WHITEPAPER

AI & SAP Security: Benefits, Risks and Prerequisites

SecurityBridge™

For many years, Artificial Intelligence has been a significant topic, finding applications in numerous industries.

With the release of OpenAI's GPT-3 language model, we have reached a significant milestone in the evolution of AI. This model can understand and generate human-like text with remarkable accuracy. Corresponding to its adoption, from January to February 2023, Darktrace researchers observed a 135% increase in "novel social engineering attacks.

As AI continues to advance, it has the dangerous potential to impact the SAP security threat landscape.

Contents:

AI's Impact on Cybersecurity: Benefits……….…..…........ Page 3
AI's Impact on Cybersecurity: Risks ……………..…........... Page 4
How can AI help improve your SAP Security Posture?... Page 7
Prerequisites for an AI-Driven SAP Security ………………... Page 9
Conclusion ………….. Page 15

AI’s Impact on Cybersecurity: Benefits

The use of AI in cybersecurity is becoming increasingly popular as it offers a range of **benefits, from automation to predictive analysis, to defenders (and, unfortunately, to attackers alike!**).

AI systems can be used to analyze large amounts of data to identify patterns and anomalies, helping organizations **detect and prevent potential cyber threats and security incidents,** more quickly and accurately than humans. Further, AI might be able to detect and even respond to threats automatically.

But not only that! AI could be used to **protect sensitive information:** encrypt sensitive data, monitor data access and identify unauthorized users, protect personal data privacy. It could possibly even enforce data usage policies and support compliance with various privacy laws. Furthermore, AI-powered tools of today can **automate repetitive and manual tasks**, freeing up security personnel to focus on more strategic initiatives.

Although this all reads like a fairytale from the marketing brochures of the leading cybersecurity solution providers in the 2010s, it is now a reality. In fact, the market for AI in cybersecurity is expected to grow significantly. It’s projected to increase from around $24 billion in 2023 to approximately $134 billion by 2030.

SAP is also no stranger to harnessing the power of AI and has been leveraging it for intelligent automation, advanced analytics, supply chain automation, and application security. According to the SAP AI Ethics Handbook, the company uses learning-based AI and says, “…systems are differentiating themselves by the fact that humans define the problem and the goal, but the behavior, rules, and relationships required for the system are learned in an automatized way. With the help of data, they train how to solve a problem and continuously adapt their function in this process.” In fact, **the use of AI runs deeply into SAP**’s finance, supply chain, procurement, human resources, and sales business applications.

AI's Impact on Cybersecurity: Risks

Although the benefits seem endless, on the other hand, **AI also presents new challenges and risks** in the SAP security landscape. As Artificial Intelligence becomes more advanced, it has the potential to be used and abused by attackers in new ways. In fact, IT threats are increasing in alignment with the number of cyberattacks. Deep Instinct's fourth edition report states that 75% of security professionals have observed an increase in cyberattacks this year, with 85% of these attacks driven by generative AI. However, the attacks' frequency not only increased, but the attacks' strategies have also become more sophisticated as the well-known MGM Grand/Caesar's breach from 2023 revealed.

For example, AI can generate **malware** capable of evading traditional cybersecurity defenses. With the amount of data and computing power available today, AI has the potential to be used to execute social engineering attacks without the victim's awareness. These attacks rely on tricking people into revealing sensitive information or taking actions that compromise their security. AI has the potential to automate social engineering attacks and make them even more convincing.

Furthermore, AI has been already reported to perfom **deepfakes**, **automated attacks, cyber espionage** and **IoT attacks**. Another advanced threat is the **manipulation** of the AI model. One example is the case of Microsoft's ChatBot, which was quickly socially engineered to become racist. The ChatBot, designed to interact with users and generate responses based on its training data, was exposed to a malicious training data set that resulted in the AI system producing racist and inflammatory responses. This incident highlights the potential for AI systems to be manipulated and the importance of carefully considering the data and algorithms used to train AI systems.

Organizations are finding it challenging to stay ahead in detecting and preventing advanced exploits with traditional cybersecurity measures. **There is a significant demand for more adaptive and advanced tools and strategies** to protect against the rapidly evolving threat landscape and defend against these automated, dynamic exploits. Now is the time for leaders to explore how to strengthen their software infrastructures and mitigate these increasingly growing risks.

