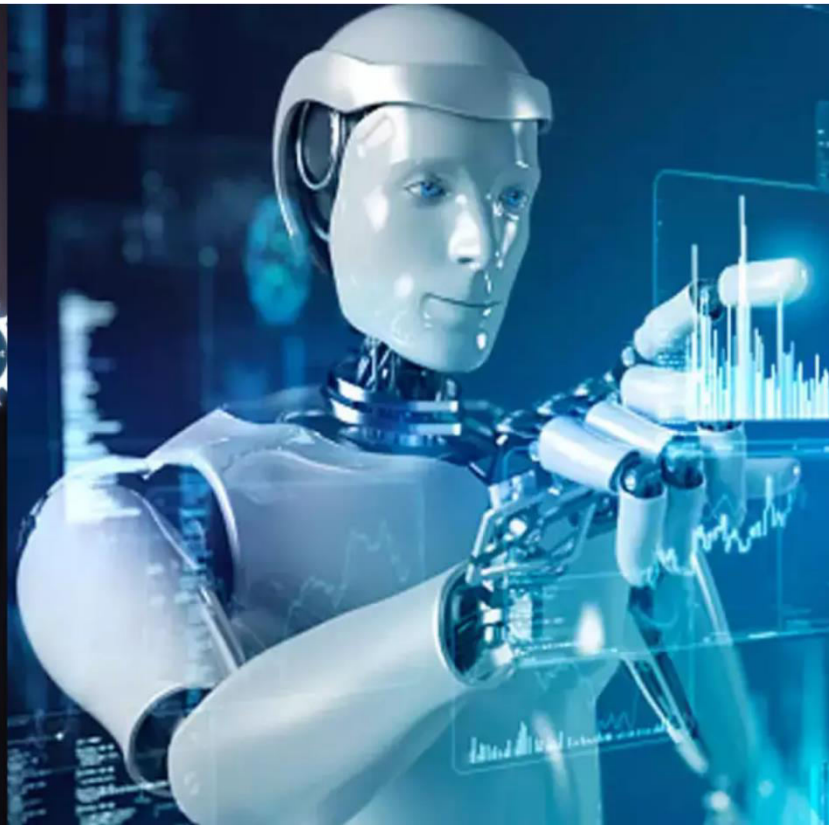
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.524

Volume 14, Issue 1, January 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401103|

CrowdStrike's Effect on Database Security

Sudheer Kolla

Unisoft Technology Inc, Aubrey, Texas, USA

ABSTRACT: The increasing use of cloud-native and hybrid databases has emerged as the current security threats have intensified the need for proper security measures. Cybersecurity firm CrowdStrike has revolutionized the database security through real-time monitoring, artificial intelligence, and the Zero Trust model. These enhance database robustness by detecting suspicious queries, unauthorized access and even internal threats. Yet, the 2024 CrowdStrike outage demonstrated the problems of over-reliance on cloud security solutions and showed that there are deep-seated issues with the overall security model. This paper evaluates CrowdStrike's contribution to the development of database security, discusses the consequences of the AI and Zero Trust concept, and analyzes the cybersecurity issues that the 2024 outage revealed. It also provides suggestions on how to improve the database security, specifically in regard to the hybrid security models, AI-based cyber defense, and policy directions for further cybersecurity development.

KEYWORDS: Database security, AI-driven cybersecurity, Zero Trust, CrowdStrike outage, cyber resilience

I. INTRODUCTION

The advent of cloud-native and hybrid databases has led to a new generation of threats and hence, there is a need to protect such systems from such threats. The attacks on the databases have become more advanced than before through the use of zero-day exploits, SQL injections, and privilege escalation [1]. These attacks target the accuracy, confidentiality and accessibility of data and hence requires constant monitoring and threat detection that is central to modern security models. There is a shift towards AI-based security models to enhance the database security and minimize the threat of attacks [2].

These challenges are well addressed by CrowdStrike, a cybersecurity firm that uses artificial intelligence, machine learning, and behavioral analysis in its Falcon platform to identify and mitigate threats [3]. The company's Zero Trust security model means that there is constant verification and only the necessary level of access is granted, which helps to reduce the risks of the database [4]. However, the 2024 CrowdStrike outage was a great concern when it comes to the impact of a centralized cloud security solution, which may point to a systemic issue [5].

