ARMOR™

BETWEEN YOU AND THE THREAT

Out of the Shadows

HOW SHADOW IT BECAME KEY TO MULTI-CLOUD STRATEGIES AND HOW YOU CAN BENEFIT FROM IT

Summary

Until recently, shadow IT has been the boogeyman in the corporate network. However, observant business leaders have noted that the unintended consequence of unauthorized cloud utilization is greater flexibility for enterprise information processes. Shadow IT can help organizations manage third-party software and solutions with greater agility and cost-efficiency. In addition, it allows business units and technology groups to take advantage of enterprise solutions without disturbing the bedrock of their larger IT infrastructure.

Of course shadow IT is not without security risks. Just like any hosting solution, the right security approach will allow an organization to enjoy its benefits while controlling its risks. If done correctly, it could be the genesis of a successful multi-cloud strategy.

This white paper explores the transformation of shadow IT from a burden to a boon and examines ways organizations can leverage a multi-cloud strategy for improved performance - while maintaining a consistent security posture.

Out of the Shadows

Lurking in the corners of your business units is a ghost infrastructure called shadow IT. No ouija board was used to open an unearthly portal, and your office campus probably wasn't built on an abandoned cemetery. These shadow IT applications—unauthorized, unaudited, and unmanaged—were invited into your network by your own workforce.

Shadow IT are the systems and solutions deployed by workers without authorization from their organization's IT team. Don't blame the employees for going rogue: they're just trying to do their jobs as effectively as possible, never thinking their little apps will have any impact on their organization's security posture.

CIOs and CTOs know shadow IT is operating inside their organizations, but most underestimate its scope. In fact, most CIOs think about 50 cloud services are running inside their companies when, according to Cisco, there are more than 730.[1] Business leaders may attempt to prevent shadow IT with security policies and stern warnings, but those who take this approach are missing an opportunity: when managed properly, shadow IT can provide an organization with a significant competitive advantage.

Enlightened executives are dragging shadow IT into the light and utilizing it as dispersed IT operating in a multi-cloud environment for enhanced performance.

730+

Most CIOs think about 50 cloud services are running inside their companies when, according to Cisco, there are more than 730.[1]

We Tried It, We Liked It and We're Bringing It to Work

The way people use their personal smartphones, tablets, and laptops has changed the way they want to perform their work. Users have come to expect the convenience of syncing documents and data across devices, thanks to services like Dropbox and Basecamp. To users, there is no difference between sharing their kids' soccer schedules and sharing their departments' quarterly sales reports.

The business strategy of many SaaS products has encouraged this crossover from the consumer market to the business market. "Land and expand" marketing starts with free subscriptions for individuals, who then invite their coworkers to sign up, and soon the entire department is using the tool. Eventually, the product may gain enough traction in the organization to catch the IT department's attention, and only then can the product be properly vetted.

Shining a Light on Shadow IT

Shadow IT is the very definition of an "unsecured cloud" because there are so many unknowns. IT has no way of knowing which applications and how many instances of each are in use, who is using them, or if they're secure, so there's no way to mitigate potential weaknesses.

The chances of redundancy within a shadow infrastructure are high; perhaps dozens or hundreds of employees all have their own accounts with a SaaS provider, and perhaps they're using the same weak single-factor passwords they've been using on their home desktops for years. Every personal account that's used to transmit or store corporate data creates another vulnerability.

Complicating things further is the ability of many SaaS products to easily share data with other SaaS products, sometimes resulting in unintended consequences. For instance, a federal agency's technology team, called 18F, recently connected its SaaS team collaboration product (Slack) with its SaaS file storage product (Google Drive), resulting in a five-month exposure of its files.[3]

Assessing the Risks of Shadow IT

Compliance Risks

Customer data and corporate intellectual property may or may not be flying back and forth between your organization's secured network and any number of unauthorized servers, creating a compliance nightmare. Whether the public cloud service is secure or not is moot; the organization with shadow IT has no way to verify that essential compliance efforts are being performed. Even worse, there is no way to document or test those aspects. This increases the potential for sensitive data to be exposed and penalties applied is a given.

Disaster Recovery

A disaster recovery plan needs to include a vendor risk management plan, but the IT team doesn't know which vendors are included in its shadow infrastructure. For that matter, IT doesn't know what types of data and documents are being stored on public clouds, or what will happen to those assets if a public cloud provider is acquired or shut down.