Trusting AI vs Zero-Trust

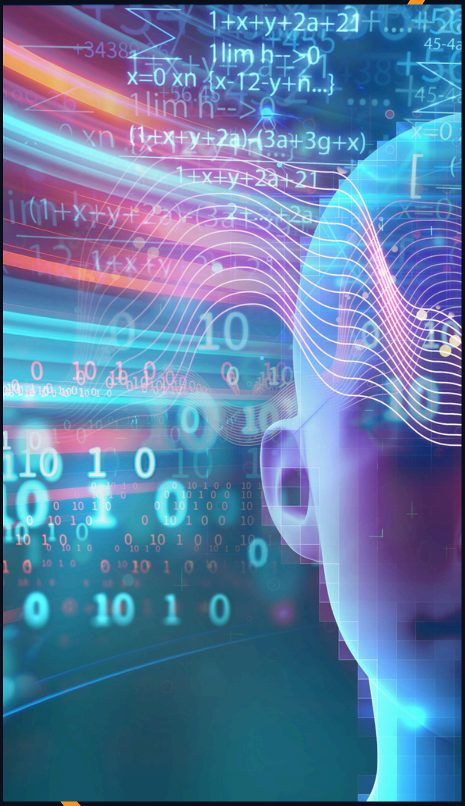
AI systems need **more transparency and explainability**. AI systems analyze vast amounts of data and make decisions based on patterns that can be difficult to understand. This lack of transparency can be a problem for organizations that need to comply with regulations and standards that require them to be able to explain their security decisions. For example, under the European Union's General Data Protection Regulation (GDPR), organizations must be able to explain the logic behind automated decisions affecting individuals.

Another of the most significant risks of AI in the cybersecurity threat landscape is the **uncertainty of its outcomes**. AI systems make decisions based on the data and algorithms they are trained on, and humans do not always verify the results. This process can create a situation where humans need to blindly trust AI without fully understanding how or why it made a certain decision.

This level of trust is a fundamental conflict with the widely adopted zero-trust strategies in cybersecurity. Zero-trust strategies emphasize the importance of verifying and authenticating every (access) request, regardless of the source. As AI matures, verifying the generated results will become more challenging, if not even impossible.

Zero-trust strategies emphasize the importance of verifying and authenticating every (access) request, regardless of the source. With AI, it is not always apparent which intention lies behind a specific answer, and it is challenging to verify the accuracy and authenticity of the information generated by AI systems.

SAP takes this level of trust one step further by defining high-risk cases that should not be touched by AI. The company's guidelines include processing personal data (relating to a natural person) and sensitive data (relating to sexual orientation, religion, or biometric data such as face imaging or voice recognition).



Another level of protection and awareness is needed

Security organizations must exercise caution and maintain **high skepticism** when interacting with AI systems. The challenge of detecting malicious AI systems will only grow as AI technology advances and becomes increasingly connected and intelligent. As AI systems improve in intelligence, they may soon be able to react dynamically to events occurring within organizations. For instance, employees may receive seemingly legitimate messages from an AI system pretending to be a support employee who has reached out due to scheduled maintenance.

This highlights the need for organizations to be **proactive in detecting and defending against malicious AI systems**. It also emphasizes the importance of educating employees on how to recognize and respond to potential social engineering attacks.

It's comforting to know that SAP has specifically called out transparency within their Guiding Principles for Artificial Intelligence. The company states, "Our systems are held to specific standards per their level of technical ability and intended usage. Their input, capabilities, intended purpose, and limitations will be communicated clearly to our customers, and we provide means for oversight and control by customers and users. They are, and will always remain, in control of the deployment of our products." These forward-thinking principles will comfort customers with concerns about embracing AI-infused technologies.

Another approach to help organizations alleviate their AI fears is to adopt a framework for ethical practices. The European Commission's Ethics Guidelines for Trustworthy AI emphasize the importance of transparency, accountability, and human oversight in developing and deploying AI systems.

