SECURANCE CONSULTING

Advantage of Insight | AI

AI ON YOUR SIDE:

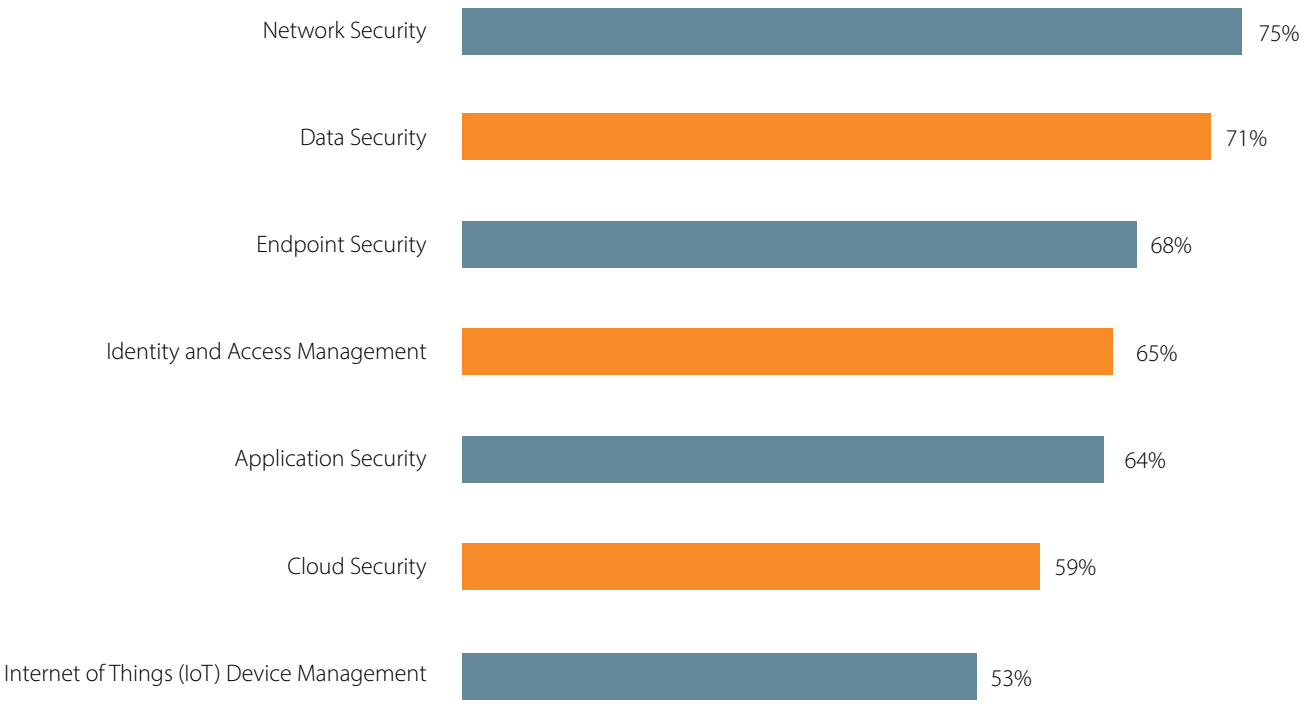
AI TOOLS TO ENHANCE SECURITY DEFENSES AND OPERATIONS

www.securanceconsulting.com

INTRODUCTION

In the evolving cyber landscape, artificial intelligence (AI) tools have emerged as a pivotal force in security operations and defenses. The role of AI in enhancing traditional security measures demonstrates how cutting-edge technologies can reshape threat detection, incident response, and overall resilience for the better. As cyber attacks grow in complexity and scale, AI tools have become imperative for organizations to stay ahead of adversaries and proactively identify and mitigate potential risks. From anomaly detection and predictive analytics to behavioral analysis and automated response mechanisms, AI can streamline and strengthen security activities in a multitude of ways to create more robust defenses.

