Trends Report 2024

A Look into the Future of IT

As the world of technology continues to develop at an accelerated pace, it's essential for businesses to stay up to date withthese changes.

With this in mind, we've compiled our very first **Trends Report for 2024.**

This forward-looking report offers valuable insights into the IT landscape touching upon important topics including the IT labour shortage, cloud security, ZTNA, and the impact of artificial intelligence (AI).

About Prival

For over two decades, we have been at the forefront of the ever-evolving information technology landscape, dedicated to helping Quebec organizations stay up to date with their IT needs.

IT Labour Shortage:

With a rising global demand for IT professionals, countries like the US, India, and China are leading the labour shortage. Particularly difficult to fill roles include cloud security. Addressing this issue requires development of internal resources and skills, with an emphasis on work-life balance to retain talent.

Cloud Security:

As more organizations adopt cloud technologies, concerns about proper configuration and security escalate. The lack of available skills in identity/access management and cloud security slow adoption rates. Key strategies for improvement include training, organization, and correct controls.

ZTNA (Zero Trust Network Access) :

Nearly all IT leaders are implementing or planning to adopt ZTNA as a way to enhance cyber security measures. Driven by remote work and evolving threats, ZTNA adoption is not without its challenges, including limited resources and the cost implications. A strategic approach to ZTNA, with phased deployment, is recommended.

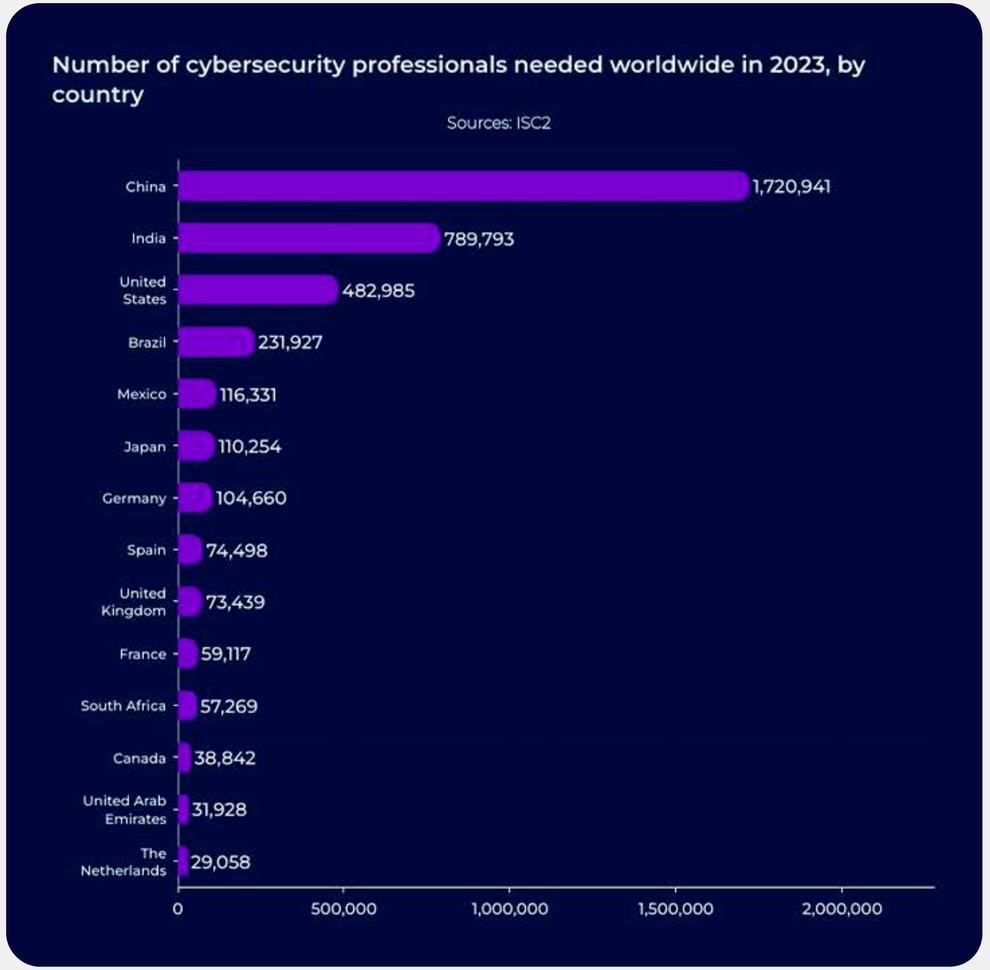
Artificial Intelligence (AI):