AI has the potential to enhance our lives in numerous ways, but it is crucial **to use it ethically and securely**. Currently, AI is already employed across various industries to boost productivity, automate tasks, and create innovative solutions: its potential for companies is huge. As AI continues to advance, its integration into business applications like ERP systems is expected to become more sophisticated and widespread. However, ethical and privacy considerations must be meticulously managed in AI's development and implementation to prevent unintended consequences, such as bias in AI decision-making or privacy violations.

It is the responsibility of every organization that owns, uses, or provides AI-based services to ensure the training models of their AI systems are protected. This may include implementing strict policies for managing and verifying the training data used by AI systems and incorporating security measures to detect and prevent manipulation of the training models.

Let's now delve into the technical side of AI for SAP Security and explore how AI can help you improve your SAP Security posture, while focusing on the prerequisites needed for a successful implementation.

How can AI help improve your SAP Security Posture?

Let's explore **AI's role in SAP Security**, highlighting some SAP security platform challenges and the importance of system hardening against exploit chains within SAP vulnerabilities.

How do we protect IT systems against AI-generated threats, and how can AI itself support us in this case?

AI-driven SAP Security?

The SAP Security community is also seeking answers to this question. As an obvious first step, AI can support SIEM and other monitoring systems by finding critical activity patterns in the giant amount of event logs created every minute in today's SAP environments.

However, **not every critical activity is malicious**. SAP Security teams must have a good understanding of their normal state within their specific landscape, including custom development, to establish a strict regime for leveraging superuser rights and privileged user access in SAP applications. Only then can they lower the “background noise” of accepted critical events to an extent that creates a realistic chance for identifying malicious activities.

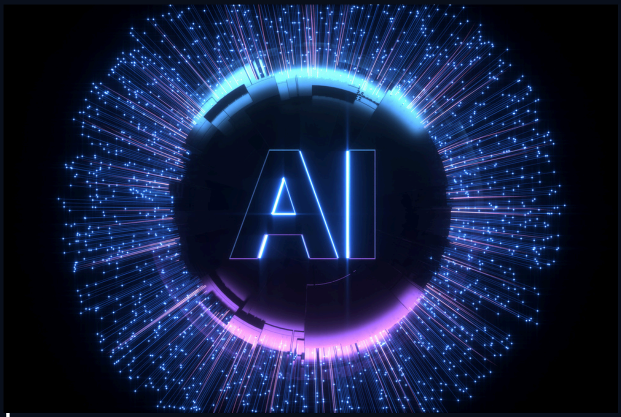
A Threat Detection solution for SAP powered by AI can be very powerful, especially for detecting cyberattacks that are chaining multiple medium or low SAP vulnerabilities. As most security remediation strategies prioritize the high and very high vulnerabilities due to resource constraints, successful attacks often exploit a chain of “leftovers”. AI can help detect these SAP Security threats, but it only can unfold its full power within a hardened SAP system and SAP Operations that embrace the principle of least user authorizations.

SAP system’s resilience is often quite low

However, we at SecurityBridge experienced a different situation when implementing our security platform for SAP customers. As our key platform modules “Threat Detection” and “Security & Compliance” are shipped with predefined security baselines and monitoring templates, we are often surprised to see how many critical alerts and findings are popping up right after initializing the event monitoring, vulnerability scan of the SAP system and custom code. As many customers are also challenged with monthly system patching, which causes red alerts in our “Patch Management” module, our SAP security experts must often diagnose quite a low resilience level of the SAP system. In such cases, even simple attack scenarios would have a good chance of being successful, or worse, remain undetected.

The combination of a low resilience level and a high amount of critical monitoring events even during normal operations, makes it almost impossible for SOC teams to respond to cyberattacks promptly. Even with the usage of an AI-based approach, the number of false positives would be too high in a system landscape with such a wide attack surface like SAP, making it a challenge to be in control of the situation. Due to the complexity of underlying technologies and the variety of customizations, **an SAP system is impossible to defend if not properly hardened**. Therefore, we recommend system hardening as a prerequisite for any AI-driven SAP Security strategy.

Prerequisites for an AI-Driven SAP Security



Part 1: Patching

An AI-driven Threat Detection approach can help identify sophisticated cyberattacks, especially those leveraging a chain of vulnerability exploits. However, while AI can point you to those issues and may automatically block certain activities or user endpoints, the SAP Security team remains responsible for responding to the attack.

