Acceleration Economy Practitioner Analysts

defining the digital first world

The Business Impact & Opportunity of

Generative AI

An AI/Hyperautomation

GUIDEBOOK

Contributing Acceleration Economy Practitioner Analysts and Guests


Aaron Back
AI & Hyperautomation POV


Kieron Allen
Cloud & Apps POV


Scott Vaughan
CMO POV


Tony Uphoff
CEO POV


Joanna Martinez
Supply Chain POV


Kenny Mullican
CIO POV


Frank Domizio
CISO POV


Bill Doerrfeld
Developer & Cybersecurity POV


Robert Wood
CISO POV

Welcome Message

Aaron Back

AI & Hyperautomation POV
Chief Content Officer
Acceleration Economy Practitioner Analyst

Acceleration Economy Practitioner Analysts
defining the digital first world

The hype around generative artificial intelligence (AI) is real. There's no denying that. However, the reality behind the hype is often glossed over as it contains uncomfortable truths that many don't want to address.

So, what are these uncomfortable truths of reality in an increasingly artificial world?

First, people should be at the forefront of every tech innovation. The genesis of these innovations has always been people, but that may not be the case in the future. No, I'm not here to be some doomsayer about AI taking over the world. What I'm suggesting is that people should not only be part of the "human in the loop" concept but should also sit outside the loop framing AI governance.

Second, the realities of AI overlap with three other areas that make up the 4 Pillars of Acceleration Economy.

1. Cloud – Including multi-cloud & hybrid cloud.
2. Cybersecurity – As a true business enabler and not the "office of no."
3. Data – Not just the bits and bytes, but data modernization, governance, and security.

AI is nothing without data, AI can be ravenous if not kept in check by cybersecurity, and AI is made possible by flexible and scalable cloud technology.

Third, decision-makers, executives, and boards of directors are faced with the hard question of, “How can we leverage AI in a strategic way that aligns with our business goals?"

Answering that question is just as unique for the person asking it as it is for the business looking to utilize AI.

So, where does this leave you, the decision-maker? This leaves you in the position to be the AI champion in your company as this guidebook will equip you with an understanding of the impact and opportunities of generative AI with insights into the “why & how."

- How and Where to Apply AI to Bolster Customer Experience
- How Generative AI Is Changing the Future of Work
- How to Know If a Software Solution Is Actually AI-Driven or If It's Just Hype
- From Malware Detection to Predictive Analytics, How AI Enhances Core Cybersecurity Functions
- How to Maintain Cybersecurity as ChatGPT and Generative AI Proliferate

Contents

AptEdge Capitalizes on Generative AI to Transform Customer Service in Support Applications

By Kieron Allen
Cloud & Apps POV

AI HYPERAUTOMATION — TOP 10 — Impact Enabler — Acceleration Economy network

There are few, if any, areas in business that AI hasn't touched. The benefits of AI, and generative AI more recently, in business processes are widely known. Still, it's not often that platforms utilizing this technology address well-established pain points while taking a dramatically different approach than other platforms.

AptEdge has one of those platforms; it's moved away from the automated chatbot and adopted generative AI to reimagine customer support, providing the first GPT-powered engine to give customer support agents within call centers immediate access to contextual knowledge from across an organization's applications, enabling them to deliver a better, more personalized experience by automating search across knowledge silos to extract answers quickly.

AptEdge addresses the challenges of data sprawl, higher ticket volumes, growing complexity of questions, and issues with agent attrition and retention. Its support-centric AI provides call-center agents with accurate answers to customer queries, slashing research time, and enabling them to deliver a better, more personalized experience by automating search across knowledge silos to extract answers quickly.

Who They Are

Founded in 2019 and headquartered in Redwood City, California, AptEdge is the brainchild of Aakrit Prasad and Anthony Kilman. Both co-founders still hold positions in the company's C-suite. AptEdge has raised a total of $12.9M over three funding rounds. The company's lead investors include Stage 2 Capital, National Grid Partners (NGP), and Unusual Ventures.

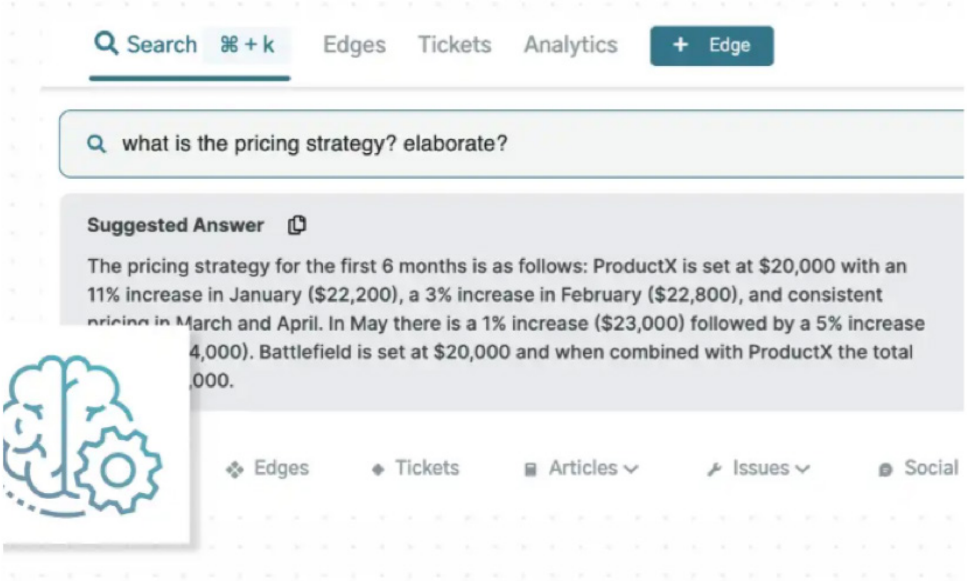
Aakrit Prasad is the CEO of AptEdge. His former roles included Head of Core APM Product at the application performance firm AppDynamics, as well as Vice President, Product and Strategy at Applitools. Anthony Kilman is the company's CTO. Prior to AptEdge, Kilman also held a number of roles at AppDynamics alongside Prasad.

