WatchGuard

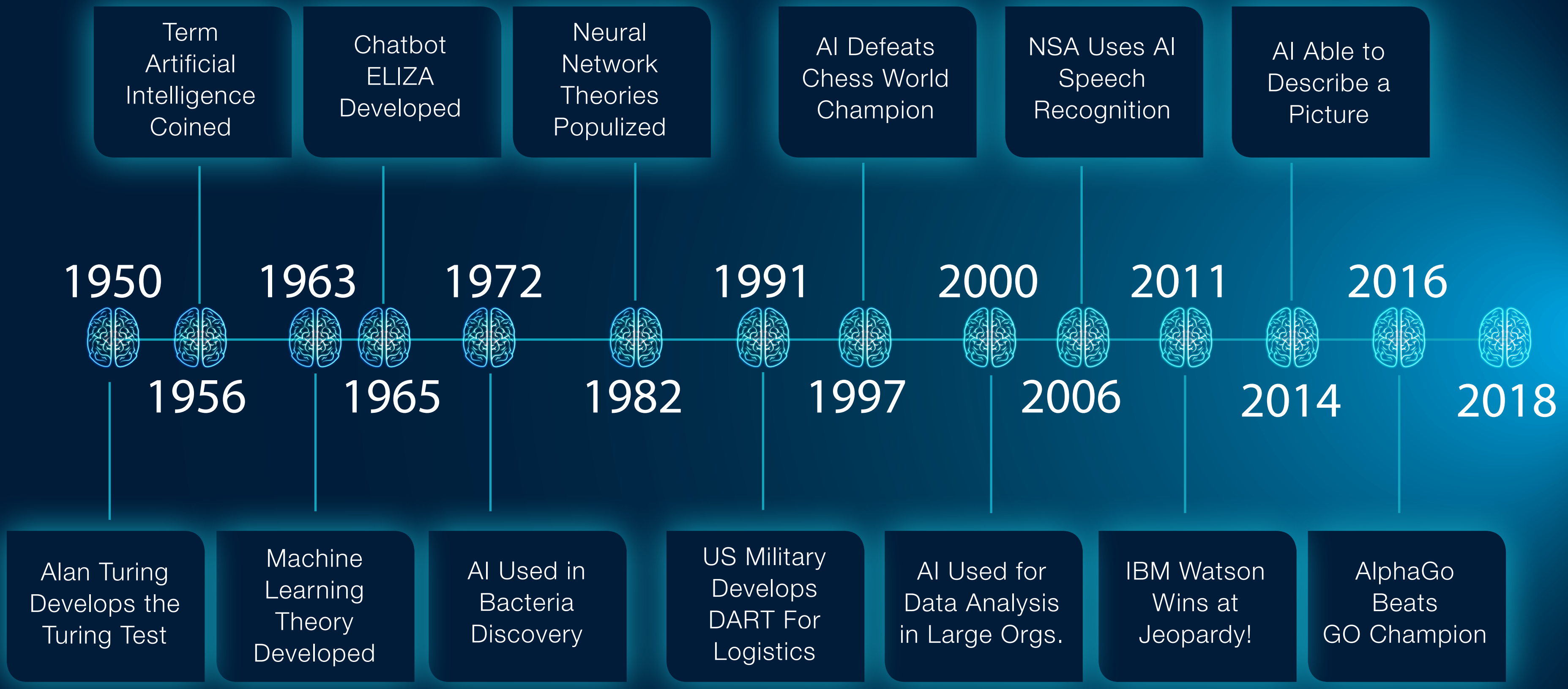
ARTIFICIAL INTELLIGENCE

An Essential Layer of Security

What Is Artificial Intelligence?

Artificial intelligence (AI) is broadly defined as the process of developing computer systems to adapt to changing circumstances and perform tasks that normally require human intelligence. While many consider AI to be a simple buzzword, the concept of artificial intelligence (AI) has been around since at least the 1950s. Pioneering computer scientists like Alan Turing posited that sometime in the future, computers would be able to emulate the work of humans and perform “intelligent” tasks, like play chess. Over the last 60 years, the hype and hope around AI has come in waves, as advances in computing technology made analyzing huge data sets possible and opened doors to new applications.

