**Marko Stanojević***
https://orcid.org/0009-0007-7241-5503
**Danilo Izgarević****
https://orcid.org/0009-0000-0785-3055

UDC: 005.934
005.591.6:004.89

DOI: 10.5937/MegRev2502051S
**Original scientific paper**
Received 15.08.2025.
Approved: 10.11.2025.

# INTEGRATION OF ARTIFICIAL INTELLIGENCE IN CORPORATE INFORMATION SECURITY SYSTEMS

**Abstract:** *As the digital landscape keeps evolving, corporate security systems are facing increasingly complex and ever-changing threats that often outstrip traditional defense strategies. This review explores how artificial intelligence (AI) is transforming corporate security through machine learning, anomaly detection, threat intelligence, and real-time decision-making support. By automating those tedious tasks, sorting through heaps of data, and enabling quick responses to potential threats, AI helps organizations strengthen their digital and physical security systems. This paper dives into the challenges that come with AI integration, like making sure data is reliable, algorithms are transparent, ethical issues are addressed, and governance standards are met. Through various case studies and a look at industry tools such as IBM Watson, Darktrace, and Microsoft Security Copilot, the review highlights how AI is increasingly shaping risk management, compliance, and cost efficiency. Ultimately, it emphasizes the need for strong AI governance frameworks and zero-trust architectures to ensure that implementation is both responsible and secure.*

**Keywords:** *Artificial Intelligence, Information Security, Corporate Security, Threat Detection, AI Governance*

* E-mail: stanojevic.marko799@gmail.com
* E-mail: daniloizgarevic@gmail.com

## 1. INTRODUCTION

As we experience this surge in digital growth, corporate security systems are confronted with a range of complex threats that traditional rule-based defenses often find hard to cope with. The advent of artificial intelligence (AI) in these systems has emerged as a vital innovation, promising a more proactive, flexible, and automated approach to safeguarding against the constantly changing risks we encounter.

Recent systematic reviews show that AI techniques like machine learning (ML), deep learning (DL), anomaly detection, and threat intelligence are significantly boosting organizations' capabilities to identify, prevent, detect, and respond to security incidents much faster than traditional methods.[1] For example, AI-driven intrusion detection systems and malware classifiers have proven to outperform static signature-based systems when it comes to spotting new or zero-day threats.[2]

In addition to boosting technical defenses, AI contributes to corporate security by providing decision support, automating routine tasks, and making resource allocation more efficient. By sifting through large data sets in real time, AI systems can spot hidden patterns and anomalies, allowing for timely alerts and proactive defense measures.[3]

Using AI in corporate security can definitely provide some great advantages, but it's important to recognize that there are also challenges that come along with it. These challenges encompass the risk of adversarial attacks on AI models, the necessity for high-quality data, and issues related to explainability and transparency. Moreover, organizations must set up appropriate governance mechanisms.[4] As more autonomous systems are rolled out, ethical and legal concerns like algorithmic bias, privacy implications, and accountability are becoming increasingly important.[5]

AI has the ability to assist security experts in identifying and prioritising threats in the context of safety. It can help them manage incident response, identify malware on a network instantly, and stop invasions before they happen. When AI

1 Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023): "Artificial intelligence for cybersecurity: Literature review and future research directions", *Information Fusion, 97*, 101804. DOI: 10.1016/j.inffus.2023.101804

2 Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024): "Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions", *Frontiers in Big Data*. DOI: 10.3389/fdata.2024.1497535

3 Radadiya, P., Shah, K. & Doshi, N. (2025): "Automating AI in Cybersecurity: A Comprehensive Literature Review", *Journal of Information Systems Engineering and Management, 10*(28s). DOI: 10.52783/jisem.v10i28s.4354

4 Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023): "Artificial intelligence for cybersecurity: Literature review and future research directions", *Information Fusion, 97*, 101804. DOI: 10.1016/j.inffus.2023.101804

5 Nott, C. (2025): "Organizational adaptation to generative AI in cybersecurity: A systematic review", *arXiv preprint arXiv:2506.12060*, https://arxiv.org/abs/2506.12060.

is used in physical security, access control, perimeter security systems, and remote monitoring become more responsive, potent, and efficient. AI significantly helps remote monitoring agents by identifying anomalous events, such as a particular movement at a location where there shouldn't be any movement at that moment. These agents can react more swiftly because they are able to comprehend the situation on the ground more quickly. Additionally, the AI can differentiate between human and generic movements, which lowers the number of false alarms.[6]

