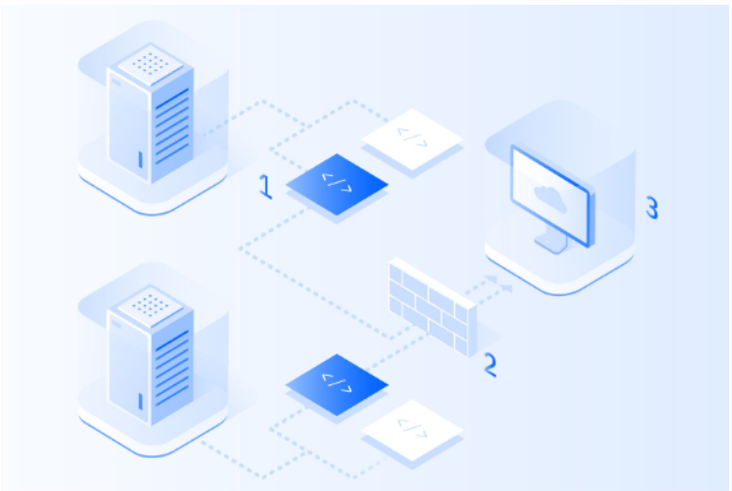
Secure to the core

IBM Storage Insights

- #IBMCloud service
- ISO/IEC 27001/27017/27018/27701 ISM certified
- Communication is initiated one way, encrypted and compressed
- Metadata at rest is AES 256-bit encrypted
- Metadata streamed to IBM Cloud is 128-bit encrypted
- Personal, identity, and application data are never accessed
- Works with IBM Enhanced Secure Support (Blue Diamond) framework for HIPAA compliance
- Dedicated vulnerability tracking and threat response team (IBM PSIRT)
- EU–US Privacy Shield and Swiss-US Privacy Shield Framework certification
- Integrated Security and Privacy by Design (SPbD)
- Meets the requirements of GDPR



How it works

1. Deploy one or more metadata collectors for redundancy or to optimize collection from data centers in different locations.
Key tip: If you monitor IBM Storage Virtualize storage systems, you can send metadata directly to IBM Storage Insights without a data collector. Learn more.
2. IBM Storage streams performance, capacity, health, and configuration metadata to IBM Storage Insights. Metadata flows in **one direction** - from your data center to IBM Cloud over HTTPS. IBM Storage can't receive data from the internet or any other entity in your network; it can only receive work requests from IBM Storage Insights.
3. In IBM Cloud, metadata is protected by physical, organizational, access, and security controls. Proxy servers are supported.

How metadata is protected

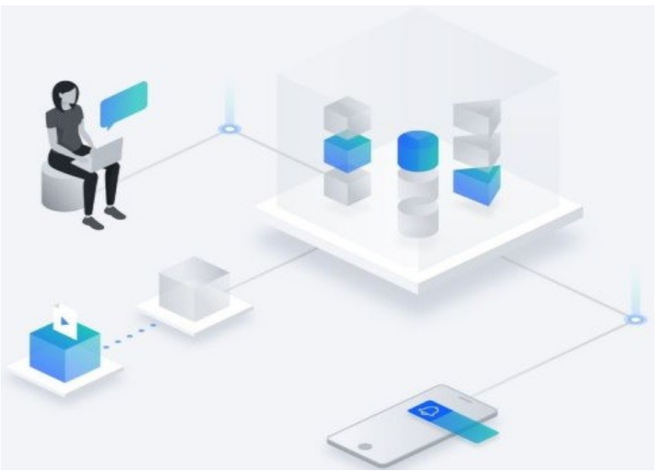
Security validated
Regular security, vulnerability, and penetration tests are conducted by IBM and external companies.

Physical protection
IBM Cloud data centers are rigorously controlled and onsite security is provided 24X7.

Secure Architecture
IBM Storage Insights is designed with a multi-tenant architecture to securely process and store the data of each customer.

Firewall security
When configuring your firewall to send metadata, you open a single, outbound path to a well-defined, secure endpoint.

Protected authentication
Multi-factor authentication provides an extra layer of protection against cyberattacks such as phishing, credential stuffing, and brute force attacks.



What metadata is collected

Metadata about your storage devices can include, but is not limited to the following information:

- Inventory and configuration metadata such as name, model, firmware, type, and more
- Inventory and configuration metadata for internal components such as volumes, pools, disks, ports, and more
- Capacity metrics such as capacity, usable capacity, used capacity, compression ratios, and more
- Performance metrics such as read and write data rates, I/O rates, response times, and more

Key fact: Use of IBM Storage Insights and the collection and use of metadata is governed by the IBM Cloud Service agreement and the IBM Storage Insights Service Description. The actual application data that is stored on your storage devices is never accessed or collected by IBM Storage Insights.

Who can access metadata

Access to metadata is carefully controlled and governed by the IBM Cloud Service Agreement and the IBM Storage Insights Service Description.

Key teams can access metadata. IBM Support, Development, DevOps have a level of access that's needed to help ensure that your day-to-day storage operations run smoothly. The wider IBM Storage Insights team has limited access to improve your product experience and help resolve any issues that you might encounter.

To access the metadata in IBM Cloud and ensure that the connection is secure, all IBM teams use a secure virtual private network (VPN) connection.

Sign up now!

https://ibm.biz/insightsreg

IBM Storage Insights Security Guide

IBM Cloud Security