Artificial Intelligence Through Time



1950 Alan Turing Develops the Turing Test

1956 Term Artificial Intelligence Coined

1963 Machine Learning Theory Developed

1965 Chatbot ELIZA Developed

1972 AI Used in Bacteria Discovery

1982 Neural Network Theories Populized

1991 US Military Develops DART For Logistics

1997 AI Defeats Chess World Champion

2000 AI Used for Data Analysis in Large Orgs.

2006 NSA Uses AI Speech Recognition

2011 IBM Watson Wins at Jeopardy!

2014 AI Able to Describe a Picture

2016 AlphaGo Beats GO Champion

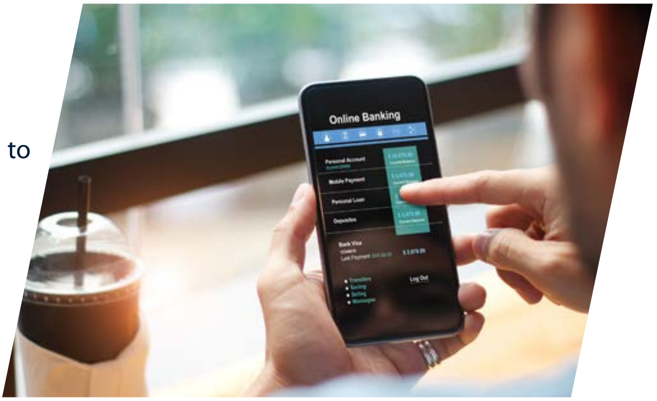
2018

AI Moves from Hype to Hero

In the last two decades we have seen AI take major strides in capability. We can point to IBM's Deep Blue narrowly defeating world chess champion Gary Kasparov in 1997, and their Watson AI defeating Jeopardy Champions Brad Rutter and Ken Jennings in 2011 as evidence that artificial intelligence had become mainstream.

Today, we rely on elements of artificial intelligence in many facets of our everyday lives:

- **Rideshare apps** like Uber and Lyft use AI and machine learning to determine fares, predict rider demand, and estimate time of arrival – even going as far as to recommend riders relocate for their pickup, based on patterns found in millions of successful and challenging pickups.
- **Depositing checks** via a smartphone requires a complex system of AI and machine learning to accurately decipher and convert handwriting on checks into text for processing.
- **Video games** have long used elements of AI to improve the challenge for the player, with enemies now able to interact with their environment and learn from past encounters with the player to increase their chances of success.
- **Music and movie** recommendation capabilities in Spotify, Netflix and Pandora apply a simple AI system to present you with new media that reflects your interests and previously expressed opinions.
- **Investment management** gets smarter, with AI taking the lead in developing financial portfolios according to investment goals and risk tolerance of the client and managing those portfolios in real time as the market changes.
- **Chatbots and virtual assistants** now serve as the front line of customer service for many brands, handling everything from recruiting to technical support.



Artificial intelligence is now an intrinsic part of our lives, and adoption of the technology promises to accelerate rapidly in the coming years. In fact, a recent report by PWC projects that the total economic impact of AI will reach $15.7 trillion by 2030.

Yet, for many, the adoption and growth of AI presents a major concern, with skeptics pointing to everything from potential loss of jobs via automation to fears about the ability of computers to perform the complex tasks, such as driving, for which they are being designed.

Cyber Criminals Getting Smart with AI

One of the biggest benefits of artificial intelligence is its ability to act as an amplifier that helps people work through large amounts of complex data and perform highly repetitive tasks that would normally require a human. Automating what traditionally would be a manual process allows criminals, especially cyber criminals, to improve targeting, expand the scale of attacks, and turbo-charge the speed at which they can create new malware. While few examples of attacks using AI have been seen thus far, security researchers have been hard at work exploring what is possible.

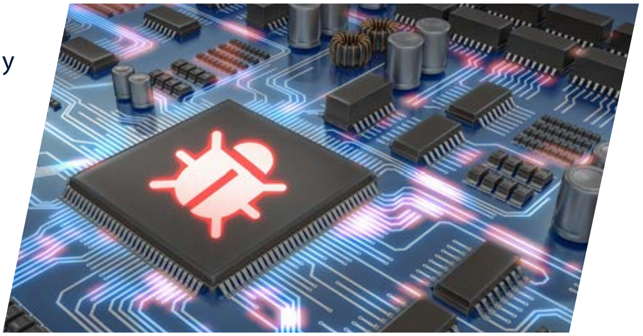
Here are few examples of the research into how attackers could use AI:

- **Bypassing CAPTCHA systems.** CAPTCHA has become an essential tool on the Internet that allows us to determine whether a visitor to our site is human or a bot. Visitors are presented with an image, checkbox or string of distorted text and asked to take an action that would normally require a human, such as identifying images that are similar to each other. Using AI techniques, researchers at Columbia University were able to get by Googles reCAPTCHA 98% of the time.