Rapid advancements in AI present opportunities across multiple sectors, particularly healthcare and marketing. However, there is a growing demand for skilled AI professionals, and ethical concerns are emerging. Balancing the value and risk of AI while addressing skill shortages is the way forward

IT Labour shortage

Summary

With about 60% of businesses claiming an understaffed cybersecurity workforce in an ISACA survey, it's apparent that the stress and work-life imbalances of the field are significant. Beyond the technical prowess, employers value problem-solving skills, teamwork, and effective communication. Certifications like CISSP are favored amongst security professionals, however positions in Cloud Security, Security Operations and Network Security present the greatest hiring challenge



Drivers

- IT positions are increasing faster than the rate of adequately trained workers.
- The trend is also influenced by the decline in enrollment in computer and information programs.

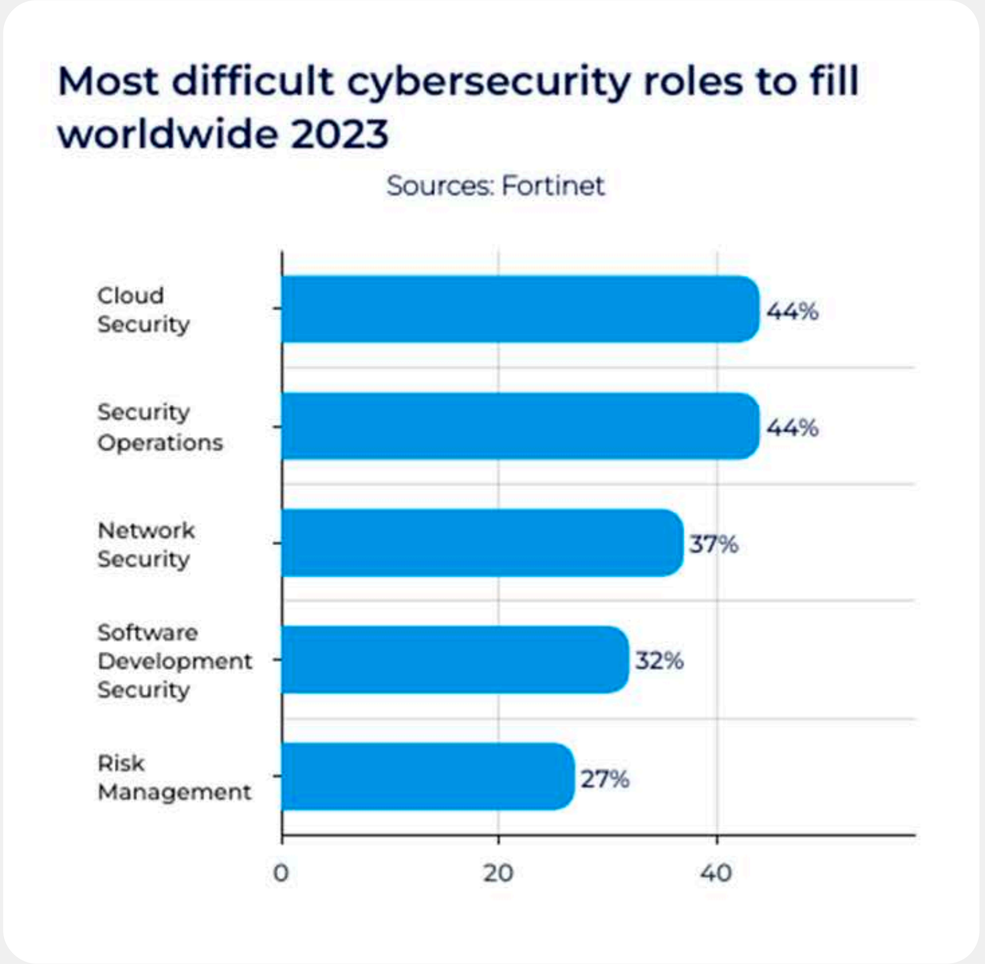
Challenges

- According to a Gartner survey, merely 20% of potential candidates are actively seeking jobs, with over half being passive job seekers.
- There's a striking talent deficit in the IT labour market, struggling to meet the demands of top skills.
- A PWC survey reveals that firms feel understaffed in cybersecurity, with 46% being somewhat understaffed and a further 13% being significantly so.
- The main reasons for cybersecurity professionals exiting their posts include: headhunting, inadequate financial incentives, limited opportunities for promotion or development, high-stress levels, and lack of support from management.