Contextual Information Sharing

We spoke with Prasad about how his previous experience led to the development of the company. "One of the biggest challenges in my operating role in the past — managing customer service support operations and core product teams — was trying to get to the root of customer escalations and reducing their impact," he says.

> *"It all came down to a lack of intel, in quick access to knowledge and information and not having an intelligence layer that can connect to all these areas of knowledge immediately to get to our answers," he continues. "We envisioned a world where you could connect to all these systems of knowledge and immediately be able to find answers in context."*
>
> **AptEdge CEO**
> Aakrit Prasad

AptEdge provides customer support agents with contextually accurate responses to customer queries. The AptEdge system centers on its generative AI-powered answer engine, AnswerGPT, which provides instant answers to customer questions, streamlining responses and supporting agents to deliver optimal customer service for internal and external requests.



The company uses AI technology to enable agents to connect and integrate with their company's knowledge sources, whether that be business applications like Slack or Teams, customer relationship management (CRM) platforms, or ticketing systems. This supports universal access to knowledge that dramatically reduces the time support agents need to research answers to queries.

Improved Call Completion Rates

AptEdge enables companies to prevent escalations, reduce ticket volume, improve resolution time, and enhance customer satisfaction, or CSAT. In regards to escalation prevention, AptEdge technology uses GPT-enabled answers, alongside machine learning-powered Edge Automation for grouping and assignment of tasks, to address most Tier 1-level issues, reducing escalations by 35%.

The company's technology crawls and finds all sources of knowledge and then taps large language models (LLMs) to create and personalize customer responses.

AptEdge reports that its technology enables a 30% increase in agent productivity by deflecting tickets using automation, while average handle time improves by 40% thanks to an increase in first-contact resolutions. And the positive impact of this increased productivity is improved CSAT.

“If you can empower every rep, every front-line team member that handles (customer) interactions with all the knowledge, the collective intelligence of the whole company, you've basically made them a superhero in the company," says Prasad.

Completing the Circle with Generative AI

Prior to the introduction of generative AI technology in late 2022, AptEdge developers already had the foundational technology in place. “The way that we approached it at its core was building an intelligence layer that connects to different repositories of information," explains Prasad.

“We built an AI layer that connects to different systems of information and also to the support systems like ServiceNow. At the root, it's all about trying to get teams to the answer as quickly as possible." Introducing generative AI into the platform enabled Prasad and his team to complete their vision for the product. “Pre-generative AI, we couldn't turn that answer into a response," says Prasad. “Generative AI models are really good at language manipulation and being able to take language as input and transform it into something else as output. We didn't have a technology to do that."

"That itself is a very hard problem to solve. For us, it was a really exciting opportunity to use generative AI to solve the last mile of our product."

Cisco Case Study: Accurate, Fast Data Capture and Access

One of AptEdge's best-known customers is the digital communications giant Cisco. We contacted the Cisco customer success team to learn more about the impact of AptEdge on its operations.

"AptEdge has been a great benefit, allowing Cisco to fully leverage internal business data repositories. It gives us greater agent response accuracy and efficiency we couldn't get to on our own, which helps reduce our Average Handling Time and deflection in other cases".

Head of Customer Success at Cisco
Charles Coaxum

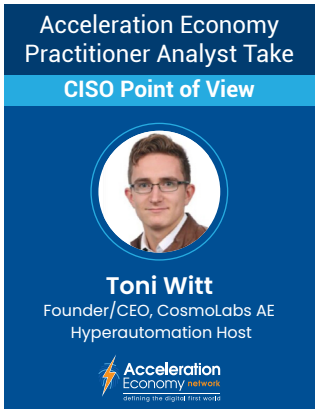
Coaxum noted some of the key benefits the company has seen since adopting AptEdge:

- Quickly and accurately answering customer inquiries in a way that provides a better customer experience than most existing chatbot technologies.
- Summarizing customer feedback and letting human agents and managers know the most common questions and complaints.
- Creating automated customer responses to common questions and inquiries.
- Summarizing internal performance metrics such as response times and customer satisfaction scores.
- Providing guides and how-to's to walk customers through any processes they might have to follow.
- Augmenting human customer service agents' ability to provide satisfactory outcomes by summarizing key points and providing checklists of items that their responses should cover.
- Onboarding new hires more quickly, from shadowing to actual customer engagement.

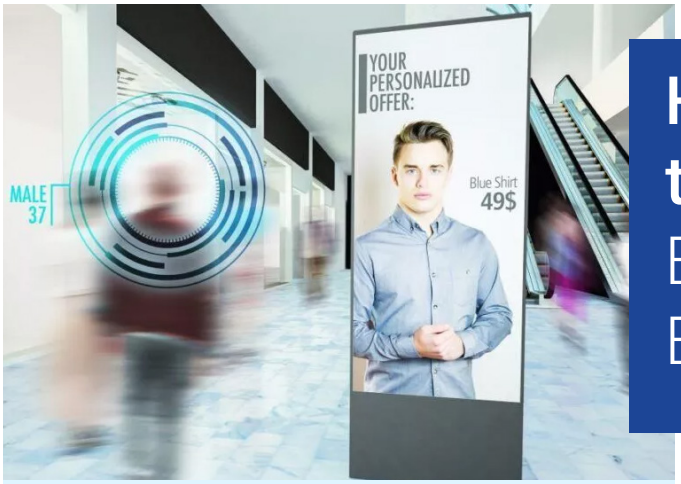
Closing Thoughts

AptEdge is tackling a common pain point in customer service: The problem of sprawl when it comes to accessing data needed to serve customers. One of the negative outcomes of becoming a data-driven organization, when governance isn't installed from day one, is dealing with dispersed data sources. The trouble is, the larger a company becomes, the more customers they serve and, when committing to digital transformation, the more data services they deploy.

