International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V71I4P115

Volume 71 Issue 4, 115-124, April 2023

Original Article

Life Science Industry: Safeguarding Sensitive Data with SAP Cloud, AI, and Cyber Security

Gaurav Singh[1], Bidyut Sarkar[2], Ravi Dave[3]

[1]*Under Armour, MD.*
[2]*IBM, NY.*
[3]*Lakeshore Learning Materials, CA.*

Received: 06 March 2023 Revised: 08 April 2023 Accepted: 19 April 2023 Published: 30 April 2023

Abstract *- If Covid-19 has taught all of us one thing, it is that the most critical industry in this world is one which helps us to save human lives, supports health care, and gets us vaccines and medicines we all need to live and fight such deadly diseases, everything else is Secondary. Life science is one of the most critical and heavily regulated industries and holds the most sensitive and protected health Care information. In this paper, we will talk about how SAP Cloud Solutions using artificial intelligence (AI), is joining forces with Cyber Security to protect sensitive data for the life science industry by using a cloud-first approach and using artificial intelligence (AI), automation, data, and analytics in one unified environment. We will further deep dive and conclude how SAP cloud services like business technology platform (BTP) using SAP enterprise threat detection (ETD) will provide an end-to-end holistic cyber resiliency and help enterprises from life science industries comply with data protection regulations worldwide.*

Keywords *- Cyber Security, SAP Cloud, SAP S4/HANA, Artificial Intelligence (AI), Business Technology Platform (BTP), SAP Enterprise Threat Detection (ETD).*

1. Introduction

The life science and healthcare industry has the highest average cost of a data breach in any industry worldwide, amounting to $10.10M; the price of a breach in the life science and healthcare industry also went up by 42% since 2020, whereas the average total cost of breach across all industries globally is $4.35M [1]. As we explained life sciences or healthcare industry is the most critical industry, and also the one, if breached, would cost the most, not just to the breached organization but also to human lives well. Hence, it becomes clear that we should do everything possible to protect and safeguard the systems/solutions used to run and process sensitive data for the life sciences industry. If we look deeply into what solutions/systems and products the life science industry operates, we will conclude that most use enterprise resource planning systems, commonly known as ERP [2]. In this paper, we are going to explain how using ERP market leader, as per Gartner for Healthcare and biotech industry, aka life sciences, SAP, and using its Cloud(S/4HANA) and AI capabilities, along with cyber solutions and services, we can protect the critical business operations and sensitive data. SAP's new cutting-edge cloud product is called S4/HANA. The SAP's cloud product and solution, especially it's business technology suite of products (BTP), uses AI and machine learning to provide cutting-edge technologies to help organizations in life sciences to build processes so that their cyber leaders can identify and protect their sensitive data and resources and detect cyber threats and incidents and be able to respond and recover [4].

We need to start by identifying the risks and the threat landscape and understand where the sensitive data exist and the different compliance and data and privacy regulations requirements a life Science enterprise needs to comply with. With cloud solutions and deployment, the data move across countries and geographies, hence data and privacy regulations like HIPAA (Health Insurance Portability and accountability act of 1996 [5], GDPR (General data protection regulations) [6] and CCPA (California consumer privacy act) [7]. As these data and privacy regulations ask for data to reside within the region, personal and sensitive data for a European citizen should not leave Europe; the public cloud deployment model may provide some challenges, even if the area for public cloud is in Europe or a region of the consumer. Furthermore, the shared tenant model with the public cloud will create issues, especially when dealing with sensitive data. So, most Life Sciences enterprises would prefer the private cloud deployment model, even though it would be more expensive than the public cloud.

With either the public cloud or private cloud model, we also need to take into consideration that security in the cloud is shared responsibly [8] [9] [10]. Therefore, life science customers should clearly understand what a cloud service provides responsibility around security and what its commitment is.

Overall, with new business transformations, more and more country and regional-specific data and privacy regulations coming in, and an ever-expanding threat landscape, the task of protecting sensitive data for Life sciences industries is becoming more and more complex, not to mention challenges the industry face due to pandemics and supply chain issues. The life science industry's process and technology are probably the most difficult due to modern connected medical devices and IoTs.

2. Literature Review

Since the Covid-19 pandemic, the resiliency of the Life sciences and the healthcare industry has been under pressure. The industry also became a significant cyber-attack victim, disrupting major hospitals and health organizations worldwide [11]. The research in [11] reviewed all published papers on cyber and the healthcare industry, including any research and even recent cyber-attacks. It concluded with finding cyber security challenges and Cyber controls one should apply to mitigate/remediate these findings and risks. The Covid drugmaker Gilead was targeted for cyber-attack by Iran linked hacker [12], which led the drugmaker to come up with a cure for covid-19, including its remdesivir medicine.

Another study highlights that the healthcare industry, which was already struggling with a pandemic, had cyber-attacks to disrupt its supply chain [12]. The supply chain, ERP, and SAP go hand in hand. This explains why deploying proper cyber security controls and using necessary technology, including modern cloud and AI, is critical.

