Bring Shadow IT into the Light:

Simple steps for a secure digital transformation

Microsoft

Introduction

Today, moving to the cloud is the cornerstone of a digital transformation strategy. The cloud can enable greater innovation, customer engagement, productivity, and business model transformation. Every organization, strategically, is in different stages on their journey to the cloud.

However, most employees have already taken enterprises into the cloud—whether their organization is ready or not—by using software as a service (SaaS) applications and cloud services at work. This is widespread across enterprises.

This trend, called shadow IT, creates challenges for organizations in IT and application management, security, and compliance. Not knowing what applications your employees are using and where sensitive data might be going introduces tremendous risk into your organization. Traditional network security solutions are simply not designed to protect data in SaaS apps and cannot give IT visibility into how employees are using the cloud.

The extent of shadow IT use is not well known by many enterprises. Some studies show that only 8 percent of companies know the scope of shadow IT at their organizations.[1] Do you know the scope in your organization?

Your company might be tackling this issue head-on, or is just starting to figure out the extent of shadow IT use (or is hesitant to even find out!). No matter where you are on the journey, you know that understanding the extent of shadow IT and managing it, is absolutely critical to the security of your organization.

Regardless of where you are with shadow IT in your organization, read on to learn about steps you should be taking today to help your company manage shadow IT, and its inherent security risks, while empowering employees to work in the ways they want.

Only
8%
of companies know the scope of shadow IT at their organizations.[1]

Understanding shadow IT

Employees expect to use the applications and devices they're most familiar with to get things done—usually without a complete understanding of the security risks. There's no way to stop it—nor should you. The reality is that shadow IT is the new normal of modern enterprises. Gaining visibility, control, and threat protection of shadow SaaS apps are the first steps in managing risk and facilitating the digital transformation that has already started at your company.

Not all cloud applications and services can meet your specific security and compliance requirements—especially if you're in a highly regulated industry. Not knowing if and where your employees are transferring sensitive data is a liability your organization cannot ignore.

Once data is transferred to the cloud, the responsibility for protecting and securing that data typically remains with your organization. Security in the cloud is a shared responsibility between you and your provider. However, ultimately, you and your organization are accountable and responsible for protecting corporate data—no matter where it is.

Know the hidden risks of shadow IT

Employees are signing up for easy-to-deploy cloud services without notifying IT who would normally perform risk assessments and fully understand the impact that using these services may have on security and compliance. Some issues that may arise are:

- Unencrypted data storage and connections to services
- Lax password and authentication requirements
- Inability to meet eDiscovery requirements
- Backup and recovery that doesn't meet internal standards
- Legal issues regarding who owns what data when using a cloud service
- Users unwittingly sharing sensitive data through public links
- Noncompliance with varying international and industry regulations

How can you protect your business without compromising innovation?

Blocking shadow IT is not the solution. Employees will always find ways around restrictions. Too rigid control deters innovation, conflicts with unplanned and demanding technology requirements, stifles productivity, and can have a negative impact on your organization's ability to keep high-caliber talent engaged.

Rather than blocking shadow cloud app usage, organizations need to think about how they can offer flexibility while extending the same protections and security they've put in place on-premises.

23%

of employees believe their departments handle security without IT's help.[2]

There are three steps to building a plan and course of action for shadow IT in your organization:

1. Gaining visibility is the first step in addressing shadow IT. Understand what applications your employees are using, where they're logging into them, and whether they're complying with your organization's security regulations. This will enable you to understand what level of risk you're at and develop strategies—such as blocking the apps that don't comply with regulations in your industry—to adjust that risk as needed.

2. Get control of cloud application use and data sharing. Develop policies that specifically define what applications are okay to use, and how and what data can be transferred to the cloud. Ensure these policies meet your company's regulatory requirements.

3. Protect against threats. Define a baseline for cloud application access and usage at your company and then look for patterns and behaviors that detract from the baseline. Decide if these anomalies are threats and develop strategies and tactics to address them.