## 2. LITERATURE REVIEW

In terms of technology, artificial intelligence refers to the capacity of a machine to carry out tasks that, until recently, required human intelligence. The capabilities of artificial intelligence software are expected to soon surpass those of humans.[7] From improving customer and employee experiences to automating repetitive work, artificial intelligence (AI) has had a significant impact on how businesses run. AI is now changing how businesses safeguard their assets, people, and property and directing them towards a more proactive security strategy. AI has been included into the security program of nearly half (46%) of the companies surveyed by Securitas Technology. As the number of applications for AI-powered security grows, this number will only go up. There are many applications for AI in security. AI is a potent instrument that will revolutionise business security and operations, from bolstering safety and security protocols to assisting companies in reviving dormant data concealed within their security architecture.[8]

Businesses are facing challenging issues with the technology's dependability and auditability as they come under increasing pressure to incorporate AI into their processes. AI expenditures are taking up new portions of many businesses' budgets. According to a KPMG survey of business executives, 67% of them said they want to invest in cyber and data security safeguards for their AI models, indicating that they prioritise security monitoring when making budgetary decisions for generative AI. Risk and compliance were mentioned as financial priorities by 52% of respondents.[9]

6 Vogel, R. (2025): *How Artificial Intelligence empowers Security Professionals to take their service delivery to a new level*, https://www.evalink.io/blog/how-artificial-intelligence-empowers-security-professionals-to-take-their-service-delivery-to-a-new-level.

7 Baltezarević, R. (2023): "Uticaj veštačke inteligencije na globalnu ekonomiju", *Megatrend revija, 20*(3), 13–24. DOI: 10.5937/MegRev2303013B

8 Securitas (2024): *10 ways AI is transforming business security and operations*, https://www.securitas.com/en/newsroom/blog/10-ways-ai-is-transforming-business-security-and-operations/.

9 Geller, E. (2025): *AI security issues dominate corporate worries, spending*, https://www.cybersecuritydive.com/news/artificial-intelligence-security-spending-reports/751685/.

Two categories of AI security can be identified based on their particular objective: weak AI and so-called strong AI (sometimes known as "superintelligence"). Weak AI security solutions function at a comparatively low level of intelligence, whereas strong AI seeks to emulate human reasoning and behaviour in order to equal or even exceed human intellectual capacity. Their capacity to carry out activities independently and automatically is already creating amazing potential for the security firms that use them, even though they do not gain a thorough understanding of the issues to be solved. Alert management, which increases the accuracy of alert verification and lowers the quantity of false alarms, is a well-known illustration of powerful AI in security.[10]

Decision-makers frequently have to choose between two competing goals when it comes to corporate security: keeping up with changing threats and making sure that limited funds are used effectively. AI can assist in resolving these issues by: a) Automating repetitive tasks: By automating processes like risk assessments, vendor reviews, and compliance audits, managers can concentrate on handling problems and making important decisions. b) Turning data overload into insights: A lot of data is produced by security systems. AI breaks through the clutter. Teams can take preemptive measures thanks to its analysis of possible threats, risk identification, bias removal, and prioritisation of actionable insights. c) Improving cost control and resource allocation: AI forecasts risks and makes sure that resources are distributed where they will have the biggest impact by analysing historical and real-time data.[11]

AI agents created especially for the corporate security sector will allow internal teams to provide services that were previously unthinkable. By speeding up the decision-making process during disruptive occurrences, these agents will not only free up staff members to work on more strategic and sophisticated tasks, but they will also help minimise financial damage. When a security crisis happens in the not-too-distant future, AI agents will explain why it matters, forecast potential outcomes, and give the responding security team practical advice. These agents will revolutionise proactive risk management in the AI era and provide personalised real-time insights for all organisations for the first time.[12]

A number of AI-powered solutions are revolutionising how companies handle security and compliance. These tools are not merely theoretical; they are actively

[10] Vogel, R. (2025): *How Artificial Intelligence empowers Security Professionals to take their service delivery to a new level*, https://www.evalink.io/blog/how-artificial-intelligence-empowers-security-professionals-to-take-their-service-delivery-to-a-new-level.

