

# AI IN ENHANCING CYBERSECURITY DEFENSES

AI technologies bring the potential to transform cybersecurity by adding a level of automation to threat detection, response, and recovery. This factsheet explores how AI can enhance cybersecurity defenses while helping to avoid the associated risks.



## BENEFITS

- Automates threat detection and response.
- Capacity to analyze vast datasets for subtle anomalies.
- Enhances incident response and recovery processes.



## RISKS

- Potential for AI-generated vulnerabilities.
- Over-reliance on automated systems.
- Challenges in securing AI models and data.

### Tips for Enhancing Cybersecurity Defenses with AI



#### Automate Routine Security Processes

AI-driven technologies are well suited to automate routine and complex security tasks. This can increase efficiency while allowing security teams to focus on strategic planning and incident response.



#### Advanced Threat Detection

Leverage AI’s capacity to process and analyze vast datasets to identify emerging threats more swiftly than traditional methods.



#### Dynamic Risk Management

AI tools can deliver real-time risk assessment. Providing insights that enable organizations to adapt their security strategies quickly.



#### Continuous Learning

Maintain continuous learning to keep security teams updated on the latest AI advancements and threats. Regular training sessions and workshops are essential.



#### Collaborative Analysis

Promote a collaborative approach to AI use in cybersecurity. Encourage teams to question, interpret, and validate AI-generated data and decisions.



#### Ethical Use of AI

Ensure AI tools are used ethically in cybersecurity. Maintain transparency in AI processes and involve human oversight in decision-making.