This paper aims at discussing the following aspects of CrowdStrike: AI-based anomaly detection, Zero Trust, and the effects of the 2024 incident on the improvement of cybersecurity measures. It also discusses possible further developments that can be made in the database security through the use of the hybrid security models, policy and the use of artificial intelligence in the detection and prevention of the threats. The study also brings out the fact that while developing cybersecurity solutions, there is need to ensure that the solutions are reliable and that there is redundancy in the security architecture. Thus, by identifying the strengths and weaknesses of CrowdStrike's approach, this research brings to the discussion about the enhancement of database security from new and sophisticated threats.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401103|

II. CYBERSECURITY RISKS TO DATABASES

For a while, cybersecurity has evolved as an advancing issue for many contemporary organizations. This is an issue triggered by numerous factors, as presented in Figure 1.

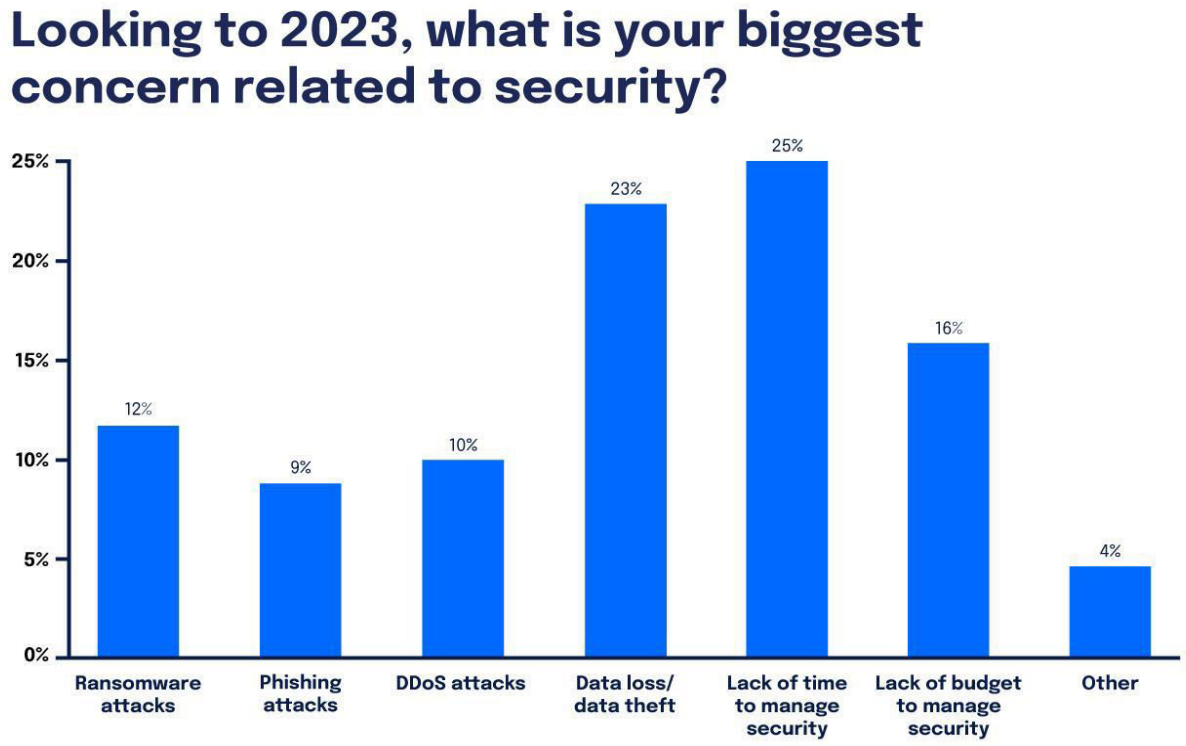


Figure 1: Some of the major contributors to cybersecurity trigger

Organizational databases have become major attractions for hackers because they contain important data for any organization. They use advanced methods such as SQL injections, brute-force attacks, and privilege escalation to take advantage of the vulnerabilities that exist in the database access control and query processing [1]. The emergence of zero-day vulnerabilities makes it even more challenging to counter cyber threats since the attackers exploit the security gaps that have not been identified and patched yet [2]. These risks are further amplified by the shift to cloud-based database management as it creates new issues like multi-tenant architectures, misconfigurations, and API security [6]. As a result, more organizations are seeking help from cybersecurity companies such as CrowdStrike for constant protection and threat intelligence to protect their databases from such emerging risks [5].

