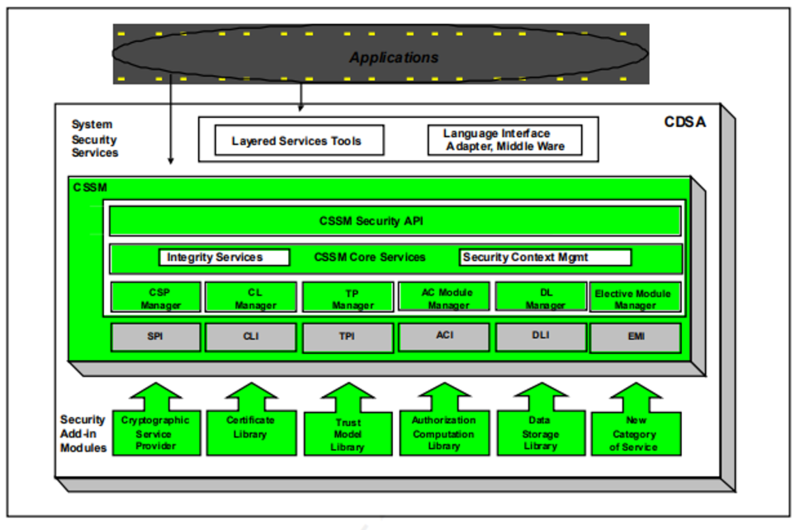
What are the types of data security?

**Top 5 Types of Data Protection**

* DATA ENCRYPTION. ...
* DATA BACKUP TO THE CLOUD. ...
* PASSWORD PROTECTION. ...
* IDENTITY AND ACCESS MANAGEMENT (IAM) ...
* INTRUSION DETECTION AND PREVENTION SOFTWARE.



**+++++++++++++++++++++++++**

**Best Practices for Securing Modern Data Architecture**

Today’s cloud-native data management platforms can help businesses unlock the potential of their data. These [modern data management and storage platforms](https://www.ibm.com/products/cloud-pak-for-data) are designed to deliver lean, high-performance architecture for agile application teams to ensure solid business outcomes, such as rapid time to market. Modern platforms, built for the cloud and in the cloud, offer benefits that make them easier to use and maintain. This helps reduce the total cost of ownership. Newer data services can often support global tasks like credit card payments and health care claims.

However, keeping data safe and compliant still presents challenges. Modern enterprises have a lot of options when it comes to securing sensitive data. So, which approach to modern architecture is best? And, how do you know you’ve defended your data thoroughly?

**Modern Solutions, Persistent Challenges**

Sometimes, the speed at which enterprise shifts to modern data architecture outpaces security and compliance tools. As such, defense teams are scrambling to find and test proactive controls to keep their modern landscapes secure. At the same time, they need to make sure baseline controls are in place to address compliance needs.

And, today’s threat actors know this is happening. They’ll take advantage of it in order to run [data breaches](https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html). This, in turn, leads to greater scrutiny in this space by policy groups and governments worldwide. Businesses need to make sure they’re up-to-date on data privacy rules across many data sources and cloud landscapes.

**Security Best Practices for Modern Data Architecture**

Finding a holistic data protection strategy can be difficult. Start with the data defense [best practices to consider](https://securityintelligence.com/posts/dont-torpedo-your-data-privacy-program-best-practices/). You’ll need a flexible and scalable approach that can simplify and streamline the process. This will give you a smooth path to an advanced data defense posture and a mature program.

**Know The Landscape**

Modern data sources that are being provisioned and set up in this landscape need to be checked for security — both for data at rest and in transit. In this case, modern data sources mean data platforms and services accessed via application programming interfaces (APIs). Data security teams now have to understand modern data architecture and [provide support for addressing defense and compliance](https://www.ibm.com/products/ibm-guardium-data-protection/database-as-a-service). Make data teams’ jobs easier by streamlining workflows to assess risks and automate fixes. Automate regular defenses by building reports for compliance ahead of time or assessing the overall health of the data landscape. Using modern [data security solutions](https://www.ibm.com/products/ibm-guardium-data-protection) that support the evolving data landscape across databases (DBs), database-as-a-service (DBaaS), files and data services can simplify the journey to secure [hybrid cloud and multicloud](https://securityintelligence.com/posts/overcoming-data-security-challenges-hybrid-multicloud-world/).

**Focus on Insight**

Another key element in this journey is making sure you have insight into data sources. Next, protect them with data-centric controls you need to minimize data risks and secure ‘crown jewels’ data in advance. This is a hallmark of a mature defensive wall. Data-centric controls, such as auditing and data insight, work well when they are applied based on your teams’ data rule sets.

Data protection solutions, which are built with [modern architectures](https://www.ibm.com/products/ibm-guardium-data-protection/database-as-a-service) that scale and secure the data landscape, are vital to help data defense teams go from being reactive to proactive. The teams can use threat analytics and machine learning-based investigations, for example, to spot and stop threats in real-time. These modern data platforms simplify workflows and automate regular tasks such as audit reporting. They can also support orchestration with built-in solutions and foster partnerships among teams.

**Is an Agent Approach Right for Your Cloud Data Protection?**

In order to support auditing and track behavior across both on-premise and cloud landscapes, data defense solutions have to provide agile and flexible deployment models. They also need to use methods suitable for gaining insight into data-level access and changes. [Data activity monitoring](https://www.ibm.com/products/ibm-guardium-data-protection) is a key element to look for. There are various ways to implement this type of solution: using agents on data sources that provide at-source scanning, using a proxy to sniff data-related traffic to and from the data source or collecting audit logs from the data source’s native audit history.

There are pros and cons to each of these collection methods. The agent- and proxy-based method is inline, which means it can perform real-time actions, such as redaction and blocking based on when rules are broken. However, not all data sources and hosted cloud providers support agent-based landscapes. Also, managing agents and proxy components can be onerous on data defense teams that need to ensure agent updates and maintenance. Agents can also be troublesome in legacy landscapes because of older versions no longer being supported.

**…. Or An Agentless Approach?**

Given the constraints that prevent using agents to monitor at source, data defense teams should understand the use and context of data sources to explore other feasible solutions. In order to make sure you can monitor the whole landscape, check criteria such as the type of processing (transactional versus analytical), type of platform and architecture (containerized DBs or hosted DBaaS), and the type of data stored (personal information, protected health data or non-sensitive data). In some cases, native data service APIs, including streaming APIs, can monitor data sources in the cloud.

Data collection through an agentless approach can provide limited support for compliance needs. Acting in real time is not possible. This method may work to support auditing data sources without critical, sensitive or regulated data. In addition to ingesting native logs from data sources, it is crucial for data defense teams to see and share actionable readings that can help spot outliers and trends in user behavior.

**Moving Forward With Modern Data Architecture**

Your teams may require both agent-based and agentless architectures for data collection and for overall data security program management. With modern architectures, [data security solutions](https://event.on24.com/eventRegistration/EventLobbyServlet?target=reg20.jsp&referrer=https%3A%2F%2Fmail.notes.na.collabserv.com%2Fverse&eventid=2875399&sessionid=1&key=26E63955E9D018F6C3FC09613335BCC2&regTag=&V2=false&sourcepage=register) can monitor data sources without an agent reducing the burden on infrastructure teams. You now have a few options to choose from: you can employ at-source monitoring for sensitive data using agents and monitor non-sensitive and internal data sources with an agentless architecture.

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

