Netwoven

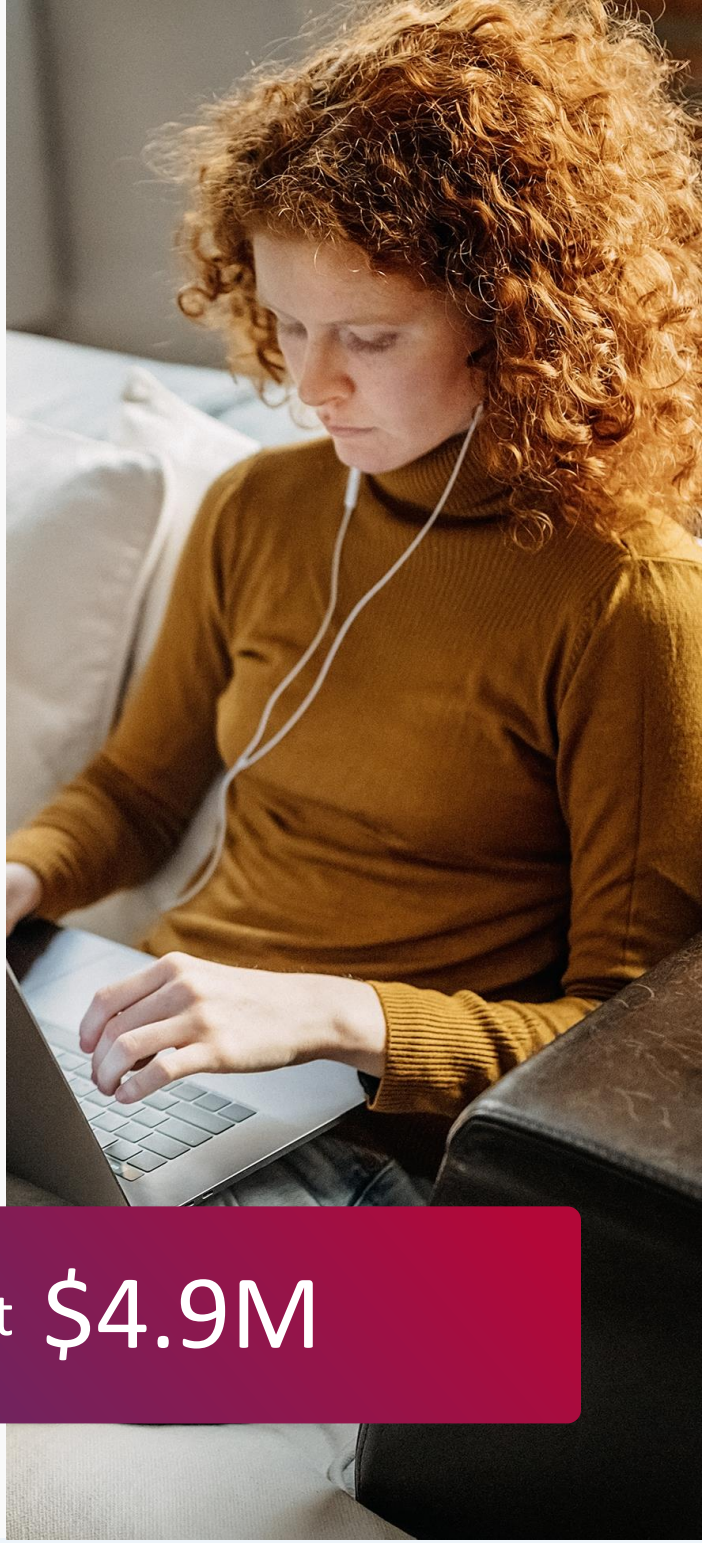
eBook

Secure Your Data in the AI Era: A Comprehensive Guide for Modern Businesses

Overview

Data security has changed significantly in the modern AI world. It is full of challenges and opportunities. In this new world of AI, organizations not only have to revamp their existing data security rules but also must create new rules to protect data that trains and operates the AI models. The impact of not having a data security strategy can be catastrophic. Here's a summary of some of the impacts:

- Financial Loss
- Reduced AI Productivity
- Inaccurate AI Models
- Compliance Risks
- Inefficient Resource Utilization
- Missed Business Opportunities
- Customer Dissatisfaction
- Increased Security Vulnerabilities



An average data breach costs about $4.9M

Source: IBM

Data Security and AI Challenges

In this eBook, Netwoven security experts discuss the following top data security challenges that organizations face:

1. Data Encryption & Masking
2. Network Segmentation
3. Data Privacy
4. Access Control
5. Secure Data Pipelines
6. Backup and Disaster Recovery
7. Vendor Contracts
8. Logging and Monitoring Capabilities
9. Data Governance
10. Future-Proofing Data Security for Advanced AI

1 Data Encryption & Masking

Organizations should ensure that appropriate encryption is in place for data at rest and in-transit. They should also adopt strong encryption algorithms and key management best practices.

Organizations should also mask sensitive information to be able to retain and share the data across systems and databases while minimizing security risks.

Use static data masking to protect sensitive data when it is moved from the production environment for the purpose of research, troubleshooting, analytics, and reporting.

Use dynamic data masking to mask data in real time for production environments. It occurs in real-time in response to user requests. Authorized users can view the original, unaltered data, and unauthorized users see masked data values.