Cybersecurity challenges, risks, and plan to mitigate those risks for hospital [43] talks about how hospitals have personally identifiable information (PII) and personal health information (PHI), and when the PII or PHI data is stolen due to cyber-attacks, it put patient's life at risk and compromise the trust between doctors/providers and patients. It also talks about how hard it is to do forensic analysis involving IOTs, medical devices, and HVAC systems. This would mean many third parties and manufacturers are involved. The study also talks about how any risk mitigation plan should start with identifying assets and understanding who is responsible for applying security patches/fixes etc. Risk analysis should also be done to determine trade-offs between risks and benefits of risk mitigation.

Protecting sensitive PII and PHI data of the life sciences and healthcare industry should start with Risk assessment. National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) [4] is a framework that should be adopted and used to build a Cyber Security program. The NIST Cyber Security framework consists of standards, guidelines, and best practices to manage cyber security for critical infrastructure. With help from NIST CSF, we need to come up with policy, standard, and procedure for our life science enterprise and then use modern SAP S4Cloud products, which further uses AI and its proprietary business technology platform (BTP) to support Cyber domains, like identity and access management, governance, risk and compliance, vulnerability management and threat monitoring and incident management. The SAP Cloud products and solutions using AI and BTP provide the necessary technology to empower people to build processes that not only transform business; it also offers essential guardrails and controls to safeguard the PHI/PII data of the enterprises [15-20].

3. Implementing SAP S4/HANA to Build and Support Cyber Security Program

As we understand the Life Science industry is a highly regulated sector with the most sensitive data to protect, we would use cloud and AI-based technology, product, and solutions to build business processes using frameworks to create security programs that would empower our people working in this industry so that they are prepared to protect the sensitive data and can quickly react to any security threat or incidents. We would start with the NIST Cyber Security Framework (NIST CSF) to build a holistic Security Program from process and policy perspectives and compensate same with technology being offered by SAP Cloud, known as SAP S4/HANA, and its AI-Based Cloud Services being provided as part of SAP BTP like SAP Cloud Identity Services (IAS/IPS/IAG) and SAP Enterprise threat detection Tool (SAP ETD), SAP ALM and other core services to properly encrypt, mask and secure the Sensitive PII and PHI Data. You would implement SAP S4/HANA Cloud for your critical business processes as your critical and core processes like supply chain management, sourcing, procurement, manufacturing and R&D, asset management like medical devices, IoTs, and financial and other essential functions of business [15].

The SAP S4/HANA would be a system of record and source of truth-telling, your crown jewels. Life science industries' digital transformation or digitization is more critical than ever. SAP S4/Cloud offerings provide all necessary products and services and control like offering private cloud services as well so that life science enterprises can not only benefit from cutting-edge technologies and solutions using cloud and AI services. It still retains control of their sensitive data and helps them to be compliant with privacy and data regulations across the globe.

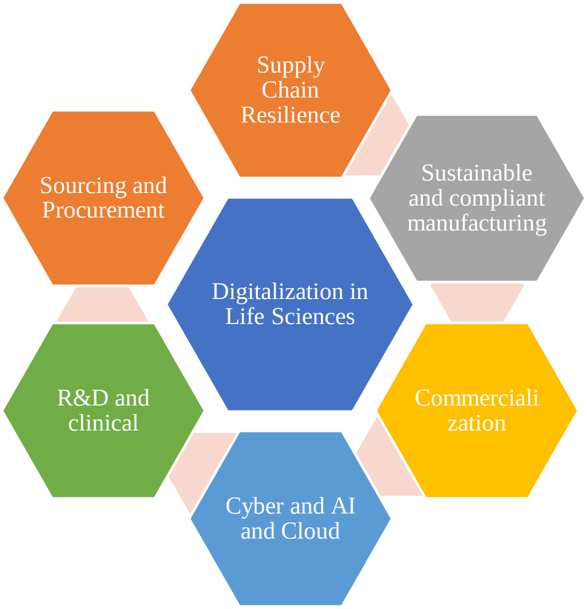


Fig. 1 Digitalization of the Life Sciences Industry and SAP [15]