AptEdge elegantly addresses the issue by connecting these sources so customers and customer service agents alike can benefit from the complete knowledge in an organization. Generative AI has provided AptEdge with another layer of functionality that, when paired with its existing AI-driven system, enables organizations to leverage more data to create more opportunities to wow their customers.



"We've all had so-so experiences with AI-powered chatbots. AptEdge is taking a different approach. Instead of focusing on autonomous agents, the company focuses on empowering human service agents with the power of AI." As a result, the customer experiences the "best of both worlds: a data-backed response with the human touch that customer service so often lacks."



How and Where to Apply AI to Bolster Customer Experience

By Scott Vaughan
CMO POV

AI HYPERAUTOMATION
TOP 10
Impact Enabler
Acceleration Economy network

"Customer experience" (CX) may mean different things to different people, but its goal is clear — to make every customer touchpoint as efficient, frictionless, and hassle-free as possible. So much so that customers increase their spending, loyalty, and advocacy for your company and products. One of the ways that companies are delivering on this goal — creating, improving, and personalizing customer experiences — is through the use of artificial intelligence (AI).

The timing couldn't be better; according to a recent McKinsey & Co. report, 71% of customers expect a personalized experience. For those customers who have a bad experience, nearly a third respond by evaluating other providers. The research found that successful personalization initiatives can result in 20% higher customer satisfaction and more than 18% higher sales conversion rates.

Where AI Delivers the Most Impact on CX

While the enthusiasm to lean on AI to bolster customer experiences is no surprise, it's important to note that the technology is neither a substitute for all human interactions, nor a blanket answer for your CX strategy. It's important to know where and how to apply AI to deliver a positive customer experience, increase customer satisfaction, and improve customer retention and revenue. Here are some of the most impactful ways that AI improves CX.

Data-Driven Insights and Predictive Analytics

One of the best applications for AI is the ability to gather, analyze, and learn from huge volumes of data. For example, with the help of AI-enabled customer journey analytics, businesses can process and organize large amounts of customer data from millions of sources rapidly. Top brands from Amazon to Zoom are using AI to capture a precise picture of both individual consumers and aggregate customer groups. AI technologies are being used to acquire, process, and analyze, across all touchpoints, all kinds of first- and third-party data, from historical and behavioral to market and demographic.

Another significant advantage for CX is AI's ability to predict client behavior by regularly learning and improving from the data it gathers and analyzes. AI employs predictive analytics with real-time decisioning algorithms to determine, in just seconds, the best engagement options between a customer and a brand. These AI-driven predictive engagement capabilities, for example, direct an online retailer to present a specific type of dress based on correlating time of year, past purchases, and upcoming life events gathered from hundreds of data points. Similarly, AI informs a bank when a customer should engage a customer around a new mortgage or loan based on recent financial transactions or purchases. The bottom line is that AI makes it possible to capitalize on big data to predict and improve customer experiences and options.

Personalization and Customization to Tailor Experiences

Using the power of AI-driven insights outlined above, AI algorithms can analyze and deliver personalized experiences. A basic example of AI-powered personalization is the technology's ability to determine a customer's preferred method of communication: Are they more likely to respond to phone, text, or email outreach? In a more advanced personalization example often used by retailers, AI helps triangulate data from new home purchases, past home furnishings purchases, and online searches to personalize recommendations for specific furniture and decor options. A deeper understanding of personal preferences translates into higher conversion rates, more sales, and happier customers.

Personalization is a powerful conversion technique, while customization is an effective way to find and introduce customers to your brand and offerings. In today's expect-it-now reality, consumers habitually use search and/or a virtual assistant — Alexa, Siri, or Google — as a first step to discovering and researching information. AI can help tailor better searches for the items customers like or want and correlate search inquiries to present specific options and offers. Customization using AI-driven data insights streamlines the customer's process of buying the products they want while delivering a memorable brand experience.

Increased Customer Responsiveness at the Speed of the Customer

Today's digital-savvy customers expect to get answers and resolutions quickly, including fast service when they need product support. In fact, according to a 2022 CX Trends Report, more than 90% of those surveyed consider fast customer service response an essential part of their overall experience. And 65% of customers believe AI will save them time and effort when interacting with a company. Customers calling out AI as a solution is a clear sign that business, customer, and tech leaders need to ensure these core solutions are in place.

Customers also want and expect to engage on their terms when interacting with companies and brands. AI self-service options, such as chatbots, virtual assistants, and interactive voice recognition, can be used to answer basic questions and quickly support and inform customers of options. Just as importantly, these tools can collect key customer information in real-time to create the best experience. Faster first-response times, decreased handling times, and shorter wait times are benefits customers can experience when you use AI to improve their experience.

Understanding and Monitoring Customer Feedback and Experiences

AI is powerful and full of potential, but it's not a blanket solution for every part of CX. Something to watch for is using AI and automation as the primary customer engagement or response option. Companies can over-automate. In my experience, AI algorithms are best used to gather and analyze customer feedback and sentiment to identify areas where the company needs to improve, which can then be addressed in many ways, including via AI. For example, AI-driven processes can be also used to flag and then proactively apply fixes before poor customer experiences and dissatisfaction occur. By using AI to automate monitor and analyze customer feedback data, companies can define and develop processes to continuously optimize and improve customer experience gaps to win, keep, and expand customer relationships.

