AI and Your Security Requirements

Artificial Intelligence can deliver a lot of opportunities to businesses, but it also poses unique challenges and risks. Understanding the security implications of AI-enabled platforms plays a central role in your ability to use the technology effectively to build a competitive advantage.

1. DATA PRIVACY AND PROTECTION

Data used by AI should be encrypted and anonymized to the fullest extent possible to protect user privacy and data integrity and guard against unauthorized access.

2. MODEL INTEGRITY

Trust but verify – practices such as frequent system checks, layered infrastructure security, ongoing feedback and behavior analysis ensure any AI system is running correctly and has not been compromised or corrupted.

3. ACCESS CONTROL

Multi-factor authentication and role-based access restrict access to AI systems, ensuring only the people with the right credentials can interact with critical components.

4. TRANSPARENCY AND AUDITING

To ensure compliance with regulations and industry standards, everything from AI decisions to the platform itself should be auditable, thereby satisfying compliance demands and fostering trust with stakeholders.

5. SECURITY AUDITS

In order to identify and remedy any potential vulnerabilities within the system, periodic security assessments are essential.

6. INCIDENT RESPONSE PLAN

Problems are a matter of when, not if. Developing and maintaining an AI-specific response plan can go a long way in addressing adverse events, minimizing risk and restoring normal operations.

7. EMPLOYEE TRAINING

Human-error is the leading cause of IT security incidents. Regular staff training on security best practices that include AI-specific guidance help team members understand their role in maintaining security.

vertikal6
TECHNOLOGY. ELEVATED.

Not sure where to start? Vertikal6 experts can help you lay out a winning AI gameplan. Contact us at [email address] or call [phone number] to schedule a complimentary strategy session.