Read the Case Study

2 Network Segmentation

Organizations should isolate AI systems and sensitive data on separate network segments.

Segregation of data and users will minimize cross-tenant attacks. They should also use firewalls & intrusion detection/prevention systems (IDS/IPS).

3 Data Privacy

Organizations should apply different techniques like k-anonymity, federated learning, or differential privacy to protect individual privacy. Organizations should also adopt the practice of data minimization by collecting and using only necessary data for any application. Often, auditing of access control is overlooked which should be part of the process.

Organizations should also enforce data retention and deletion more rigorously. This is not a new concept; however, it is more important than ever to ensure that old data is not left behind for AI systems to pick up and expose.

4 Access Control

Organizations should follow the same rules of access control to ensure that only authorized personnel can access sensitive data and AI models. Multi-factor authentication should also be in place along with Role Based Access Control (RBAC).

5 Secure Data Pipelines

Organizations should implement data validation and sanitization at ingestion points. They should also use secure data transfer protocols.

6 Backup and Disaster Recovery

Organizations should update their backup and recovery processes to accommodate AI models and put proper security in place so AI models do not pickup content from saved data.

7 Vendor Contracts

Since AI systems work with your data, it is important for organizations to update their contracts with AI vendors, suppliers, and customers regarding the use of their data in the AI models of the respective parties

72% **In 2023, data compromises increased by 72% compared to the previous year**

Source: securitymagazine

8 Logging and Monitoring Capabilities

Dashboards need to be enhanced to improve logging and monitoring capabilities to expose AI threats on enterprise data. Here are some metrics to consider when assessing the effectiveness of AI in enhancing your security posture:

- Number of AI Security Alerts
- Investigation Time
- False Positives
- Dwell Time
- Cost of a Security Breach
- SOC Analyst Productivity
- Detection and Response Time
- Compliance Metrics
- User Behavior Analytics

9 Data Governance

If you haven't put a data governance framework in place, now is the time. Doing so will enable you to effectively manage data classification, lifecycle, and policies.

70%

Organizations that conduct regular security training have reported up to a 70% reduction in staff-related security incidents.

Source: keepnetlabs

Watch Data Governance Webinar

10 Future-Proofing Data Security for Advanced AI

Organizations should prepare for quantum computing and its impact on data security. AI has accelerated the threat with quantum computing. Read Harvest Now Decrypt Later (HLDL) which provides more details on the challenges and recommendations.

Discover Real Success Stories

A leading multi-billion-dollar automotive conglomerate develops a custom AI Chatbot solution to increase productivity securely for its associates and contractors.

Read the Case Study

Find out more about the potential of AI within the Microsoft 365 suite at your workplace.

Learn More

Read the CISO overview guide on securing your organization in the world of AI.

Read More

Download the CISO Guide on AI and Security!

Conclusion

As we navigate the AI era, data security has become more critical and complex than ever before. The integration of AI technologies into our business processes and systems presents both unprecedented opportunities and significant challenges for data protection.

Key takeaways from this guide include:

1. The need for robust data encryption and network segmentation to protect sensitive information.
2. The importance of implementing strong data privacy measures, including techniques like k-anonymity and federated learning.
3. The critical role of access control and secure data pipelines in maintaining data integrity.
4. The necessity of updating backup and disaster recovery processes to account for AI models.
5. The value of comprehensive data governance frameworks and employee training programs.
6. The importance of future-proofing data security strategies, particularly in light of emerging technologies like quantum computing.

Organizations must adapt their data security practices to meet the evolving landscape of AI-driven threats and opportunities. This involves not only implementing technical safeguards but also fostering a culture of data security awareness throughout the organization.

Remember, data security in the AI era is not a one-time effort but an ongoing process of adaptation, vigilance, and continuous improvement. By following the guidelines outlined in this document and staying committed to data security best practices, organizations can confidently navigate the challenges and opportunities of the AI-driven future.

Netwoven

Why Netwoven?

Netwoven is a full-service security provider. As a member of Microsoft's Intelligent Security Association (MISA) and a Microsoft Solutions Partner specializing in security, our services include:

- Advisory Services
- Deployment Services
- Solution Development Services
- Migration Services
- Managed Services

Microsoft Solutions Partner
Security

Specialist
Identity and Access Management
Information Protection and Governance

Microsoft Solutions Partner
Microsoft Cloud

Microsoft Intelligent Security Association
Microsoft

"The client has taken a comprehensive approach to protecting sensitive information both inside and outside the organization while ensuring there was no impact on collaboration. Netwoven's extensive technical expertise and willingness to work with Microsoft's product engineering combined with their unique approach to designing solutions with a business-centric view allowed them to make the best use of Microsoft's offerings to meet the company's information protection needs. "

Enrique Saggese

Principal Program Manager, Microsoft

Next Steps

Click **here** to learn more about Netwoven security and other services. Feel free to book a time **here** to discuss your security priorities.

+1 877 638 9683

info@netwoven.com

netwoven.com

About Us

Netwoven

We shepherd organizations safely through the cloud transformation journey by unravelling complex business problems.

By partnering with us, our clients securely collaborate globally, improve business operations, build new products and solutions with deeper insights, and reduce cyber security risks.