LAKERA

Build vs. Buy

A Practical Guide to Security Solutions for GenAI Applications

Introduction

As Generative AI is taking industries by storm, the need for strong security solutions to protect these systems is growing. Businesses must decide whether to build their own security measures in-house or purchase ready-made solutions. This choice involves balancing factors like cost, time, scalability, and the required expertise. Building offers more control but comes with higher costs and risks, while buying can be faster and more cost-effective but may limit customization.

This article highlights why buying a security solution is the most practical and effective approach for GenAI applications. Building an in-house solution may seem appealing, but it comes with significant risks, costs, and challenges that are often underestimated. We explore these factors to help you make an informed decision that best secures your business.

Key Considerations

In the sections below, we'll be examining the following aspects of the buy vs build dilemma:

Total Cost of Ownership (TCO)
Long-term costs associated with each approach, including ongoing maintenance.

Security Features
Coverage of security capabilities and input supported.

Time to Market
Speed of implementation and deployment to production.

Scalability
The ability to grow together with the needs of the organization.

Effectiveness
Accuracy and usability of the defenses in-app and by team members.

Compliance
How comprehensively each option meets regulatory requirements.

Up-to-Date Security
The ability to stay current with emerging threats.

Expertise Required
The level of in-house expertise needed.

PROS AND CONS

Building Security Solutions In-House

Building a custom solution can offer significant advantages in terms of customization, control, and integration, but it also comes with notable challenges, including high costs, time demands, and increased risks.

+ Pros

Customization

Building your own security solution allows you to tailor it precisely to your organization's specific needs. This means you can design and implement security features that align perfectly with your operational requirements and industry standards. As your organization grows or changes, you can adapt and evolve the solution to meet new challenges or incorporate additional functionalities.

Control

By building in-house, you maintain full control over your security protocols and the overall development roadmap. This control extends to every aspect of the solution, from data handling to the integration of emerging technologies. This autonomy can be particularly important for organizations with stringent security or compliance requirements, where every detail of the solution must be meticulously managed.

Integration

A custom-built security solution can be designed to integrate natively with your existing infrastructure. This minimizes compatibility issues and allows for a tailored implementation process, ensuring that the security measures work harmoniously with your current systems and workflows.

– Cons

High Costs

Development

Building a security solution from scratch requires a significant upfront investment. This includes not only the initial development costs but also ongoing expenses for maintenance, improvements, updating to new threats, and scaling the solution as your organization grows.

Infrastructure

Building an in-house solution often leads to higher costs, particularly if GPU-based infrastructure is required to run machine learning. These costs can range from $50,000 to $100,000 per year, depending on the scale and complexity. Moreover, in-house solutions tend to be less resource-optimized and may not achieve the economies of scale that off-the-shelf solutions benefit from.

Human Resources

Developing and maintaining a custom security solution requires a specialized team with deep expertise in both AI and cybersecurity. Given the nascent stage of GenAI security, talent in this area is particularly scarce and in high demand, leading to increased competition and costs. Acquiring or training the necessary expertise for in-house development is both challenging and expensive.

Time

Development Time

Creating a robust, effective security solution is a time-consuming process. From initial design to final deployment, the timeline can stretch over many months, or even years, depending on the complexity of the solution and the resources available.

Updating & Maintenance

Once deployed, your in-house solution will require continuous updates, monitoring, and maintenance to stay effective against evolving threats. This ongoing commitment of time and resources can be a significant burden, particularly for smaller teams. Without the expertise and resources to keep your solution updated, you risk falling behind on the latest threats, making your system vulnerable. This is why relying on a specialized vendor who can ensure your protections evolve with the threat landscape is crucial.