- The most challenging roles to fill are often those involving identity/access management and cloud security skills.
- The time taken to fill a cybersecurity position is often extensive, spanning several months.

Recommendations

- Transform IT job descriptions into captivating postings that not only outline the necessary skills but also inspire candidates to become part of you IT team.
- Strive to ensure a healthy work-life balance in your team and re-imagine IT job descriptions to attract potential hires.
- When assessing candidates, consider their soft skills like teamwork, problem-solving abilities, and communication skills to ensure they'll be a good fit for your team.
- Regularly conduct pay benchmark analysis and incorporate flexibility in your compensation strategy.
- Invest in certification opportunities as part of your training and development programs.
- Provide flexible working conditions and encourage diversity, equity, and inclusion initiatives to appeal to a wider candidate pool.
- Automate aspects of the job through technology to reduce repetitive tasks and improve job satisfaction.
- Be more open to hiring entry-level candidates who can evolve with your team.



Cloud Security

Summary

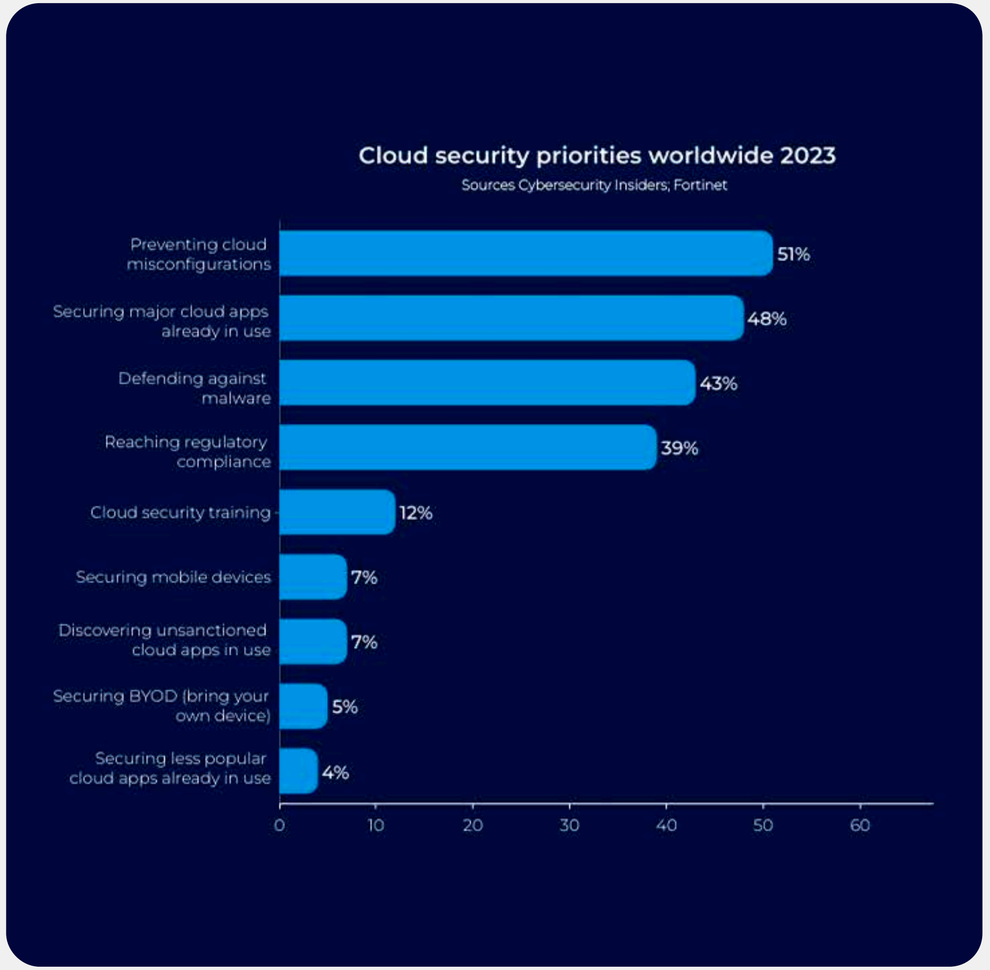
Despite the continuous adoption of the cloud, several factors like inadequate knowledge and resources for securing various cloud setups pose significant concerns among IT professionals.

