participate in this system to ensure that security vulnerabilities identified directly in our services or in internal, or 3rd party components used by our services, are remediated in a timely manner and that customers are notified of any vulnerabilities that may directly affect them when appropriate.


**Workload Security Management**

Workload security management is implemented consistently though each of our deployment models. The Watson Security team leverages various industry standard tools, automation, and well defined repeatable processes to provide a robust Cloud Workload Security Management program. Security is
integrated into DevOps initiatives, Watson has a dedicated security staff that focuses exclusively on Watson Cloud offerings, security functions are automated allowing the environment to easily scale while ensuring consistency, and tools are in place to validate Watson APIs are secure prior to deployment. The Watson Security team manages:

- **Admin and privileged user access management** to the infrastructure ensuring the appropriate accounts, privileges, and authentication settings are in place and that multi factor authentication is implemented across the environment.
- **Privileged user activity tracking** is performed though log monitoring and user behavior analysis.
- **Malware protection** is in place where technically feasible
- **Continuous configuration monitoring and management** is integrated into our Secure Engineering process as well as continually monitoring workload configurations to avoid any drift from the expected values defined within configuration templates used at the time of deployment.
- **Host based firewalls and software defined networking** is in place and adds additional protection to ensure the appropriate isolation to protect client data while also providing additional endpoint access control, auditing, and identity and access management controls.
- **Inbound and outbound API configurations** are managed through an advanced application proxy that also provides authentication, authorization, TLS termination, dynamic routing, control, and integration.
- **DevOps configuration management** systems are used to ensure recipes are created and deployed to manage security configuration parameters during the workload build and configuration process building a consistently secure implementation every time.
- **IDS (Intrusion Detection System)/IPS (Intrusion Protection System)** is in place and monitored to ensure only appropriate traffic is sent to the services. Network traffic is monitored to and from the workload and logs are collected and sent to be analyzed by QRadar and the IBM SOC (Security Operations Center) team.
- **DDoS protection** is implemented for inbound circuits to data centers.
- **Log monitoring** is in place across the infrastructure that performs event correlation and detection. Events are constantly monitored by QRadar and the dedicated IBM SOC to identify abnormal behavior and provide alerts should an incident be detected.

**Physical security**

The Watson infrastructure is hosted within the IBM Cloud that has been reviewed by independent auditors to be SSAE16 Type II SOC 1, 2, and 3 compliant per the American Institute of Certified Public Accountants.

Physical security of IBM property is defined at the global level and includes a layered approach that includes site, building, data center, and data center partitions. Employees have limited physical access based on their job requirements to systems that host Watson on the IBM Cloud offerings.

Physical building security is maintained at various levels that are based on a categorization of security requirements for any physically partitioned area. The security includes but is not limited to gates, badge locks, cipher locks, key locks and biometrics, video monitoring and access logs. Data centers do not have first floor windows. Data center emergency doors are alarmed.
Human Resource security

IBM Human Resource policies determine the required background checks and monitoring for employees. These policies are based on applicable local laws. Employees with elevated system privileges are subject to more stringent requirements.

All IBM employees are required to take annual security education and to read and certify annually that they comply with established IBM Business Conduct Guidelines (BCGs). For more information about the BCGs, see http://www.ibm.com/investor/governance/business-conduct-guidelines.wss.

IBM Vendor Partners

Different companies can have different security practices while still conforming to prudent security principles. Watson vendor partners are carefully vetted and required to provide equally robust security practices in the area for which they provide their services.

Security Incident Management

A global management process for security incidents is employed and is applicable to the systems that host the Watson as a Service offering. This process is communicated to IBM employees and management, and is monitored 24x7x365 by trained IBM employees.

Additional information available here: https://www.ibm.com/security/secure-engineering/process.html

Identity and Access Management for Services

Identity and Access Management for Services is managed by users through the IBM Cloud. All services that are organized into a resource group in your account are managed by using IBM Cloud Identity and Access Management (IAM). Account owners are automatically assigned the account administrator role for Cloud IAM. As the account administrator, you can assign and manage access for users, create resource groups, provision service instances, and all other tasks that can be delegated by assigning the Cloud IAM roles. You provide access for users and service IDs by creating policies that set a target for the user or service ID to access and a role which defines what type of access is allowed. Additional details can be found here: https://console.bluemix.net/docs/iam/users_roles.html#userroles. Watson specific details available below:

When a user subscribes to use a shared service, in the public environment they are provided with an access URL, UserId and Password for each service. They will be allowed to use the Public Shared Services by making REST API calls using the URL and providing the UserId and Password in the basic-auth format in the HTTP header. All access to any of the Services are over TLS connections.