Percentage of Organizations using AI Cybersecurity Tools to Enhance[1]:

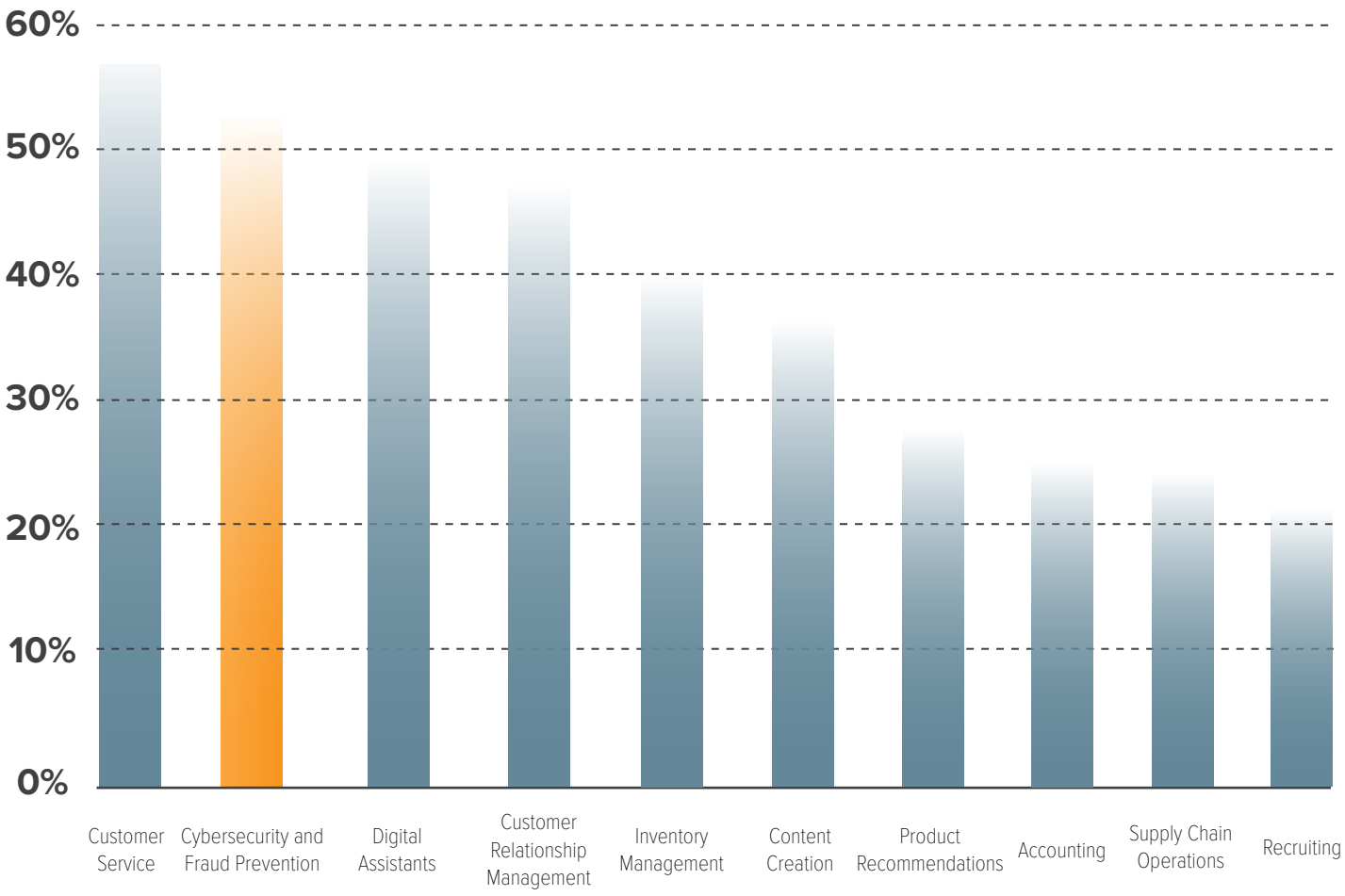


Cybersecurity is becoming a major concern for businesses, as employees shift to remote work and cloud use, creating new vulnerable environments susceptible to data breaches. Of the 850 executives surveyed, 75 percent said they are adopting AI to mitigate these cybersecurity risks, with roughly 40 percent currently using, or planning to use by next year, proprietary solutions or commercial tools with AI embedded.[2]

