Managed Methods

Whitepaper

Shadow IT:
Discover What's Hiding in Your Cloud

Shadow IT can lead to significant risk, higher costs, and greater inefficiencies. ManagedMethods' Cloud Access Monitor highlights shadow IT to help companies manage risk.

Executive Summary

We've entered a new era of the cloud economy. In the early days of cloud computing, IT departments tested the waters with one or two Software-as-a-Service (SaaS) applications but still preferred the internal data center for the most important applications. Today, "think cloud first" is the mindset for not only IT but also line of business groups and even individual workers when considering how to get work done. Cloud-based collaboration and data sharing tools can be especially helpful in boosting productivity and increasing communications with and among employees, partners and customers.

This boom in cloud application usage creates a real dilemma for most organizations. They want to use cloud computing for the multitude of benefits it provides, but it often creates a situation where the IT department doesn't know what all is in use. These applications that are out of IT's purview are known as "shadow IT."

Shadow IT can put organizations at risk in several ways. Many cloud-based applications, especially those that are geared toward consumer usage, don't have the level of security controls that businesses need. For example, data stored in a consumer-oriented cloud storage application not be secured using security best practices. If an employee uploads sensitive or confidential information to that application, not only is the data highly vulnerable to a breach but the organization may be non-compliant with corporate governance or regulatory requirements. So the question is, how can the organization control shadow IT without interfering with worker productivity?

There's a new class of technology solutions that aim to fill this need and to shine the light on cloud-based shadow IT. Gartner has dubbed this class of products and services Cloud Access Security Broker, or CASB. CASB solutions help companies discover what cloud applications are in use and then control them in ways that adhere to corporate policies.

The drawback to many CASB solutions is that they require organizations to send private logs or activity data to a third party for monitoring and analysis. Unfortunately this implementation is unsuitable for many organizations that do not want to send, or are prohibited from sending, logs or metadata to third party providers,

Now there is a software-based CASB solution that allows the customer organization to determine how to implement it: on-premise, hybrid, or fully in the cloud. ManagedMethods' Cloud Access Monitor helps companies discover, monitor and control cloud applications without losing control over their log and activity metadata. Companies gain visibility over what is in use, which then enables setting security policies, evaluating and selecting corporate standard cloud applications, and negotiating site licenses.

This white paper focuses on the importance of discovering all the cloud applications in use so they can be effectively controlled according to company policies, while at the same time enabling worker productivity.

Background: The Cloud Economy Today

A few short years ago, a company that wanted to utilize a SaaS application had to build a business case to justify the move. These days companies don't have to justify "why cloud" – the benefits are proven and obvious:

- Applications can be deployed in hours rather than months or years, thus providing business value very quickly.
- Companies make a minimal investment in hardware and software, and the "pay as you go" subscription model pins expenses to the Operating Expenses budget rather than the more elusive Capital Expenses budget.
- Software vendors typically deliver frequent updates of their SaaS application's features, functions and capabilities, allowing customers to do more with minimal investment.

Thus it's no surprise that SaaS applications now provide core business functions throughout the enterprise. Marketing and Sales teams use CRM and automation tools like Salesforce and Marketo. Finance and HR departments run their business on accounting and employment applications like NetSuite and Workday. Entire enterprises run productivity and collaboration applications like Office 365 and Google Docs. Practically every business unit relies on cloud-based productivity applications that have become integral to their mission.

As a result, Goldman Sachs projects that spending on cloud computing infrastructure and platforms will grow at a 30 percent CAGR from 2013 through 2018, compared with just 5 percent growth for enterprise IT overall.[1] Quite simply, cloud is the way to go.

An October 2014 Ponemon Institute survey of nearly 2,000 IT and IT security practitioners confirms this growth. Respondents estimate that cloud use will increase at their companies over the next two years. Today respondents estimate that 33 percent of their organizations' total IT and data processing requirements are met by using cloud resources. This is expected to increase to an average of 41 percent of IT and data processing requirements.[2] However, the findings also reveal that organizations have difficulty in managing the risk without applying the right governance practices.