Cybersecurity has benefited from artificial intelligence since it provides early identification of threats. Artificial intelligence-based security systems monitor queries, usage patterns, and other activity and behavior that can be indicative of a security threat and then alert the system before the threat can develop into a large-scale security threat [1]. Machine learning models improve security by identifying unauthorized access and other threats like data leakage, privilege escalation, and movement within a network [2]. However, there are also certain challenges concerning the use of AI in cybersecurity like the problem of false positives, AI would learn from its adversaries, and the susceptibility of the AI models since new threats may be developed hence requiring the models to be updated [7]. These threats suggest that there is need to integrate AI with other methodologies which include MFA as well as RBAC to come up with the best database security model [6].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401103|

Falcon is an artificial intelligence aimed at processing security threats occurring in databases in real time at CrowdStrike. Thus, the system can bank on the patterns of query execution, privileges granted, and other information changes that are indicative of cyber-attack [1]. Behavioral analytics enhances security by analyzing and interferes such actions as, malicious scripts, unauthorized SQL queries, and insider threats before they escalate to full blown breaches [2]. Further, the Zero Trust model adopted in the platform means that every request to the database is constantly checked for approval, thus minimizing the risks that are brought about by compromised credentials or escalation of privilege [4]. However, the 2024 outage showed how dangerous it can be to rely on a single security provider and how important it is to have a diverse security structure to enhance security and reduce the risks in the security structures [5].

III. THE 2024 CROWDSTRIKE OUTAGE: IMPLICATIONS FOR CYBERSECURITY

On July 19, 2024, a new update by CrowdStrike impacted millions of devices and led to system failures in the finance, healthcare, and government databases [4]. This disruption exposed serious flaws in the centralized model of cloud security where companies are left open to cyber risks for a while due to lack of continuous security monitoring [5]. The incident raised issues of vendor lock in and the structural vulnerabilities of cloud-based security solutions while using a single vendor provider [6].

It had several direct effects on the security of the databases. First, the lack of real-time monitoring means that organizations could not detect or respond to threats during the period of time when the system was down, thus making it easier for potential attackers to breach security [6]. Second, the absence of automated threat identification increased the exposure of databases to cybercriminals [5]. Lastly, the disruption brought out the importance of business continuity planning, as organizations that relied on CrowdStrike's security solutions had to scramble for other means of managing risks due to the lack of functional security systems [4].

This event was quite informative and helped me to consolidate knowledge about the protection of databases and the prevention of cyber threats. It is crucial for organizations to implement a combination of security measures to avoid being caught unprepared in case their vendors fail; they should have backup security strategies in place [7, 8]. Using automatic mechanisms to roll back security updates may go a long way in avoiding the disruptions, while offering a quick way of recovering security systems in the event of software failures [6]. Furthermore, it is possible to reduce the likelihood of large-scale outages of database security by using a multi-level security strategy that includes multiple providers and on-premise security components used in conjunction with the cloud [5].

The case of CrowdStrike is a good example of how database should be protected from cyber threats where the redundancy and multi-layered security model should be implemented [9]. In this case, the analysis of the causes and effects of the incident can help organizations improve their cybersecurity measures and become more prepared for the challenges of the modern world [4].

IV. CHALLENGES AND LIMITATIONS OF CROWDSTRIKE'S SECURITY MODEL

Despite the improvements that CrowdStrike has put in place to improve the security of databases, the security model of the company has some drawbacks and limitations that need to be rectified. One of the issues is that organizations rely heavily on cloud security solutions and may have a single weak link if they are fully dependent on cloud providers [10]. The 2024 outage was a clear indication that the centralized security models are dangerous since organizations that relied only on CrowdStrike were left with no way of monitoring or protecting their databases for several weeks [5]. This incident proved that although cloud security solutions are elastic and self-service, they are not immune to systematic risks, especially when the companies have no on-premises backup security to prevent possible failures (Tripathi, 2024).

