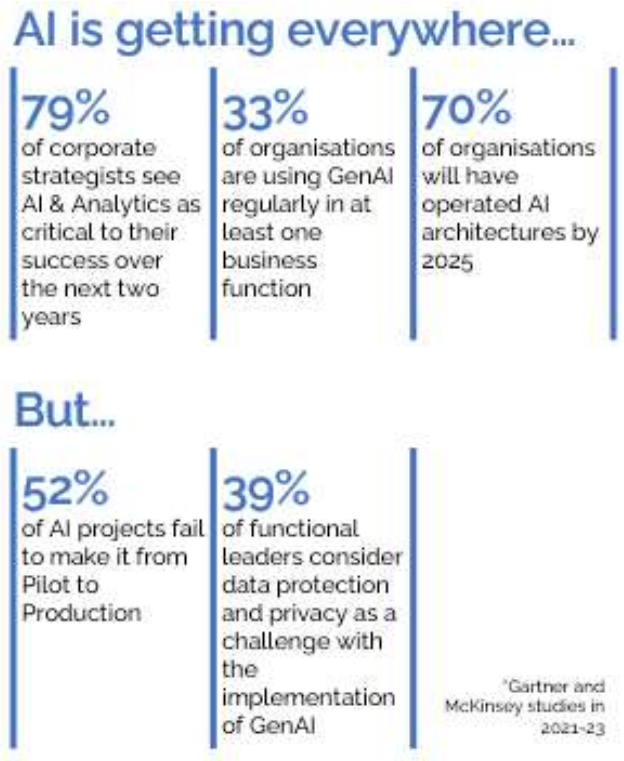
Digital Trend #3: Power of AI

Digital Trends – The Power of AI

In this article, we will explore the gathering momentum of Generative AI (GenAI). We look at the challenges and preparation that organisations have to consider when looking to make best use and secure use of GenAI, or even run their own implementations. We also describe a number of use cases that we have seen in the market that have particular relevance to the corporate IT department.

The rise of AI is pervasive

In Ronald's recent LinkedIn article on the Power of AI, the examples provided showcase the diverse ways in which companies are leveraging AI and machine learning to drive innovation and to enhance productivity and efficiency of their operations. Looking ahead, we can anticipate continued growth and change towards adoption of AI applications, particularly in areas such as explainable AI, responsible AI and AI ethics, as well as increased adoption of AI for sustainability and environmental initiatives.



Challenges to the growth of Gen AI

Many of the leaders of tech Innovation have expressed confidence about the once-in-a-lifetime transformative nature of GenAI. Mark Zuckerberg emphasised the importance of building "too fast rather than too late," to avoid falling behind in the AI race. Similarly, Google's Sundar Pichai stressed to shareholders and analysts that the risk of underinvesting is dramatically greater than the risk of overinvesting. Most investments have been funnelled into three areas so far:

- Hardware (AI chips in particular)
- Software (primarily in the form of Large Language Models)
- Datacentres (space expansion)

Clearly, Big Tech is taking the long view, but while these investments are necessary, here at Atos, we believe they will not be the only drivers of widespread GenAI adoption. Based on our experience working with clients on numerous GenAI initiatives, we have observed that projects so far have only had relatively small budgets, as large enterprises wait to see demonstrable ROI before investing further.

In a recent blog post, Adil Tahiri, Atos' Head of CTO and Client Advisory Group gave his view that this will not change any time soon. He stated:

- The AI market is still in it's early stages, with many enterprises experimenting with pilots and proofs of concept that are naturally limited in scope and budget.
- Generative AI adoption is driven by individual use cases rather than a broad, mass-market product or service.
- Projects are relatively high-touch, because they require high levels of customisation to adapt the tech to business-specific context and unique needs.
- Similar to cloud, GenAI will be gradually integrated with existing processes and workflows. However, given the deeper level of integration required with people and processes, it may take longer to become mainstream.
- There is still reluctance based on the well-documented ethical, technical, sustainability and privacy challenges — as well as the possibility of displacing human workers (we talk about this more in our article for Autonomous Operations).
- Given today's macroeconomic uncertainty, enterprises want "quick wins" with immediate impact and fast ROI — neither of which are certain with GenAI.

