What is shadow IT?

Terence Wong
April 7, 2022 • 6 mins

In a traditional organization, the IT department oversees and manages all IT resources. However, with such easy access to cloud-based IT resources, impatient and time-poor employees often find it simpler and quicker to spin up IT infrastructure themselves, rather than filling out requests and waiting for the IT department. When employees create and use their own IT resources that are invisible to the IT department, this is known as shadow IT.

In 2017, Gartner predicted that the IT department would make fewer technology decisions and individual business units would begin to select technology for their teams, amounting to 38% of technology purchases. In 2019, Everest Group predicted that more than 50% of technology spending in organizations was due to shadow IT. The rise of cloud technology compounds this problem, making it easier than ever for employees to use unapproved IT resources.

Shadow IT poses new questions for organizations. These include:

- How should IT departments respond to shadow IT?
- Is it realistic, or even practical, to track 100% of all IT resources?
- Should there be a more managed approach with accepted risk?
- What tools can help manage shadow IT?

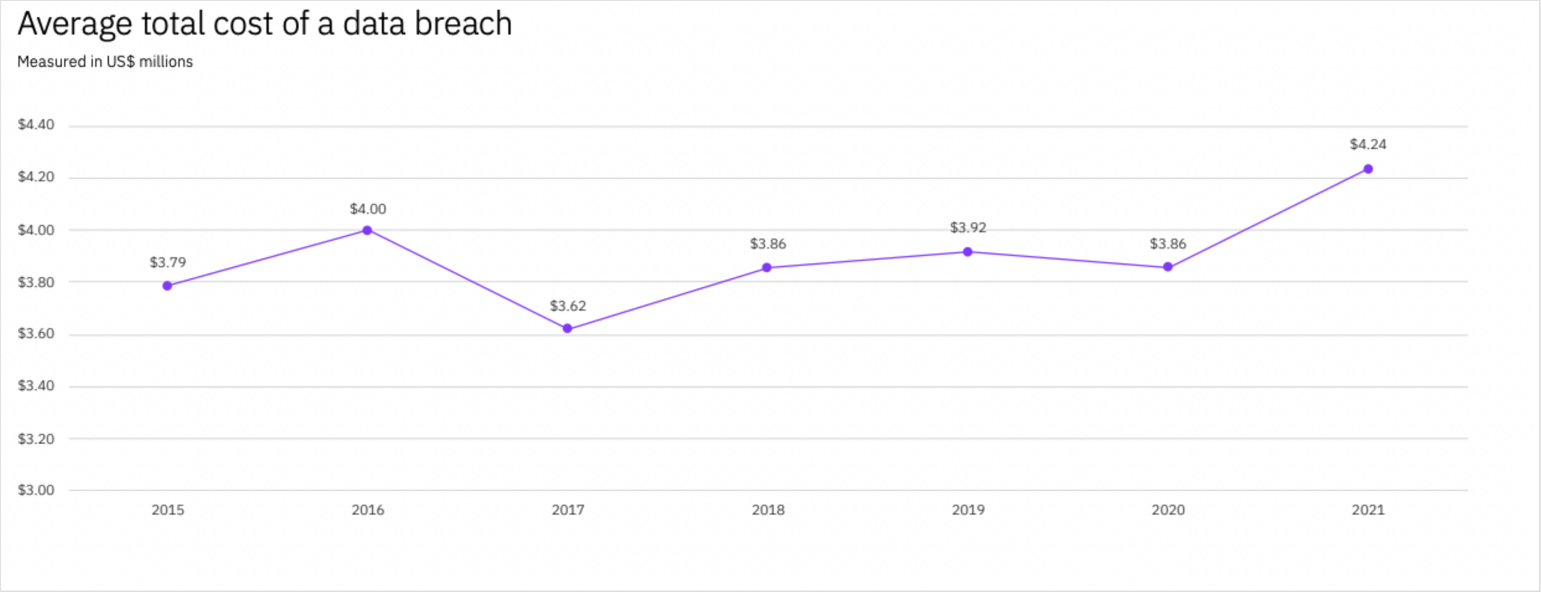
This post explores these questions.

Costs to the business

More teams are taking advantage of shadow IT and this increases the risks of security breaches, as the resources are outside the control of IT departments.

A study by EMC estimates that data loss and downtime contribute to $1.7 trillion in losses each year due to shadow IT security breaches.

In IBM's 2021 Cost of Data Breach Report, the average cost of a data breach rose from USD 3.86 million to USD 4.24million from 2020 to 2021.