Drivers

- Varied data protection measures exist in the cloud and on-premise environments.
- Backups are common in both scenarios, whereas multi-factor authentication is more prevalent in the cloud, and on-premises environments less emphasize on data loss prevention.
- The most typical security incidents in the cloud are phishing, targeted attacks on cloud infrastructure, and user account compromise

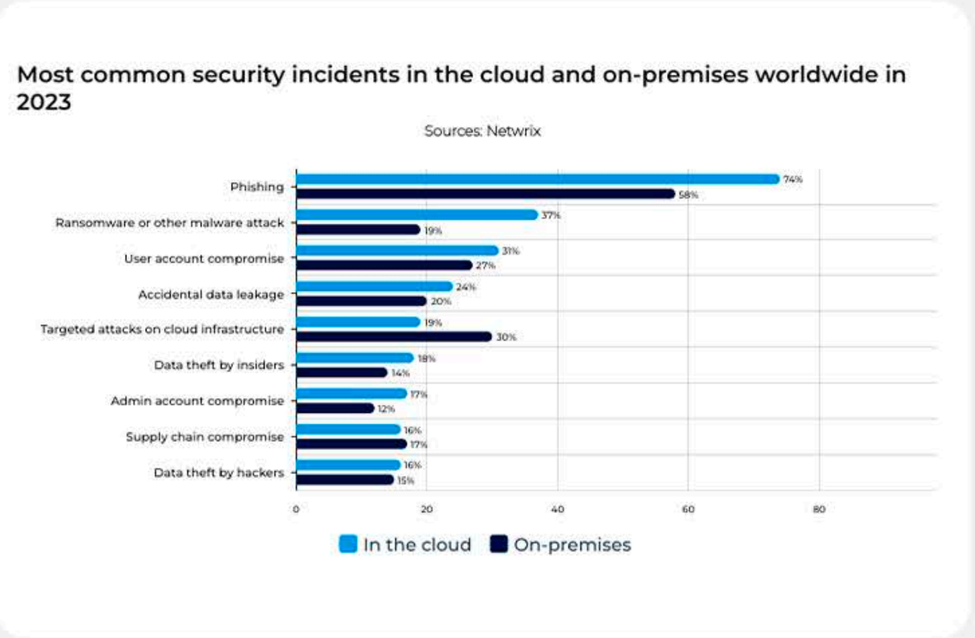
Challenges

- The complexity of securing the cloud is exacerbated by the lack of trained professionals.
- Cloud cybersecurity roles are highly sought after by companies, but tough to fill.
- The most common cause of breaches is misconfigurations
- The top priorities for companies in cloud security are securing major cloud apps and defending against malware.
- Multi-cloud environments pose challenges in securing the right skills and ensuring data protection and privacy.



Recommandations

- Ensure your team is equipped with the necessary knowledge to make informed decisions on the type of cloud and the appropriate controls to employ.
- At the business level, set clear security outcomes to protect people, data, and brand reputation.
- Identify and mitigate the technical risks associated with the desired business outcomes.
- Once the optimal architecture is chosen, determine the security controls to be applied.
- Provide training and certification opportunities to keep up with the ever-evolving cybersecurity requirements.
- Consider employing 3rd party controls in multi-cloud environments for a consistent user interface, policy unification, and simpler cloud management.
- Implement cloud security measures phase-by-phase, initially securing sensitive apps and gradually broadening the scope
- Consider using clientless Zero Trust Network Access (ZTNA) for VPN replacement and incorporate agent-based ZTNA into a wider Secure Access Service Edge (SASE) framework.



Zero Trust Network Access (ZTNA)

