How to Detect and Control Shadow IT

TechRounder PDF Edition

Live article: https://www.techrounder.com/technology/how-to-detect-and-control-shadow-it/

By Vipin PG | Published January 6, 2023 | Updated January 4, 2026 | Format: Guide | 6 min read

Quick answer

Shadow IT refers to the use of information technology systems, services, or software within an organization without the knowledge or approval of the organization's IT department. Shadow IT includes using unauthorized software or services and using unauthorized networks or cloud services.

Shadow IT refers to the use of information technology systems, services, or software within an organization without the knowledge or approval of the organization's IT department. Shadow IT includes using unauthorized software or services and using unauthorized networks or cloud services.

A McAfee study concluded that 80% of employees have admitted to using unapproved SaaS tools to complete their work.

Shadow IT is difficult to control. But, it needs to be controlled. Why?

It can pose several risks to organizations, including security vulnerabilities, data breaches, compliance issues, and potential legal liabilities. It can also create problems with integration and interoperability and difficulties in managing and supporting the IT systems being used.

Why do employees resort to shadow IT?

Shadow IT is done on SaaS applications that companies don't officially procure. The applications used in any organization can be classified into three categories:

1. IT managed applications
2. Non-IT managed applications (mainly done by department heads of different teams)
3. Employee purchases

Shadow IT falls into the third category. But first, let's deep-dive into some of the reasons why employees do shadow IT:

- The company approval process is too long - employees feel they can't wait for long.
- On average, employees nowadays are more tech-savvy compared to previous years. As a result, they don't feel the need to involve people from the IT teams before making technological decisions.
- There's an increasing number of cloud services accessible to employees.
- Teams cannot rely on in-house developers to build a solution to the existing problem - it is much easier to find a ready-to-use solution.
- Employees might feel their productivity increases when they use certain applications (daily tasks can be completed faster with the help of certain tools). For instance, an employee might feel like a video chat application is important for certain small tasks.
- There's a mismatch between the development teams and other departments. For instance, a business-side employee might need an application that the development team might not necessarily agree with and vice versa.

How to detect shadow IT?

The most primitive way is to send out a form to all employees. The form should ask for the names of the applications/software tools they use.

Consolidate all the answers in a spreadsheet. Compare the applications to the ones that the company's IT department has officially procured. Shadow IT is all the applications that are not procured through the official channel.

This method can work for companies that are small or mid-tier.

The best bet for large organizations is to have an automated application discovery system (more on below).

Companies with strict regulatory requirements can invest in a smart, automated tool such as a SaaS management platform. However, sending out forms is a cumbersome process, especially when there are hundreds of employees.

A complete application portfolio discovery involves:

- The number of existing licenses
- The purchase type
- The total number of seats
- The renewal period for each application
- The total amount spent (on deployment, subscriptions, etc.)

Once the applications are detected, the first step is to perform a risk assessment.

How many applications are active? How many tools are being utilized up to their optimal level? Are all the applications compliant? Is there any application that runs the risk of a security breach?

What are the risks involved with shadow IT?

The first and most common risk is that of security.

If employees use applications without the approval of IT departments, the following risks can arise:

- Most applications integrate with existing systems - meaning that existing data is fed into those applications. This poses a potential data breach risk.
- The IT team may not be aware of the new application and won't be able to provide support when the need arises (to fix bugs or an error due to a broken application).
- There's a risk that the employee uses an application that results in non-compliance with industry regulations.
- Different team members might be using other applications for the same task, resulting in inefficiencies.
- The IT department will not know that the new applications/tools take up extra space or bandwidth.

How can companies control shadow IT?

For ease, let's create a simple framework that companies can follow to prevent shadow IT. The framework consists of four steps:

Discovery of Shadow IT

The first step in preventing shadow IT is identifying its existence within the organization. This can be done through the following:

A cloud access security broker (CASB):

With a CASB, data can be collected related to the websites used by employees.

However, using a CASB means you're breaching employees' privacy. A CASB is also not great at discovering new SaaS applications. The employee might be using local credentials for the SaaS applications, which can't be detected.

Regular audits

The software used within the company can be found through regular audits and assessments of the IT infrastructure.

Mitigating the risk of shadow IT

If you've detected some unauthorized software being used, the next step is to mitigate the risk. The first step is to check if the vendor has the required certifications (the best-case scenario).

If the answer is not affirmative, check whether confidential or sensitive data is compromised through the software. Do reverse engineering to check the systems integrated with the tool and then check the data used in those systems.

Shadow IT accounts need to be secured

A SaaS tool can be accessed through any device, so it's much harder to secure than hardware. If you come across a SaaS tool that violates the policy of a company or if an employee has left the organization, the account needs to be locked.

The IT team needs to ensure that no one has access to the system. The account should then be de-provisioned.

Take steps to reduce shadow IT

If a particular SaaS application is risky for the company, then all employees need to stop using it with immediate effect.

Clear policies and procedures for using IT systems and services should be established.

In addition, it provides employees with the tools and resources they need to do their jobs effectively and regularly monitors and audits IT systems to ensure compliance.

If the problem of shadow IT persists, then the best route forward is to set up secure points. Have an additional layer of security. Block access to the most commonly used SaaS sites by employees.

A smart alternative would be to analyze why employees use a particular SaaS application too often. This implies that the existing applications aren't good enough or don't serve their respective purposes. An effective IT department will ensure to procure of such SaaS solutions instead of banning access.

A quick summary of Shadow IT

Let's analyze some of the key takeaways related to Shadow IT that were discussed in this article:

1. Companies should have clear policies and procedures that outline the acceptable use of IT resources and the appropriate channels for acquiring and implementing new technology. These policies should be communicated to all employees and consistently enforced.

2. Encourage open communication between employees and IT departments. Identify areas where employees may be using shadow IT and allow IT departments to address any needs or concerns driving employees to seek alternative technology solutions.

3. Ensure that the IT department can provide adequate employee support. Reduce the temptation for employees to seek alternative solutions when they are having issues with company-approved technology.

4. It is important to regularly review and update IT policies and procedures to ensure that they align with the organization’s changing needs and its employees.

Ultimately, the goal is not only to prevent the development of shadow IT but to ensure that the company is effectively managing its IT resources. The best way to do this is to allow teams to have a say in the software that should be procured. This way, the most utility can be gained from the existing software, and shadow IT can also be prevented.

References

1. skyhighsecurity.com - en-us / cybersecurity-defined - https://www.skyhighsecurity.com/en-us/cybersecurity-defined/what-is-cloud-security.html

2. zluri.com - blog / shadow-it - https://www.zluri.com/blog/shadow-it/

3. cloudcodes.com - blog / what-is-shadow-it-and-its-impacts.html - https://www.cloudcodes.com/blog/what-is-shadow-it-and-its-impacts.html