Even if the IT team were able to hunt down all the data and documents contained within its shadow infrastructure, recovery times couldn't be estimated and service level agreements (SLAs) wouldn't be met because the data is under the control of third parties who have not agreed to any SLAs of their own.

Financial Risks

Imagine if Walmart paid retail for every item on its shelves; it would lose the benefit of economies of scale. That's what happens when departments buy licenses for a few employees. This isn't a problem when it occurs in a single department, but when it occurs in many departments, the chance to negotiate for bulk rates is lost and costs explode.

In addition, shadow IT tends to foster redundancies. If one department buys a license that allows up to 25 users but only uses 10 of those licenses, there are 15 licenses going unused. If another department makes the same purchase from the same provider, the company has paid for 50 licenses and wasted 30 of them. These numbers add up and the impact can ripple throughout the organization.

An organization that ignores its shadow IT not only incurs these risks and others, but it also misses opportunities. When properly managed as a multi-cloud environment, shadow IT enables businesses to respond to fluctuating needs with great speed and little cost.

The Silver Lining of a Multi-Cloud Strategy

Briefly putting the risks of shadow IT aside, we can focus on the benefits. Advancements like desktop-as-a-service through Amazon Workspace, application development-as-a-service from Google, database-as-a-service from Mongo, and even genetic sequencing-as-a-service from IBM's Watson supercomputer ensure that users are going to keep layering on more unauthorized applications to meet their specialized needs. Rather than fight a losing battle, IT departments need to embrace shadow IT by adopting a multi-cloud approach.

A multi-cloud strategy allows individual business groups to tailor cloud offerings to meet their specific needs. This may not sound exciting at first glance, but it actually delivers a dramatic competitive advantage. All departments perform specialized tasks, and IT doesn't have visibility of how each group performs its work or which software features will improve its productivity. Because IT lacks the information necessary to make recommendations for or against the purchase of certain packages, departments can perform better when they are allowed to choose and test software tools independently. This decreases reliance on the IT team and reduces the costs of internal resources. The result is greater flexibility across the organization.

The ability to easily provision and deprovision applications can help companies improve their agility with little or no upfront investment. Today, software engineers don't have to write and test every piece of code; instead, almost every facet of software development is available as a service so engineers can grab bits and pieces on demand and bring their products to market faster. Along the way, they can try new technologies and choose to keep or drop them, depending on what makes sense for the product strategy—and when a product strategy changes, pivoting can happen rapidly. Innovation can happen on the fly.

A multi-cloud strategy makes sense in a business environment where agility is essential to success. However, an effective consistent security program must be in place for a multi-cloud strategy to succeed.

Transforming Shadow IT Into a Secure Multi-Cloud Environment

Once the business understands how they will utilize shadow IT, they can begin consolidating their diverse collection of shadow IT into a secure multi-cloud ecosystem. Like any IT policy change, the rollout of this strategy will impact every department. For instance, when redundant SaaS products are in use in different departments, all but one should be retained.

While this may initially be an unpopular move, it is essential for security and operational efficiency. That's why transparency is critical during this process. Users who understand the reason their tools were phased out are more likely to accept the change gracefully.

Methods to create transparency include:

- **Develop a matrix.** Illustrate and explain the criteria used to determine which technologies will be allowed to remain.
- **Shadow their app use.** Learning how applications are used in the course of their workday and which technologies they use in conjunction with the app or device in question. This may reveal unexpected information and inform the decisions on which products will make the cut.
- **Listen.** Listening to users is especially important when they've chosen a shadow service over an authorized service that is already in place. The choice of a shadow solution may indicate a shortcoming in the authorized service, and the CIO needs to know whether that deficiency was overlooked during the procurement stage or whether needs have changed since it was purchased.

Steps to Securing Your Shadow

1. Inventory your shadow IT

Use network monitoring tools to find connected devices and check firewall and other log files to identify cloud services. Once cloud services have been identified, they can be categorized and examined in more depth.

2. Conduct risk assessments on the applications

Once an inventory of the cloud services has been completed, the security team can map business needs to security levels. Gaps will be discovered, which can then be corrected by a dedicated in-house team that can design and monitor a solution, by a third-party solution that is implemented by the IT and security teams, or by a cloud security provider.