AI IN 2024

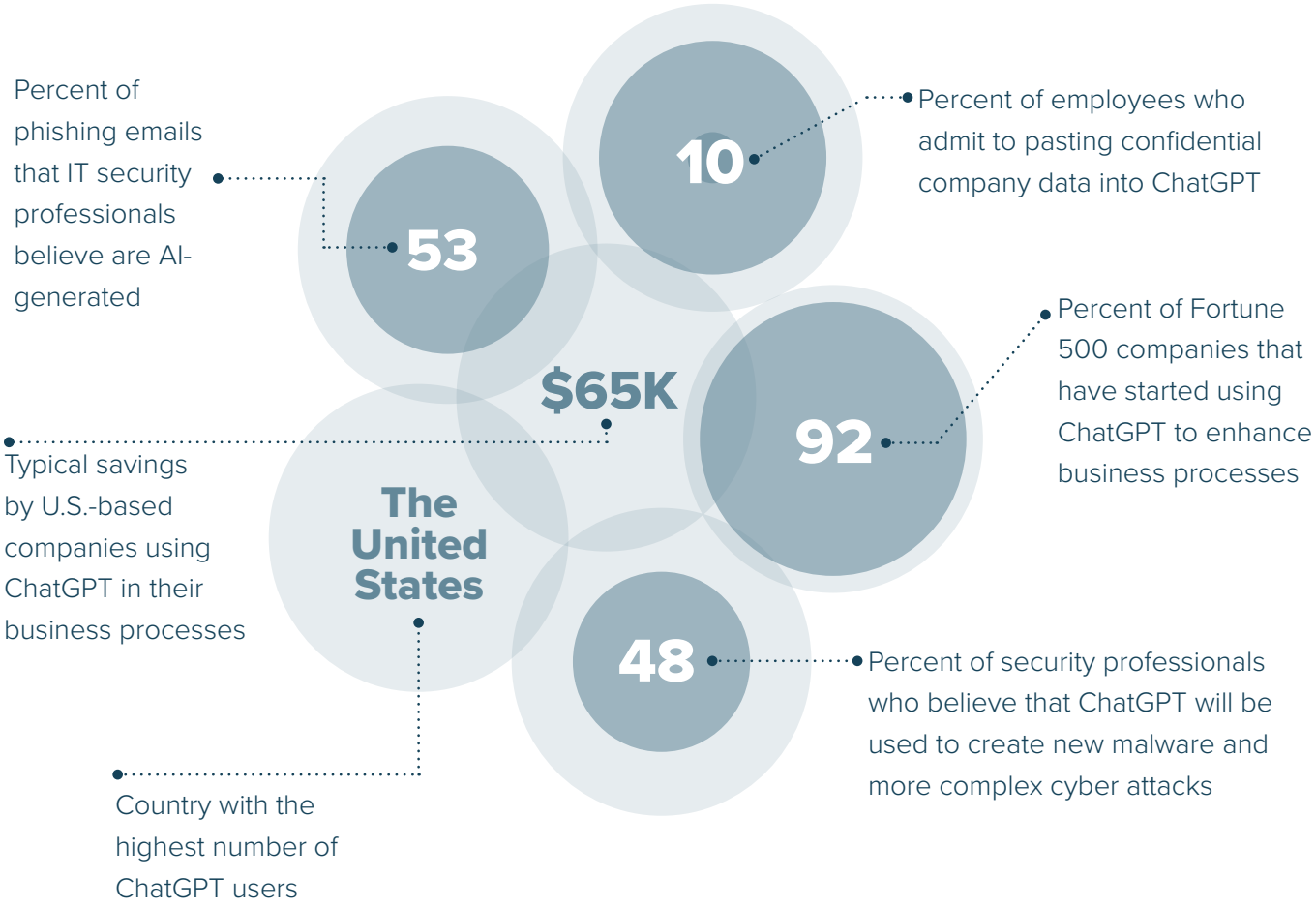
In 2022, the generative AI (GenAI) boom emerged. In 2023, AI took root in the business world with an explosion of foundational AI systems and large language models (LLMs). Now, AI has become an inseparable part of the workforce as companies seek to utilize commercial LLM solutions and | or establish their own enterprise AI systems to enhance business workflows, automate processes, and secure the IT environment.