The problem with CrowdStrike's security model is that the use of artificial intelligence in security is not a simple matter. While AI is extensively used in the identification of the anomalies and protection against cyber threats, it is not without its drawbacks. It was ascertained that AI-based security systems tend to produce false alarms, which in turn require intervention that may be unwarranted and thus interfere with normal database operations [1]. Moreover, AI-based systems are susceptible to adversarial attacks where the attackers feed the machine learning models with wrong information to get past the security measures [2]. This requires constant improvement and training of the AI algorithms

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401103|

to adapt to the new forms and types of attacks, which creates operational challenges for AI-based cybersecurity solutions [7].

Other factors that affect organizations that use CrowdStrike's security solutions include data sovereignty and compliance concerns. There are many legislations in different countries that prohibit the transfer of data to other countries and insist on data residency [6]. Thus, CrowdStrike, as a cloud-based security provider, may not be in compliance with data protection laws in the regulated sectors. Challenges that may arise when organizations in these industries use CrowdStrike's services may force them to add extra layers of compliance or seek other solutions that are more suitable for the specific regional regulations [5].

Another weakness of CrowdStrike is that this solution requires regular updates and is configured to work with cloud services for the best performance. On one hand, automated updates assist in making sure that organizations get the latest security patches; on the other hand, they pose some risks, as seen in the 2024 software update failure [4]. The organization's which rely on the real-time security updates may be affected as these updates can create compatibility problems or lead to system failures. This underlines the importance of having proper rollback strategies as well as testing of security patches before implementation to prevent negative impacts on database security [6].

These challenges have revealed the need for organizations to have a hybrid cloud and on-premise security solution in place. Despite the robust database security offered by CrowdStrike with its AI security and Zero Trust enforcement, it is necessary to introduce backup and failover solutions to mitigate risks of potential cyber threats. Thus, the mentioned limitations can be managed to maximize the advantages of using CrowdStrike security solutions while minimizing the risks.

V. FUTURE DIRECTIONS FOR CYBERSECURITY IN DATABASE PROTECTION

The future of database cybersecurity needs to take lessons from the recent events such as CrowdStrike outage to enhance security architecture. A major advancement is the shift to using hybrid security models that integrate cloud security solutions with the local security systems [11]. Despite the advancement in cloud security through automation and AI as provided by CrowdStrike, organizations still require contingency measures for security of their databases in the event of failures by the providers [5]. To minimize reliance on a single provider, various organizations can adopt hybrid security frameworks to enhance the continuous security of databases [6].

Other areas that will be crucial for enhancing the database security include development of artificial intelligence. The current AI-based cybersecurity solutions have to be developed to include learning models to improve on their effectiveness in identifying new threats [1]. This include enhancing the ability of anomaly detection to reduce false positive and false negative and combining the use of AI with behavioral analysis for better threat detection [2]. Also, organizations should ensure that more money is spent on the research and development of explainability of machine learning to ensure that the AI makes decisions on security issues [7].

Another important factor that will define the future of database protection is the compliance with the regulatory requirements and cybersecurity measures. The government and industries should set standards that need to be followed by cloud security providers in areas like security patch management, data sovereignty, and threat intelligence sharing [4]. Adopting standard security frameworks will go a long way in avoiding the problems associated with lock-in and improve the security and interoperability of cybersecurity [6]. In addition, regulatory authorities should engage cybersecurity companies to help in the formulation of strategies that would help organizations deal with such threats since they will be provided with the best solutions [5].

Another area that requires enhancement is the construction of more robust cybersecurity architectures that have backup and failover procedures. There is the need for organizations to develop sound incident handling processes that include the ability to roll back security updates that may cause further harm to the databases [6]. Furthermore, it is possible to increase the security by using distributed security models where security is implemented on different levels of an organization's IT infrastructure to avoid failures at one level [4]. In this way, the organizations can strengthen their resilience to the cyber threats while ensuring the constant protection of the database.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401103|

As threats to databases become more and more complex, it is now necessary to implement an effective security strategy that includes artificial intelligence, hybrid security architecture and models, compliance with legal requirements, and sophisticated incident handling procedures. Through these innovations, organizations can establish a strong cybersecurity environment that can effectively counter the emerging and more complex and persistent cyber threats to databases.

