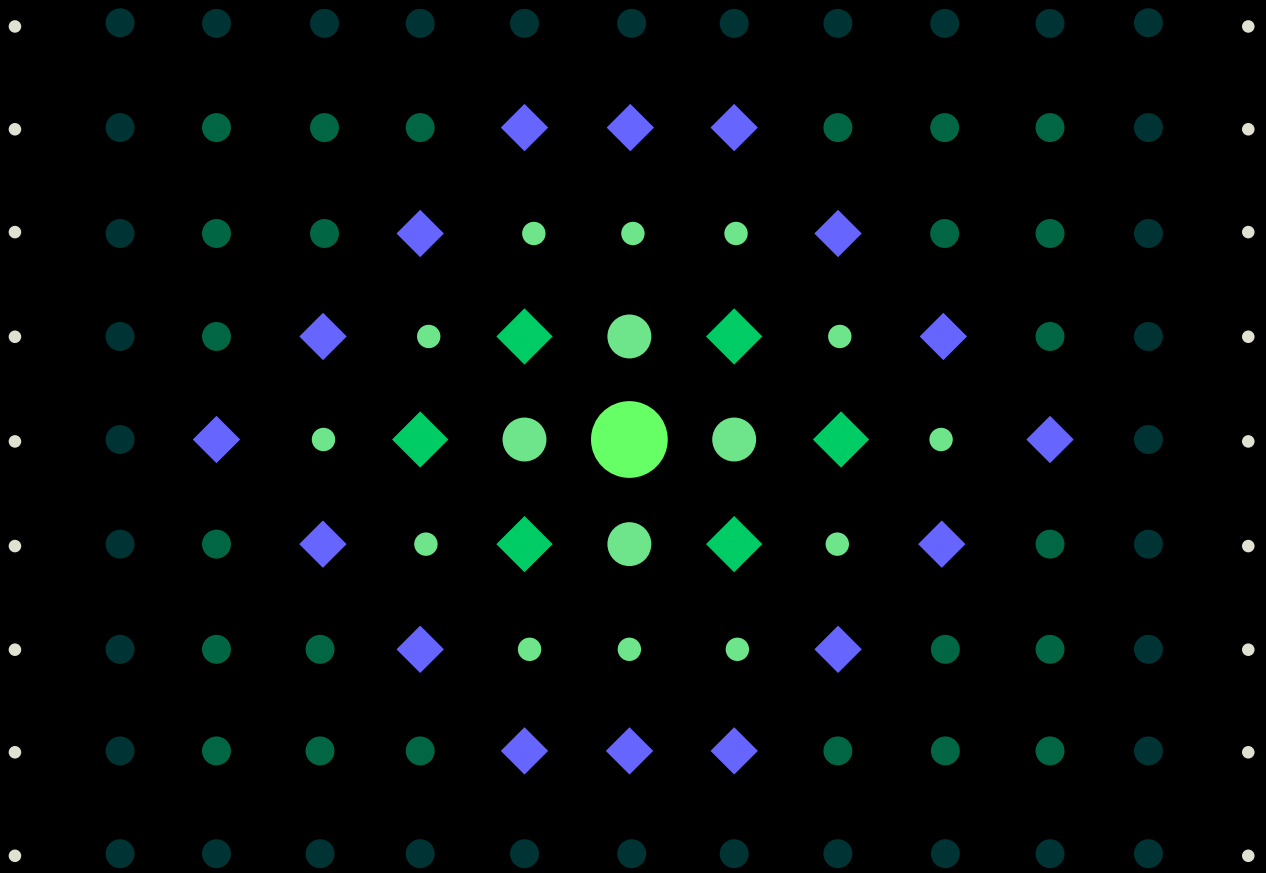
CYERA

EBOOK

Business Advancement Through Generative AI: A Secure Transition



www.cyera.io | info@cyera.io

Table Of Contents

Introduction

The unprecedented, rapid advancement of technology over the last thirty years has surpassed all expectations. From the internet to the smartphone, as a society, we have embraced the transformative power of tech. Artificial intelligence (AI) is the latest innovation disrupting convention—and already, information about AI is rife with misinformation and fear-mongering.