- **Improving the accuracy and scope of phishing.** A reported 76% of organizations fell victim to phishing attacks in 2017, and in response many organizations have implemented rigorous programs to train their employees to identify phishing attempts to prevent these attacks. With AI, cyber criminals have a tool that can be used to parse through huge volumes of data about their targets, and craft messages that will produce a higher degree of success. Security researches at ZeroFox demonstrated such an approach for targeting Twitter users with SNAP_R (Social Network Automated Phishing with Reconnaissance). SNAP_R uses AI to identify valuable targets and quickly develop a profile of that target based on what they have tweeted in the past. Using this approach, they were able to get targets to click on malicious links 30% of the time (compared to the 5-15% success rate of other automated approaches).

- **Developing highly evasive malware.** Hackers have long relied on scripts and toolkits to develop and distribute malware, but as cyber defense has become more intelligent and sophisticated our adversaries have turned to low-level artificial intelligence techniques to boost the evasiveness of malware. Malware authors have started to use AI to perform checks to identify hardware configurations and the environment they are in (e.g., a sandbox vs. a physical machine), as well as determine if a human is operating the machine at the time. DeepLocker, developed by researchers with IBM Research, demonstrates the dangers of weaponized artificial intelligence in malware. DeepLocker's AI is trained to ensure that its payload only executes when it reaches a specific target, relying on three layers of concealment to prevent security tools from identifying the theat.

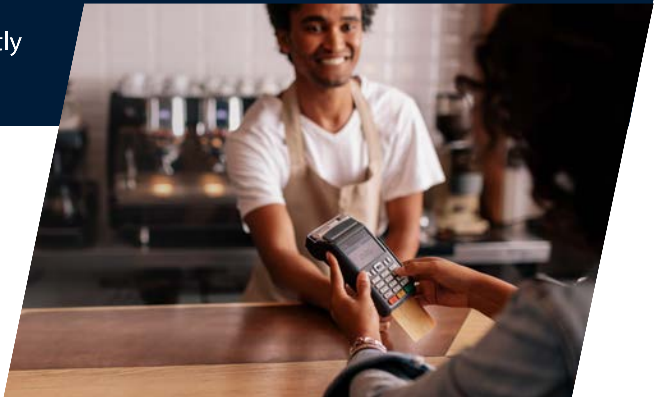
As the cyber security arms race heats up, it's fair to say we are nearing a new phase, one where AI and machine learning will play an increasingly important role in both attack and defense.



An Essential Layer of Security for Businesses of All Sizes

Cyber attacks occur in the blink of an eye. A single point of infection can spread like wildfire from endpoint to endpoint; location to location; and business to business. Traditional approaches to protection rely heavily on manual processes and preestablished policies to block attacks that fail to keep up with the ever-evolving nature of threats.

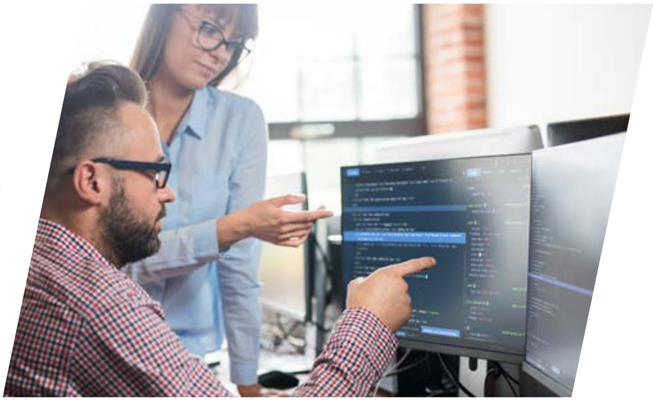
Parsing through huge volumes of threat indicators is an intensive, time-consuming process for even the most skilled teams. Chances are your IT teams are already overwhelmed with alerts and false positives, leaving attacks to go unnoticed for months at a time. This is where AI can provide a tremendous amount of value. With a foundation of artificial intelligence, you can save time, correlate more data, make faster decisions, minimize human error, and predict future threat trends while greatly improving your security posture.



What problems can AI help to solve?

Scarcity of Security Expertise

- Many organizations, especially small businesses, lack both headcount and expertise when it comes to security. IT teams are often operating in blended roles, wearing multiple hats of responsibility. AI enables the automation of security processes, which is a time-saver that allows IT to spend more time on business-critical tasks. In effect, AI can perform functions that would normally require a skilled security analyst, making sense of huge volumes of security data, and automatically acting to improve your security posture.