So, what should businesses do? Invest now and take the short-term hit in hopes of an exponential return down the road, or ignore the advice of the Big Tech leaders and take a "wait and see" approach? It's hard to predict whether GenAI will live up to the hype, but there are a few key factors that could help the cause:

1. Convergence & scale: It may only be possible to reach the full potential of GenAI by the aggregation of numerous small-scale projects across different industries and use cases, to generate a significant overall market.

2. Holistic investment: Sustained investments will be required, but not just in hardware and software. Equal attention must be directed to creating adoption levers through education and skill development, policy, and tax incentives or grants for companies adopting GenAI, more VC funding for AI start-ups, or even consortiums made up of competitive GenAI players.

3. Patience: We urgently need a reset of expectations across the board, among enterprises, technology providers, analysts and investors. GenAI is a powerful tool, but it should not be forced. Using it properly takes work, careful planning and attention to details.

Here at Atos, we have created numerous proofs of concept and use cases across multiple industries, and we firmly believe that GenAI is truly a game changer. We are no longer seeing just potential, but actual results. However, we also believe that the future isn't just about technological advancements — it's equally about ubiquitously embedding it into everyday business operations to create real and widespread impact. With Gen AI, the best results will not be achieved by the most powerful platform. It takes a complete approach that considers context, goals and constraints — enabling strategy and culture to evolve together. An organisation's culture is likely to determine the speed, success or failure of adoption, despite careful planning and due diligence, and will have a greater influence than

the technology itself. The critical adoption challenges are resistance to change, risk aversion, siloed structures and a lack of GenAI literacy that leads to a fear of the unknown. Overcoming these challenges requires a culture change which will occur gradually and at varying speeds across different organisations. This is why we believe the best results will not be achieved with the most powerful platform. It takes a complete ecosystem that includes solution accelerators, consultancy services, industry-specific knowledge, and behavioural change management to overcome AI adoption challenges. The right approach to delivering effective GenAI is co-creation between enterprises and their technology partners, taking into consideration the proper context, business goals and constraints — enabling strategy and culture to evolve together.

GenAI use cases for the IT Department

1. Atos Proactive Experience Center

As mentioned in a couple of other Digital Trends responses for Heineken, Atos has an industry-leading relationship with Nexthink. Atos manages more than 1.6 million Nexthink-deployed devices across the globe, for more than 30 customers. Atos is the first SI to achieve such a large installed base, Atos is Nexthink's #1 Managed Services Strategic Partner, and has the highest rate of adoption of the tools globally, with 200 use cases. Atos awarded as Nexthink's 'Global Partner of the Year' in 2021-22.

A unique and strong co-innovation programme exists between the two organisations, and using Nexthink's capabilities, Atos has developed a set of services called 'Proactive Experience Center',