Think back to the advent of email or the cloud. When first introduced to the public, these technologies inspired both excitement and fear, much like AI has today. There were ample security concerns about email, the cloud, and the internet at large. But many will argue the benefits of these technologies outweighed the concerns. With the right practices in place, we can minimize the risks of AI usage.

Mitigating risk as businesses experiment with AI is a primary concern for security leaders. IP leakage, privacy violations and misuse relative to information governance policies can result in compliance violations, fines, and a loss of customer trust. Cyera empowers you to protect the data you need, minimize the data you don't, and optimize your Amazon Web Services (AWS) cloud spend in the process.

Cyera continuously discovers and automatically classifies all of your data in AWS – including finding data you didn't know existed, but that might be in scope for your next generative AI project. The platform identifies sensitive data at risk and pinpoints security and compliance exposures, then remediates those exposures to keep your business moving forward securely.

Cyera provides detailed context on your data, identities, and access across S3, RDS databases and both databases and file servers deployed over EC2. We also show you how data is created, used, and moved across environments to secure your entire data landscape from a single, operational data security platform. With Cyera, you can understand the risks and benefits each piece of data represents, freeing you to build on.

Defining Generative AI and Its Business Value

Generative AI is the combination of artificial intelligence, predictive analytics, and deep learning. It's essentially an engine of creation—producing highly relevant outcomes and critical insights by drawing from a body of data. In today's fast-paced world, businesses recognize the potential of generative AI in delivering effective solutions to various challenges.

Here are some impactful applications of generative AI:

Content Creation

Marketing teams can harness generative AI models, such as GPT-3, to generate blog posts, social media content, product descriptions, and more with ease. This innovative approach enables efficient content production while allowing marketing professionals to focus on other important tasks, such as strategizing new campaigns and analyzing past performance.

Lead Generation

Chatbots and automated conversations powered by generative AI can collect valuable information from website visitors and potential leads. These tools can engage users in focused discussions and guide them through the initial stages of the sales process, optimizing outcomes and providing valuable data for future strategies.

Customer Service

Generative AI models can expedite sales and customer service by automating email and instant messaging responses to customers. This allows for more timely, consistent service delivery. It also enables businesses to handle a larger volume of requests without overwhelming staff.

Personalized Recommendations

A generative AI model can examine data like browser cookies and purchase history to generate hyper-personalized product, service, or content recommendations. This customized approach can assist firms in increasing client satisfaction and conversions.

Despite its compelling benefits, generative AI introduces a host of potential data-related issues, such as data security and privacy concerns. Organizations must develop policies and follow best practices to ensure the safe and secure deployment of generative AI technology.

Recognizing the Data Security Challenges Introduced by Generative AI

Recent findings from a Forrester Consulting report underscore the need for vigilance when leveraging the power of generative AI. According to the study, an alarming 57% of security directors identified the misuse of generative AI as the primary threat concerning potential data breaches within companies.

Here are some of the top data security and privacy concerns:

Collection of Personally Identifiable Information (PII) via Chatbots

Chatbots changed customer service forever. Their ability to respond to customers in real-time with relevant information makes them attractive to consumers, and enterprises that implement chatbots save time and money. However, in order for chatbots to work, they need data. This data, which includes but is not limited to names, email addresses, phone numbers, or even more sensitive data like social security numbers or financial information, has the potential to increase data exposure and compliance risks for your organization.

Internal Risk Potential

Entering PII or intellectual property (IP) into an AI system can compromise compartmentalization efforts. When employees input sensitive or protected data into an AI system, they inadvertently risk exposing it to unintended internal actors. This breach can undermine active security measures, increasing risk.

Use of PII in AI models

If your enterprise is interested in training its own AI model, it is crucial to follow PII guidelines when selecting its training data. This most often necessitates strict adherence to privacy guidelines, including informed consent for AI algorithm enhancement. Failure to comply exposes businesses to penalties under laws like the previously mentioned CCPA or GDPR.