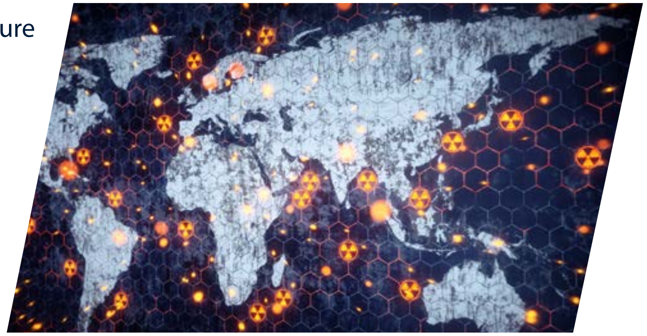


Resource Constraints

- SIEM and security management tools are out of reach for many smaller organizations who are operating on tight budgets. Although the data is there, time constraints mean much of it cannot be analyzed and consumed in time to be effective. When properly implemented, AI can perform correlation, analysis and scoring for you, while learning from multiple threat intelligence sources to ensure cyber vigilance. What's more, AI gives you the ability to automate remediation with minimal disruption to your business.

Threat of Zero Day and Evasive Malware

- Policies and signatures can quickly become obsolete and out of date, leaving significant security gaps when used alone. AI provides intelligent layers of defense, able to detect and defeat malware much earlier than legacy approaches. When properly trained, AI offers predictive protections that anticipate future threats, without needing signatures, Cloud connectivity, etc. AI can look at hundreds of thousands of characteristics of a given file and rapidly determine the threat level of the file.



AI: Your Team's Automated Security Analyst

Every security analyst's goal is to prevent attacks as efficiently as possible, while being able to detect and respond to threats as early as possible. Through automation, AI is like having a skilled security analyst that works 24/7/365 to keep you safe.

AI enables the automation of:

PREVENTION
Without needing signatures or Cloud connectivity

DETECTION
Through self-learning tools for static and dynamic analysis

RESPONSE
Through correlated threat scoring

AI in the WatchGuard Portfolio

Artificial intelligence within the WatchGuard security services portfolio acts as a force multiplier that enables the automation of processes, and greatly enhances our coverage against emerging threats. As security implementations of AI continue to mature, it will connect all our portfolio platforms to provide the deepest insights in the simplest, most actionable way, and enable state-of-the-art defenses against future attacks.

What can you expect from AI in the WatchGuard portfolio?

Predictive Protection. The delay between when a malware strain is discovered, and when the signatures, heuristics, and behavioral patterns can be applied presents a significant challenge. IntelligentAV provides predictive coverage against malware threats an average of 25 months before they are seen in the wild.

Shortened Time-to-Detection. Detecting and killing highly evasive malware strains in a timely manner requires the knowledge and ability to look for thousands of malicious indicators. ThreatSync, in conjunction with our APT Blocker security service, detects and automatically sends suspicious files for deep analysis in a next-generation Cloud sandbox. APT Blocker leverages AI during the deep inspection process to perform comprehensive analysis on files.

Automated Threat Defense. Artificial intelligence makes it possible to collect vast amounts of data from nearly every source imaginable and use that data to automatically train for secure outcomes. IntelligentAV, APT Blocker, and ThreatSync are constantly evolving from a steady stream of new data and feedback and applying this training to improve your security posture.

Given the sophistication of emerging threats, and the speed at which threats evolve, artificial intelligence represents an essential tool in the cyber arms race for organizations of all sizes. As a leader in security, WatchGuard continues to find new ways to advance our products and services with AI technologies.

THE WATCHGUARD SECURITY PORTFOLIO

Network Security

In addition to delivering enterprise-grade security, our platform is designed from the ground up to focus on ease of deployment, use, and ongoing management, making WatchGuard the ideal solution for SMB, midsize, and distributed enterprise organizations worldwide.

Secure Wi-Fi

WatchGuard's Secure Wi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.

Multi-Factor Authentication

WatchGuard AuthPoint® is the right solution to close the password-driven security gap that leaves companies vulnerable to a breach. It provides multi-factor authentication on an easy-to-use Cloud platform. Our unique approach adds "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

Find out more

For additional details, talk to your authorized WatchGuard reseller or visit **https://www.watchguard.com.**

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

WatchGuard

North America Sales: 1.800.734.9905 • International Sales: 1.206.613.0895 • Web: www.watchguard.com

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis.
Part No. WGCE671403_010819