[11] Pronect-it (2025): *How AI Can Transform Corporate Security Management: Balancing Risk and Opportunity*, https://pronect-it.com/how-ai-can-transform-security-management/.

[12] Crowley, R. (2025): *How AI Agents Will Reimagine Corporate Security Departments*, https://www.securityinfowatch.com/security-executives/article/55310445/how-ai-agents-will-reimagine-corporate-security-departments.

influencing how businesses manage risks, safeguard data, and maintain regulatory compliance. A few examples are as follows: a) Darktrace: This tool employs machine learning to automatically detect and address dangers in digital settings. b) Cylance: Proactive endpoint protection using AI-based predictive analytics. c) IBM Watson for cyber security: Determines subtle dangers that conventional systems could overlook by analysing unstructured data. d) Microsoft security copilot: Improves security operations by identifying threats, analysing security data, and suggesting actions using generative AI. For companies in the Microsoft ecosystem, this product is especially helpful because it speeds up incident response and increases security teams' overall effectiveness.[13]

To successfully integrate artificial intelligence into corporate security systems, effective governance mechanisms are vital. They provide a necessary framework for ensuring transparency, accountability, and compliance with ethical and legal standards. Organizations should really focus on weaving AI governance into their corporate, IT, and data governance structures. Corporate governance is all about setting the strategic direction, IT governance deals with the technical implementation, and data governance looks after data quality, privacy, and usage.[14] For instance, within an AI governance framework, identifying risks like algorithmic bias, data breaches, and those mysterious "black box" models is crucial. To safeguard the integrity of autonomous decisions, we need to put in place algorithm audits and oversight mechanisms, including human-in-the-loop controls.[15] By skillfully bringing these governance practices together, we can ensure that AI systems used in security settings operate not just as advanced tools, but as reliable and well-documented components that align with risk management strategies and meet the expectations of stakeholders. The impact of virtual communication on privacy protection and data processing laws is significant, particularly when it involves AI systems that generate and analyze vast amounts of sensor and communication data.[16]

To really grasp the practical impact of these advancements, we can look at a few recent case studies that offer clear examples. Take Kempower, a Finnish tech company, for instance. They effectively harnessed generative AI to quicken the process of developing their Information Security Management System (ISMS) in line with ISO 27001 standards. This tactic significantly reduced the time and effort

13 Tribe (2025): *AI in Security: Corporate Security and Compliance - Safeguarding Data and Navigating Regulations*, https://www.tribe.ai/applied-ai/ai-in-corporate-security-and-compliance.

14 Mäntymäki, M., Minkkinen, M., Birkstedt, T. & Viljanen, M. (2022): "Defining organizational AI governance", *AI Ethics, 2*, 603–609. DOI: 10.1007/s43681-022-00143-x

15 Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2022): "Governance of artificial intelligence: A risk and guideline-based integrative framework" *Government Information Quarterly, 39*(4), 101685. DOI: 10.1016/j.giq.2022.101685

16 Baltezarevic, I. & Baltezarević, R. (2020): „Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku", *Megatrend Revija*, *17(4),* 27-40. DOI: 10.5937/MegRev2004027B

involved in defining, documenting, and implementing key security controls.[17] In a similar vein, various companies in critical fields like finance and infrastructure are turning to large language models (LLMs) for tasks like threat modeling, security automation, and compliance management. However, these implementations still face ongoing challenges, including the necessity for human oversight, the need for model explainability, and the ability to withstand manipulation.[18]

In another case, an AI-powered insider risk management system utilizing behavioral analytics and dynamic risk scoring was able to cut incident response times by 47%. This system also decreased false positives and increased detection accuracy, illustrating the operational benefits of AI when it's deployed in a structured and well-governed manner.[19] Taking a wider industry view, IBM's annual security report pointed out that businesses that integrated advanced AI and automation into their security operations were able to cut the average data breach lifecycle by more than 100 days. They also saw a notable decrease in breach costs compared to those that didn't.[20]