Most Common Ways Companies Use AI[3]



As of November 2023, one of the most popular AI models, OpenAI's ChatGPT, offers unique, customizable versions of the LLM, referred to as Generative Pretrained Transformers (GPTs). Organizations and individual users alike can tailor their versions of ChatGPT to meet specific business or personal needs. GPTs do not require coding, allowing virtually anyone to develop their own AI model. Additionally, OpenAI has increased data privacy protections for users of custom GPTs. Conversations with GPTs are not shared with OpenAI's developers; in the public version of ChatGPT, the developers can access users' inputs to train the model. If a GPT uses third-party APIs, the user chooses whether the data can be sent to that API, including an option to remove the entire account from model training.[4]

2024 ChatGPT Statistics[5]



AI giants Google and OpenAI are betting big on going small. Both are developing user-friendly platforms that allow people to customize powerful LLMs and make their own mini chatbots that cater to their specific needs—no coding skills required, allowing anyone to become a GenAI developer.[6]

AI TOOLS TO ENHANCE SECURITY DEFENSES

One of the most promising applications of enterprise AI is to automate and improve IT security operations. Cybersecurity presents unique challenges, including an evolving threat landscape, vast attack surface, and an enormous skill gap and talent shortage. Since AI can analyze massive amounts of data, identify patterns that people might miss, and improve its capabilities over time, organizations can quickly identify threats, shorten response times, and reduce the overall cost of a cyber attack. Below are some of the most common use cases for AI in cybersecurity:

Threat Detection | Management | Response

AI can collect, integrate, and analyze data from thousands of control points and provide greater visibility into network communications, traffic, and endpoint devices. AI can also recognize patterns and anomalous behavior, identify threats accurately and at scale, and filter out non-threatening activities to reduce false positives at a volume and speed that human defenders cannot match. AI-driven automation capabilities can not only isolate threats by device, user, or location, they can also initiate notification and escalation measures. By reducing the time required to analyze, investigate, and prioritize alerts, security teams can spend more time remediating vulnerabilities and containing potential breaches.

AI-powered Remediation

More advanced applications of AI are helping security teams remediate threats faster and more easily. Some AI-powered tools can even process security alerts and offer users step-by-step remediation instructions based on input from the user, resulting in more effective and tailored remediation recommendations. AI-powered remediation tools can also analyze historical data and learn from past incidents to identify recurring security issues and recommend proactive measures to address them. This enables IT staff to fix failing controls to pass tests, get audit-ready faster, and improve their overall security and compliance posture.

Dynamic Deception Capabilities

Deceiving threat detection capabilities is a common tactic bad actors use to evade detection before launching an attack, but IT staff can fight back. AI can be used to power deception techniques, such as fooling attackers with realistic vulnerability projections and effective baits that defend organizations against advanced threats. These techniques enable the creation of highly realistic scenarios that mimic legitimate system behavior and lure hackers into revealing their presence, allowing organizations to gain valuable insights into adversary tactics and identify potential security weaknesses. Furthermore, AI can enhance the adaptability of deception strategies in response to emerging threats and cyber attacks.

Stronger Passwords using LLMs

In the wrong hands, bad actors can use automated tactics and LLMs to crack common passwords in no time at all. While this may seem daunting, AI has the potential to improve password security by enhancing the complexity of generated passwords and strength estimation algorithms. AI-powered algorithms can also analyze user behavior patterns to identify and flag potentially compromised accounts, prompting users to update their passwords proactively. Additionally, LLMs can assist organizations in implementing robust password policies tailored to individual user behaviors and risk profiles.

AI-based Patch Management

With technology constantly changing, manual approaches to patch management cannot keep up, leaving systems vulnerable to data breaches. AI-based patch management systems can help identify, prioritize, and even address vulnerabilities with much less manual intervention required. Moreover, AI-driven patch management solutions can adapt to evolving threats and vulnerabilities in real time. With AI's assistance, security teams can streamline their patch management processes, reduce the window of exposure to known vulnerabilities, efficiently allocate resources, and mitigate the risk of data breaches without overwhelming manual effort.

Automated Penetration Testing

While there have been automated vulnerability assessment and penetration testing tools available for many years now, AI can simplify this process even more by quickly scanning networks and gathering data to determine the best exploitation path for the IT professional, reducing the level of effort required. By leveraging machine learning algorithms, these tools can uncover complex vulnerabilities that traditional testing methods may not detect.