AI and Customer Experience Are a Winning Combination

With customers and revenue on their minds every day, business and tech leaders are confidently applying the power of AI to monitor, learn, and deliver personalized experiences. Improving CX starts with using AI to process and analyze all the data that impacts customers in order to deliver a better experience. Today, every touchpoint is an opportunity to win or lose a customer; staying on top of, and optimizing, every one of those touchpoints is a great reason to enlist the help of AI. Now is the time to bring your leaders together to discuss where and how the technology can be used to improve customer experiences.

Acceleration Economy Practitioner Analyst Take

AI & Hyperautomation POV

Aaron Back

Chief Content Officer, Acceleration Economy

The key point that Scott made that jumped out is "personalization." The concern that AI may replace human jobs can be alleviated by incorporating human involvement in personalizing the customer experience, which can have a positive impact. And as Scott noted, "Personalization is a powerful conversion technique, while customization is an effective way to find and introduce customers to your brand and offerings." Keeping humans in the loop during creation and personalization will create a more human, personal experience for customers. People can spot fake or "dumb" bots — so keeping people involved throughout is a must!

How Generative AI Is Changing the Future of Work

By Tony Uphoff
CEO POV

AI HYPERAUTOMATION
TOP 10
Impact Enabler
Acceleration Economy network

My career has given me a ringside seat at every technology revolution of the last 30 years. It's been remarkable to bear witness to so many new technologies as they were introduced; some that went on to truly change the world and others that faded into obscurity. Hey, I think I may still have my Palm Pilot in a drawer somewhere!

We are currently in the midst of a technology revolution with the recent introduction of ChatGPT and the rapid development of generative AI. The resulting impact is resonating far earlier and more significantly than any other new technology introduction that I can recall.

Where and How Work Is Already Changing

As the progeny of cutting-edge large-language models (LLMs) like OpenAI's GPT-4, generative AI is transforming industries and the future of work in ways that we could not have fathomed just a few years ago. Here are just three areas where this is already happening:

Creative industries: The creative industries have long been considered the bastion of human ingenuity and imagination. However, generative AI is now demonstrating the capacity to be both a collaborator and a creator. AI-generated content, from copywriting and website design to video game music and visual art, is blurring the lines between human and machine-made creations.

Take, for example, the burgeoning field of AI-assisted design. Generative AI can generate thousands of design options in a matter of minutes, drastically reducing the time and effort required by human designers. This newfound efficiency, and scale, is not only allowing creative professionals to dedicate more time to refining and perfecting their work, but also enabling them to explore new realms of creative expression.

Moreover, the democratization of creative tools has created a new class of "citizen designers" — individuals with little to no formal design training who are leveraging AI-powered applications to bring their visions to life.

Decision-making and management: As the sheer volume of data available to businesses continues to grow exponentially, so, too, does the need for faster and more effective decision-making. Generative AI is emerging as a powerful tool, transforming the way businesses strategize, innovate, and adapt.

With AI-powered decision engines, organizations can quickly analyze vast amounts of information, identify patterns, and generate actionable insights — far beyond the capabilities of even the most experienced human experts. In addition, generative AI can simulate complex scenarios and predict potential outcomes, providing executives with the foresight needed to make more informed decisions and avoid costly mistakes.

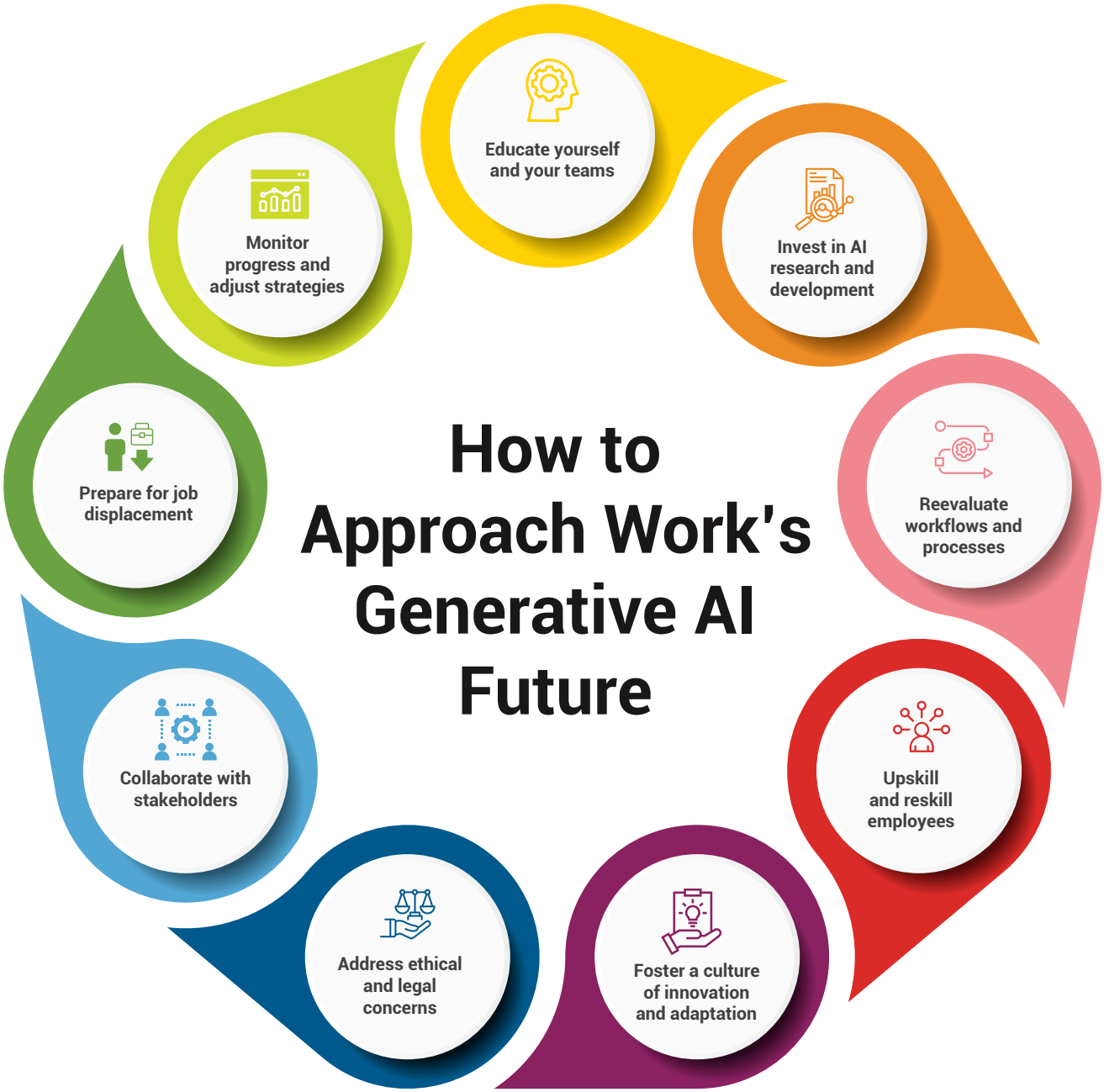
Generative AI is also becoming an invaluable asset in human resources. By analyzing workforce data and organizational structures, these AI systems can recommend optimal team compositions, identify skill gaps, and even predict attrition rates. Such insights can help organizations build stronger, more resilient, and more diverse teams, ultimately driving better business results.