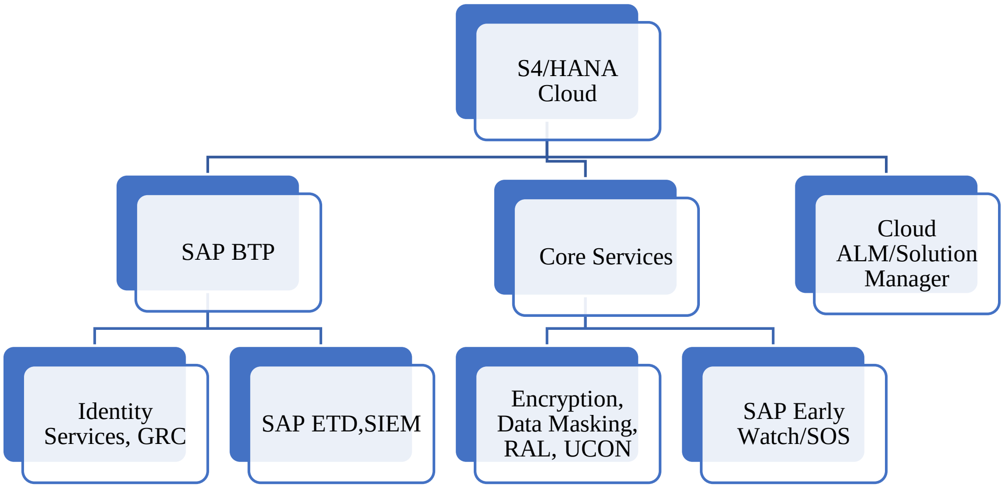


Fig. 2 SAP S4/HANA Products

SAP S4/HANA cloud offering provides public, private, and hybrid model so that you can choose the best model which makes sense to your business and provide the best return on investment (ROI) while providing all necessary controls to safeguard your business goals to protect your sensitive data and continue to innovate and deliver new medicines via R&D and clinical research.

With SAP S4/HANA implementation, you can support building your Cyber Security program based on the NIST CSF framework. We will go into detail about how each SAP S4/Cloud product and service would be used for each phase of NIST CSF so that we can protect the life science critical business processes and sensitive data.

The NIST Cyber Security framework, or NIST CSF, consists of five phases. It starts from Identifying or knowing what we need to protect(asset/data) to protecting and then detecting any cyber threats or incidents, responding to duplicates, and finally recovering from them.

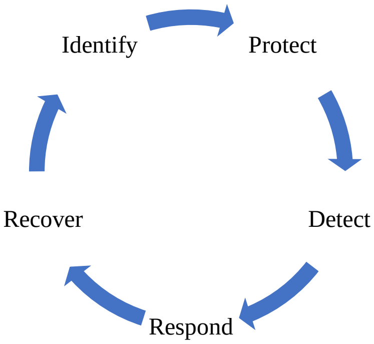
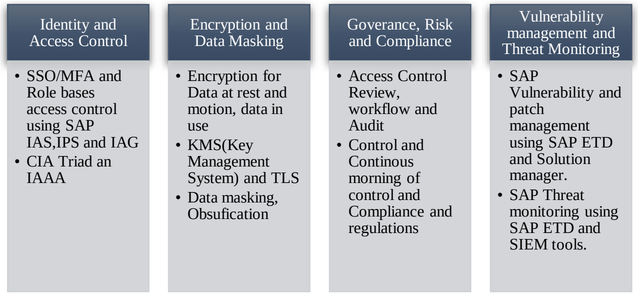


Fig. 3 NIST Cyber Security framework [4]

3.1. Identify – SAP Focusses Run, Cloud ALM & Solution Manager

We cannot protect what we do not know; the same goes for sensitive asset, which holds sensitive PII and PHI data for life science industries. Start with using SAP Cloud ALM, and SAP focussed run using solution manager to document and design your business processes and all SAP asset inventories. SAP Cloud ALM helps with your S4/HANA business transformation, which enables you to plan, design, test, deploy, operate, and continuously improve your S4/HANA SAP solutions [22]. It also allows accurate time monitoring and analytics capabilities to manage risks and ensure compliance. Using Cloud ALM and SAP focussed run and Solution manager, you can not only address the entire life cycle of your application deployments, build and document business processes critical for your business, you also maintain inventory of all SAP systems, which holds your sensitive information. This helps us to know and categorize our systems based on critical/sensitive data they possess and process. We also learn how good or bad our systems are around vulnerabilities and patches to develop a baseline following the SAP Security baseline document per the SAP Security operations map [24-26,44]. Knowing what we need to protect and what our critical systems, business processes, and assets hold and process sensitive data would help us correctly classify our assets/data to put required compensating control to mitigate the risks. This is probably one thing and foundation we need to get right, and these SAP Cloud Solutions and S/4 HANA at its core help us start our Cyber Security program journey on the right foot. Now as we know what we need to protect, we will go into the next phase of how we need to protect it.

3.2. Protect – SAP Cloud BTP, IAS/IPS/IAG, Data Masking, UCON, RAL, Encryption



Identity and Access Control
- SSO/MFA and Role bases access control using SAP IAS,IPS and IAG
- CIA Triad an IAAA

Encryption and Data Masking
- Encryption for Data at rest and motion, data in use
- KMS(Key Management System) and TLS
- Data masking, Obsufication

Goverance, Risk and Compliance
- Access Control Review, workflow and Audit
- Control and Continous morning of control and Compliance and regulations

Vulnerability management and Threat Monitoring
- SAP Vulnerability and patch management using SAP ETD and Solution manager.
- SAP Threat monitoring using SAP ETD and SIEM tools.

Fig. 4 Control and Processes to Protect your sensitive data.

The protection phase of NIST CSF is all controls you would define and security processes and tools you would implement to safeguard your sensitive data, whether it is using critical management services to encrypt your backup and cloud services, calling, or simply using TLS for encryption data in motion, or masking or obfuscating the data itself, which are sensitive.