AI-powered Risk Assessments

AI can also be used to automate risk assessments, improving accuracy, reliability, and efficiency, and saving security teams significant time. These types of AI tools can evaluate and analyze risks based on existing data from a risk library and other data sources, and automatically generate risk reports. Some AI-powered risk assessment solutions can even determine the likelihood and impact of a risk, suggest a treatment plan to respond to the risk, and define the residual likelihood and impact of the risk after treatment.[7]

The average savings for organizations that use security AI and automation is $1.76 million.[8]

Enhanced Threat Intelligence

Cyber threat intelligence is evidence-based knowledge about existing or emerging threats. It encompasses context, mechanisms, indicators, implications, and remediation plans and plays a crucial role in understanding bad actors' motives, targets, and attack behaviors. GenAI is increasingly being deployed in threat intelligence solutions to transform how analysts work. AI models can churn through the collected data at speeds and scales beyond human capabilities, reducing the analyst's workload and allowing them to dedicate their time to other security initiatives, such as proactive threat hunting and remediation.[9]

Popular AI Cybersecurity Tools

While many enterprises have opted to develop their own AI security solutions, there are commercial tools available, as well. The examples listed below cover a range of security requirements, including threat intelligence, password security, dynamic deception techniques, patch management, and penetration testing.

- Google's Cloud Security AI Workbench includes a suite of cybersecurity tools to help analysts detect, report, contain, and remediate security threats and vulnerabilities.
- OpenAI's PassGPT is a password-guessing model built on LLMs. The main objective of PassGPT is to decode the cryptic features of human-generated passwords with the aim of giving users stronger and more complex passwords to use.
- Acalvio's AI-powered ShadowPlex platform uses AI to provide autonomous deception techniques that deceive attackers with realistic vulnerability projections and effective baits and lures, providing IT staff with key insights regarding their threat landscape.
- GitHub's Copilot AI developer tool provides contextualized assistance throughout the software development lifecycle, from code completions and chat assistance to code explanations, enabling developers to increase productivity and accelerate the pace of software development.
- Open-source AI penetration testing tools, such as DeepExploit and NodeZero, offer faster, cost-effective alternatives to traditional penetration testing services because they are fully automated and use machine learning to enhance parts of the testing process, including intelligence gathering, threat modeling, vulnerability analysis, and exploitation.
- Securance Consulting's Software as a Service (SaaS) threat intelligence platform, CTIQ, uses advanced AI algorithms to deliver clear, relevant, and actionable data. This platform is designed to counter alert fatigue in cybersecurity, ensuring that threats are not missed and that immediate, proportionate countermeasures are carried out.

A recent study found that about 67 percent of security practitioners have already tested AI's ability to perform security tasks. Another 55 percent of organizations will incorporate AI security tools this year, the top use cases being creating rules, simulating attacks, detecting compliance violations, reducing false positives, and classifying anomalies. C-suites are largely behind that push, as confirmed by 82 percent of respondents.[10]

CONCLUSION

AI on Your Side

The integration of AI tools into security operations has ushered in a new era of resilience in the face of escalating cyber threats. As attackers' tactics and techniques continue to mature, AI will become essential to maintaining a secure IT environment. The synergy between human expertise and machine intelligence offers a formidable defense against both known and unforeseen threats, empowering organizations with heightened defenses. Future developments and innovations in AI tools will ensure that enterprises can protect digital assets in a dynamic threat environment.

ABOUT SECURANCE

Securance has more than two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://www.capgemini.com/ch-en/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf
2. https://research.aimultiple.com/cyber-security-stats/
3. https://explodingtopics.com/blog/companies-using-ai
4. https://openai.com/blog/introducing-gpts
5. https://www.enterpriseappstoday.com/stats/chatgpt-statistics.html
6. https://www.technologyreview.com/2024/01/04/1086046/whats-next-for-ai-in-2024/
7. https://secureframe.com/blog/ai-in-cybersecurity
8. https://www.ibm.com/reports/data-breach
9. https://www.forbes.com/sites/forbestechcouncil/2023/07/21/how-ai-enabled-threat-intelligence-is-becoming-our-future/?sh=45c4f555727e
10. https://venturebeat.com/security/google-cloud-and-csa-2024-will-bring-significant-generative-ai-adoption-in-cybersecurity-driven-by-c-suite/

AI on Your Side: AI Tools to Enhance Security Defenses and Operations

SECURANCE CONSULTING
Advantage of Insight AI

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com