Skill Development and the workforce: As generative AI continues to reshape entire industries, the nature of work itself is changing, necessitating a reevaluation of the skills required for success. Many tasks that were once the exclusive domain of humans are now performed by AI, leading to fears of job displacement and a widening skills gap.

While it is true that some roles may become obsolete, it is equally important to recognize the tremendous opportunities that generative AI presents. In much the same way that the internet created entirely new categories of jobs, generative AI will give rise to new industries and roles that we have yet to conceive.

How to Approach Work's Generative AI Future

To prepare for how generative AI will change the future of work, business leaders should consider the following strategies:



Educate yourself and your teams: Business leaders should develop a strong understanding of generative AI technologies and their potential applications. This will help them to identify opportunities to leverage the technology within their organization and to prepare their teams for new workflows and responsibilities.

Invest in AI research and development: Businesses should consider investing in AI research and development, either by developing in-house expertise or by partnering with AI-focused companies and the related partners ecosystem.

Reevaluate workflows and processes: Leaders should review their existing workflows and processes to identify areas that could be improved or automated using generative AI. This might involve reorganizing teams, automating certain tasks, or integrating AI tools into existing systems.

Upskill and reskill employees: As generative AI is likely to change the nature of certain roles, it's crucial for business leaders to ensure their employees have the necessary skills to adapt. This might involve offering training programs or supporting employees in learning new skills.

Foster a culture of innovation and adaptation: To succeed in a world where generative AI is increasingly prevalent, businesses must be able to innovate and adapt quickly. Leaders should encourage a culture that embraces change and experimentation, empowering employees to find new ways of working with AI technologies.

Address ethical and legal concerns: Generative AI raises new ethical and legal questions; business leaders should be proactive in addressing these issues. This might involve developing policies around data privacy, security, and AI usage, as well as ensuring that AI systems are transparent and fair.

Collaborate with stakeholders: To fully realize the potential of generative AI, businesses should collaborate with stakeholders, including customers, suppliers, and regulators. This can help to identify new opportunities and address potential concerns.

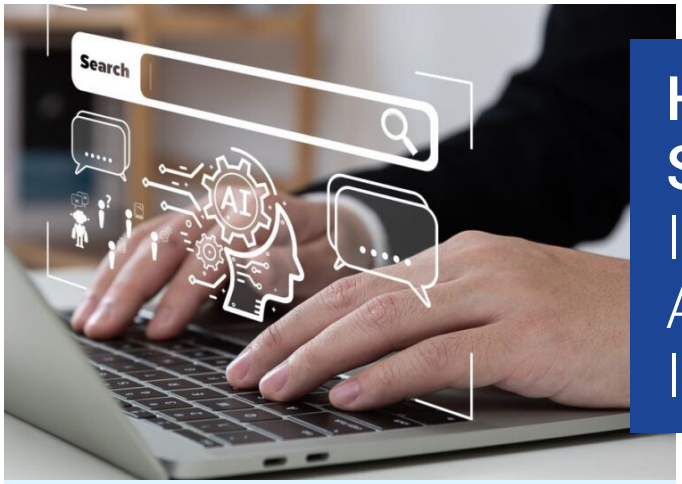
Prepare for job displacement: While generative AI holds the potential to create new jobs, it may also displace some existing roles. Business leaders should be prepared to manage this transition by offering support to employees whose jobs may be affected. This includes everything from providing severance packages to job placement assistance to retraining opportunities.

Monitor progress and adjust strategies: As the AI landscape continues to evolve, business leaders should regularly assess their strategies and adjust as needed. This will help them to stay ahead of the curve and capitalize on new developments in generative AI.

Final Thoughts

Generative AI is an exciting and disruptive new technology that is still in early development. It's clear, however, that it will continue to change work in profound ways. Business leaders cannot ignore it. Start now by educating yourself and your organizations on how to harness the power — cleverly, ethically, and responsibly — of this remarkable new technology.

Whether it is FOMO (fear of missing out) or FOMU (fear of messing up), every business tech leader is pulling together their teams to understand the impact of generative AI on their business. Many articles have been published on AI technology and the myriad of applications, but few address the next step — what does this mean for the talent and workforce we will need to compete? Tony's analysis provides both a sense of perspective and a rational approach every leader can take, now. Addressing AI-accelerated workforce needs has short- and long-term ramifications for everything from hiring to learning and development to organizational structure. His best advice in this analysis is urging leaders to "start addressing the workforce requirements now."