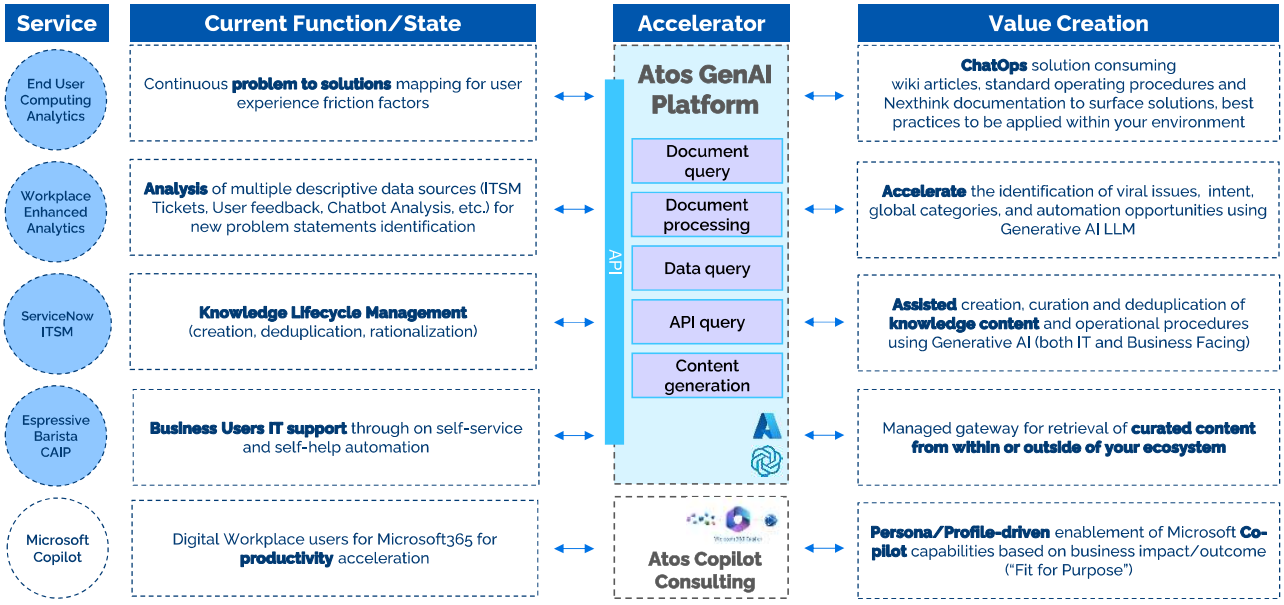
Atos's Nexthink platforms work to monitor the true usability of End User devices and applications, which are analysed through sophisticated AI tools, and give predictive and proactive insight into potential issues so they can be resolved before they occur. Data captured on a continuous basis cover workplace analytics, proactive remediations and self-healing tools, to record resulting 'Device Experience (DEX) Scores', which indicate the ability for individual end users to use their IT in an efficient, productive and stress-free manner.

Information that can be continuously captured and analysed for DEX include:

- Hardware Device Performances and Thresholds
- Browser performances
- User interactions with devices and applications
- Cloud Applications Performances and Thresholds
- Infrastructure, Applications and APIs

These data points are fed into a realtime, optimised data platform, with an appropriately domain-specific, extensible data model and query engine powered by GenAI. This permits data insights to be automatically aligned,

Below" The Atos GenAI Platform is an aggregator and accelerator of existing service solution building blocks, brought together into a single, integrated AI-powered business user support function.



standardised and exported - in the correct format - to data lakes, IT Service Management toolsets such as ServiceNow, Configuration Management Databases, Chatbots, and other, complementary experience management tools such as Qualtrics, for onward processing. As mentioned, Use Cases are numerous and include:

- Measurement and management of Digital Experience in the End User environments
- Driving Productivity through proactive fault resolution
- Measuring and optimising adoption of new technologies, licencing, green agendas
- Optimisation of the Digital Workplace and contributing to day-to-day risk reduction.

Proactive Experience Center: Example Client Case Study and Outcomes

Through the detailed analytics of the Nexthink tools, we can proactively resolve inefficiencies and latent causes of potential issues, before they manifest themselves as productivity-impacting incidents, often by automated means. At an Atos client we delivered:

191 TB of System Temp files removed across 69,000 devices, avoiding potential disruptive capacity or corruption issues

45% Reduction in tickets for avoided issues on devices being monitor ed and reported by Nexthink tools

Large de-prioritisation of time-bound replacement of otherwise healthy devices, avoiding needless refresh costs

75% reduction in numbers of devices not restarted after 3 days, avoiding potential security, instability or corruption issues

57% reduction in devices with uncompliant non-Enterprise OS Editions, and 95% reduction in devices where Windows was not correctly activated, avoiding licencing issues, costs and potential reputational damage

6,000 devices identified for proactive replacement of out-of-warranty hard disk drives, known to be prone to failure, avoiding potential data losses.

