Ebook

Why On-Premise Solutions Are Best For Data Security In Financial Compliance

Ensuring Data Security While Providing Reliable Data-Driven Solutions

Table of Content

Introduction

Data breaches have emerged as a major concern for the corporate world at large, particularly impacting the technology sector. For example, on September 25th, 2023, SONY, a multinational technology company, fell victim to a ransomware attack orchestrated by the group Ransomware.vc. The group, after discovering and leveraging a security vulnerability in Progress Software's MOVEit file transfer platform, which was employed by SONY and various other businesses and government entities, instigated the cyberattack. They claimed to have extracted over 6,000 files, including build logs and Java files, and threatened to sell the stolen data as SONY refused to comply with their payment demands.[1]

This incident underscores the growing threat landscape, marked by the proliferation of sophisticated ransomware designed to circumvent security systems. In light of such challenges, on-premise solutions are poised to be a much more secure option compared to cloud-based solutions, which often have fewer security layers in comparison to their on-premise counterparts.

So, what is an on-premise solution?

> “ An on-premise solution refers to a computing infrastructure where the hardware and software resources are deployed within the physical premises of an organization.”

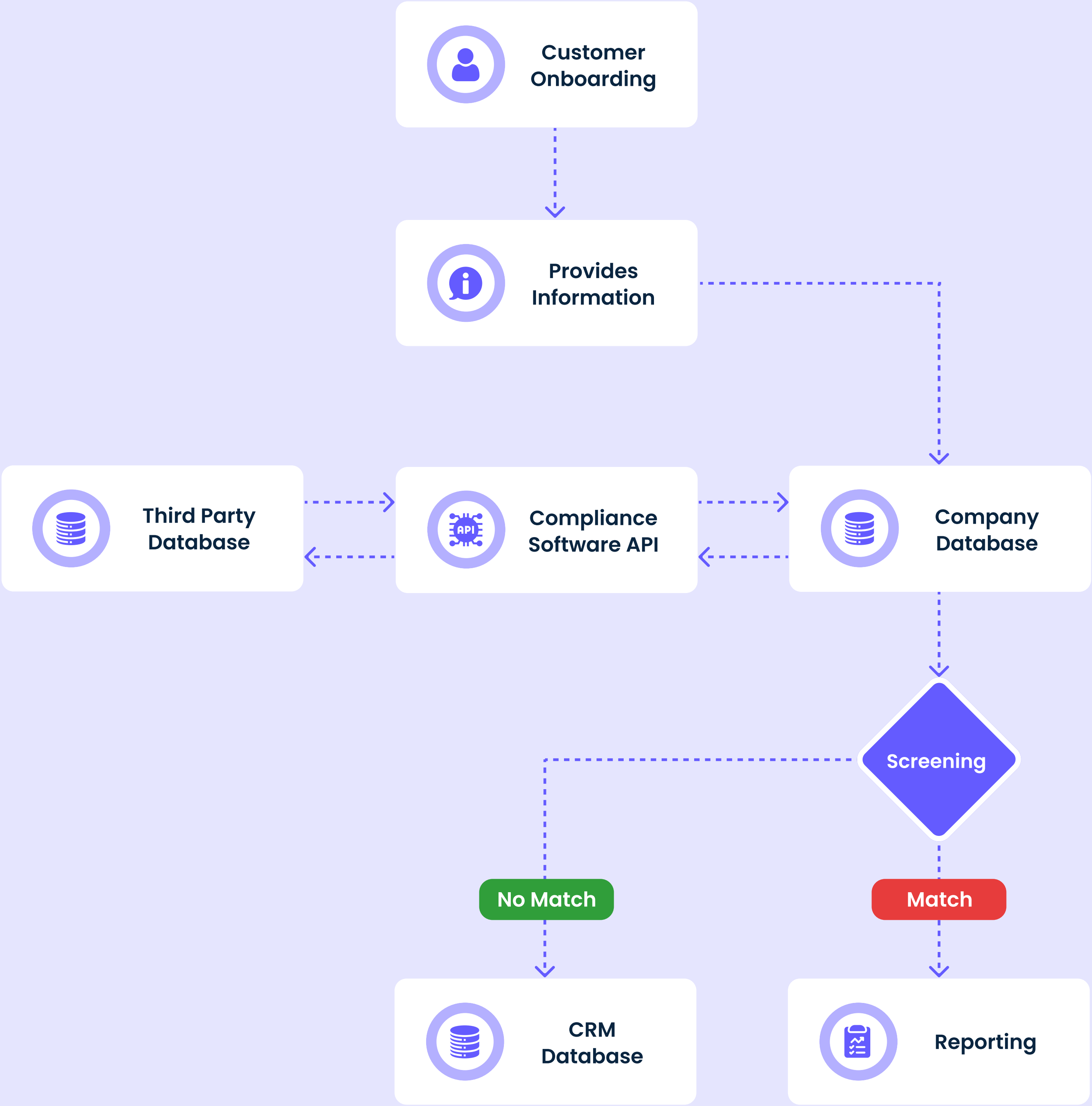
In contrast, hosted solutions entail storing the database in a third-party-managed data center, where the organization still owns the database but the hardware is overseen by the data center.