By implementing continuous verification of all access requests throughout AI infrastructure, the zero-trust architecture removes the implicit trust assumptions that give traditional systems their security flaws. This foundation facilitates autonomous threat detection capabilities that identify ransomware and security anomalies in real-time using AI-powered identification, enabling quick responses that reduce the impact on company. Continuous monitoring offers continuous security posture assessment and threat detection that finds possible vulnerabilities before they are exploited, while policy enforcement mechanisms automatically apply data governance rules and access controls, guaranteeing consistent protection without constant manual intervention. Model protection features that protect the intellectual property in trained models and thwart adversarial attacks that might jeopardise the integrity of AI systems are also part of this all-inclusive approach. Governance and visibility tools provide comprehensive oversight of data usage and access patterns, allowing organisations to retain control over their AI initiatives.[21]

---

17 Niemeläinen, A., Waseem, M., & Mikkonen, T. (2024): "Enhancing productivity with AI during the development of an ISMS: Case Kempower", *arXiv preprint arXiv:2409.19029*, https://arxiv.org/abs/2409.19029.

18 Nott, C. (2025): "Organizational adaptation to generative AI in cybersecurity: A systematic review", *arXiv preprint arXiv:2506.12060*, https://arxiv.org/abs/2506.12060.

19 Koli, L., Kalra, S., Thakur, R., Saifi, A., & Singh, K. (2025): AI-Driven IRM: Transforming insider risk management with adaptive scoring and LLM-based threat detection, *arXiv preprint arXiv:2505.03796*. https://arxiv.org/abs/2505.03796.

20 Columbus, L. (2023): "Study reveals how AI, automation protect enterprises against data breache", *VentureBeat*, https://venturebeat.com/security/ibm-study-reveals-how-ai-automation-protect-enterprises-against-data-breaches/.

21 Giddings, M. (2025): *Enterprise-Grade Security and Governance the Trust Foundation of AI Factories*, https://www.netapp.com/blog/enterprise-ai-security-zero-trust-ai-factory/.

## 3. CONCLUSION

Integrating artificial intelligence into corporate security systems is a game-changer for how organizations protect their assets, data, and staff. With the rise of increasingly complex and widespread threats, AI stands out as a proactive, adaptable, and scalable solution that significantly improves both digital and physical security. From improving threat detection and incident response to optimizing resource management and reducing human mistakes, AI tools are revolutionizing our security landscape.

While welcoming AI into the world of security opens up some thrilling possibilities, it also presents a number of challenges we need to tackle. We can't overlook important issues such as data quality, transparency in models, algorithmic bias, and governance. It's essential for organizations to build governance frameworks that are not only efficient but also adhere to legal standards and ethical practices, all while supporting their operational goals. For AI systems to function both safely and effectively, it's vital to integrate essential elements like zero-trust architectures, constant monitoring, and the involvement of humans in the process.

In the future, research needs to hone in on establishing standardized frameworks for AI governance within the security sector. We need to work on making complex models more understandable and investigate how AI interacts with emerging technologies like quantum computing and blockchain. As the corporate threat landscape evolves, collaboration among technologists, policymakers, and security professionals will be key to ensuring that AI is a source of resilience rather than risk. By taking on the opportunities and responsibilities of AI, organizations can build security systems that are intelligent, ethical, and equipped to face the challenges that lie ahead.

## Literature


- Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024): "Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions", *Frontiers in Big Data*. DOI: 10.3389/fdata.2024.1497535
- Baltezarevic, I. & Baltezarević, R. (2020): „Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku", *Megatrend Revija*, *17(4),* 27-40. DOI: 10.5937/MegRev2004027B
- Baltezarević, R. (2023): "Uticaj veštačke inteligencije na globalnu ekonomiju", *Megatrend revija, 20*(3), 13–24. DOI: 10.5937/MegRev2303013B
- Columbus, L. (2023): "Study reveals how AI, automation protect enterprises against data breaches", *VentureBeat*, https://venturebeat.com/security/