Risk Assessment Questions

Questions to consider when assessing the risk of your shadow IT resources:

- ? *What type of data will be in your environment?*
- ? *Does your data have compliance or regulatory requirements?*
- ? *Where are the majority of your data hosted?*
- ? *Do you have the staff, technology and processes to effectively manage the security of your environment today?*

3. Find the winners and kick out the losers

Drop services that didn't pass the risk assessment and discourage the use of free services because they tend to proliferate and become hard to manage. To keep things under control moving forward, set up alerts that notify the IT team when unauthorized services are detected. Redundant purchases and functions will emerge, and these need to be streamlined. That's going to take some diplomatic outreach to the business units, so initiatives to secure shadow IT will need a strong executive sponsor.

Steps to Securing Your Shadow

4. Understand shared responsibilities

While the operations of your cloud can be eased with the help of a managed security services provider, you remain responsible for controlling your risk. This is because there are many players involved in a multi-cloud strategy; a worker performing a simple task may use multiple apps that pull data from different storage providers and transmit that data using different infrastructure platforms. There is no way for any one provider to know exactly what is running in or on their environment.

A strong patching program must be in place. The vendors contributing to the multi-cloud environment won't all have the same level of vulnerability testing that would be expected from a big vendor, and their apps are not likely to have security integrated into their software development lifecycle. A managed security services provider can help find and fix conflicts between apps that might cause security gaps, but the ultimate responsibility is yours.

5. Classify data to reduce risk

Businesses need to know which of their data sets and workloads are covered by regulations, which products in the multi-cloud will use, store, or transmit that data, and whether those vendors are compliant. Unstructured data, such as text messages and documents, must also be evaluated.

6. Put ownership and processes in place

The IT team needs to consistently gather information from users about the tools they intend to deploy. By talking to users about the reasons behind their adoption of shadow services, the IT team can uncover common causes that may be useful in constructing checklists and processes to push out to the lines of business. These information-gathering tools must be easy for users to access and complete, and should also be part of an overarching transparent process so that participation remains high.

In addition, executives will need to work together to review cloud services on a regular basis, ensuring that efforts to manage multiple clouds as part of a company-wide strategy. The whole company needs to understand the priority level of bringing shadow IT under the IT umbrella or the organization will become trapped in an endless game of catch-up.

Embrace Your Shadow

As the cloud becomes cheaper and more reliable and users become more sophisticated and demanding, organizations will no longer be able to treat shadow IT as a secondary set of tools that can go ignored until there's a problem. In the same way, we read headlines about data breaches caused by insider threats today, tomorrow we're going to see more headlines blaming those disasters on unauthorized applications. That's already begun, as evidenced by the Slack hack.

The benefits of a multi-cloud strategy—agility, productivity, and cost–efficiency—are significant, but so is the effort required to secure dispersed IT. Companies lacking the bandwidth or the in-house expertise have the option of bringing in outside experts to manage the work for them.

A cloud security provider will already know which log files to examine and how to rapidly identify data flowing in and out of the network without authorization. Likewise, a cloud security provider will be familiar with most cloud services and the quality of their security postures, which will cut cycles from the project and help keep costs under control.

Companies that struggle with maintaining compliance of their authorized systems will find their challenges exponentially greater when dispersed IT is thrown into the mix. This is where a cloud security provider can add value beyond speed and cost. Auditing an environment with a heavy shadow IT component is a complicated and time-consuming process that eats up resources and isn't guaranteed to yield satisfactory results. Offloading this work to an expert is a practical move. In addition, a cloud security provider with experience in PCI, HIPAA, and other regulatory requirements can also help conduct gap analyses, remediation, ongoing compliance monitoring, and incident response and forensics.

Armor security specialists and engineers develop a plan to secure, license, monitor, and manage your entire multi-cloud environment. Advanced onboarding services, custom policies and upgrading, and managed load-testing ensure a smooth implementation and ongoing customer satisfaction. We help your organization leverage agility without sacrificing security.

Sources

1. Corbin, K. (2015, August 10). CIOs vastly underestimate extent of shadow IT.

   Retrieved August 18, 2016, from CIO: http://www.cio.com/article/2968281/cio-role/cios-vastly-underestimate-extent-of-shadow-it.html

2. Frost & Sullivan. (2013). The Hidden Truth Behind Shadow IT.

3. McCabe, D. (2016, 05 13). Government tech team in hot water for 'data breach' tied to Slack.

   Retrieved from The Hill: http://thehill.com/policy/technology/279885-watchdog-hits-government-tech-team-for-security-issues-linked-to-slack