Summary

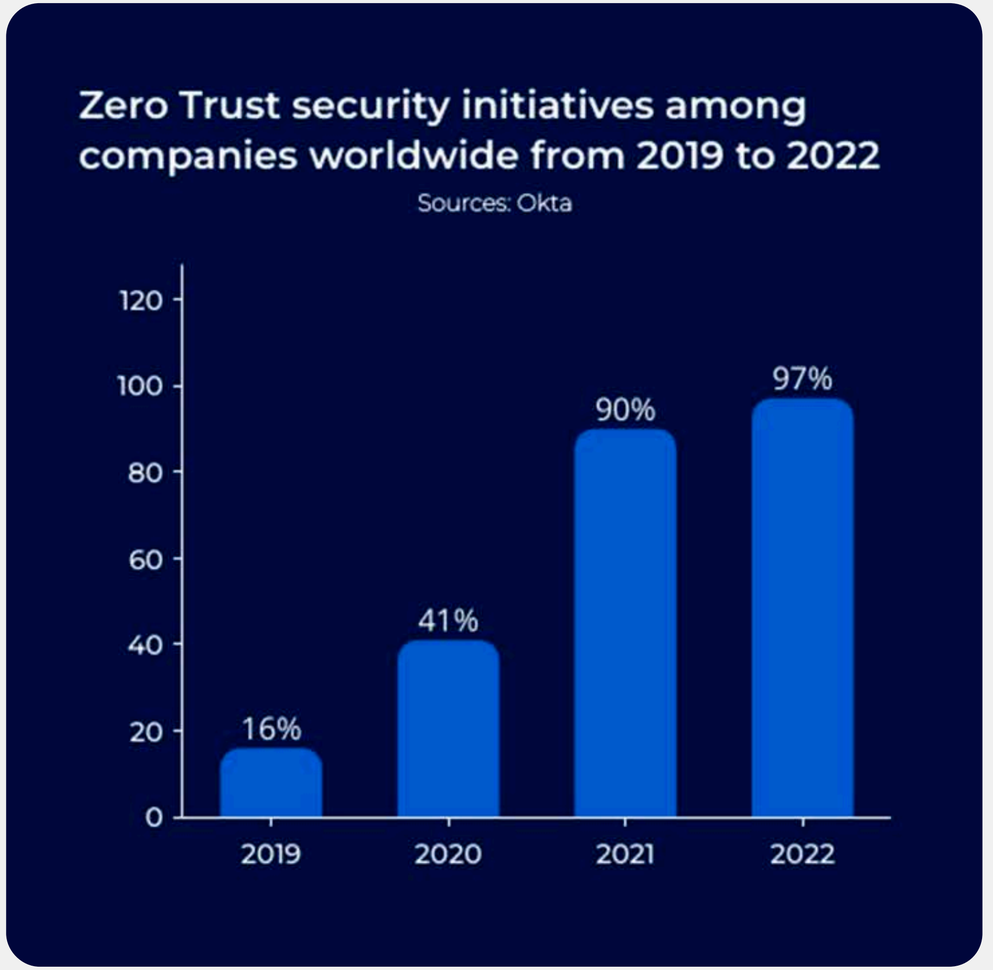
The Zero Trust Network Access (ZTNA) approach is widely accepted by IT leaders as a viable method to enhance cybersecurity. Vendor product consolidation is increasingly incorporating ZTNA as part of their SASE and SSE architecture solutions.

Drivers

- The rise of Remote Work and Flexible Work Settings
- An Evolving Threat Landscape
- Changing Boundaries of Enterprise Networks
- The growing interest in the ZTNA market is driven by end-user organizations focusing on zero trust strategies and cloud adoption.

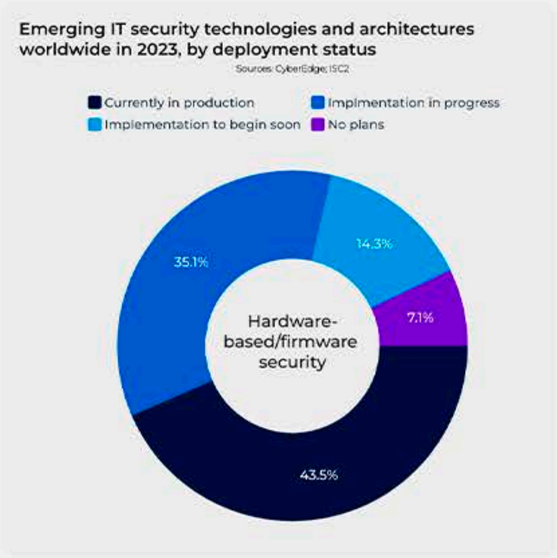
Challenges

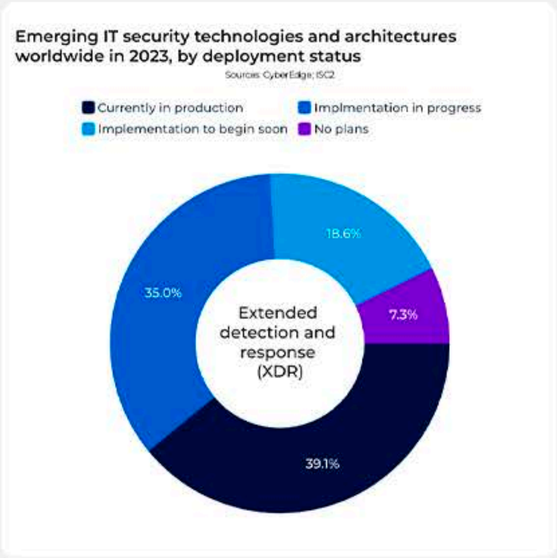
- Securing appropriate resources represents a key hurdle in ZTNA adoption.
- Organizations confront leadership and technological obstacles, such as outdated technology and financial concerns.
- Lack of understanding and awareness about ZTNA among IT professionals poses a challenge to its implementation.