Once implemented, through comparisons of Device Experience Scores before and after the implementation of proactive tools, the benefit was clear:

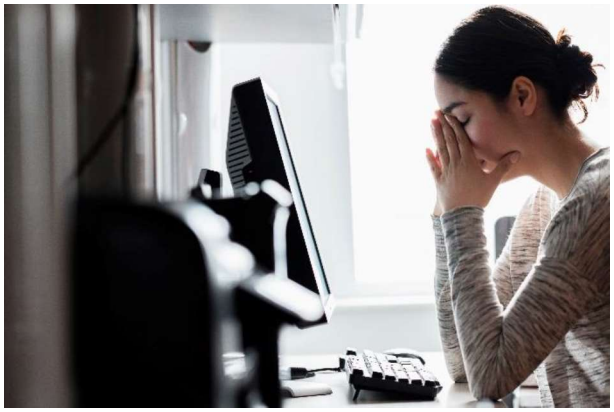
5.3% increase in DEX Device Score (6.76 up to 7.12) in just one month, and a 4.3% increase in Overall DEX Score (6.85 up to 7.15) in just one month

2. Securing the Digital Workplace with GenAI

As digital transformation changes how we work and do business, keeping our systems secure has become more important than ever. With more enterprises using hybrid work models and connected systems, the number of vulnerabilities is growing rapidly. Today's digital workplaces have many computers connected to the internet, including Internet of Things (IoT) nodes and mobile devices. These, along with data being constantly shared, create a complex network that is hard to protect. This complexity has led to a huge increase in security alerts, making it tough to spot and respond to potential threats. However, AI has the power to transform digital workplace security.

No security team, no matter how big or skilled, can handle the sheer number of alerts coming from these various sources. The need for flexible work and anywhere access adds to the challenge. Companies can't just lock everything down without affecting productivity, connectivity and agility. AI helps organisations manage the complexities of today's digital world with greater ease and assurance, by making security operations more efficient and effective. One of

the main challenges that security teams face is the huge amount of data and alerts that they have to process and prioritise. According to IBM's 'Cost Of Data Breach Report (2020) report, the average enterprise generates over 200,000 security events per day, of which only about 20% are relevant. Moreover, the average time to identify and contain a breach is 280 days, which can result in significant financial and reputational losses.



AI can help internal security teams overcome these challenges by automatically analysing large volumes of data, filtering out false positives, and identifying the most critical threats. Just as large language models (LLMs) can help GenAIs process information, understand context and find answers, AI-driven security can use similar techniques to understand the context and intent of malicious actors. This enables cybersecurity specialists to quickly detect and respond to complex and stealthy attacks like Advanced Persistent Threats (APTs), ransomware or zero-day exploits. AI can also help cybersecurity teams automate and orchestrate their response actions, such as isolating infected devices, blocking malicious domains or notifying users. AI can leverage predefined playbooks and workflows or suggest the optimal course of action based on historical data and best practices. This can reduce the manual workload and human errors and improve the consistency and quality of the response. It is recognised that technology has the power to enhance employee experience. This is equally applicable to staff who run and maintain corporate IT services. The main causes of stress and burnout are staffing shortages, high volumes of alerts, pressure to meet performance metrics, and the lack of career development opportunities. AI can help technical teams reduce stress and burnout by automating routine tasks, such as triaging alerts, collecting evidence or generating reports. This can free up time and resources for security analysts to focus on more complex threats, investigations and strategic activities. For example, they can spend more time redesigning core operational processes, ensuring that collected data is of the highest quality, or developing new skills and capabilities. New technology can also empower cybersecurity analysts to become data scientists and security architects, leveraging AI to create and optimise their own models and solutions. This can increase job satisfaction and retention, and foster a more innovative, collaborative workplace culture.

One of the ultimate goals of security operations is to shift from a reactive and defensive posture to a proactive and strategic one. This means that instead of waiting for attacks to happen and responding to them, cybersecurity teams can anticipate and prevent them, or even deter and disrupt them. This improves the resilience and maturity of security operations and aligns them with the business objectives and priorities. AI can help cybersecurity teams by providing analytics that predict and prevent future threats. For example, it can analyse large amounts of data to predict future attacks and suggest the best solutions and strategies based on risk, impact and cost. It helps security teams use their resources wisely and show the value of their security operations.