Reducing the attack surface is key

Ideally, the SAP Security team is ahead of the potential threat by continuously hardening the SAP system. Therefore, reducing the attack surface of an SAP system through hardening is a prerequisite for any AI-driven SAP Security approach.
The attack surface is the sum of all possible entry points or attack vectors, where an unauthorized attacker can access a system or application to extract data or manipulate sensitive information. The smaller the attack surface, the easier it is to protect. The SAP attack surface is by nature quite large, and reducing it means implementing various best practices.

Patching helps reduce the attack surface

Among those best practices for hardening the system and reducing its attack surface, **the mitigation of known vulnerabilities** is one of the most straightforward tasks to start with. Every month, SAP releases patches for known vulnerabilities in SAP systems. Understanding their severity, their impact on your SAP landscape and their relevance to a specific system is key for efficient and short-term system patching. Therefore, SecurityBridge helps customers with a guided approach to balance between patch severity and implementation effort within the relevant patches for a specific SAP system. This allows customers to burn down their SAP patch implementation backlog efficiently and fast.

Automation and live recommendations allow efficient patching

Automating the implementation of SAP notes and patches is an additional way to increase the efficiency of this process in the customer’s organization. While this is obvious from a high-level perspective, SAP Security experts know how complex and heterogeneous the SAP patch management topic is. This makes automation very challenging.

Nevertheless, SecurityBridge is also innovating in this area of SAP Security by providing automated implementation for the majority of SAP Notes. Only patches without manual steps and are considered safe to be deployed in the target system are released through this automated procedure. SecurityBridge performs a special internal patch assessment to ensure safety in this case.

Following the principle of a guided approach, SecurityBridge helps customers with **recommendations for each vulnerability finding and SAP patch**, based on expert knowledge and feedback from our community. Every newly discovered vulnerability starts a race between attackers and defenders, who can only win by either implementing compensating controls or if available, installing the patch before the exploitation. As time is of the essence in this scenario, SecurityBridge provides live recommendation updates to all customers, so they can instantly benefit from the community feedback.

Part 2: System Hardening

How system configurations and settings impact your attack surface

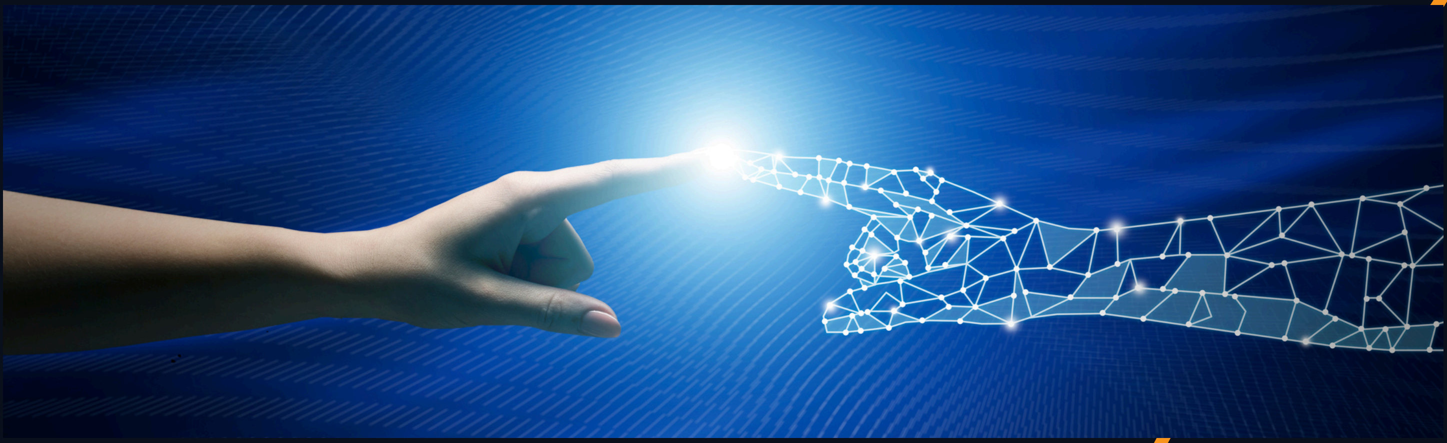
While Patch Management helps you implement code fixes for known vulnerabilities in the system code, your SAP system still has a huge number of parameters and settings that influence the behavior of the application. Quite a few of them are security-related and have a significant impact on your attack surface.