As per the SAP Security operations map [26], we can divide our processes into four buckets or verticals. The first area would be defining identity and access control, starting from the basic cyber security principal of the CIA (Confidentiality, Integrity, and Availability) [30]. The CIA triad asks us to follow the least privilege access and need-to-know model, meaning only provide the least access needed to someone to perform their job. For the life sciences industry, tracking the most miniature privilege model and the need to know as we talk about PII/PHI and the most sensitive data becomes more critical. Therefore, we should build proper roles-based access control (RBAC) and provide access per someone’s job roles and responsibilities. SAP’s S4/HANA and its BTP Services like SAP IAS (Identity authentication service), IPS (Identity provisioning Service), and IAS (Identity Governance Service), we can genuinely implement, identify and access control which would help us to protect data and cover each piece for IAAA model, which stands for Identity, Authentication, Authorization and auditing or accountability. With IAS/IPS/IAG implementation, we can automate the entire life cycle of Identities for our life science enterprise, including Single Sign On (SSO) and Multi-factor authentication. Stolen and compromised credentials are the most common cause of data breaches [33], and using SSO and MFA using SAP BTP IAS, we can mitigate that risk and put necessary controls. Having SSO and MFA would probably be the first and foremost and most effective control to prevent data breaches and cyber incidents for life science industries or any other industry. Hence, MFA and role-based access control using IAS/IPS and IAG would ensure we mitigate that risk and control any lateral movement or the possibility of taking over user credentials. PS and IAG complement IAS with authorization, user provisioning, and putting controls around user access reviews and necessary audit logging capabilities to have an auditable log around identity and access control, covering all aspects of the IAAA model.

After we have built all controls around identity and access control, we will work on securing the sensitive data available in various places. To protect sensitive data, SAP provides a tool like UI masking to mask and obfuscate sensitive data while being used on the application side [35]. The UI masking, information life cycle management, and RAL (Read Access logging) provide necessary control and processes to mask/obfuscate sensitive data and include auditing and logging so that we know whom all are accessing and processing the sensitive data from a confidentiality and integrity perspective. In addition, we will be using standard encryption, Key Management Services (KMS), and TLS to secure and encrypt the sensitive data in use, data in rest, and data in motion on the database, operating system, file system, and network level.

Whereas IAS and IPS take care of identity, authentication, and authorization, IAG, along with the traditional Governance, Risk, and Compliance (GRC) system, help us define risk framework and define controls against those risks and risk registry so that we do continuous control monitoring for our entire S4/HANA landscape, which host and maintain sensitive PII and PHI data for life science industry [27-29]. As we understand, the Life Science industry is a heaving regulated industry; we need to use SAP GRC to define controls around access management, Including Segregation of Duties to avoid fraud, and also implement a risk and control matrix (RACM) and have an automated continuous control monitoring so that any exception to controls are monitored. Management takes appropriate action to remediate those exceptions/issues. SAP GRC integrates with IAG to support the on-prem and cloud SAP landscape, including SAP S4/HANA. As a result, we have one integrated governance process covering all critical assets, systems, and business processes. We can also use GRC to track and verify compliance against regulations like HIPAA, GDPR, SOX, etc. As we understand security is a shared responsibility in the cloud model, we rely on cloud providers' artifacts like SOC1, SOC2, and SOC3 for many compliance needs.

The last bucket/vertical in the protect section would be vulnerability management and threat monitoring so that we not only know vulnerabilities in our system, we are quickly patching them. An exposure and patch management program protects your critical systems and sensitive data. Knowing your systems’ vulnerabilities is one of the top reasons for data breaches. SAP Enterprise threat detection (ETD) tool, solution manager, early watch report and security optimization services, and SAP security patch days report help you assess your systems against known vulnerabilities but also help us develop an excellent patching process. SAP ETD also allows us to track exploits, threats, and known vulnerabilities so that any attempts to exploit these from threat vectors trigger alerts so that the security operation center (SOC) and respective teams can take detect these threats when it happens [20] [25] [27].

3.3. Detect - SAP Cloud ETD using AI

The next phase after protection would be detection. This is where our incident response or SOC team comes into the picture. As we all understand not, only some organizations have a big soc team AI, Cloud, and machine learning to augment monitoring, dashboards, etc., and even help us know signatures and exploits. SAP enterprise threat detection (ETD) using AI, machine learning, cloud technology, and analytics help us achieve and add detection and response, and recovery capabilities.

SAP ETD comes with pre-defined attack patterns and sap-related incidents, which lets you do risk-based and prioritized alerting to help you comply with data protection and audit regulations [19-20] [36] like HIPAA, GDPR, etc., from the life science industry. It also works as SIEM (Security Incident and Event Monitoring) for your SAP S4/HANA landscape, aggregating different log sources from applications and databases holding and processing your sensitive data. SAP ETD also complements and integrates with other SIEM tools like Splunk, etc., to give you and your Security operations team a holistic view of advancing persistent threats and incidents across your landscape. Using AI, machine learning analytics around all aggregated data helps detect anomalies, etc.