Source: IBM

There are also compliance concerns for businesses in highly regulated industries. The General Data Protection Regulation (GDPR) imposes strict regulations on organizations anywhere they collect data from people in the European Union (EU). There are harsh fines for offenders reaching into the tens of millions of euros. As shadow IT increases, it becomes harder to ensure that only authorized employees are accessing sensitive data.

Shadow IT affects operational costs, too. When shadow IT is left unmanaged, services become decentralized as each business unit procures IT for its own needs. One business unit may prefer one product while another prefers its competitor. This can also lead to unpredictable operation costs of cloud infrastructure. Think of all the unmonitored VMs created for a single purpose, always running but never torn down. By allowing business units to procure their own IT infrastructure, businesses lose the benefits of their buying power and their ability to reduce the cost of IT infrastructure.

The true costs of shadow IT come down to a growing unknown resource that has operational and security risks.

Why do employees use shadow IT?

The primary motivation to use shadow IT is convenience.

IT policies can be rigorous. Often, it's easier and faster for employees to procure an IT solution themselves, rather than go through the IT department. Employees may also prefer specific solutions over a prescribed one, exacerbating the issue. Rather than dealing with support tickets, employees might find another solution to the problem, again introducing shadow IT.

Unfortunately, the people who use shadow IT solutions don't usually realize the consequences. They just want to get their job done in a streamlined and efficient way.

Self-service runbooks can address this by ensuring a streamlined experience with governance that gives employees the ability to spin up the infrastructure they need without avoiding the IT department.

Risk mitigation

The unknown nature of shadow IT increases the risk profile of an organization. Shadow IT is wide-spread and growing, so it's a matter of managing the risk. Gartner suggests three risk mitigation strategies to address this:

- Use data security governance to balance local business unit IT (BUIT) growth objectives against the risk of data breaches and financial liabilities
- Deploy shadow IT discovery and data protection tools to enable the safe selection, deployment, and notification of unauthorized cloud services
- Use data security governance to develop and orchestrate consistent security policies across all BUIT for each prioritized dataset

Shadow IT requires governance, discovery, and protection. The solution must be streamlined and minimize time spent in support.

The Shadow IT discovery lifecycle

This image from Microsoft's blog post demonstrates the stages of the shadow IT discovery lifecycle. This supports that any solution to shadow IT should have governance but also compliance.

Source: Microsoft

Reducing the barriers to compliance while maintaining governance is an important step towards managing shadow IT. Octopus Deploy's Runbooks feature helps achieve compliance and governance across an organization.

What is a runbook?

A runbook is a reusable way to execute a commonly repeated task. The types of tasks runbooks can automate include minimizing application downtime, simplifying routine maintenance, and providing self-service operations. Let's look at a request the operations team might receive, refreshing the data in a test database.

Typically, when a developer needs to refresh the data in a test database, the following actions need to be performed:

1. The developer creates a request to the support team to refresh the data in their database.
2. The support team reviews the request to understand the requirements.
3. If the support team needs additional information, they request it from the developer.
4. When the support team has everything they need to action the request, they run through the process of refreshing the data in the database.

Depending on the support team's workload and turnaround, this request could take anywhere from minutes to days, and often the developer has no visibility into the timeline. Runbooks help avoid these pitfalls.

The steps to refresh the data in the database can be captured and executed by a runbook. Runbooks also include all the permissions to execute the task, meaning the runbook can be self-service. This allows the user to execute the task without requesting and waiting for a support team member.

Any task that can be automated can be captured in a runbook, allowing team members to complete tasks that previously needed a dedicated team.

Runbooks also introduce consistency. Imagine a self-service runbook for creating a new AWS account. Users need to set access levels, VPC settings, and other IAM considerations. If 50 different users try to set up an account, this could result in 50 different types of users, which is another challenge. If you apply this to creating VMs, container registries, or other PaaS infrastructure, it's easy to see the issues with shadow IT.

Using runbooks can restrict this process and standardize IT resources. Operations teams can use runbooks to enable monitoring and security on IT resources.

Though runbooks don't solve every hurdle with shadow IT, runbooks can improve IT resource governance and ease of use for end users. According to MRC on managing shadow IT risk:

> The goal of this step is controlled, self-service solutions. Any software you provide must meet two important criteria:
>
> - Self-service: Users must use the solution without bothering IT.
> - Control: IT must still be able to control data and user access.
>
> When you deliver controlled, self-service options, your business gets the best of both worlds. Users get the solutions they need quickly, and IT can still secure the data and applications."

Runbooks let operations teams monitor resources and provide security. They also allow employees to self-serve problems without support.

Conclusion

Shadow IT is any IT resource that lies outside the organization's control. It gives rise to problems with several risks and high costs to businesses.