It is key for the security of your business-critical SAP systems that you harden them. This involves changing the (sometimes insecure) default settings and parameters to more secure values and configuring system logging to ensure proper forensics and capture all necessary records.

It also includes securing communication between the different systems and technical components via various APIs, like HTTP or RFC, and activating only those Internet Communication Framework (ICF) services you need. It is beneficial to harden these typical technical components responsible for communications like your SAP Router, Message Server, Web Dispatcher, and Internet Communication Manager (ICM) based on best-practice security recommendations. Do not forget to extend this security focus to other systems and components that all play an integral part in your SAP landscape like JAVA systems, SAP Business Objects, connected cloud-based systems, printers and scanners, etc.

Managing access to your SAP systems is crucial for further reducing the attack surface. Make sure you follow the principle of least privileges within user authorizations and keep the group of users with elevated privileges (especially SAP_ALL) small. Also, check the settings of the RFC destinations in your SAP landscape. Prevent someone from accessing a critical system from a less critical one through an unsecured RFC call. This safeguards against directory traversal attacks which are very dangerous in SAP environments.

These are pivotal topics to consider. Without them, no AI-based security monitoring system can protect your SAP application from being hacked. It would be a walk in the park for cybercriminals because your systems would have too many open back doors.



Follow security recommendations and automate compliance checks

You don’t need to reinvent the wheel when configuring your SAP system. **There are many configuration guidelines and baselines available**, like the SAP Security Baseline or checklists from various SAP user groups such as the German-speaking user group, DSAG. Moreover, they all have one thing in common: they are highly comprehensive. Following these guidelines also ensures the compliance of your SAP system with common security frameworks or regulations, like SOX, NIST, or KRITIS.

SAP Security experts know how cumbersome it is to get the SAP system “clean” and how tedious it is to “stay clean” as there are always changes happening in an SAP environment. Therefore, automating these Security & Compliance checks is a key success factor for SAP system hardening.

The SecurityBridge Platform helps you automate all SAP system checks needed to ensure security and compliance with all relevant security frameworks or regulations. It uses multiple baselines in parallel, including the SAP Security Baseline and the DSAG Security Guideline to ensure secure parameters across all SAP stacks, technical components, and layers. In addition, it validates user authorizations, interface configurations, and other application controls for providing administrative recommendations to further reduce the attack surface.

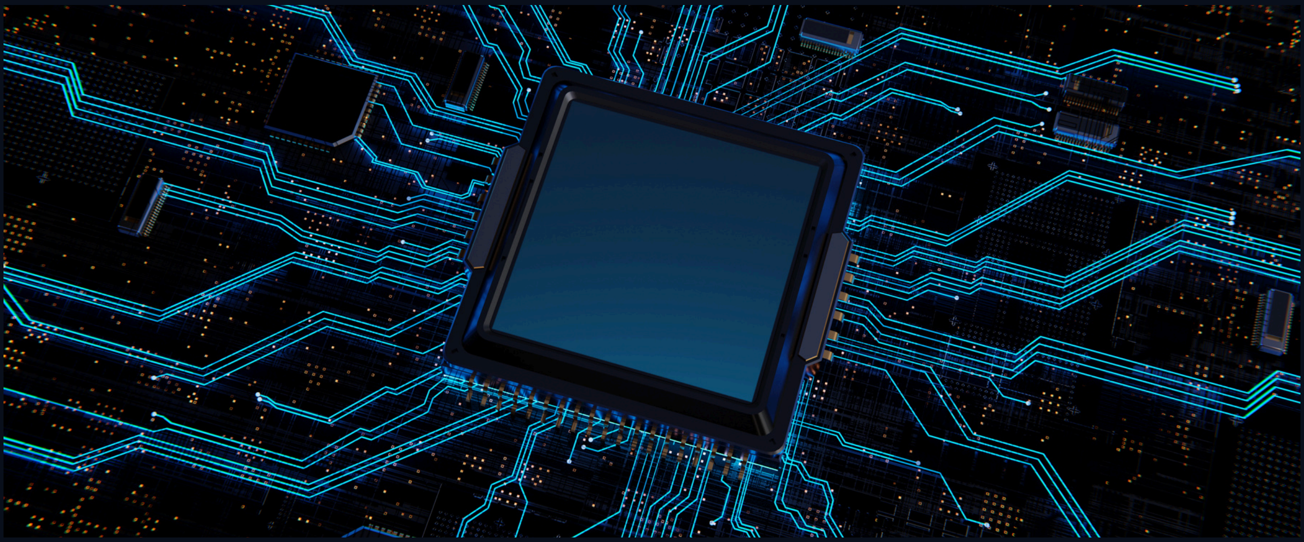
These recommendations are presented as a daily updated Security Roadmap for SAP with ranked findings based on a balance between exploitation risk and resolution complexity. Starting with the “low hanging fruits” that have a high risk but can be mitigated easily, the roadmap also provides all necessary details for decision-making and the recommended parameter values. With these, you are on the best track to harden your SAP systems and ensure their maintenance on that level moving forward. Finally, the SecurityBridge Platform provides compliance reports based on various regulations, like SOX or NIST, making the next SAP Security audit a walk in the park for you.