3.4. Respond and Recover-SAP Cloud ETD, GRC/IAG, BC/DR

The last phases of the NIST CSF framework are to respond and recover from cyber incidents. In today’s digital and all-connected world, we must always be ready for cyber breaches and incidents. As we say, it’s not about if; it’s about when. So especially for the life science industry and health care, as we understand this is one of the topmost industries being cyber attacked more than any other industry, we need to have a well-documented, tested incident response process and team. The people, process, and technology all must come together ideally so that we cannot only detect these cyber incidents but can also quickly contain and stop any lateral movement by responding to it and recovering quickly. SAP ETD helps us to do forensic analysis by providing a comprehensive view of the incident context, related events, and affected systems. It uses user pseudonymization and resolution when there is evidence of attack or misuse. SAP ETD collects data from different systems like GRC/IAG and other systems logs to provide a comprehensive view of incidents and Dashboard. It also uses direct kernel API to receive logs so that a bad actor who is already in cannot manipulate logs and alerts. After we have responded to cyber incidents and stopped lateral movement using SAP ETD and other SAP cloud services like IAG/GRC, we need to use all the data/reports we got from ETD and use our Backup and Disaster recovery (BC/DR) process to recover from the incidents as quickly as possible. The Recovery process of NIST CSF would rely on people and techniques to ensure we have an exemplary BC/DR process and documentation, which is tested multiple times so that when the actual incident or disaster occurs, we can quickly recover from it. The automation around backup and restoring the services, whether a full cloud SaaS or hybrid model where we have the infrastructure (IaaS), or platform (PaaS), would be essential. SAP S4/HANA, with its inbuilt high availability and disaster recovery model in different regions and availability zone, does help us to recover from such cyber incidents faster than you would in the traditional On-Prem model. Also, for the life science industry, we need to make sure we understand our compliance and regulatory asks around any data breaches or Cyber Incidents as sometimes it cannot be a cost to operations like not being able to operate a hospital to provide critical services, the regulatory fine from not following the regulations can be a considerable business risk as well. So, the process around Incident response should include due diligence and due care around legal and regulatory ask. Automation using SAP GRC with these regulations will also come in handy here, along with SAP ETD and its AI capabilities which would provide the correct information to our cyber leaders to engage legal and law enforcement on time, resulting in any cyber incident reporting as well if needed.

A good Cyber Insurance policy, processes, and technology would help all life science industries mitigate and even transfer some risks due to cyber-attacks and ransomware.

4. SAP Cloud Products and Services Supporting various Security Phases of the Cyber Program and Operations

- SAP-Focused Run: This tool provides a centralized view of an organization's IT landscape, including its SAP systems. It allows organizations to monitor and manage the health and performance of their SAP systems and provides insights into security vulnerabilities and risks. With this tool, organizations can proactively identify and address security threats before they become significant issues.
- SAP ALM: This is another tool designed to help organizations manage the lifecycle of their SAP systems. It provides a range of features and functions that can help organizations monitor and optimize the performance of their SAP systems, including security-related issues. With this tool, organizations can ensure that their SAP systems are always up-to-date and secure.
- SAP Cloud IAS/IPS/IAG/GRC: This suite of solutions provides identity and access management, intrusion prevention, governance, risk, and compliance solutions for cloud-based SAP applications. It helps organizations ensure that only authorized users can access their SAP applications and data and provides real-time monitoring and alerts to detect and respond to security threats.
- SAP ETD/SIEM: This solution provides real-time threat detection and incident response capabilities, helping organizations identify and respond to security threats. It uses advanced analytics and machine learning to detect anomalous behavior and potential threats and provides alerts and notifications to help organizations act quickly.
- SAP UI Masking: SAP UI masking is a security solution to protect sensitive data in the SAP application user interface (UI). It enables organizations to securely mask or hide confidential data such as financial information, personal data, or intellectual property from unauthorized users. This solution is essential for the life science industry, where protecting sensitive data is critical to ensure regulatory compliance and patient privacy.

By implementing SAP UI masking, life science organizations can significantly reduce the risk of data breaches, insider threats, and unauthorized access to sensitive data. This solution allows organizations to define and manage data masking policies based on specific user roles, ensuring only authorized users can view or access sensitive data. Additionally, SAP UI masking can easily be integrated with other SAP security solutions, such as SAP Single Sign-On (SSO) and SAP Access Control, enabling organizations to create a comprehensive security framework for their SAP applications.

- SAP BTP Identify Services: SAP Business Technology Platform (BTP) offers a suite of Identify Services that can be used to protect the life science industry from cybersecurity threats. SAP Cloud Identity service provides identity and access management solutions for cloud-based applications, which are increasingly popular. It allows companies to manage user identities, access permissions, and security policies across multiple cloud platforms.
- SAP RAL/UCON: SAP Read Access Logging (RAL) is a security feature that allows you to monitor and log access to sensitive data in your SAP system. It is designed to help organizations comply with data protection regulations and prevent unauthorized access to sensitive data. Organizations can identify potential security breaches and unauthorized access to sensitive data using SAP RAL. The logged data can generate reports and alerts to notify security personnel of suspicious activity. Additionally, the logged data can be used for auditing purposes to ensure compliance with regulatory requirements. UCON help to protect remote calls in and out from SAP systems. By implementing these solutions models using SAP solutions, life science organizations can improve their security posture by controlling and monitoring access to sensitive data and resources.