Risk

Expertise

Building a security solution in-house carries significant risks, especially if your team lacks the necessary expertise. Security is a high-stakes field where mistakes can be costly, and the consequences of a defense failure can be severe for your organization. Even if your system feels secure at launch, keeping it updated is an ongoing and complex challenge. New threats are constantly emerging, and without the right knowledge and experience, there's a high likelihood that vulnerabilities will be overlooked. This could lead to breaches or compliance failures, particularly in the fast-evolving space of GenAI where developments are happening at a rapid

pace. Staying ahead of these threats requires not just expertise at launch but continuous vigilance and proactive updates, which can be a heavy burden for in-house teams to manage.

Vendor Lock-In

Many organizations choose to build in-house security solutions by leveraging existing LLMs from providers like OpenAI, fine-tuning them to fit their needs. While this approach can speed up development and offer advanced capabilities, it also creates a significant dependency on the chosen provider. This vendor lock-in can make it challenging and costly to switch providers or adapt to new technologies as your needs evolve. Over time, your security infrastructure might become tightly coupled with the LLM provider's roadmap, limiting your flexibility and innovation.

In summary, while building your own security solution offers customization and control, it also requires a significant investment of time, money, and expertise.

For organizations with the resources and specific needs that justify this approach, the benefits can be substantial. However, for many, the cons—particularly the high costs, risks, and potential vendor lock-in—may outweigh the potential advantages.

PROS AND CONS

Buying a Security Solution

When considering whether to buy a security solution for your GenAI applications, it's important to weigh the benefits of quick deployment and lower upfront costs against potential drawbacks like limited customization and vendor dependence.

+ Pros

Cost-Effectiveness

Initial Investment

One of the main advantages of buying a security solution is the lower upfront cost compared to building one from scratch. With a purchased solution, you can avoid the significant expenses associated with development, infrastructure, and human resources that come with an in-house build. This makes it a more accessible option, especially for smaller organizations or those with limited budgets.

Updating & Maintenance

The solution often comes with regular updates and ongoing support as part of the package. This means you don’t have to worry about dedicating resources to maintain and update the system to keep it secure against newly arising threats—these tasks are handled by the provider, reducing your long-term operational costs and allowing your team to focus on core business activities.

Speed

Time to Market

Buying a security solution allows for much faster implementation compared to building one. Ready-to-deploy solutions can be up and running quickly, unblocking innovation and enabling your organization to stay ahead in a competitive market. This speed is crucial, particularly in fast-moving industries where delays can result in missed opportunities.

Support

The solution typically includes comprehensive training and support, which helps accelerate the learning curve for your in-house team. This support ensures that your team can effectively use and manage the solution, even if they don't have deep expertise in AI security. The availability of ongoing support also provides peace of mind, knowing that help is readily available if issues arise.

Scalability

Designed to Scale

The security solution is often designed with scalability in mind, allowing it to grow alongside your business. As your organization's needs evolve, the solution can adapt and expand without requiring significant overhauls or additional investments. This flexibility ensures that your security infrastructure remains robust and effective as your business scales.

— Cons

Limited Customization

One of the primary drawbacks of buying a security solution is the limited ability to customize it to your specific needs. While many off-the-shelf options offer some degree of flexibility, they may not provide the deep customization that a tailored, in-house solution can offer. This can be a significant limitation if your organization has unique security requirements or operates in a highly regulated niche industry where specific protocols are essential.

Vendor Dependence

When you purchase a security solution, you become reliant on the provider for updates, support, and ongoing maintenance. This dependence can be a double-edged sword; while it reduces your internal workload, it also means that your security infrastructure is tied to the provider's performance and business decisions. If the provider fails to deliver timely updates or goes out of business, your security could be compromised.

Coverage Limitations

A ready-made security solution may not cover all of your specific requirements right out of the box. While these solutions are designed to address a broad range of needs, they might not fully align with your organization's unique environment or security challenges. This can result in gaps in coverage that need to be addressed through additional tools or custom configurations, which can add complexity and cost.

All in all, buying a security solution offers significant advantages in terms of cost-effectiveness, speed, and scalability, making it an attractive option for many organizations.