VI. CONCLUSION

The threats that are being posed to databases are ever evolving at a very fast pace and this calls for the constant development of new security measures that can be put in place to counter these threats. AI threat detection, Zero Trust, and real-time monitoring have been some of the major contributions made by CrowdStrike in enhancing database security. However, the recent CrowdStrike incident in 2024 was a wakeup call to organizations to diversify their cloud security solutions and have multiple layers of security in their cybersecurity strategy. Organizations need to employ multilayered security measures that involve both cloud and traditional security measures in order to have constant protection of the database even during provider failure.

Despite the significant role of artificial intelligence in contemporary cybersecurity, organizations need to optimize the AI models to minimize false positives, increase the ability to detect anomalies, and increase the transparency of security decisions. Also, there is a need to enhance the regulatory measures to meet the requirements of data sovereignty and to promote cybersecurity readiness. Incorporating multiple layers of security to the database, developing effective response plans, and integrating AI in threat identification are some of the ways that would help organizations prevent new threats to their databases and reduce the damage that could be caused by a cyber-security breach.

Thus, the future of database security will depend on the ability to innovate while at the same time strengthening the defenses. Businesses need to be on the defensive and work on their strategies on a daily basis to adapt to the ever-changing threat environment. Therefore, the implementation of AI security solutions together with the hybrid frameworks and compliance with the requirements of the legislation will help to enhance the security measures and prepare the companies for the further confrontation of the digital threats.

REFERENCES

[1] L. Y. Por, Z. Dai, S. J. Leem, Y. Chen, J. Yang, F. Binbeshr, K. Y. Phan and C. S. Ku, "A Systematic Literature Review on AI-Based Methods and Challenges in Detecting Zero-Day Attacks," IEEE Access, vol. 12, 2024.
[2] I. Naseer, "The crowdstrike incident: Analysis and unveiling the intricacies of modern cybersecurity breaches," World Journal of Advanced Engineering Technology and Services, vol. 13, no. 01, p. 728–733, 2024.
[3] P. Banerjee, "CrowdStrike Cyber Incident vs. Past Major Cyber Incidents: Analysis and Solutions," International Journal for Multidisciplinary Research (IJFMR), vol. 6, no. 4, 2024.
[4] P. Tripathi, "The CrowdStrike debacle: What it means for cybersecurity and software supply chains," orfonline.org, 2024. [Online]. Available: https://www.orfonline.org/expert-speak/the-crowdstrike-debacle-what-it-means-for-cybersecurity-and-software-supply-chains. [Accessed 31 June 2024].
[5] A. S. George, "When Trust Fails: Examining Systemic Risk in the Digital Economy from the 2024 CrowdStrike Outage," Partners Universal Multidisciplinary Research Journal (PUMRJ), vol. 01, no. 02, pp. 134-152, 2024.
[6] P. Swire, D. Kennedy-Mayo, D. Bagley, S. Krasser, A. Modak and C. Bausewein, "Risks to cybersecurity from data localization, organized by techniques, tactics and procedures," Journal of Cyber Policy, vol. 9, no. 1, pp. 20-51, 2024.
[7] Y. A. Abdelkarim, "Exploring the Preventive Contribution of Data Localisation Against Information Technology Outages: The CrowdStrike Case," Journal of Research, Innovation, and Technologies, vol. III, no. 2(6), pp. 95-107, 2024.
[8] N. R. Kotha, "Analyzing the 2024 CrowdStrike Outage: Implications for SaaS-Dependent Cybersecurity Architectures," International Journal for Research in Applied Science & Engineering Technology, vol. 12, no. XI, pp. 2156-2161, 2024.
[9] H. Li, W. J. Kettinger and S. Yoo, "Analysis of the CrowdStrike Software Update Failure," Journal of Management Information Systems, vol. 41, no. 1, pp. 206-235, 2024.
[10] J. Tilbury and S. Flowerday, "Humans and Automation: Augmenting Security Operation Centers," JCP, vol. 4, no. 3, pp. 388-409, 2024.
[11] C. Mavani, H. K. Mistry, R. Patel and A. Goswami, "The Role of Cybersecurity in Protecting Intellectual Property," International JOurnal on Recent and Innovation Trends in COmputing and Communication, vol. 12, no. 2, pp. 529-538, 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details