How to Know If a Software Solution Is Actually AI-Driven or If It's Just Hype

By Joanna Martinez
Supply Chain POV

AI HYPERAUTOMATION — TOP 10 — Impact Enabler — Acceleration Economy network

In a recent conversation with the CEO of a software start-up, I asked if his product incorporated artificial intelligence (AI) or machine learning (ML). There was a long hesitation, and he responded "yes," somewhat tentatively, almost as though that was the response he suspected I would want to hear. The fact that he had to think about it made me pause. His company provides a service that aggregates data useful to a certain industry. It looked pretty much like a straight mathematical calculation, a spreadsheet in high gear. A very helpful service, but no apparent AI at play.

I chuckled at his response because today it seems as though everyone tells you that their product is AI-based. It has even spawned the term, "AI washing," which is the claim that an application uses AI when in fact it does not.

Don't Get Lost in the "AI Wash"

Go to any conference, and AI washing abounds. I'm never sure if it's malicious or a training issue, where the sales team just doesn't understand what AI is all about. If the sales team doesn't understand it, how are you going to understand it? Short of getting into the guts of the training models, datasets, and software development, how do you know what you're looking at is truly AI? So, in the spirit of "buyer beware," this analysis lays out some considerations, steps, and questions you can ask to be more "buyer aware" on your AI shopping journey.

Check the Company Website

Sometimes it feels as though "artificial intelligence" is the word of the year. Because it's being discussed and debated in so many aspects of life, a company that uses AI will reference it on and throughout its website as a key feature. Any company employing AI is highly likely to be promoting this fact to ensure that potential clients are aware of it.

Ask for the Value Proposition

Similarly, representatives from the company should be able to clearly articulate the value that AI brings to the product they are selling you. They should be able to not only describe the problem they are solving, but also quantify how their product differs from competitors.

You Get What You Pay For

If you are looking at multiple providers across a category, the AI solution will likely not be the lowest cost. AI requires a specialized, highly skilled team and needs to operate on the latest platform to support it; this will likely result in a higher price point than a similar non-AI product.

Vet the Development Team's Bench Strength

Any enterprise with an AI solution will have a development team with significant bench strength. This team will be deep in AI talent and the provider will likely be making a big splash when a new AI practitioner joins the firm. The website bios and LinkedIn profiles of key people on the development team should clearly reference AI or machine learning. Look for data scientists, engineers, and architects. These terms should be in the language they use and the examples they cite. They should be able to explain how their system uses AI and ML to adapt to your specific environment and business, along with how it delivers desired outcomes.

Look for Data Complexity

A little self-reflection here: What's the result you are looking for? If the problem you are trying to solve is a straightforward task with no need for sophisticated algorithms or models, an AI-based solution may be overkill. But if it isn't, you'll need to look for AI that's deep, broad, and powerful.

Software that is AI-driven will have many moving parts. It will be pulling data from multiple sources. The more data that is processed over time, the more the model adjusts and the "smarter" it gets, yielding ever-improving results. Pre-AI, a predictive model on sales, might extrapolate history or consider

demographics. An AI-based software solution will factor in data from many additional and disparate sources, perhaps adding weather, competitive information, Consumer Price Index (CPI) predictions, growth information about key customers, and other data points. If the software is not extracting data from large datasets, it's not using AI.

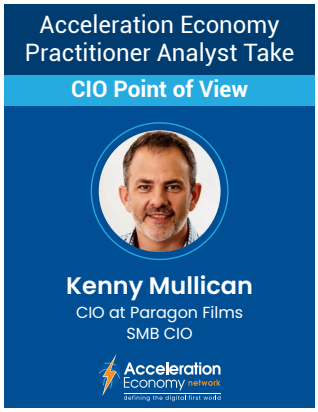
Ask for Endorsements from Actual Clients

This is the piece we always say we are going to do, and rarely follow through on. The supplier should be showcasing customers who have quantifiable results, and you should be calling these customers. Remember, it's not the technology you are buying; it's the outcome.

But Wait, Do You Actually Need AI?

Before I wrap up, a quick reminder: Not every piece of technology needs AI or machine learning capabilities. Most routers, barcode scanners, GPS systems, and point-of-sale (POS) systems , for example, perform basic functions perfectly well and their output doesn't build on past results. So take a close and informed look at each and every piece of technology you are considering for an upgrade, and make sure that AI will actually make it better, faster, and smarter.

Bottom line? The next time you are contemplating a purchase, don't just take the salesperson's "AI" word for it. There's plenty of hype out there, but increasingly there's even more that's mind-blowingly powerful. Use this list as a guide and "kick the tires" a bit. It will help you make the right decision for your business.



As the hype surrounding AI has hit a fever pitch, it is worth looking under the covers to see if AI is really adding value to the products you are considering. There are definitely use cases where AI can be a game changer, but even in those cases, you want to find out how AI is being used. Joanna's analysis gives some straightforward ways to look past the marketing buzzwords and get the real story.

From Malware Detection to Predictive Analytics, How AI Enhances Core Cybersecurity Functions

By Kenny Mullican
Cloud Expert POV

CYBERSECURITY
TOP 10
Business Enabler
Acceleration Economy network

A few years ago, a fellow CIO reached out to me for advice on choosing between two cybersecurity-managed service providers. Since my company had experience working with both providers, I could offer a fair comparison. After discussing her company's options, she mentioned that her company was likely going with provider X, primarily because it claimed to use artificial intelligence (AI) in its product, while the other company didn't mention the technology at all. She didn't have much additional information, but the AI aspect appeared to be a significant differentiator in her company's decision-making process.