What Lurks in the Shadows

Despite the tremendous market growth of SaaS and the undeniable benefits, the extensive use of cloud applications also has a dark side. When workgroups or individuals contract for and utilize cloud apps on their own – i.e., without IT's knowledge or participation in selecting or evaluating the services – it creates an unintended problem. People have the best intentions to use these applications to get work done or to increase collaboration and productivity. What they don't realize is that they are creating a management problem known as shadow IT.

[1] Louis Columbus, Forbes, "Roundup of Cloud Computing Forecasts and Market Estimates, 2015," January 24, 2015

[2] Ponemon Institute LLC, " The Challenges of Cloud Information Governance: A Global Data Security Study," October 2014

Gartner defines shadow IT as technology spending and implementation that is outside the purview of the IT Department. It's a bigger problem than most organizations realize. Consider:

- The Ponemon Institute reports that an average of 50 percent of cloud services are deployed by departments other than corporate IT. What's more, an average of 44 percent of corporate data stored in cloud environments is not managed or controlled by the IT department.[3]
- A Cloud Security Alliance survey says only 8 percent of companies know the scope of shadow IT in use within their computing environments. Seventy-two percent of survey respondents say they don't know how pervasive the problem is but they sure would like to know.[4]

Why does shadow IT matter? What's wrong with letting individuals and business groups choose their own cloud applications, especially if it helps them be more effective in their jobs? The main concern is that shadow IT introduces risk, costs and inefficiencies. For example:

- A company loses control over its data when workers can move it into any cloud applications they want to use, and there is no central accountability for the data. Consequently, data may be at risk of loss or theft, which is a huge liability for the company. Further, the data may not be included in business continuity or disaster recovery plans because the location – and perhaps the very existence – of the data is unknown to IT.
- If data isn't properly protected and accounted for, the company may be out of compliance with regulatory requirements such as SOX, PCI or HIPAA. One industry study found that among users of cloud-based file sharing applications, 22 percent have uploaded sensitive information such as personally identifiable information (PII) or payment card information to one of these services.[5] Non-compliance can lead to huge fines and other consequences.
- If the same data is stored in multiple places (such as individual Dropbox accounts or competing applications), it can get outdated and out of sync with official data stores. People can be working on and making decisions based on out-of-date information, and collaboration can be difficult if data is in disparate applications.
- It can be costly for the company to have numerous versions of the same type of application. For instance, it's not uncommon for an enterprise to discover there are a dozen or more cloud storage systems in use. Using so many different services can cost more than standardizing on one or two services and negotiating an enterprise license for the preferred services.

It's clear to see, shadow IT can pose many serious problems for an organization.

[3] Ponemon Institute LLC, " The Challenges of Cloud Information Governance: A Global Data Security Study," October 2014

[4] Cloud Security Alliance, "Cloud Adoption Practices & Priorities Survey Report," January 2015

[5] Cloud Security Alliance blog, "The Top 10 Cloud Services In Government That Don't Encrypt Data At Rest," May 7, 2015

Shining a Light on Shadow IT: From Darkness to Visibility

The problem of shadow IT in the cloud is growing worse each year. Twelve years ago technology spending outside of IT was 20 percent of total technology spending; it will become almost 90 percent by the end of the decade, according to Gartner, Inc.[6] Companies need to discover how serious a problem they have and then do something about it to avoid the types of problems discussed above.

This need is addressed by a classification of products and services collectively known as Cloud Access Security Brokers (CASB), a term used by Gartner analysts. (You might also hear the term Cloud Access Control, or CAC, used by analysts with the company 451 Research. We'll use CASB, as it seems to be more common.) CASB tools are designed to be security, visibility and policy enforcement points placed between cloud services and the consumers of those services. There are two main functions of CASB solutions: monitoring and policy enforcement.

The monitoring portion of the solution provides visibility into the cloud applications in use by members of an organization. This is typically done by analyzing the actual traffic or logs of the traffic going between an organization's devices and the various cloud services. The monitoring tool is typically able to report on which cloud apps are in use, by whom, when, and how often. The information gleaned from the monitoring process helps the organization make informed decisions about policies pertaining to the cloud services. Companies are often surprised to see the extent of previously unknown cloud services in use. Many organizations underestimate their use of cloud services by 80 percent or more.