But aside from that, AI also plays a key role in understanding employee behaviour. It can sort through huge volumes of usage data to identify actions that make the organisation vulnerable. Pinpointing risky behaviours or instances when security protocols are ignored helps cybersecurity teams create training and awareness programmes that improve security habits. AI can also highlight areas where user practices need improvement. It suggests changes and real-time reminders to encourage better security practices, making employees active participants in protecting the organisation. Finally, AI can monitor how well your strategies are working. It tracks user adoption and compliance, showing which

methods are effective and which need adjustment. This makes AI a crucial tool in the digital workplace — for both technical security and fostering a strong security culture.

3. AIOps transforming IT Service Management

Atos is a leading IT systems integrator, and so naturally, IT Operations is where we see the greatest impact from GenAI.

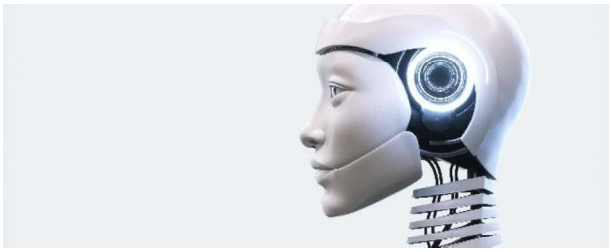
AI is being successfully employed in the development of software, writing code, programming and testing applications with automated development processes. But the greatest new horizon we are seeing is in AIOps – the convergence of AI in IT operations.

Over the last few decades, IT operations has been led by skilled professionals responding to alerts for incidents and triaging them according to urgency, impact and severity. Straightforward incidents are resolved quickly at first line support, whilst more complex issues are routed to the correct specialist resolver teams. With AIOps, an AI learning model controls a Robotic Process Automation (RPA) engine, which intelligently automates the first three or four steps of the IT Service Management (ITSM) process. It effectively augments the human effort required to gather, analyse and summarise the relevant data, prioritises incidents, and triggers the automated and manual actions necessary for resolution. It's arduous and time consuming to evaluate and act on hundreds of alerts per day, but AIOps can pinpoint in seconds what a human might take hours to find.

This has the potential to deliver massive time and resourcing benefits. A GenAI-powered "robot tech engineer" has potential in any area of ITSM, from incident management and change management to the orchestration of servers, applications and databases. This means that using AIOps, a two-person team could operationally manage the same IT landscape as ten people previously – from initial monitoring, through to ensuring human resolution of the most challenging or complicated incidents.

AIOps will dramatically accelerate every ITSM process, contributing to the ultimate goal of reducing time to repair - a key metric in ITSM. In some cases, it could even prevent problems from happening. The benefits are significant. Given that any outage is a potential disruption to the business, reducing the time to repair from eight hours to eight minutes is of huge value to enterprises and IT teams.

Crucially, this is not about taking human intelligence out of ITSM. Rather, it removes the burden of lower-value tasks so your talented IT specialists can focus on applying human insight and ingenuity where it can be best used. One area where AIOps truly excels is in handling the vast volumes of data involved in ITSM. It can be arduous and time consuming to evaluate hundreds of alerts per day, to determine which have the biggest impacts and assess their precise root causes. Across thousands of IT assets and services, AIOps can pinpoint in seconds what it might take hours for a human to find.



Imagine, for example, the eventual possibility of an initial call between six IT experts who are all discussing a complex, high-priority incident. Also on the call is the AI tech engineer, ready to provide a comprehensive analysis of what caused the problem, what systems it is impacting, and the next best action. Everyone on the call can interrogate the robot in real time to quickly determine the best outcome for the business.

Risk mitigation is obviously important when dealing with incidents which affect business availability. In discussions with enterprises, we

have listened to their concerns about the perceived risks of handing processes over to machines. The same questions emerged in the early days of process automation in ITSM. The reality is that when an AIOps model can simulate a million ways to solve a problem and continuously self-learn, it becomes highly effective – and even faster than the most experienced human engineer. However, any AI application is only as good as the datasets on which it is trained — and the learning models it creates from them. In this case, success depends on how you select and use data sources and how exhaustively the model is trained. A key factor is setting the right success parameters to ensure the right outcomes, and knowing at which points to transfer the process to a human.