SAP Information Lifecycle Management (SAP ILM): Safeguards the privacy of your customers’ data and helps to automatically archive and retain data, as well as decommission legacy systems, while balancing total ownership costs, risks, and legal compliance. Implementing this life science industry can safeguard its sensitive data but also helps us comply with privacy and data protection regulations [37].

Implementing SAP S4Cloud AI technology to mitigate cyber risks around sensitive data for the life science industry has resulted in several positive outcomes.

This includes improved data security by using real-time detection and mitigating cyber threats using SAP BTP offered by SAP S4Cloud and its services like BTP and AI to implement products and services to build business processes for Life Science and healthcare enterprises able to protect and secure sensitive PII and PHI data. There is no single tool or product that can solve all Cyber risks. Still, with a combination of products, services, and tools offered by SAP S4 Cloud using AI, we can very well remediate cyber threats for the industry and help them secure the sensitive data they possess.

The business transformation journey for life science enterprises to implement SAP S4Cloud solutions may look complex on a surface level. Still, we if start from frameworks like NIST cyber security framework and build policies, standards, and procedures to support and drive to implement solutions and business processes and empower our people who are responsible for safeguarding the sensitive data, we would provide a win-win situation both for Business and Cyber which in term would help us to serve humankind and save lives.

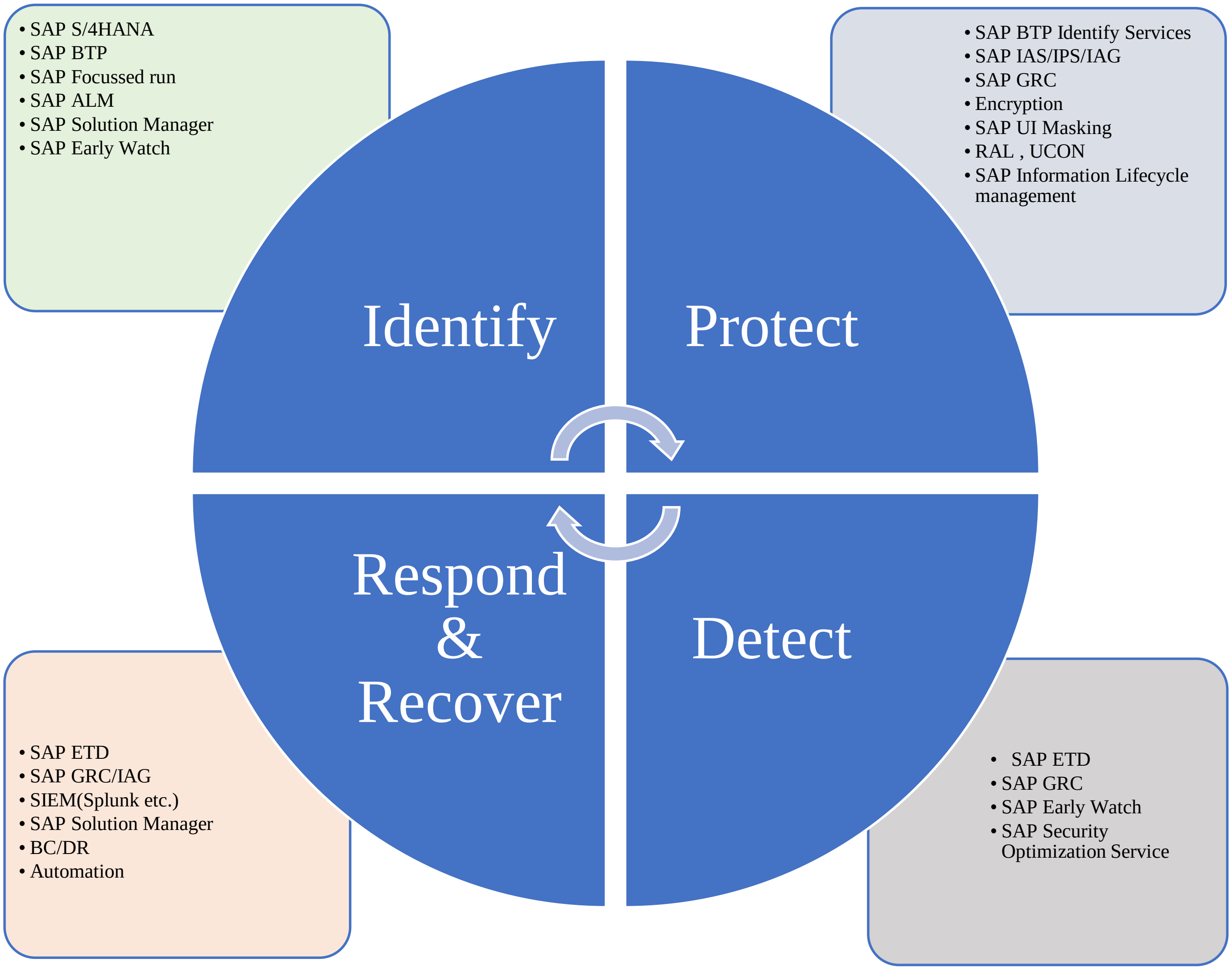


Fig. 5 SAP Tools and Solutions to Protect Life Science Industry

5. Conclusion

In conclusion, our findings suggest that a combination of technological solutions provided by SAP S/4HANA Cloud, including its services such as BTP and AI, are required to effectively implement products and services for developing business processes in the Life Science industry. In light of the need to safeguard sensitive PII and PHI data, it is crucial to note that no single tool or product can fully address all potential cyber risks. However, leveraging the various products, services, and tools provided by SAP BTP services and incorporating AI capabilities makes it possible to effectively remediate cyber risks for this industry and enhance its ability to secure sensitive data. As the Life science industry continues to face increasing cyber threats, as mentioned in this paper, organizations must adopt a proactive approach to cybersecurity and implement advanced cloud solutions to ensure the protection of sensitive data and the continued provision of safe and reliable services.

6. Results

Category of Cyber Attack	Type of Life Science Industry	Impact	Proposed Solution/ Mitigation Plan
A ransomware attack – The year 2020	Clinical research organization	The attackers were able to encrypt the organization's sensitive data and demanded a ransom in exchange for the decryption key. This resulted in significant downtime and financial losses for the organization, as well as potential harm to the patients whose data was compromised [38]	To prevent such incidents, it is critical to implement adequate cybersecurity measures, such as those provided by SAP Cloud, AI, and Cyber Security solutions. These tools offer advanced identity and access management, intrusion prevention, and threat detection capabilities that can help safeguard sensitive data and prevent cyber-attacks in the life science industry.