Security Concerns Within the Tools

Sometimes, the risk isn't inherited from your own organization's actions. It comes from the tools you use.

In March 2023, OpenAI was forced to temporarily deactivate ChatGPT to rectify a defect that allowed users to view the chat titles from another user's concurrent chat history. The same glitch led to a data leak, exposing the names, email addresses, and credit card information of GPT Plus subscribers. A third party, Group-IB, reported that they detected information from over 100,000 compromised ChatGPT accounts for sale on darknet marketplaces.

With thoughtfully implemented data practices and robust protective measures, we can navigate and control these concerns effectively.

Mitigating the Risks of Generative AI

Implementing rigorous, industry-aligned best practices helps organizations mitigate AI misuse risks. Building thoughtful oversight into the AI generation process, conducting regular audits for content and data security adherence, and maintaining a robust ethical framework are all critical in ensuring that generative AI serves its rightful role as a catalyst for growth.

Below are a few key data security strategies enterprises can implement today:

Conduct a Detailed Data Inventory and Risk Assessment

Before you can implement data security measures, you need to understand what you're protecting. Gaining insight into the breadth of your organization's data and pinpointing potential weak spots are crucial steps toward formulating custom security measures that fit the distinct requirements of your business.

Classify Your Data

Organizations can better manage data security by classifying data as PII, financial data, IP, etc. This can be used to create Standard Operating Procedures (SOPs) for AI usage. For example, your organization could implement a policy stating that absolutely no PII can be used in generative AI applications.

Educate and Inform About Appropriate Usage

Appropriate AI usage is crucial for data security. It is imperative that employees are aware of the risks associated with AI and are educated about appropriate use. Clear, comprehensive guidelines can ensure that everyone in the organization uses AI tools securely and responsibly.

Leverage Risk Mitigation Tools

Solutions like SafeType, which can flag and anonymize sensitive data inputted into ChatGPT, or enterprise browsers are excellent additions to data security measures.

Implement Human Oversight

Despite all technological precautions, human oversight remains indispensable and should be implemented where necessary.

Risks associated with generative AI are real, but by diligently following these strategies, organizations can safely leverage AI's potential while mitigating threats.

Leading the Future of Generative AI with Lessons from the Past

Although the advent of AI has undoubtedly re-stoked some of the fears felt in response to previous technological milestones, the human capacity for adaptation alongside broader technological development affirms that, even as AI continues to shape our world, we are well-equipped to confront the security challenges that lay ahead.

Establishing the Data Security Foundation with Cyera

> "Cyera's vision is to enable every business to realize the full potential of their data using AI—collaboration, connection with customers, insights that fuel innovation—to power a new era of development, growth, and productivity."
>
> Yotam Segev, Cyera Co-Founder and CEO

Harnessing the benefits of generative AI while maintaining a strong security posture is achievable. Cyera helps businesses securely explore generative AI, offering unparalleled capabilities to identify and fortify vulnerabilities and create the transparency needed to secure the data. By leveraging Cyera, businesses can automatically discover, classify, add context to data while informing their teams about the types of data ingested by generative AI platforms like ChatGPT.

Generative AI is the latest technology disrupting the status quo, and with that comes reasonable concerns about its safety and efficacy. Fortunately, enterprises are well-positioned to take advantage of AI with the right best practices, controls, and partnerships.

About Cyera

Cyera is the data security company that gives businesses deep context on their data, applying proper, continuous controls to assure cyber-resilience and compliance. Cyera takes a data-centric approach to security across your data landscape, empowering security teams to know where their data is, what exposes it to risk, and take immediate action to remediate exposures. Backed by leading investors, including Sequoia, Accel, Cyberstarts and Redpoint Ventures, Cyera is redefining how companies secure data in the cloud. To learn more, visit www.cyera.io

Trusted By

LifeLabs · ACV · Cboe · Mercury Financial · Veolia · Cystic Fibrosis Foundation · Advance · UTA

aws PARTNER Security Software Competency