The Atos R&D team has been working on an integrated AIOps offering, and based on our vision and progress so far, the team has a roadmap for the next two years. As we progress, we would be happy to share updates with you. As with any transformative programme, this won't be a big bang. We are working on incremental proofs of concept, starting with straightforward incidents and building from there. At every step, the purpose is to support and empower human IT engineers to maximise the value they deliver to your enterprise.

GenAI-powered IT service management will be a game-changer — especially in combination with capabilities such as Atos Bridge, which connects ITSM performance directly to business performance and orchestrates the necessary outcomes. Integrating AIOps will provide enterprises with next-generation IT — resilient, adaptive and optimised — delivering exactly what the business needs at every touchpoint.

4. How could Atos support Heineken as partner on your AI journey?

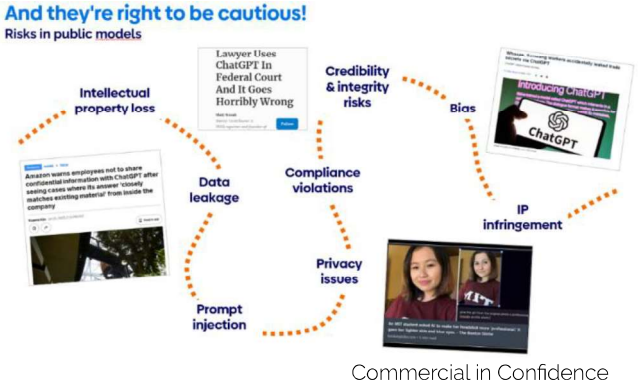
With the latest advancements in LLMs (Large Language Models) and transformer ANN (Artificial Neural Networks) Generative AI is democratised and now widely available in a myriad of variants. However, to prevent an explosion of non-standard, point solutions, companies need to make GenAI available for all employees in a controlled way. Atos supports this by providing a platform for companies that keeps the data secured, while allowing motivated employees to create their own use cases, with prompt engineering and Retrieval-Augmented Generation (RAG), which enables the optimisation of LLM outputs without changing the underlying model itself. This will lead to more specific models for specific organisations and business groups, and provides context-aware answers to prompts using the most recent set of data. Atos supports its customers across a range of industries on their AI journey, through a portfolio of services and solutions tailored to their specific needs:

a. AI Strategy and Consulting: AI provides strategic consulting services to help our customers to define their AI policies and roadmap, identify use cases and opportunities for AI adoption that align with our customers business objectives

b. AI Implementation and Integration: Atos assists in implementing AI platforms and solutions, connecting classical RPA-type AI and Gen AI, leveraging machine learning models and advanced analytics to address specific challenges within various industries – such as demand forecasting, inventory optimisation and personalised customer experiences.

c. Data Management and Analytics: Atos offers expertise in managing and analysing large datasets, enabling its customers to extract valuable insights that drive operational efficiency, enhance customer engagement and inform strategic decision making.

d. Sovereign AI: Organisations do not want their data to leak and feed third party data and language models, they want to ensure their data is only used in-house, and no intellectual property is being made available to the outside world. However, they still wish to leverage the



power of external AI and its vast amount of data and language models. Our portfolio helps to keep confidential data, models and training on-premise, and protect from some LLM provider usage terms which permit use of customer data in model training,

Atos and Dell Technologies have collaborated to offer the set-up of an optimised, on-premise infrastructure, and provide end-to-end customised services for the safe production and maintenance of AI models. This allows our customers to smoothly move their AI models to production, protect their data and access low-latency use cases – while still leveraging outside sources beyond more limited in-house trained models. This approach can help to mitigate the risk of using public AI models within your organisation.

More information on Sovereign AI can be found here:

https://atos.net/en/lp/sovereign-ai

e. AI-powered Digital Transformation: Atos supports its customer in their digital transformation efforts by integrating AI into various aspects of their operations, such as supply chain management, marketing, sales optimisation and customer services. We also provide the means to keep AI used for internal process optimisation separate from that used for business growth and market optimisation so that they can progress at different rates.