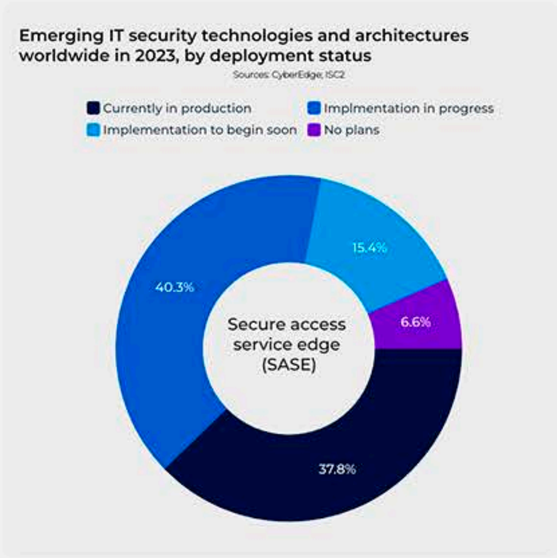


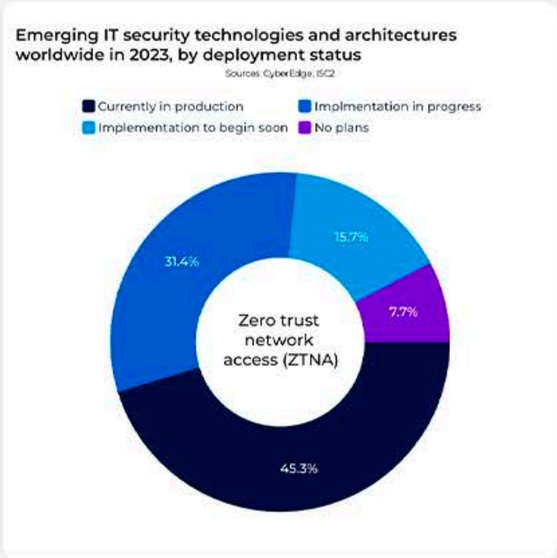
Recommandations

- Formulate a comprehensive zero trust strategy with focus on mitigating risks and mature identity/access management prior to opting for ZTNA solutions.
- Roll out ZTNA in a phased manner, firstly securing sensitive apps, and then widening the scope.
- Prioritize VPN replacement with clientless ZTNA and blend agent-based ZTNA in a larger Secure Access Service Edge (SASE) framework.
- Choose vendors that meet security prerequisites, minimize attack points, and support dynamic access control policies consistent with zero trust norms.
- Enlighten the leadership team about zero trust as an overarching security concept rather than a singular product.
  Artificial Intelligence