Part 3: Custom Code Cleansing

While Patch Management helps you to remediate known vulnerabilities in the SAP system code, your custom applications developed by your organization or externals still contain quite a lot of technical debt. Among these, many code vulnerabilities allow data breaches or provide an easy path for cyber criminals to infiltrate your SAP system.

Too often, SAP teams consider themselves to be on the safe side as most of the custom code is unused. However, even unused code increases the attack surface of the application as it can be processed anytime.
Therefore**, SAP customers are facing a large attack surface due to accumulated code vulnerabilities when scanning their custom applications for the first time**, leveraging either the SAP Code Inspector or third-party solutions like the SecurityBridge Code Vulnerability Analyzer.

Unfortunately, immediate remediation is not possible as fixing all these vulnerabilities at once will require unlimited development resources. Additionally, the testing effort required before deploying all these corrections at once in production is gigantic. Therefore, we have gathered a set of recommendations for you to consider when approaching those code vulnerabilities.



Recommendations for cleansing code vulnerabilities in SAP custom applications

Start with raising awareness for secure coding practices. It is crucial for your development team to know how to build an ABAP custom application without vulnerabilities. You don't necessarily need extensive training; the findings of the SecurityBridge Code Vulnerability Analyzer provide explanations and recommendations for secure ABAP statements, as well as aiding in categorizing the findings. Those that "must-be-fixed" are a showstopper for any code deployment into production. Findings that "can-be-fixed" give the developer the flexibility to decide based on project time constraints or application impact.

Note that such an ABAP code cleanup will be a long process. Thus, instead of a big code remediation project, you might want to start with **establishing a simple but effective security gateway within your development process**. By scanning each transport for vulnerabilities before importing it into test systems, you ensure that you are not introducing new insecure code. SecurityBridge helps your development team to write secure code by design and easily integrates with SAP Code Inspector and the ABAP Test Cockpit. It also scans every SAP transport request for code vulnerabilities before importing it into the system, keeping insecure third-party code away from your SAP environment.