Security and Compliance: As AI adoption brings new considerations for cybersecurity and privacy, Atos also provides solutions to ensure that AI implementations comply with industry regulations and best practices, safeguarding sensitive information and maintaining customer trust. Atos provides support in building AI infrastructure and ensuring robust cybersecurity measures for AI systems but also using AI based cybersecurity technology – including implementation of secure storage, processing and ensuring compliance with data protection regulations.

f. Training and Support: Atos offers training and support to ensure that organisations have the necessary expertise to effectively use AI solutions. This may involve educating teams on AI best practices, as well as providing ongoing support for AI implementation and maintenance.

This allows our customers to smoothly move their AI models to production, protect their data and access low-latency use cases – while still leveraging outside sources beyond more limited in-house trained models. This approach can help to mitigate the risk of using public AI models within your organisation.

Atos Customer Examples

Atos Foundational Generative AI platform

Dedicated Azure instance managed by Atos including 2-factor authentication provided by Atos

Private and Secure ChatGPT via Atos' Liza

MS Teams bot on top of RAG solutions for micro learning for the following use cases:

- Boost Compliance with competition regulations
- Optimize Football Association strategy formulation
- Improve UEFA Crisis Management Playbook Knowledge transfer to Football clubs

Delivered Project management, Data transformation services, Prompt engineering and End user training

UEFA EURO2024 GERMANY

Predictive maintenance of water networks

Atos' data teams are integrated into an agile team to build and put into production the predictive models on network overflows, allowing Scottish Water to gain expertise in innovative AI approaches.

Scottish Water

Advancing together to harness technology for biodiversity conservation

We are harnessing artificial intelligence and digital technologies for accelerate and enhance data collection and analysis for wildlife conservation. Atos and WWF have defined the following projects by which conservation organizations and other stakeholders could benefit from Atos' technological expertise.

Automating biodiversity surveillance – The first project brings greater automation to the monitoring of important ecosystems. Atos experts are working to combine the use of artificial intelligence to analyze satellite imagery with the development of algorithms which identify patterns over time in order to identify patterns which might indicate a negative biodiversity impact.

Predicting & preventing epidemic risk – The second project focuses on predicting hotspots of emergence for zoonoses – diseases that jump between species, including humans. Atos teams are developing machine learning algorithms to analyze demographic, environmental, animal health and pathogen data, in order to identify patterns and predict hotspots where new disease outbreaks may occur.

Improving tech tools – The third project aims at improving an existing solution known as SMART – a Spatial Monitoring and Reporting Tool – which is already used by 50,000 agents in over 100 countries to support wildlife and ecosystem conservation.

In summary

AI is not a silver bullet that can replace human intelligence and expertise. Rather, it is a powerful ally that augments and complements human capabilities, decision making and skills. As organisations embrace AI, it's important to learn how to leverage its strengths and overcome its limitations; for instance, it's still key for organisations to secure their own data while using different large language models for evaluation and creation of new information, and avoid the disclosure of confidential sources used for training of models – our Sovereign AI offering can help mitigate this risk.

Armed with this understanding, GenAI can be harnessed to enhance productivity, speed responses to internal and external factors, and create more secure workplaces. It is also enabling enterprises to take a proactive, human-centric approach to efficiency, reducing employee fatigue and burnout by automating repetitive, unfulfilling and routine tasks.

Atos – your partner in harnessing the Power of AI

Atos is well placed and would be delighted to help Heineken on your journey. Atos is one of the world's largest IT providers, and innovation and expertise is our core business. Atos has considerable skills and experience in developing and implementing relevant and robust Generative AI solutions for our customers. We're also experts in a wealth of linked technologies such as hybrid cloud, cybersecurity, technology, application and decarbonisation services.

We have been a Gartner Leader for many years in digital workplace services, hybrid cloud infrastructure and datacentre services. We are also ranked Number 1 worldwide in managed security services by revenue.

Our 92,000 skilled individuals bring together agility and ability, designing imaginative, creative solutions that help our clients anticipate what matters most to their customers, stakeholders and employees, and create lasting value in today's world.

Security
Experience
Connection
Innovation