Conversely, cloud-based solutions utilize external servers from third-party vendors for storing, handling, and processing data. These cloud systems, accessible online, replace traditional non-digital systems and offer benefits like flexibility, easy maintenance, and scalability.

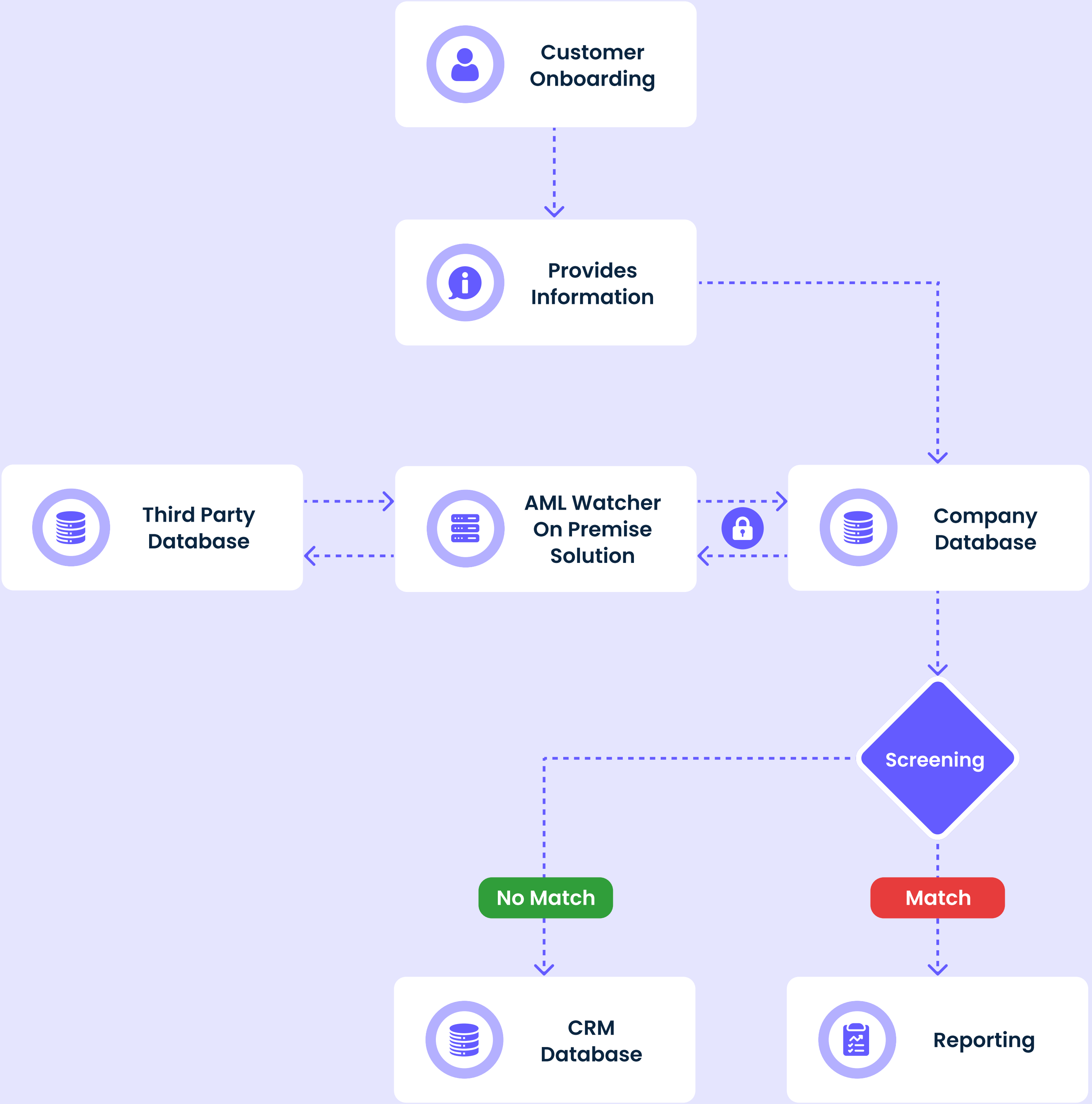
The main difference revolves around who owns and manages the hardware and software. On-premise solutions require organizations to handle their own infrastructure, including space, utilities, and staff. In contrast, cloud systems are handled by external providers, taking care of tasks like updates, backups, recovery, and support from a remote location.