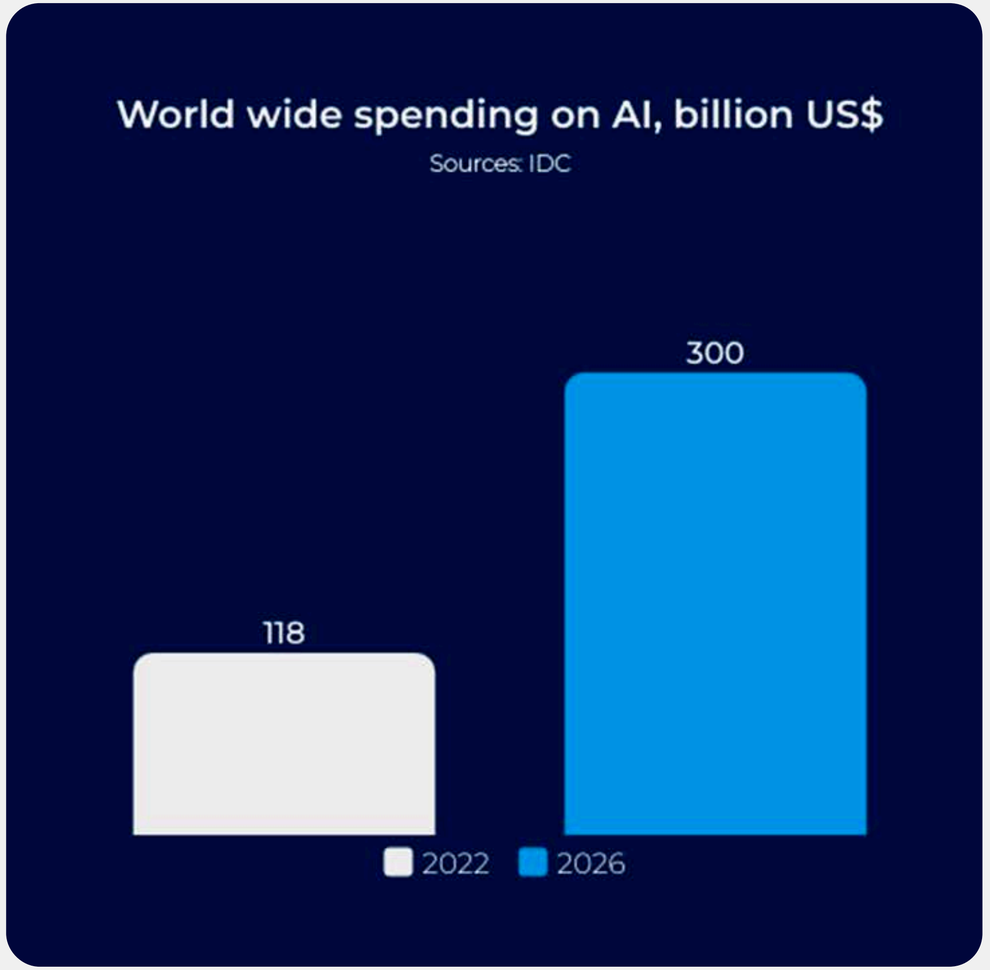




Artificial Intelligence (IA)

Summary

Artificial Intelligence (AI) is currently made up of machine learning, robotics, Artificial Neural Networks (ANNs), and Natural Language Processing (NLP). The rapid progress of AI techniques, with generative AI anticipated to expand further in 2024, often leaves businesses struggling to keep up and incorporate these developments into their functioning. To efficiently manage such innovations, leading organizations are making strategic investments in vital AI assets like talent acquisition, nurturing a culture that encourages experimental innovation, data an
governance, which offer stability in the face of future technological shifts.



Drivers

- The ever-expanding scope of AI and its potential to revolutionize industries drive organizations to invest in this innovative technology.
- The increasing availability of data and advancements in computing power enable the development and application of advanced AI techniques.
- Organizations are also motivated by the potential for cost savings, increased efficiency, and competitive advantage that AI can provide.
- The increasing number and complexity of cyber threats require advanced, automated solutions such as AI.
- The potential cost savings and efficiency gains from implementing AI drive its adoption in the cybersecurity realm.
- AI-powered tools can process and analyze vast amounts of data quickly and accurately, providing valuable insights for threat detection and response.

