AUGMENTT

The Complete Guide to Gaining Control of Shadow IT

V 1.0

AUGMENTT TECHNOLOGY

ISSUED	REVISED
01.01.2021	01.25.2021

Table of Contents

AUGMENTT

INTRODUCTION

The COVID-19 global pandemic is upending business operations around the world. The sudden and swift shift of millions of workers from on-site to remote work environments challenged and continues to challenge organizations as never before.

In the rush to virtually connect remote workers to the workplace, however, employers and MSPs may have overlooked security — and cybercriminals have already begun to take advantage.

This is the kind of situation that gives MSPs and cybersecurity teams nightmares. Employees are now using unsupported software (Shadow IT) that opens tons of vulnerabilities.

This leads to a host of new challenges. Your technicians are now trying to manage businesses that have employees scattered all over with poor security standards.

Not all is lost, securing your clients' remote work teams now will likely save much time and money later and give your clients a long-term advantage. To do this, it's necessary to detect and eliminate (or at the very least manage) Shadow IT.

We give you the strategy to do this in the following eBook.

What is Shadow IT?

Gartner has found that shadow IT can account for 30 to 40% of IT spend in large organizations.

Such a large amount should be enough to scare any IT executive. But what exactly is shadow IT?

Shadow IT refers to software that is built, deployed, maintained, and managed without the involvement of an organization's IT department.

The accessibility and prevalence of SaaS tools–they're just a few clicks away–means that employees can bypass security controls.

In other words, all someone needs are a laptop, an internet connection, and a credit card and an employee can get started more quickly and less expensively than going through official IT channels.

This leads to a host of problems, from unsecured data to compliance headaches.

AUGMENTT

Why Does Shadow IT Exist?

Shadow IT exists because it's easy. As individuals, organizations, and enterprises have become more comfortable with cloud offerings, the corporate world has become far more accepting as well.

With it, expectations have changed. People now want their IT to be faster, better, and cheaper. (It's often MSPs that add 'secure' and 'compliant' to that list.)

These desires explain why shadow IT exists. Often, the rise in shadow applications is because IT departments are not keeping up with the ever-changing expectations of the business. This is a risk in and of itself, as this adaptability is critical when facing increased competition outside the organization.

IT departments need to keep up with this demand – but they also need to maintain innovation momentum and rapid delivery, and deliver secure and compliant offerings. They can't become a blocker, but they also have to deal with the real risk of shadow IT.

It's definitely not an easy task, but talking from experience it's certainly an achievable one.

The Shadow IT Problem Created by Remote Work

Business continuity and adaptation was the focus for many during the early weeks of the Coronavirus crisis.

Businesses drastically increased capacity to meet the needs of businesses and consumers: virtual meetings, live streaming, automated customer assistance, business intelligence driven by machine learning, online education, and more.

In the rush, many companies and their MSPs compressed or ignored their standard security processes. While understandable given the speed the business demanded, those policies exist to protect the business from bad actors (internal and external).

The reason these things take time is most companies have very complex IT environments. Many employees now use remote desktops and unapproved file sharing and applications. (This is where shadow IT comes into play.)

Consequently, many companies can't answer a basic question: "what applications are my employees using right now?" This means that security breaches could be occurring as we type this and remain undiscovered for months.

This creates tons of other issues, including:

Without deep visibility and granular control over data-sharing activities in SaaS applications, the risks of inadvertent or malicious data leakage grow as users share sensitive data, sometimes to untrusted users or applications.

Poor password practices can go unchecked as people sign up for new accounts, they may use weak passwords or reuse old passwords.

Just as it's your responsibility to protect data in SaaS applications, your clients also need to protect their users. Managing access rights to numerous SaaS applications is complex, leading to mistakes such as employees being given higher access rights than they need.

SaaS applications are often the first insertion points for malware and the last exfiltration points for data loss, and as such, they need to be protected from malware threats.

Consider this scenario. A member of your client's human resources team uploads employee data to a shared folder within an unsanctioned file-sharing SaaS application. The data happens to include the health plan account number for each employee.

Personal health information (PHI), including health insurance account numbers, is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Inappropriate storage or sharing of this type of content could mean your company is noncompliant with the regulation and subject to hefty fines.

There are hundreds of examples of this seemingly innocuous behavior that can create major risks to your clients' businesses.

How to Find Shadow IT

Generally, there are three possible strategies for the collection of shadow IT information: 1) technical analyses 2) interpretation of help desk requests and 3) direct surveys of employees.

Depending on the company size and model as well as on the authorization of each department, some companies also look at the statements from the accounting department to help their analysis. (That's because as soon as shadow software costs money, it will appear in financial statements and can be identified and traced.)

The problem with all of those methods bar the technical analysis is that they are time-consuming and can be inaccurate.

A technical analysis or SaaS audit enables you to bring these apps out of the shadows. Then once you've found what these applications are you can either make them more secure or shutter them completely.

How does it work?

Regardless of the data source, our platform Augmentt Discover can extract critical SaaS usage data and provide you with actionable results using an advanced log frame analysis framework. This includes trended usage over time, by individuals or entire departments.

We're able to do this by maintaining one of the largest known SaaS Application databases in the industry. It currently contains over 15,000 vendors and applications, including 50+ sub-categories and 20 different security, financial, and productivity and profiles.

How to Secure the Newly Discovered Shadow IT

Telling staff not to sign up to SaaS apps "because they can't" will likely get you nowhere. That's especially the case if they see no other option to enable their work.

Plus, as we've written before, sometimes Shadow IT can make your employees more productive. That's because:

Shadow IT solutions often fill a gap between what's available to the employee and what they need. Employees are generally happier and more productive when they're able to use the tools they know and like. (Some companies even list it in their job postings as a benefit — further proving how critical the right tools are to attracting and retaining talent.)