Not Petya ransomware attack – The year 2017	Pharmaceutical company	The attack led to significant disruptions in the company's operations and caused the loss of approximately $870 million in revenue [39].	After the Not Petya attack, the company implemented various mitigation measures, including restoring IT systems, enhancing security controls, and reviewing security procedures. They also conducted a thorough investigation to understand how the attack occurred and to prevent similar attacks in the future. It also highlights why having good comprehensive cyber insurance for the life science and health care industry is necessary in the new world.
Cyber Attack, Identity Theft – Year 2018	Pharmaceutical company	It resulted in a data breach affecting the personal information of approximately 6,000 employees [40].	Network segmentation can help limit the lateral movement of attackers in the network and contain the attack within a specific segment. In addition, intrusion detection and prevention systems can help detect and respond to attacks in real-time by identifying and blocking suspicious activity before it can cause harm. Finally, regular data backups and secure storage can help ensure that critical data can be quickly restored during a successful attack, minimizing the impact on the organization.
Cyber Attack, Identity Theft – Year 2018	Medical diagnostic and research company	The company experienced a cyberattack that resulted in a data breach affecting approximately 7.7 million customers. The attack targeted a third-party billing collections vendor, which stored customer data. The attack compromised personal and financial information, including names, dates of birth, addresses, phone numbers, credit card numbers, and bank account information [41].	The company implemented new security measures to prevent similar incidents in the future, including increasing the frequency of third-party security assessments and requiring vendors to implement data security measures consistent with the company's standards.

References

[1] IBM Report on Cost of Data Breach 2022. [Online]. Available: https://www.ibm.com/reports/data-breach

[2] Best Healthcare ERP Solutions: Compare Key Features. [Online]. Available: https://www.cioinsight.com/enterprise-apps/healthcare-erp-system-features/

[3] Gartner Cloud ERP for Product-Centric Enterprises. [Online]. Available: https://www.gartner.com/reviews/market/cloud-erp-for-product-centric-enterprises

[4] NIST Cyber Security Framework. [Online]. Available: https://www.nist.gov/cyberframework

[5] Health Information Policy, HIPAA. [Online]. Available: https://www.hhs.gov/hipaa/index.html

[6] General Data Protection Regulation. [Online]. Available: https://gdpr.eu/

[7] California Consumer Privacy Act. [Online]. Available: https://oag.ca.gov/privacy/ccpa

[8] SAP BTP Cloud Shared Responsibility Model. [Online]. Available: https://help.sap.com/docs/btp/best-practices/shared-responsibility-model-between-you-and-sap?locale=en-US

[9] AWS Cloud Compliance Shared Responsibility Model. [Online]. Available: https://aws.amazon.com/compliance/shared-responsibility-model/

[10] ISC2 Responsibility and Accountability in the Cloud. [Online]. Available: https://www.isc2.org/Articles/Responsibility-and-Accountability-in-the-Cloud

[11] Ying He et al., "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review," *Journal of Medical Internet Research*, vol. 23, no. 4, p. e21747, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Reuters US Healthcare Targeted Cyber Attack. [Online]. Available: https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex-idUSKBN22K2EV

[13] Vencelin Gino V, and Amit KR Ghosh, "Enhancing Cyber Security Measures For Online Learning Platforms," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 11, pp. 1-5, 2021. [CrossRef] [Publisher Link]