Traditional security solutions, such as firewalls, intrusion prevention systems, and data loss prevention tools, are not designed to give IT comprehensive visibility into, or control over, how employees are using SaaS apps and cloud services.

IT needs tools that are specifically designed to monitor how employees are using cloud applications, help manage risk across the cloud services in use, extend internal security requirements into the cloud, and help enforce reasonable and effective SaaS policies.

With better visibility, protection, and control over shadow IT, you can mitigate risk while giving employees the flexibility to use familiar apps without sacrificing the security and compliance your organization demands.

87% of senior managers admit to regularly uploading work files to a personal email or cloud account.[3]

What is a Cloud Access Security Broker?

A Cloud Access Security Broker (CASB) is one of the solutions available today to help you manage shadow IT. A CASB extends your security policies into the cloud. It starts by giving you a detailed picture of what cloud applications employees are using, and provides you with the tools to control that usage and protect your organization.

Here's how a CASB can help you execute against your three-part plan:

VISIBILITY

A good CASB solution starts by first discovering all the cloud applications in your network, from all devices, and then providing a detailed risk assessment for each service discovered.

Some CASBs rely on installing agents on all company devices, a process that is both cumbersome and ineffective in the age of BYOD. A more modern approach relies on collecting information from firewalls and proxies.

Some solutions assign cloud services an individual risk score, allowing IT to see how their organization is operating in the cloud and to determine which apps to sanction.

CONTROL

Even after you have an approved list of sanctioned apps, you want to maintain control over how they are being used. This is especially important if your organization operates in a highly regulated industry, such as finance, healthcare, or government.

A CASB should allow you to set and enforce granular policies to provide IT with comprehensive control over sanctioned apps. It should automate enforcement of your policies. For example, the CASB solution can detect if a user is trying to share a set of sensitive data and automatically restrict the ability to share that data with users outside of your organization who shouldn't have access to critical company data.

You should be able to use these controls to extend any existing enterprise DLP policies to your SaaS applications and to run dynamic reports on violations of your policies.

PROTECTION

With comprehensive visibility into how employees are using the cloud, a CASB should then provide you with ongoing, enhanced threat protection for your cloud apps and help you stay ahead of cyber threats.

Every CASB vendor provides a different level of threat detection. At the advanced level, you can expect machine learning to learn how each user interacts with each SaaS app and behavioral analytics that can then assess the level of risk in each transaction.

This might include impossible use scenarios, such as simultaneous logons from two countries, or other suspicious behavior such as the sudden download of terabytes of data, or multiple failed logon attempts—which may signify a brute force attack.

Make shadow IT work for you

Better visibility, control, and protection can help you manage shadow IT. In addition, IT must work with employees to establish a SaaS policy that aligns to business goals.

Keep an open dialogue with line of business managers that allows them to evaluate SaaS options and aims to provide employees with secure access to a broad range of SaaS apps.

Once you have established a realistic SaaS policy, communicate it broadly to the company and work with business leaders to share these policies with their groups.

Help employees understand ways they can protect the organization, and share insights into high-profile data breaches reported in the media to raise awareness among employees of impacts of a security incident.

By following a few simple steps to managing shadow IT, developing a reasonable SaaS policy in partnership with business groups, and educating employees on the risks and the role they play in cybersecurity, you will be on your way to enabling a secure digital transformation in your organization.

> Once you have established a realistic SaaS policy, communicate it broadly to the company and work with business leaders to share these policies with their groups.

Learn more about how Microsoft can help you bring shadow IT into the light.

PROTECT APPS AND DATA

References

1 "Cloud Adoption Practices & Priorities Survey Report." Cloud Security Alliance. January 2015. https://downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf

2 Worley, Candace. "Shadow IT: Mitigating Security Risks." CSO. June 21, 2016. http://www.csoonline.com/article/3083775/security/shadow-it-mitigating-security-risks.html

3 "On the Pulse: Information Security Risk in American Business." Stroz Friedberg. 2013. https://www.strozfriedberg.com/wp-content/uploads/2014/01/Stroz-Friedberg_On-the-Pulse_Information-Security-in-American-Business.pdf