[1] Spangler, T. (2023, October 6). Sony Discloses Data Breach That Exposed Info on Almost 6800 Employees and Family Members. Variety. Retrieved January 30, 2024, from https://variety.com/2023/digital/news/sony-data-breach-hack-6800-employees-family-members-1235747145/

Conventional Information Flows



AML Watcher Information Flows



Customer Onboarding

Provides Information

Third Party Database

AML Watcher On Premise Solution

Company Database

Screening

No Match

Match

CRM Database

Reporting

Instrumentality of On-Premise Solutions for Data Security

In scenarios where data security is of utmost importance, on-premise solutions prove instrumental, particularly in highly regulated industries. Industries such as finance or healthcare, which adhere to strict compliance requirements, favor on-premises setups to retain full control over data security and regulatory compliance. Moreover, organizations relying on legacy systems find on-premises solutions advantageous as they integrate and coexist with existing environments. For those handling highly sensitive data, such as government agencies or defense contractors, maintaining data on-premises becomes imperative to mitigate risks associated with external data storage.

Key Use-Cases:

Highly Regulated Industries

On-premises solutions are pivotal for organizations in finance and healthcare, ensuring stringent compliance adherence.

Legacy System Integration

On-premise setups facilitate the seamless integration of data security measures with existing legacy systems.

Data Sensitivity Concerns

Entities dealing with highly sensitive data, like government agencies, find on-premises solutions crucial to minimize external data storage risks. By keeping data within their own secure infrastructure, these entities can exert greater control over access, implement stringent security measures, and reduce exposure to external threats, ensuring a higher level of data protection and compliance with regulatory standards.

Ban on Microsoft, Google, and Apple Software in German Schools Due to Data Sovereignty Concerns

"In response to heightened concerns about data sovereignty and privacy, the Hesse Commissioner for Data Protection and Freedom of Information has banned the use of cloud-based software from Microsoft, Google, and Apple in German schools. The decision stems from worries about data storage in a European cloud, which is accessible to US authorities, emphasizing the critical role of data sovereignty in addressing security and privacy issues." [2]

Below are key data security regulations, each designed to ensure the responsible handling and protection of personal information, reflecting diverse global initiatives and legal frameworks across different industries and sectors.