This experience stayed with me, and as AI has gained prominence, it raises a question: Is AI genuinely a crucial component of a cybersecurity technology offering, or is it merely a buzzword that companies use to attract potential customers?

Cybersecurity With and Without AI

Indeed, AI does play a vital role in today's cybersecurity technology. However, it's essential to grasp how AI is effectively employed in cybersecurity to make informed choices when selecting a technology product or provider. I took a look at several cybersecurity technology features that I have worked with for years and looked into how incorporating AI into them might enhance their effectiveness. Here's what I found:

Anomaly Detection

Without AI: Security analysts manually monitor logs, network traffic, and system behavior, relying on predefined rules and thresholds to identify anomalies. This process can be time-consuming and may not catch new or evolving threats. Whenever I see demos of rule-based software, I think: "Who is ever going to have time to sit and write all these rules manually?"

With AI: AI can process massive amounts of data in real time, detecting threats early and reducing potential damage. AI can identify new and evolving threats more effectively than manual methods. As a CIO with a small staff, I need the cybersecurity software we use to constantly adapt to the threat landscape automatically, without my team having to constantly configure it.

Malware Detection and Prevention

Without AI: Traditional antivirus solutions rely on signature-based detection, which requires constant updates to identify new malware variants. This approach is very reactive. Someone has to have already found the malware, identified it, and provided an update that mitigates the threat.

With AI: AI-powered solutions can analyze file characteristics and behavior patterns to detect and prevent malware, including previously unseen variants. AI offers better protection against emerging threats. This is one benefit that gives me peace of mind, because I am much more concerned about a brand new threat that doesn't match any known signature. Technology that can detect these zero-day threats, as they are often called, is crucial.

Threat intelligence

Without AI: Security analysts gather and analyze threat intelligence from various sources manually, which can be time-consuming and might miss crucial information. There are many good threat intelligence sources — mostly services and news outlets — that you can subscribe to. However, the prospect of sifting through all of them to try and determine which ones were relevant to my company in an era when even the threats themselves are increasingly AI-supported, seems daunting and offers diminishing returns.

With AI: AI can automatically collect, analyze, and prioritize threat intelligence, helping organizations stay updated on the latest threats and improve their security posture more efficiently. This is what AI is good at, and getting better at: sifting through large amounts of data and quickly determining what information is relevant to my needs.

Predictive Analytics

Without AI: Security teams rely on historical trends and expert judgment to predict future threats, which may not accurately anticipate new attack vectors.

With AI: AI can analyze historical data and identify patterns to predict future threats, enabling proactive defense and more effective resource allocation. The bad actors are constantly trying to stay ahead of the defensive technology. It is critical that the software be able to predict the next move rather than just react based on historical trends.

User and Entity Behavior Analytics (UEBA)

Without AI: Identifying insider threats or compromised accounts may involve manual monitoring and analysis, which can be labor-intensive and less effective. I've tried to think of all the different ways that a user might "do something unexpected" and it is a very complicated process.

With AI: Because it's been trained on so much user and entity behavior data, AI can monitor and analyze user and entity behavior patterns more efficiently and accurately identify potential threats, and at scale. It is much better to let the software learn what "expected" behavior looks like, so anything outside of that can raise a flag.

What to Look for in an AI Cybersecurity Provider

AI offers numerous enhancements to existing cybersecurity technology and practices, and the features mentioned above serve as a solid foundation for a requirements list. However, when considering potential providers for your AI cybersecurity transformation, it's crucial to ask them how their technology addresses these aforementioned aspects, not to mention the following:

1. **Integration and compatibility:** Ensure that the vendor's AI-driven cybersecurity solutions can be seamlessly integrated with your existing IT infrastructure, security tools, and processes. Compatibility with current systems is crucial for a smooth implementation and maximum effectiveness. It can be discouraging to find out after you have purchased a solution that it doesn't "play well" with the rest of your technology stack.
2. **Data privacy and compliance:** Ensure the vendor adheres to data privacy regulations and industry standards applicable to your organization. AI-driven cybersecurity solutions may process large amounts of sensitive data, so it's crucial to verify that the vendor has robust data protection policies and practices in place.
3. **Training and support:** Assess the vendor's commitment to providing training, support, and resources for your organization. This includes understanding how it will help you manage the AI-driven cybersecurity solutions, as well as provide ongoing support for any issues or questions that may arise.
4. **Transparency and explainability:** Assess the vendor's commitment to providing transparent and explainable AI solutions. This is important for understanding the reasoning behind AI-generated decisions and maintaining accountability within your organization. I think this may be difficult for some providers, as they may be afraid to divulge too many details of how their technology works. Even if you encounter resistance, it's important to find out as much as you can.
5. **Continuous improvement:** Ensure that the vendor is committed to continuously auditing and improving their AI models and algorithms, as well as staying updated on the latest advancements in AI and cybersecurity. We've seen how rapidly AI technology has progressed recently. There's no excuse for any provider to refrain from making its technology better.

Final Thoughts

AI has become a vital component of effective cybersecurity strategies, offering numerous advantages over traditional approaches. By understanding the ways that AI can enhance security measures and considering key factors when selecting a provider, organizations can harness the technology's ability to better protect their digital assets and stay ahead of emerging threats. As a CIO, recognizing the importance of AI in cybersecurity and making informed decisions is not only crucial for the success of your organization, but also a testament to your commitment to staying at the forefront of technological advancements.

Acceleration Economy
Practitioner Analyst Take

CISO Point of View

Frank Domizio
Deputy CISO
Centers for Medicare & Medicaid Services

Acceleration Economy network
defining the digital first world

I love how Kenny brings forward the power of AI when it is applied to different elements of our cybersecurity stacks. AI can help us more efficiently sift through the mounds of security telemetry that our teams are presented with each and every day. In the hands of a well-trained person, AI can really be a force multiplier in helping to increase the security of our environments. One thing to consider, you do not want to use AI for the sake of using AI. This is a phenomenon I like to call "deploying a buzzword." Kenny hit on a lot of the great applications there are for AI in your security stack. There is no need to shoehorn AI into your environment just to say you're using AI.

