Overcoming AI data security challenges with an embedded approach

Following the wave of excitement surrounding the incredible possibilities of AI, comes the reality of deploying AI in the enterprise at scale. IT leaders face significant risks and challenges, including data ownership and protection, security of information, the accuracy of AI results, and the cost of operating at scale.

AI market trends

1. **AI integration:** Businesses are rapidly adopting AI to drive insights, automation, and innovation. 85% of business leaders expect an increase in the use of AI and predictive analytics models.[1]
2. **Managing data risks:** Data integrity is the biggest risk that businesses are actively managing or mitigating with AI deployment. [1]
3. **Risk planning:** 66% percent of businesses that do not yet have a formal AI risk management function aim to have one in the next three years. [1]

Deployment challenges

Data ownership and control

Deploying AI in a business presents significant challenges related to data ownership and control. Clear policies must be established to define intellectual property rights and determine who owns the data, particularly when it involves third-party sources or customer information. Ensuring transparency and building trust with stakeholders about how their data is used is paramount for successful AI deployment.

Security of information

Data security is a crucial concern when integrating AI into business operations. AI solutions often require vast amounts of sensitive data, making them prime targets for cyberattacks. The

1901 S Bascom Ave Suite 1650, Campbell CA 95008

dynamic nature of AI models, which can evolve and adapt, adds an additional layer of complexity in maintaining security, necessitating continuous monitoring and updating of security protocols to address emerging threats.

Accuracy of AI results

It is essential that AI generates accurate, consistent and reliable outcomes without drift to maintain operational integrity and trust. AI models are only as good as the data they are trained on, which means that any biases or inaccuracies in the training data can lead to flawed outcomes. Additionally, real-world applications often involve unpredictable variables that can affect AI performance. Businesses must invest in rigorous testing and validation processes and allow for effective human oversight for high accuracy levels.

Cost of operating at scale

The cost of operating AI at scale can become prohibitively high for many businesses. Beyond the initial investment in developing a pilot or first use case, scaling out across the whole enterprise dramatically increases expenses related to data storage, processing power, and inference costs. It also requires specialized talent to manage and optimize these AI solutions. Businesses must carefully plan and budget for these future costs and build in ways to get economies of scale from AI operations, balancing the potential benefits with the financial outlay.

Security, control, results you can trust

Bruviti's specialized Equipment AI is built for seamless integration with your existing IT infrastructure, focusing on enhanced security and rapid deployment. It operates securely within your organizational firewall, ensuring that sensitive data stays within the organization. The Equipment AI is designed from the ground up to be deployed within 5-7 weeks. It is embedded directly into your environment, giving you full control and ownership.

Challenges	Bruviti Equipment AI solution
Data ownership and control	Bruviti Equipment AI implements robust, firewalled data protocols that operate within the enterprise's secure systems. This protects the enterprise from unauthorized access and potential breaches, reinforcing control over the data lifecycle. All data and modifications are traceable and fully documented to clearly define data ownership, usage rights and establish accountability. As the data resides inside the enterprise's network, there is no chance of access to proprietary insights. Additionally, regular audits and assessments help maintain compliance and identify potential vulnerabilities in data protection practices.
Security of information	Since Bruviti AI solutions are designed to be embedded within your existing, secure enterprise IT environment, they ensure that your data remains in-house, mitigating the risk of data leakage. By utilizing controlled sandbox environments, Equipment AI effectively isolates testing and development processes from live data environments,

	to maintain the integrity of the actual data. All data used in LLMs is automatically stripped of any personally identifiable information to preserve privacy and comply with data protection regulations.
Accuracy of AI results	Bruviti AI models are regularly tuned with real-time data to prevent drift. The LLMs are trained on relevant data sets for each specific task to deliver precise and consistent output, at the lowest cost. Additionally, Equipment AI includes proactive checks and alerts to maintain accuracy, along with human oversight mechanisms that allow for continuous validation and improvement of AI output. This helps prevent errors and hallucination to ensure outcomes you can trust.
Costs of operating at scale	Bruviti manages the costs of operating AI at scale by strategically implementing a phased approach, beginning with pilot projects to assess feasibility. By utilizing cloud-based AI services, it embeds within your enterprise ecosystem, offering scalability with cost control. Efficient data management practices such as data compression, context management, and caching, reduce usage costs. Additionally, Bruviti's automation tools streamline operations and minimize manual intervention, while the scalability of enterprise-ready pre-built integrations results in better utilization of existing infrastructure and an easy-to-use low/no-code user interface.

Keep your data secure with Bruviti AI

In the AI industry, success depends on combining great AI performance with strong security measures. While public LLMs and techniques are good starting points, their limitations and risks become clear in real-world business settings. It's important to use a thorough AI strategy that values both AI excellence and strong security.

At Bruviti, our goal is to help you use AI to achieve important business results, with a focus on control, security, and reducing risks. By placing the power of AI in your hands, we empower you to extract sustainable value from the training and learning of AI models to deliver outcomes tailor-made to your organization's unique requirements and goals.

By adopting Bruviti's embedded AI approach, you can overcome the challenges of data security in AI applications. Our solution not only protects your data but also enhances the efficacy and reliability of AI deployments, empowering your business to leverage cutting-edge technology with confidence and security.

Discover the power of Bruviti's secure AI—get a live demo today.

1. KPMG – Responsible AI and the challenge of AI risk

1901 S Bascom Ave Suite 1650, Campbell CA 95008