Businesses need more governance, discovery, and protection of IT assets. Employees want more streamlined processes and the ability to solve problems without too many support tickets.

Runbooks can solve these issues by providing a self-service way to run common tasks. Applying this concept to a problem like setting up cloud accounts provides standardization for IT assets.

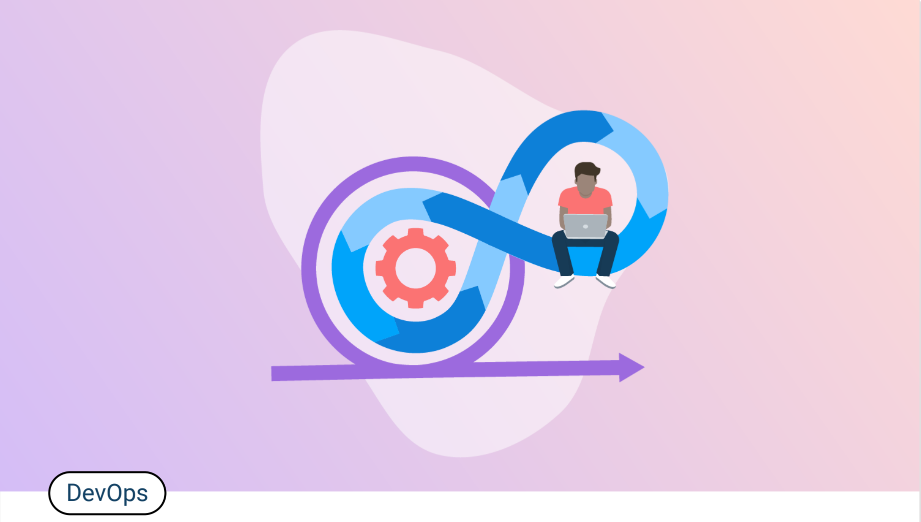
Read the rest of our Runbooks series.

Happy deployments!

Tagged with: DevOps Runbooks Series Runbooks

Related posts

DevOps



DevOps

Comparing Lean, Agile, and Continuous

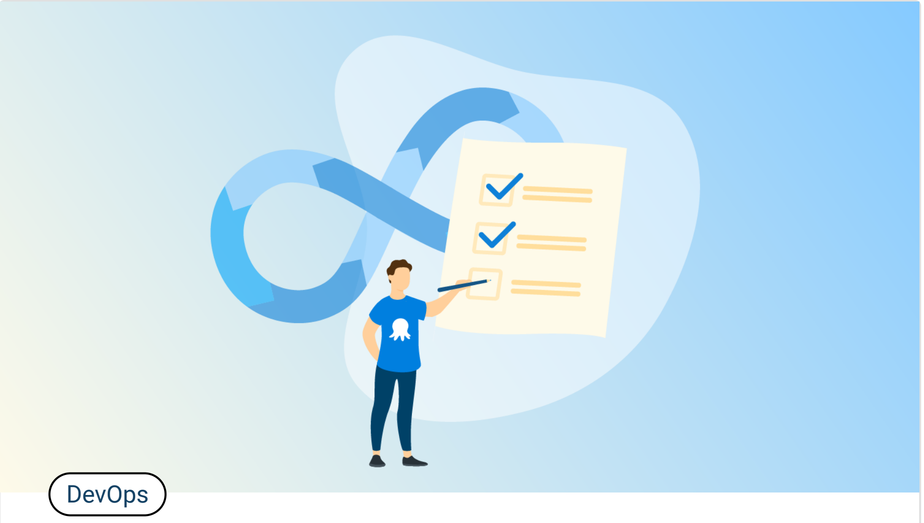
Common mistakes in DevOps metrics

Steve Fenton

Delivery

Steve Fenton

December 5, 2022 • 6 mins



DevOps

Best practices for CI/CD

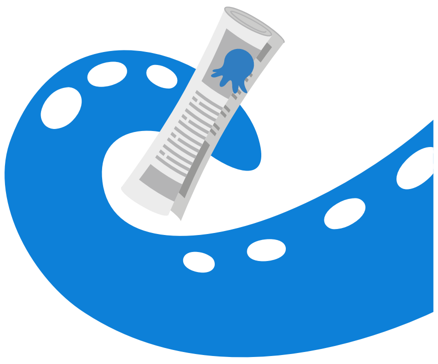
Terence Wong

November 30, 2022 • 5 mins

Newsletter

Logged in as Terence Wong (terence.wong@octopus.com)

Join ~48,000 DevOps professionals and sign up for the latest Octopus news, events, and opinions. No spam. Unsubscribe at any time.



Subscribe

Your privacy is important to us. Read more in our Privacy Policy.