ibm-study-reveals-how-ai-automation-protect-enterprises-against-data-breaches/.
- Crowley,R.(2025):*HowAIAgentsWillReimagineCorporateSecurityDepartments*, https://www.securityinfowatch.com/security-executives/article/55310445/how-ai-agents-will-reimagine-corporate-security-departments.
- Geller, E. (2025): *AI security issues dominate corporate worries, spending*, https://www.cybersecuritydive.com/news/artificial-intelligence-security-spending-reports/751685/.
- Giddings, M. (2025): *Enterprise-Grade Security and Governance The Trust Foundation of AI Factories*, https://www.netapp.com/blog/enterprise-ai-security-zero-trust-ai-factory/.
- Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023): "Artificial intelligence for cybersecurity: Literature review and future research directions", *Information Fusion, 97*, 101804. DOI: 10.1016/j.inffus.2023.101804
- Koli, L., Kalra, S., Thakur, R., Saifi, A., & Singh, K. (2025): "AI-Driven IRM: Transforming insider risk management with adaptive scoring and LLM-based threat detection", *arXiv preprint arXiv:2505.03796*, https://arxiv.org/abs/2505.03796.
- Mäntymäki, M., Minkkinen, M., Birkstedt, T. & Viljanen, M. (2022): "Defining organizational AI governance", *AI Ethics, 2*, 603–609. DOI: 10.1007/s43681-022-00143-x
- Niemeläinen, A., Waseem, M., & Mikkonen, T. (2024): "Enhancing productivity with AI during the development of an ISMS: Case Kempower", *arXiv preprint arXiv:2409.19029*, https://arxiv.org/abs/2409.19029.
- Nott, C. (2025): "Organizational adaptation to generative AI in cybersecurity: A systematic review", *arXiv preprint arXiv:2506.12060*, https://arxiv.org/abs/2506.12060.
- Pronect-it (2025): *How AI Can Transform Corporate Security Management: Balancing Risk and Opportunity*, https://pronect-it.com/how-ai-can-transform-security-management/.
- Radadiya, P., Shah, K. & Doshi, N. (2025): "Automating AI in Cybersecurity: A Comprehensive Literature Review", *Journal of Information Systems Engineering and Management, 10*(28s). DOI: 10.52783/jisem.v10i28s.4354
- Securitas (2024): *10 ways AI is transforming business security and operations*, https://www.securitas.com/en/newsroom/blog/10-ways-ai-is-transforming-business-security-and-operations/.
- Tribe (2025): *AI in Security: Corporate Security and Compliance - Safeguarding Data and Navigating Regulations*, https://www.tribe.ai/applied-ai/ai-in-corporate-security-and-compliance.

- Vogel, R. (2025): *How Artificial Intelligence empowers Security Professionals to take their service delivery to a new level*, https://www.evalink.io/blog/how-artificial-intelligence-empowers-security-professionals-to-take-their-service-delivery-to-a-new-level.
- Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2022): "Governance of artificial intelligence: A risk and guideline-based integrative framework", *Government Information Quarterly, 39*(4), 101685. DOI: 10.1016/j.giq.2022.101685

**Marko Stanojević**
**Danilo Izgarević**

**Originalni naučni rad**
Primljen 15.08.2025.
Odobren 10.11.2025.

# INTEGRACIJA VEŠTAČKE INTELIGENCIJE U SISTEME KORPORATIVNE BEZBEDNOSTI

**Sažetak:** *Kako se digitalni pejzaž stalno razvija, korporativni bezbednosni sistemi se suočavaju sa sve složenijim i stalno promenljivim pretnjama koje često nadmašuju tradicionalne odbrambene strategije. Ovaj pregledni rad istražuje kako veštačka inteligencija (AI) transformiše korporativnu bezbednost kroz mašinsko učenje, otkrivanje anomalija, obaveštajne podatke o pretnjama i podršku u donošenju odluka u realnom vremenu. Automatizacijom tih zamornih zadataka, sortiranjem gomila podataka i omogućavanjem brzih odgovora na potencijalne pretnje, AI pomaže organizacijama da ojačaju svoje digitalne i fizičke bezbednosne sisteme. Ovaj rad se bavi izazovima koji dolaze sa integracijom AI, kao što je osiguravanje da su podaci pouzdani, algoritmi transparentni, da se rešavaju etička pitanja i da se ispunjavaju standardi upravljanja. Kroz različite studije slučaja i pogled na industrijske alate kao što su IBM Watson, Darktrace i Microsoft Security Copilot, rad ističe kako AI sve više oblikuje upravljanje rizicima, usklađenost i efikasnost troškova. Na kraju krajeva, naglašava potrebu za jakim okvirima za upravljanje AI i arhitekturama nultog poverenja kako bi se osiguralo da je implementacija i odgovorna i bezbedna.*

**Ključne reči:** *Veštačka inteligencija, Korporativna bezbednost, Otkrivanje pretnji, Upravljanje veštačkom inteligencijom*