WHAT IS SHADOW AI?

In its Top 10 Strategic Technology Trends for 2020, Gartner discusses Shadow AI as a key issue that organizations are going to have to contend with in the coming years. Gartner defines a strategic technology trend as "one with substantial disruptive potential that is beginning to break out of an emerging state into broader impact and use, or which is rapidly growing with a high degree of volatility reaching tipping points over the next five years."

Per that definition, identified trends have the potential to significantly impact organizations and, thus, should be proactively addressed by enterprises. In its report, Gartner predicts that by 2022, 30% of organizations that use AI for decision-making will have to address shadow AI as *the* biggest risk to effective decisions. To be prepared for this, organizations should develop AI policies and strategies that protect against the risks of shadow AI, thus allowing organizations to enjoy some of the technology's benefits.

Understanding Shadow AI

Over recent decades, shadow IT has become a well-known and well-addressed issue for organizations of all sizes. Shadow IT broadly refers to employees using apps or infrastructure that are outside of the control of the organization's IT department. As this has become increasingly prevalent, organizations have put policies in place, often known as BYOD - Bring Your Own Device - to allow employees to use this technology while also allowing the organization to have some control over it. Specifically, it's important that organizations have some control over security, access, reliability, backups, and privacy of devices and technology that employees are using.

Much like other areas of technology, the increased deployment of AI will lead to an increase in the shadow AI environment. Shadow AI simply refers to AI solutions that are not officially known or under the control of the IT department. In addition to specifically addressing shadow AI, in its report, Gartner notes that the democratization of technology will be a key trend in 2020. The democratization of technology means making technology more accessible without the need for extensive training, expertise, or expense. This is a positive trend in many ways, yet a natural result of democratization is shadow AI. As more people have access to AI, there will be more AI usage and solutions that are outside of the control of IT organizations.

Additionally, many organizations lack a unified approach to AI solutions. Instead, they have individual teams or units working to develop and implement AI. This can lead to disconnected solutions that are essentially siloed from IT and other departments and that can contribute to the rise of shadow AI.

Like shadow IT, there are pros and cons to the development of shadow AI. On the one hand, it can be an effective way to bring about innovation and to allow individuals and teams to develop innovative solutions. With it, however, come concerns over security, communication, monitoring, deployment, and scalability.

Benefits and Concerns of Shadow AI

While it obviously raises some organizational concerns, shadow AI is not inherently a bad thing. In fact, it can provide an effective way for organizations to benefit from new technology and some of the increase in productivity and efficiency that AI offers. Further, it can allow individuals and teams to innovate and to come up with AI solutions that are specific to their tasks. Again, this can lead to more efficient and productive teams with better outcomes. Plus, it can improve employee morale and lead to more engaged employees.

At the same time, however, it raises a number of concerns. AI solutions that are outside of the control of IT are difficult to monitor and control. This makes it hard for organizations to ensure that proper security measures are in place and that technology is being appropriately used. Additionally, when AI solutions are siloed throughout an enterprise, it's difficult to share data and information throughout the organization. While shadow AI is not necessarily a bad thing, it's important to effectively manage AI to reduce some of the risks and concerns that are associated with shadow AI.

Shadow AI Management

As AI becomes more accessible and spreads throughout more aspects of organizations, a key issue for enterprises in the coming years is how to properly address this new technology and, with it, the rise of shadow AI. What this means is that going forward, managing AI isn't going to simply be about managing and expanding models. Instead, it's also going to be about managing and preparing for the increase of shadow AI.

Managing the rise of shadow AI requires an organization-wide approach that includes a thorough governance strategy and well-defined policies. This is particularly important as AI begins to spread throughout all aspects of an organization, including marketing, research, legal, HR, and even recruiting. Given its complexities and its likely rise across enterprises, effective AI strategies are going to require increasingly complex procedures, policies, and governance.

When considering AI management, strategies developed to address shadow IT are often a good

place to start. Effective policies thoroughly address key issues including:

- Access Control. This should include organizational management over who has access to AI solutions, including models and data. An important aspect of access control is ensuring that access can be revoked whenever necessary, for example, when an employee leaves the organization.
- Monitoring. Your organization should be able to track the usage of all AI solutions. This helps to determine its effectiveness and to ensure that it's being used appropriately.
- Deployment. It's necessary to be able to manage the distribution of AI solutions as well as any new versions. A good deployment strategy also allows for tracing AI solutions back to the development process.
- Security. Security is obviously a central issue when dealing with AI management. It's important that your organization is able to enforce security controls in order to avoid attacks or data breaches.

The foundations of shadow IT policies are a good starting point for shadow AI policies. Yet, when developing your organization's strategy, it's important to appreciate the additional complexities that come with AI. IT simply involves technology, whereas AI is broader and will require some new approaches to apps, businesses, and even people. That said, starting with a strong shadow IT strategy is a good place to start.

In addition to developing effective AI strategies and policies, many organizations are working to shift their approach to AI. Rather than having siloed innovation or solutions that are specific to departments, consider shifting to a more centralized platform that can be deployed and used throughout your organization.

Broadly speaking, as AI becomes increasingly mainstream, it becomes more important to centralize this technology. Doing so will limit shadow AI while also allowing organizations to more effectively monitor, control, and deploy AI solutions. Further, creating a centralized platform will lead to having the necessary architecture and infrastructure to scale AI solutions. While this might seem like a big shift for many organizations, creating a more centralized solution can help your organization better utilize AI solutions while limiting the risks that often are associated with them.

Conclusion

To help manage some of the risks associated with it, it's important that organizations are aware of shadow AI and its anticipated rise. Creating an AI strategy and shadow AI policies can help to address some of the concerns, allowing organizations to maximize benefits from this technology. Additionally, centralizing AI solutions and creating organization-wide solutions can make it easier for your organization to reduce shadow AI and to more effectively scale, monitor, deploy, and secure AI solutions.