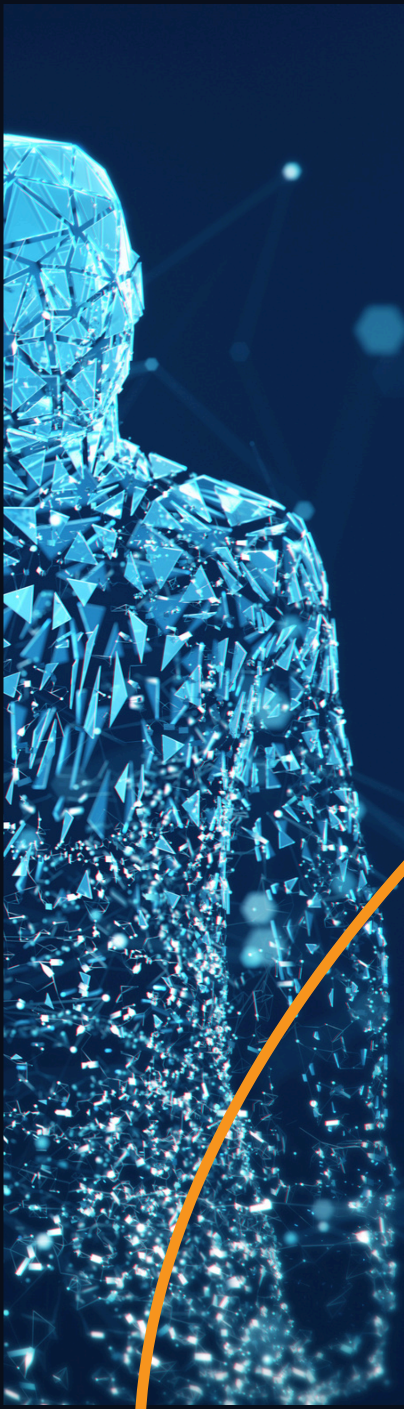
Next, you can work on **cleansing existing custom code and reduce the number of vulnerabilities in your legacy applications step by step**. Focus on the code that is used. Unused code with vulnerabilities should be ideally eliminated or commented out if you want to keep it as a reference. This ensures that it cannot be executed, consequently preventing impact on your attack surface. In the used code, look for vulnerabilities with a high exploitation risk or findings with a high severity and a big impact. Those that are easy to solve should be at the top of your backlog. Ideally, you could align your remediation work with other application changes to minimize testing effort.

These recommendations will help you improve the security rating of your code base over time while keeping new vulnerabilities away from your SAP landscape. However, if there are critical vulnerabilities in your custom code, ensure that your SAP Security Monitoring informs you when the code with critical findings is executed in your system. This happens automatically with the SecurityBridge Threat Detection, allowing SAP teams to double-check that it is intentional and not a cyberattack.

Conclusion

Integrating AI into SAP and its application in cybersecurity brings benefits and a caution flag. AI simplifies many aspects of analysis and processes, and SAP recognizes this value by implementing it across various business applications.

However, full reliance on AI without checks, balances, and transparency introduces risks and challenges. Blind trust in AI decision-making contradicts the principle of verifying and authenticating data. Organizations must balance AI's pattern recognition with a human check. The uncertainty of AI outcomes and the potential for its use in malicious attacks highlight the importance of exercising caution and skepticism when integrating AI into cybersecurity and the SAP security landscape.



As we explored, **it would be inconvenient to start an AI-based SAP Security strategy without taking care of some crucial prerequisites**, like reducing the attack surface through patching and system hardening, mitigating known vulnerabilities, and cleansing the existing custom code. SecurityBridge is always at the forefront of innovation and is currently working on an AI integration within our platform to improve existing capabilities for protecting SAP environments holistically.

To sum up, **organizations have a fundamental role to play**: leaders must carefully consider the risks and limitations of AI and implement appropriate and ethical measures to protect their employees, systems, and data. They must stay informed, train their teams, and conduct regular security audits.

Combining human scrutiny and AI applications will allow companies to manage cybersecurity risks and provide trustworthy data outcomes.

About SecurityBridge:

SecurityBridge is a unique, holistic, natively integrated SAP security platform, addressing all factors needed to detect and respond to internal and external attacks against mission-critical business applications running SAP. SecurityBridge's advanced approach to protecting SAP NetWeaver, ABAP, and S/4HANA platforms reveals exploits, and uncovers previously unknown vulnerabilities, directing and enabling remediation before any harm is done.

SECURITYBRIDGE.COM/REQUEST-DEMO

CONTACT US

Europe (Headquarters)

+49 (841) 93914840
Munchenerstr. 49
85051 Ingolstadt, Germany

United States

+1 (416) 821 0850
228 Park Ave S PMB 89765
New York, New York
10003-1502 US

Netherlands

Kraijenhoffstraat 137A
1018RG Amsterdam
Netherlands

Info@SecurityBridge.com
SecurityBridge.com

Security Bridge