[14] Salem T. Argaw et al., "Cybersecurity of Hospitals: Discussing the Challenges and Working towards Mitigating the Risks," *BMC Medical Informatics and Decision Making*, vol. 20, p. 146, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Life Science Industry Solutions from SAP. [Online]. Available: https://www.sap.com/industries/life-sciences.html

[16] Accenture, Life Sciences Industry and SAP. [Online]. Available: https://www.accenture.com/us-en/services/life-sciences/value-case-sap

[17] eBook, Transforming Life Sciences with SAP. [Online]. Available: https://www.sap.com/dmc/exp/2022-09-84988-life-sciences-ebook/index.html

[18] The future of Life Science Industry is in the cloud [Online]. Available: https://www.sap.com/documents/2022/04/68f9a608-257e-0010-bca6-c68f7e60039b.html

[19] SAP News, Enterprise Threat Detection Cloud [Online]. Available: https://news.sap.com/2021/07/sap-enterprise-threat-detection-cloud-based-managed-service/

[20] SAP Help, Enterprise Threat Detection Cloud Edition [Online]. Available: https://help.sap.com/docs/SAP_ENTERPRISE_THREAT_DETECTION_CLOUD_EDITION

[21] Gaurav Singh, SAP Insider, Expert Insight Article. [Online]. Available: https://sapinsider.org/expert-insights/protect-your-sustainability-goals-with-sap-cybersecurity/

[22] SAP Support, Cloud ALM [Online]. Available: https://support.sap.com/en/alm/sap-cloud-alm.html

[23] Sanjeev Kumar, "Data Intelligence and Planning using AI and Machine Learning with SAP Analytics Cloud - SAC," *International Journal of Computer Trends and Technology*, vol. 69, no. 2, pp. 1-4, 2021. [CrossRef] [Publisher Link]

[24] SAP Security whitepaper, Managing Security with SAP Solution Manager [Online]. Available: https://layersevensecurity.com/managing-security-with-sap-solution-manager/

[25] SAP Insider. [Online]. Available: https://sapinsider.org/topic/sap-system-administration/sap-solution-manager/

[26] The SAP Secure Operations Map. [Online]. Available: https://www.sap.com/documents/2017/03/14cf06b2-af7c-0010-82c7-eda71af511fa.html

[27] SAP Security Whitepapers [Online]. Available: https://support.sap.com/en/security-whitepapers.html

[28] Marko Sommer, SAP Blog. [Online]. Available: https://blogs.sap.com/2021/09/24/single-sign-on-sap-reference-architecture-for-identity-access-management/

[29] Marko Sommer, SAP Blog [Online]. Available: https://blogs.sap.com/2020/06/24/evolving-identity-authentication-and-identity-provisioning-into-sap-cloud-identity-services/

[30] TechTarget, CIA Triad. [Online]. Available: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

[31] SC Magazine, Ransomware Attacks Persist in Healthcare. [Online]. Available: https://www.scmagazine.com/analysis/ransomware/ransomware-attacks-persist-in-healthcare-as-impacts-on-patient-safety-rise

[32] AAMC News, Growing Ransomware Attack to Hospitals. [Online]. Available: https://www.bitlyft.com/resources/the-growing-threat-of-ransomware-attacks-on-hospitals

[33] UK News, Most Common Cause of Data Breach. [Online]. Available: https://www.sutcliffeinsurance.co.uk/news/8-most-common-causes-of-data-breach/

[34] IAAA Definition. [Online]. Available: https://thorteaches.com/cissp-iaaa/

[35] Masood Ahmed, SAP Blog, UI Mask to Achieve Compliance [Online]. Available: https://blogs.sap.com/2022/11/25/the-hidden-gem-using-ui-masking-to-acheive-compliance/

[36] Martin Mueller, SAP Blog ETD and SIEM. [Online]. Available: https://blogs.sap.com/2019/07/22/sap-enterprise-threat-detection-etd-and-security-information-and-event-management-siem.-what-is-the-difference-and-how-can-they-work-together/

[37] SAP UCON [Online]. Available: https://www.sap.com/documents/2015/07/ccf7ed8e-5b7c-0010-82c7-eda71af511fa.html

[38] The New York Times, Clinical Trials Ransomware Attack. [Online]. Available: https://www.nytimes.com/2020/10/03/technology/clinical-trials-ransomware-attack-drugmakers.html

[39] Josephine Wolff, Brookings Edu. [Online]. Available: https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/

[40] Chris Souza, Pharma Exec. [Online]. Available: https://www.pharmexec.com/view/lessons-pharma-merck-cyber-attack

[41] AMCA Breach Exposed 7.7m patient data [Online]. Available: https://www.fiercehealthcare.com/tech/amca-breach-may-have-exposed-data-7-7m-labcorp-patients

[42] Ravi Dave, Bidyut Sarkar, Gaurav Singh, "Revolutionizing Business Processes with SAP Technology: A Buyer's Perspective," *International Journal of Computer Trends and Technology*, vol. 71, no. 4, pp. 1-7, 2023. [Crossref] [Publisher Link]

[43] FBI Alert Health Care Industry Cyber Attack. [Online]. Available: https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/

[44] SAP Help, SAP Solution Manager. [Online]. Available: https://help.sap.com/docs/