When a user subscribes to a premium service, they are assigned an exclusive instance of the service, and they are provided with an access URL, UserId and Password for each service. They will be allowed to access the Premium Service by making REST API calls using the URL and providing the UserId and Password in the basic-auth format in the HTTP header. Optionally:
• Users can request access to the premium instance be restricted to a specific list of egress IPs, which means any request coming from IPs other than those white listed will be rejected even if they had valid credentials in the Authorization HTTP Header.
• Users can request that all access to the premium instance be made only via mutually-authenticated TLS connections. In order to setup the mutually-authenticated TLS access they will need to provide the IBM Watson team with a Certificate Signing Request (CSR) for their private key, the certificate will be generated and signed by the Watson Platform CA, and then sent to the premium instance user to be used with all calls to the Premium Instance.

A Dedicated environment is a physically isolated environment set up exclusively for the Customer. This environment will be assigned a unique network path and accessed via a unique hostname that will be provided to the customer. All service instances used by the customer will be hosted in this isolated environment. Access to this environment can be setup in any one of the following methods:
1. Open access over TLS using the Unique internet host name.
2. Only mutually-authenticated TLS connection using the Unique internet host name.
3. VPN only access to the environment, the dedicated domain (IP) will not be accessible or available on the public Internet.
4. Connect using a Direct Link (leased line) between the Customer network and the Dedicated environment.

Users will still need to subscribe to use the services hosted in the Dedicated environment, and they are provided with an access URL, UserId and Password for each service as described above. They will need to make the REST API calls using the URL and providing the UserId and Password in the basic-auth format in the HTTP header.

**Industry Certifications**

IBM Watson services are ISO27001, ISO27017, and ISO27018 compliant, and are rapidly evolving to support other types of regulated workloads. Compliance of Watson Services are maintained through regular reviews by both IBM internal and 3rd party auditors.

**Governance, Risk, and Compliance**

The Watson data compliance strategy is built upon widely accepted Governance, Risk, and Compliance (GRC) principles as shown in Figure 3.
Governance

The Security Policy is established by IBM Corporate Directives that are defined by our dedicated Chief Information Security Officer (CISO) office and is enforced though regular audits and self-assessment.

Watson security controls are designed to meet industry standard controls and are intended to assist with compliance to external regulations in the healthcare and financial sectors such as HIPAA, HITECH, and FFIEC when and where applicable.

Risk Management

IBM recognizes risk assessment to be an important factor in security and has established a periodic risk assessment process that is applicable to the systems that host Watson on the IBM Cloud. Assessments are entered into the IBM Governance, Risk, and Compliance program to determine and manage the current risk posture and are regularly reviewed with senior management.

On occasion, deviations from the written security practice might be discovered through an audit or other means. When conditions warrant, systems might be taken offline for a deviation until remedial actions are taken. Deviations must be applied for by using a defined process, approved by the Chief Information Security Officer (CISO), tracked to closure, and remediated with interim measures until a final remediation is completed.

Compliance
Audits and Self-Assessment

IBM assesses and audits compliance against internal policies and ISO27001 standards. Assessments can include:

- Self-assessment of security controls
- Penetration testing
- Independent internal audits that are performed by using the security principle of separation of duties
- 3rd party auditors (SSAE16, ISO27001, and government regulatory agencies)

External Audit

IBM Watson has a team of professionals that are prepared to respond to external audits that are required under applicable law or regulation.

Additional resources for information related to IBM and Watson security

- ISO 27001 certificate: https://ibm.biz/BdjWav
- ISO 27017 certificate: https://ibm.biz/BdjWam
- ISO 27018 certificate: https://ibm.biz/BdjWak
- Full list of IBM products covered under 27001: https://ibm.biz/BdjWab
- IBM Cloud Services data security and privacy principles: https://ibm.biz/Bdsm3x
- Additional details around IBM Cloud compliance: https://www.ibm.com/cloud/compliance
- How to secure your applications using Watson Services: https://www.ibm.com/cloud/garage/content/architecture/securityArchitecture/overview