However, it's important to consider the potential downsides, including limited customization, vendor dependence, and the possibility of incomplete coverage. Weighing these factors against your organization's specific needs and capabilities will help you determine whether buying is the right choice for your GenAI security strategy.

CHECKLIST

Should You Buy or Build a Security Solution?

Use this checklist to evaluate whether buying or building a security solution for your GenAI applications is the best choice for your organization.

If you find that you require extensive customization, have a substantial budget and timeline, and possess in-house expertise, building might be a consideration.

However, if speed, cost-effectiveness, and staying current with threats are your priorities, buying will likely be the better choice.

1. Security Needs Assessment

What are the specific security needs of your organization?

- [ ] What are the specific security needs of your organization that existing solutions in the market aren't capable of addressing?
- [ ] Do you require advanced customization to tackle unique security threats that you believe no vendors are able to fully meet?
- [ ] Are there industry-specific security standards that off-the-shelf solutions will struggle to satisfy?
- [ ] How important is it for your security protocols to adapt as your organization evolves, and do you think this flexibility is not achievable with market solutions?

2. Budget

What is the available budget for security solutions?

- [ ] Can your budget accommodate the higher upfront costs associated with building a custom solution?
- [ ] Are you prepared for ongoing costs related to development, maintenance, and updates if building in-house?
- [ ] Would a lower initial investment in a purchased solution free up resources for other areas of your business?

3. Timeline

How quickly do you need the solution implemented?

- [ ] Is there an urgent need to deploy security measures, requiring a faster time to market?
- [ ] Can your organization afford the longer development time associated with building a solution in-house?
- [ ] Does your timeline allow for thorough testing and iterative improvements if building internally?

4. In-House Expertise

Do you have the necessary machine learning and AI security expertise, or can you afford to acquire it?

- [ ] Does your team have the required skills to develop and maintain a security solution?
- [ ] Are you able to hire or train specialists to handle the complexities of AI security?
- [ ] Would relying on a purchased solution reduce the need for in-house expertise and allow your team to focus on core business functions?

5. Compliance Requirements

What are the regulatory requirements your solution must meet?

- [ ] Are there strict compliance standards (e.g., GDPR, HIPAA) that your security solution must adhere to and can a purchased solution meet these?
- [ ] If building in-house, do you have the resources to ensure ongoing compliance as regulations change?

6. Long-Term Strategy

Does your organization plan to scale rapidly, and how does each option support that?

- [ ] Is scalability a key consideration for your security solution?
- [ ] How well does a purchased solution accommodate growth and evolving security needs?
- [ ] Can an in-house solution be developed with the flexibility to scale as your organization expands?

As you work through this checklist, if you find that the answers to the questions increasingly point toward the benefits of a purchased solution, your best option will become clear. This structured approach will help you confidently decide whether buying or building a security solution is the right choice to support your GenAI security strategy.

Conclusion

For most organizations, buying a security solution is the more practical choice, especially if you need quick implementation, scalability, and ongoing expert support. Ready-made solutions are designed to be deployed quickly and are backed by dedicated teams that handle updates and maintenance, allowing your organization to focus on its core business objectives without the burden of managing complex security infrastructures.

However, there are exceptions where building a custom solution might be more appropriate. If your organization has highly specific security requirements or if the available market solutions fall short in

addressing your bespoke use cases, developing an in-house solution could be a viable option. This approach is only recommended if you have, or can acquire, the necessary machine-learning and AI security expertise to build and maintain an effective solution.

Ultimately, it's crucial to thoroughly evaluate both options in the context of your organization's unique needs and long-term goals. Whether you choose to buy or build, the key is to ensure that your security solution effectively protects your Generative AI applications and supports the growth and evolution of your business.

Want to learn more about how Lakera Guard can help you build secure AI?

Stop worrying about security risks and start moving your exciting GenAI applications into production. Sign up for a free-forever Community Plan or get in touch with us to learn more.

Book a Demo