Regulation	GDPR (General Data Protection Regulation)	HIPAA Privacy Rule	PCI DSS (Payment Card Industry Data Security Standard)	CCPA (California Consumer Privacy Act)
Enacted by	European Parliament and Council of the EU	104th United States Congress	Payment Card Industry Security Standards Council	California State Legislature
Effective Since	May 25, 2018	April 14, 2003	December 15, 2004	January 1, 2020
Main Purpose	Obtain consent, minimal data storage, and robust data protection	Safeguard protected health information (PHI) and medical records	Secure payment card transactions against data theft and fraud	Obtain consent, provide transparency, and protect personal information
Key Definitions	Personal data Information related to a natural person	"PHI": Information regarding a person's health status	N/A	Personal information": Information identifying or relating to a consumer
Applicability	Businesses in the EU and those handling EU residents' data	Covered entities in the United States	Businesses processing debit or credit card transactions	Businesses in California meeting specific criteria

[2] . HBDI bans Microsoft products following data sovereignty concerns. (n.d.). Senetas. Retrieved January 31, 2024, from

The Threat to Data Security

In the 2023 Thales study, human error, cited by 55% of respondents, surpasses vulnerabilities (21%) as the primary cause of cloud data breaches. The study highlights concerns about digital sovereignty affecting 83% of respondents, while 62% grapple with the complexity of encryption key management. Additionally, the report notes a 4% increase in cloud data breaches from the previous year, reaching 39%. Notably, three-quarters of businesses acknowledge that over 40% of their cloud-stored data is sensitive, but only 45% of this sensitive data is encrypted.[3]

Building Blocks of On-Premise Solutions

Reliability:

The internal network remains consistently accessible as it operates independently of the internet and external factors.

Complete Control

Vigilant monitoring of maintenance and upgrades provides complete control over data, hardware systems, and software.

Tailored Nature

Companies have the autonomy to independently adjust server hardware, offering increased flexibility and customization options.

Enhanced Security

Storing data on the organization's servers enables the implementation of additional data protection measures, ensuring an elevated level of security.

Regulatory Compliance:

For businesses governed by regulatory controls like HIPAA or FERPA, On-Premise solutions are essential for compliance. They facilitate adherence to regulations and improved management through localized data storage and processing.

[3] Retrieved January 30, 2024, from https://variety.com/2023/digital/news/sony-data-breach-hack-6800-employees-family-members-1235747145/

How AML Watcher Meets These Requirements and Beyond?

✓ Real-Time Data Synchronization

AML Watcher's On-Premise Solution ensures real-time synchronization with your database, guaranteeing that your AML data is consistently updated and readily available. This facilitates prompt compliance without delays.

✓ Complete Data Security

We prioritize the security of your data. Our solution is designed to maintain the confidentiality of your AML data, with a commitment to not track user information. Your compliance endeavors remain private and safeguarded.

✓ Unlimited Access

With this unrestricted access to the AML database, you can enhance due diligence measures, streamline compliance processes, and stay ahead in identifying potential risks.

✓ User Privacy Guarantee

Your privacy is paramount. AML Watcher refrains from tracking searches or any user information, creating a secure and confidential environment tailored to your compliance requirements.

How It Operates

Our On-Premise Solution integrates effectively with your existing infrastructure, facilitating a real-time connection to the AML database. As your data undergoes updates, your AML information follows suit, ensuring you have the most recent insights for well-informed decision-making. This robust integration not only enhances operational efficiency but also strengthens your overall risk management framework, providing a comprehensive solution tailored to your organization's needs.

Addressing Common Concerns

Some businesses express concerns that on-premise systems pose challenges in scalability, flexibility, and upfront financial commitments, hindering adaptability to demand fluctuations and requiring meticulous cost considerations.

All these challenges might create the impression that on-premise solutions are difficult. However, it's essential to realize that while upfront costs may appear significant for managers and finance departments focused on quarterly reports, the financial consequences of penalties resulting from data breaches or ransomware attacks are considerably higher, leading to substantial reputational damage. Moreover, addressing scalability and integration concerns, modern on-premise solutions come with tailored features that effectively mitigate these challenges.

AML Watcher

Turn Insights into Strategy

Get in touch for more information:

✉ info@amlwatcher.com

🌐 amlwatcher.com