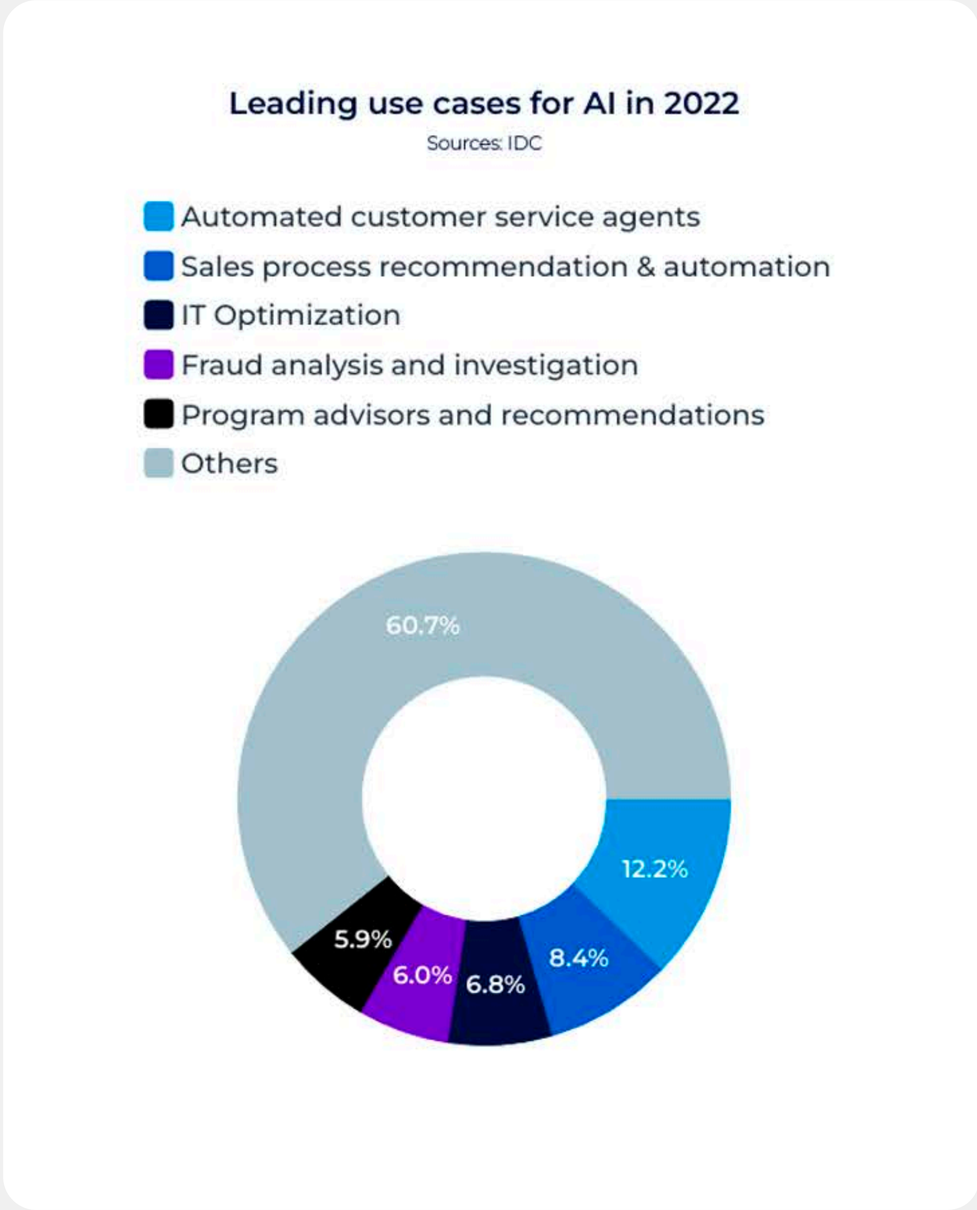
Challenges

- Finding highly skilled AI professionals, such as Data Engineers, Machine Learning specialists, AI Data Scientists, and Data Architects, is a major challenge.
- The rise of unethical AI applications, including bias, deepfakes, and AI-powered malware, adds concern to the AI landscape.

Recommandations

Artificial Intelligence (AI) has already made a significant impact on the business landscape, and its transformative power will continue to shape the future. To stay ahead of the competition and maximize efficiency through AI integration, we propose the implementation of the following strategies:

- Integrate enterprise knowledge with AI for a unique edge; use generative AI for data analytics.
- Embrace an AI systems approach, integrating models, code, and data within larger ecosystems; and anticipate application rationalization and composable architecture.
- Tackle the skill gap and operating model challenges by upskilling stakeholders and IT staff for the effective management of scalable AI systems.
- Balance the benefits and risks of AI by pursuing ecosystem-wide value, creating diverse AI use cases, and adopting iterative approaches for strategy evolution.



Conclusion

Thank you for your time and interest in our Trends-2024 report.

We will continue to monitor these topics and develop on them in the following months to make sure you keep up with the evolving landscape.

Have suggestions? Your feedback is crucial in improving the quality of the content we provide.

Sources :

- 5 Best Practices for CIOs to Effectively Attract and Hire Top IT Talent - Gartner
- Artificial Intelligence Primer for 2024
- Market Guide for Zero Trust Network Access, 14 August 2023 - Gartner.
- Digital & Trends - Artificial intelligence: in depth market analysis
- Digital Trends – Cloud Security - Statista Report.
- Digital trends – ZTNA – Statista Report
- Digital trends – IT Skills
- Industries & Markets - Artificial Intelligence (AI) In business
- https://www.govtech.com/
- Ethical concerns mount as AI takes bigger decision-making role — Harvard Gazette