

ARTIFICIAL INTELLEGENCE

Artificial intelligence is the simulation of human intelligence processes by machines, especially computer systems. Specific applications of AI include expert systems, natural language processing, speech recognition and machine vision.

# How does AI work

AI systems work by ingesting large amounts of labeled training data, analyzing the data for correlations and patterns, and using these patterns to make predictions about future states. In this way, a chatbot that is fed examples of text chats can learn to produce lifelike exchanges with people, or an image recognition tool can learn to identify and describe objects in images by reviewing millions of examples.

AI programming focuses on three cognitive skills: learning, reasoning and self- correction.

**Learning processes.** This aspect of AI programming focuses on acquiring data and creating rules for how to turn the data into actionable information. The rules, which are called [algorithms](https://www.techtarget.com/whatis/definition/algorithm).

**Reasoning processes.** This aspect of AI programming focuses on choosing the right algorithm to reach a desired outcome.

**Self-correction processes.** This aspect of AI programming is designed to continually fine-tune algorithms and ensure they provide the most accurate results possible

# Why is artificial intelligence important

AI is important because it can give enterprises insights into their operations that they may not have been aware of previously and because.AI can perform tasks better than humans. Particularly when it comes to repetitive, detail- oriented tasks like analyzing large numbers of legal documents to ensure relevant fields are filled in properly, AI tools often complete jobs quickly and with relatively few errors.

# Advantages and Disadvantages of AI

[Artificial neural networks](https://www.techtarget.com/searchenterpriseai/definition/neural-network) and deep learning artificial intelligence technologies are quickly evolving, primarily because AI processes large amounts of data

much faster and makes predictions more accurately than humanly possible.

**Advantages**

* Good at detail-oriented jobs
* Reduced time for data-heavy tasks
* Delivers consistent results
* AI-powered virtual agents are always available.

## Disadvantages

* Expensive
* Requires deep technical expertise
* Limited supply of qualified workers to build AI tools
* Only knows what it's been shown
* Lack of ability to generalize from one task to another.
* oriented jobs

# Types of AI

AI can be categorized into four types, beginning with the task-specific intelligent systems in wide use today and progressing to sentient systems,

which do not yet exist. The categories are as follows:

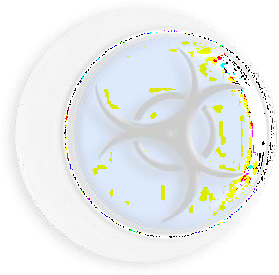
* **Type 1: Reactive machines.** These AI systems have no memory and are task specific.
* **Type 2: Limited memory.** These AI systems have memory, so they can use past experiences to inform future decisions. Some of the decision-making functions in self-driving cars are designed this way.
* **Type 3: Theory of mind.** Theory of mind is a psychology term. When applied to AI, it means that the system would have the social intelligence to understand emotions. This type of AI will be able to infer human intentions and predict behavior, a necessary skill for AI systems to become integral members of human teams.
* **Type 4: Self-awareness.** In this category, AI systems have a sense of self, which gives them consciousness. Machines with self- awareness understand their own current state. This type of AI does not yet exist.

# AI in Cybersecurity

AI and machine learning are now becoming essential to information security, as these technologies are capable of swiftly analyzing millions of data sets and tracking down a wide variety of cyber threats — from malware menaces to shady behavior that might result in a phishing attack.

These technologies continually learn and improve, drawing data from past experiences and present to pinpoint new varieties of attacks that can occur today or tomorrow.

## Advantages of AI in Cybersecurity

AI presents many advantages and applications in a variety of areas, cybersecurity being one of them. With fast-evolving cyberattacks and rapid multiplication of devices happening today, AI and machine learning can help to keep abreast with cybercriminals, automate threat detection, and respond more effectively than conventional software-driven or manual techniques.

Here are a few advantages and applications of using AI in cybersecurity:

## Detecting New Threats

AI can be used to spot cyber threats and possibly malicious activities. Traditional software systems simply cannot keep pace with the sheer number of new malware created every week, so this is an area AI can really help with.

By using sophisticated algorithms, AI systems are being trained to detect malware, run pattern recognition, and detect even the minutest behaviors of malware or ransomware attacks before it enters the system.

AI allows for superior predictive intelligence with natural language processing which curates data on its own by scraping through articles, news, and studies on cyber threats.

This can give intelligence of new anomalies, cyberattacks, and prevention strategies. After all, cybercriminals follow trends too so what’s popular with them changes constantly.

## Battling Bots

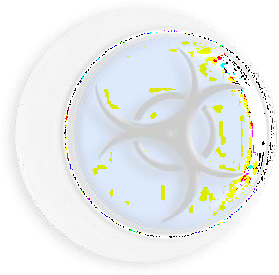
Bots make up a huge chunk of internet traffic today, and they can be dangerous. From account takeovers with stolen credentials to bogus account creation and data fraud, bots can be a real menace.

You can’t tackle automated threats with manual responses alone. AI and machine learning help build a thorough understanding of website traffic and distinguish between good bots (like search engine crawlers), bad bots, and humans.

AI enables us to analyze a vast amount of data and allows cybersecurity teams to adapt their strategy to a continually altering landscape.

## Breach Risk Prediction

AI systems help determine the IT asset inventory which is an accurate and detailed record of all devices, users, and applications with different levels of access to various systems.

Now, considering the asset inventory and threat exposure (as discussed above), AI- based systems can predict how and where you are most likely to be compromised so that you can plan and allocate resources towards areas of most vulnerabilities.

Prescriptive insights from AI-based analysis enables you to configure and improve controls and processes to reinforce your cyber resilience.

## Downsides of AI in Cybersecurity

The advantages discussed above are just a small chunk of the potential of AI in improving cybersecurity.

However, as with anything, there are also some downsides to using AI in this field. In order to build and maintain an AI system, organizations would need substantially more resources and financial investments.

Furthermore, as AI systems are trained using data sets, you must acquire many distinct sets of malware codes, non-malicious codes, and anomalies. Acquiring all of these data sets is time-intensive and requires investments that most organizations cannot afford.

Without huge volumes of data and events, AI systems can render incorrect results and/or false positives. And getting inaccurate data from unreliable sources can even backfire.

Another major downside is that cybercriminals can also use AI to analyze their malware and launch more advanced attacks.

## Conclusion

AI is fast emerging as a must-have technology for enhancing the performance of IT security teams. Humans can no longer scale to sufficiently secure an enterprise-level attack surface, and AI gives the much-needed analysis and threat identification that can be used by security professionals to minimize breach risk and enhance security posture.

Moreover, AI can help discover and prioritize risks, direct incident response, and identify malware attacks before they come into the picture.

So, even with the potential downsides, AI will serve to drive cybersecurity forward and help organizations create a more robust security posture