How to Maintain Cybersecurity as ChatGPT and Generative AI Proliferate

By Bill Doerrfeld
Developer & Cybersecurity POV

CYBERSECURITY
TOP 10
Business Enabler
Acceleration Economy network

The usage of apps such as ChatGPT by the workforce is growing. Powered by large language models (LLM) like GPT-3.5 and GPT-4, the generative AI chatbot is being leveraged by employees in countless ways to create code snippets, articles, documentation, social posts, content summaries, and more. However, as we've witnessed recently, ChatGPT presents security dilemmas and ethical concerns, making business leaders uneasy.

Generative AI is still relatively untested and full of potential security concerns, such as leaking sensitive information or company secrets. ChatGPT has also been on the hot seat for revealing user prompts and "hallucinating" false information. Due to these incidents, a handful of corporations have outright banned its use or sought to govern it with rigid policies.

Below, we'll consider the security implications of using ChatGPT and cover the emerging security and privacy concerns around LLMs and LLM-based apps. We'll outline why some organizations are banning these tools while others are going all in on them, and we'll consider the best course of action to balance this newfound "intelligence" with the security oversight it deserves.

Emerging ChatGPT Security Concerns

The first emerging concern around ChatGPT is the leakage of sensitive information. A report from Cyberhaven found 6.5% of employees have pasted company data into ChatGPT. Sensitive data makes up 11% of what employees paste into ChatGPT — this could include confidential information, intellectual

property, client data, source code, financials, or regulated information. Depending on the use case, this may be breaking geographic or sector-specific data privacy regulations.

For example, three separate engineers at Samsung recently shared sensitive corporate information with the AI bot to find errors in semiconductor code, optimize Samsung equipment code, and summarize meeting notes. But divulging trade secrets with an LLM-based tool is highly risky since it might use your inputs to retrain the algorithm and include them verbatim in future responses. Due to fears about how generative AI could negatively impact the financial industry, JPMorgan temporarily restricted employee use of ChatGPT, and it was followed by similar actions from Goldman Sachs and Citi.

ChatGPT also experienced a significant bug that leaked user conversation histories. The privacy breach was so alarming that it prompted Italy to outright ban the tool while it investigates possible data privacy violations. The app's ability to recall specific pieces of information and usernames is another great concern for privacy.

Furthermore, since ChatGPT has scoured the public web, its outputs may include intellectual property from third-party sources. We know this because it turns out that it's pretty easy to track down the exact source used in the model creation. Known as a training data extraction attack, this is when you query the language model to recover individual training examples, explains a Cornell University paper. In addition to the skimming of training data, the tool's ability to recall specific pieces of information and usernames is another great concern for privacy.

Recommendations to Secure ChatGPT Usage

A handful of large corporations, including Amazon, Microsoft, and Walmart, have issued warnings to employees regarding the use of LLM-based apps. But even small-to-medium enterprises have a role in protecting their employee's usage of potentially harmful tools. So, how can leaders respond to the new barrage of ChatGPT-prompted security problems? Well, here are some tactics for executives to consider:

Implement a policy governing the use of AI services: New generative AI policies should apply to all employees and their devices, whether on-premises or remote workers. Share this policy with anyone with access to corporate information or intellectual property (IP), including employees, contractors, and partners.

Prohibit entering sensitive information into any LLM: Ensure employees know the dangers of leaking confidential, proprietary, or trade secrets into AI chatbots or language models. This includes personal identifiable information (PII) too. Enter a clause about generative AI into your standard confidentiality agreements.

Ensure employees are not leaking intellectual property: As with clearly sensitive information, consider also limiting how employees feed IP into LLMs and LLM-based tools. This might include designs, blog posts, documentation, or other internal resources that are not intended to be published on the Web.

Follow the AI's guidelines: Reading up on the LLM tool's guidelines can help inform a security posture. For example, the ChatGPT creator OpenAI's user guide for the tool clearly states: "We are not able to delete specific prompts from your history. Please don't share any sensitive information in your conversations."

Consider generative AI security solutions: Vendors like Cyberhaven have created a layer to keep confidential data out of public AI models. Of course, this may be overkill — simply communicating your company policy is hopefully enough to prevent misuse.

Halt AI usage completely: This option is not off the table. Many organizations have put strict temporary bans on ChatGPT while the industry weighs the repercussions and ethical concerns. For example, in an open letter, Elon Musk and other AI experts have asked the industry to pause giant AI experiments for the next six months while society grapples with its repercussions. (Watch what our practitioner analysts had to say on the letter signed by Musk and others).

The Move to AI

Looking to the future, the move toward greater AI adoption seems inevitable. Acumen Research and Consulting predicts that by 2030, the global generative AI market will have reached $110.8 billion, growing at 34.3% CAGR. And many businesses are positively integrating generative AI to power application development, customer service functions, research efforts, content creation, and other areas.

Due to its many benefits, disallowing generative AI completely could put an enterprise at a disadvantage. Thus, leaders must carefully consider its adoption and implement new policies to address possible security violations.

Acceleration Economy Practitioner Analyst Take

CISO Point of View

Robert Wood

Centers for Medicare & Medicaid Services

Acceleration Economy network

defining the digital first world

The thing that sticks out to me from Bill's article is the concept of AI hallucinating false information. The confidence that people place in technology, especially when it's heralded as revolutionary, introduces tremendous risk for anyone building a process on top of such technologies. It goes to show that a well-designed process with the appropriate controls in place is not going anywhere soon.