What we're getting at is that a shadow IT policy that allows employees to experiment with new tools while mitigating Shadow IT risks is a competitive advantage. It's also achievable.

On top of this, once you discover the SaaS apps in the shadows, you'll likely find there is a wider range of tools than you expected.

For example, your client's sales team might be using a CRM, and their human resource team might find itself texting candidates from a text messaging service. These SaaS applications will be used daily and by many end-users with varying degrees of technical familiarity.

Due to business continuity, you're not going to want to shutter these applications and will likely want to secure them instead.

The Unique Challenges of Securing SaaS Apps

Many SaaS applications don't have granular security controls that can recognize managed (corporate-owned) versus unmanaged devices and enforce access rules accordingly.

Although some recognize and block unmanaged devices, they don't have the ability to selectively allow access to certain functionality.

Completely blocking users from using their personal devices to access the SaaS applications and data they need to do their jobs effectively is often not a viable option.

Secondly, many organizations aren't aware that security is a shared responsibility with the cloud service or application provider.

In other words, although the cloud service provider secures the components of the cloud infrastructure, it's the SaaS customer's responsibility to protect users and data.

Finally, SaaS applications are particularly vulnerable to malware threats, making them effective distribution media for cybercriminals. Features such as automatic syncing make it easy to instantly distribute malware.

Evaluate Your SaaS Vendors

The problems are often already incepted at the first stage – procurement. Typically, in organizations, people will go out and purchase an application to cover a specific need.

These purchases are important since the application might be of strategic significance. A disadvantage of this is that these types of purchases need to happen quickly and tend to omit the involvement of IT. This contributes to the problem of Shadow IT.

Many SaaS providers can share some sort of report on their security posture. You could also create an internal checklist or questionnaire for your clients to evaluate the security of the provider.

You should consider asking questions like:

- How will they let you know of known or suspected incidents, and when?
- How will the provider monitor the solution themselves?
- How do they install security patches, ensure versions are current and keep the solution free from security vulnerabilities?

Many SaaS providers can provide evidence to indicate how well they have implemented their security. For example, the Cloud Security Alliance's (CSA) Security Trust Assurance and Risk (STAR) Program is one third-party certification.

Finally, some vendors share the results of their own security tests or allow customers to perform penetration tests; this provides a better understanding of vendor security practices.

Reconsider Your Security Architecture

The adoption of SaaS means that you'll also need to reconsider your client's broader security architecture.

Many cloud providers recommend whitelisting solutions to enable their customers' employees to access a particular solution via their office network.

As we mentioned before, the problem with this approach is that it's now easy for employees to bypass the office network and use other connections to the solutions they use–especially given the proliferation of remote working.

People might not even log into an office network at all, so IT has to ensure that these endpoints are secure even when they're not connected to the network.

Beyond a BYOD security plan, you should also include additional security measures for their SaaS apps like multifactor authentication.

Deploy a security product that differentiates access between managed and unmanaged devices to protect against the increased security risks inherent with personal devices. For instance, you could allow downloads to managed devices but block them for unmanaged ones while enabling access to core functionality.

Secure Your Weakest Link

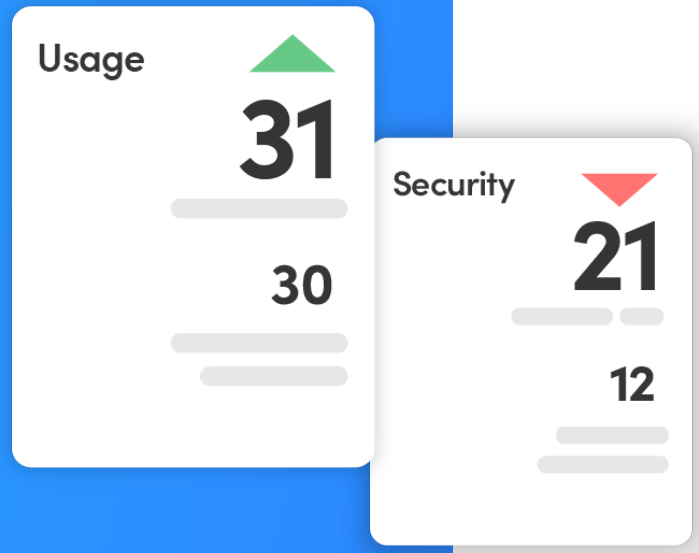
Most employees don't use shadow IT with bad intentions but to complete tasks that companies – and they need to be honest with themselves at this point – have not provided the right tools for.

In other words, most employees don't recognize the security risks of their actions. To reduce these, employees need to be trained, and you need to make sure that they understand the risks connected to shadow IT. You need to create awareness for unauthorized systems and software.

Start with user training and interactive coaching to identify and help change risky behavior. Then, give your security team tools to help them monitor and govern SaaS application permissions.

Look for a product with robust access controls, including:

- Multi-factor authentication (MFA) to strengthen access control
- Role-based access control
- Protection for administrative accounts
- User access monitoring that can detect malicious or risky behavior



Gaining Control of Shadow IT

Most businesses will agree that the benefits of SaaS applications—improved agility, faster time to market, greater productivity, easier collaboration, and more—outweigh the challenges of managing their usage for proper security and governance.

However, with employees using more SaaS applications every day and storing company information, including sensitive data, in the cloud, MSP leaders must take immediate steps to protect their clients from data loss, malware threats, noncompliance, and other serious risks to the business.

AUGMENTT

Take back control of your software,
get in touch with us today.

www.augmentt.com

e: info@augmentt.com

p: 1-888-670-8444