Solution Brief

5 Steps to Detect and Control Shadow IT

Employees at every company will naturally use the best tool available to get their job done. For knowledge workers, this often means using an online SaaS application, which mayor may not be officially sanctioned by the central IT group. Many use the term shadow IT, or now more frequently referred to as business-ledIT, to describe the purchase of technology that is not officially sanctioned by IT. As the number of SaaS applications have increased, workers have naturally adopted a slew of online tools, and most of the shadow IT today are SaaS applications. Despite the industry's best efforts, shadow IT has not gotten smaller but has increased and is close to becoming legitimized as a viable IT strategy that provides competitive benefits.

The traditional strategy was to stop shadow IT in all forms because of the security risks. However, the risks of all shadow IT are not equal, and there are documented benefits for companies that allow employees to acquire the technology they view as the best tool for their job. So rather than stopping shadow IT, a better strategy for CIOs and CISOs is to implement tools that set up the appropriate guard rails to control it to ensure that employees adopt tools that adhere to the company's security and compliance policies.

Based on the work Grip has done with hundreds of companies, we have seen the following five step framework highly effective in helping companies create a secure, workable framework.

1. Discover Shadow IT

The first step to controlling shadow IT is to identify it to get a complete picture of the extent to which shadow IT is prevalent in your organization. Much of the shadow IT is aaS, and even hardware technology almost always has a SaaS component to run it. Most companies use a CASB for SaaS discovery and security, but we often receive the feedback that CASBs are too noisy. They do a great job of collecting the data and identifying who is going to which website. However, what they are not as good at is discovering new SaaS applications that are being used in a company. The data may be there, but an analyst usually must do additional work to figure out whether an account has been created, especially if the user is using local user credentials and not an identity provider. It would be better if the correlated data were presented to the analyst so that they just need to take action and achieve the desired security outcome.

The solution to discovering shadow IT is to select a tool or method that is automated and provides the right trigger, i.e., account has been created using business credentials outside of the other IAM solutions. Having all this information in logs or having to merge or triangulate data on some regular basis is surely a process destined to fail. A tool like Grip's SaaS security control plane is recommended for this step.

2. Prioritize Shadow IT Risk Mitigation

You never know when an employee will acquire technology, and there will be peaks and valleys. What you can know for sure is that there will be a steady stream of new technologies that your employees will acquire and start using. Depending on the number of employees in your company, it can range from a few per week to tens or even hundreds. Given the volume of shadow IT entering the company, prioritization becomes extremely important because the risks vary.

Prioritizing risk mitigation is critical a critical step. You cannot always use a hammer to de-risk shadow IT because not all shadow IT are nails. The level of risk a technology poses to your company goes beyond whether the vendor has received industry certifications such as SOC2 or ISO 27001. These certifications are commonplace, and even startups are now receiving them. Rather than focusing on the risk of the vendor's controls, a better approach is to assess enterprise risk based on the following factors such as:

· Does the employee understand the company's security and risk policies for using buying and using technology, software, or SaaS?
· Will any sensitive, confidential, or regulated data be used?
· Who within the business line organization approved the use of the technology?
· What systems will the technology be integrated with?
· Will any non-employees be users of this technology?
· How many other users in the company are there?

3. Secure Shadow IT Accounts

Securing shadow IT is often easier said than done. Hardware is straightforward assuming you are able locate the physical device in a location or on a network. Software, almost always SaaS, is much harder because it can be accessed from a company network on a managed device or from a different location using an unmanaged device. SaaS security products, for example CASBs, assume that you can control the network, identity, or device, but the reality is that you may not control any of them.

The best way to secure SaaS is to lock the SaaS account itself if you feel it violates company policy or if the employee is no longer with the company. De-provisioning the account itself is still desirable but securing it so that nobody has access to the account is a critical first step.

4. Orchestrate Security Across Control Points Mitigate Shadow IT Risk

Once the shadow technology has been secured, the next step is to orchestrate the securing of this application through other secure points. For example, if a SaaS application has been deemed as being too risky, then every user of that application in the company should stop using it.

As an additional layer of security, you may want to block access to the SaaS site on the network or set an alert every time somebody creates a new account.
Orchestration is also important when data from threat intelligence feeds or third-party risk management systems indicate that a SaaS application has been breached or that credentials have been found on a marketplace. Users with breached credentials should be forced to go through every account they have and reset their password. Though all of this is possible in some way with existing tools, the actual workflows have often not been designed. SaaS security products with out of the box automation goes a long way towards ensuring that security teams unify the control points, analytics, telemetry, and operations to secure and control shadow SaaS.

5. Embrace Shadow IT—Securely

No matter how hard you try, shadow SaaS will continue to grow. In many ways, it is like the bring your own device (BYOD) trend that is now standard at most companies. As consumer technology became as powerful as enterprise products, workers found it easy and more convenient to use their consumer devices for work. Eventually companies gave in, and products designed to allow BYOD were adopted because the benefits outweighed the costs. The same thing is happening with shadow IT, and more specifically SaaS. Workers no longer need IT's assistance or permission to purchase the most powerful applications in the world. They just need an email address and credit card, oftentimes using free accounts that can be upgraded later. IT and security teams need to acknowledge the benefits and create a framework that lets employees use the right tool for the job while maintaining governance and control over the technologies and data of the company.Technology like RBI can be used but may not be enough.

Identifying Shadow SaaS with Grip

When detecting shadow IT and attempting to control it, it is vital to understand their security impact shadow IT can have. At Grip, we offer a platform that simplifies identifying shadow SaaS called the SaaS Security Control Plane (SSCP). This technology enables your business to discover, prioritize, protect, and organize SaaS security.
Our shadow SaaS discovery solution requires fewer personnel and resources than competitors and takes less time to install. To learn more about SaaS security with Grip, download the datasheet today or if your are interested in a demo to see how an SSCP can help your SaaS security program, you can get a free SaaS security risk assessment from Grip today!