The enforcement portion of the solution allows an organization to enforce policies on the cloud application traffic and to apply security measures such as data encryption or loss prevention. Policies are enforced on traffic as it goes through a gateway service on the way to the various cloud applications. For example, traffic intended for high risk applications can be blocked; data going into enterprise SaaS applications can be encrypted before reaching the application; all transactions for specific applications can be logged for audit trail purposes; and so on. The enforcement capabilities of a CASB tool are intended to bring the typical types of data center policies and control measures to cloud applications that may or may not have security controls.

CASB tools bring much needed enterprise visibility and policy enforcement capabilities to a range of cloud services. Organizations now have the ability to manage and control what's happening in the cloud—even if the applications have been considered shadow IT. They are no longer in the dark.

There's one significant drawback to many vendors' implementations of their CASB tools. Quite often, the tools require routing log and/or activity metadata to the vendor's cloud service in order to perform the application monitoring tasks. This can be a show stopper for organizations that are prohibited from sending activity data (which is often the superset of all data being sent to SaaS services), or that don't want to send their activity data offsite to a third party. Therein lies the challenge: organizations need the capabilities of a CASB solution, but they also need a style of deployment that fits their data governance policies.

[6] Gartner, Inc., press release, "Gartner Says Every Budget is Becoming an IT Budget," October 22, 2012

Filling the Need with Flexibility: ManagedMethods' Cloud Access Monitor

Cloud Access Monitor is the application monitoring component of ManagedMethods' CASB solution. It is used by security teams to discover all the cloud applications that are being used by the organization—including those in the shadows.

Cloud Access Monitor is an industry first software solution with a choice of deployment options. Customers choose if they want to deploy Cloud Access Monitor fully on-premise, hybrid on-premise/cloud, or fully cloud-hosted. ManagedMethods gives organizations the choice to deploy CASB as they need or want to have it. Most importantly, this solution meets the needs of organizations that are required, or prefer, to keep their private log and activity data on-premise.

While many other CASB solutions use log files to discover cloud applications, ManagedMethods passively captures traffic as it comes in or goes out of an enterprise network, as shown in Figure 1. The solution looks at data coming off a Switch Port Analyzer (SPAN) port or firewall, giving the ability to analyze the traffic in real-time with no intrusion and no latency. This passive monitoring, either in live production or safely offline, gives a definitive answer to the question "Where is my enterprise exposing information to the cloud?"

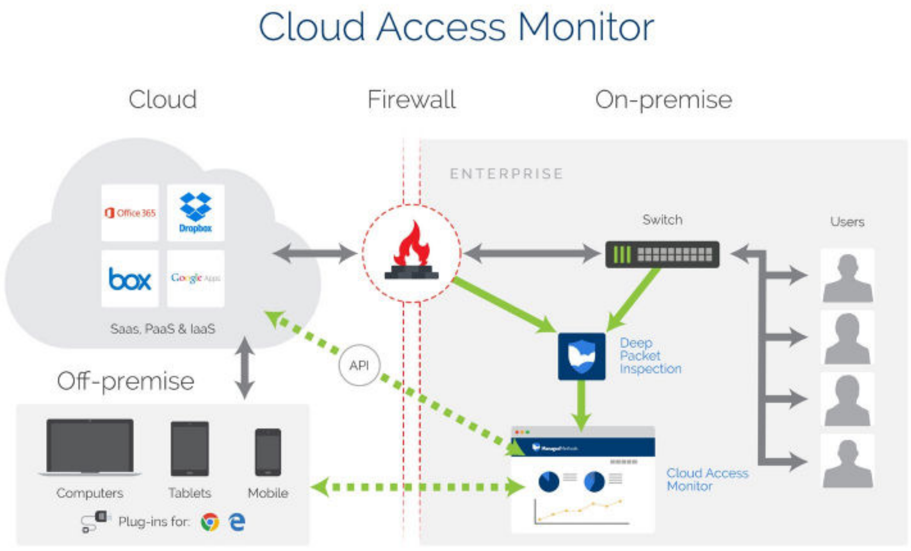

Figure 1: The Architecture of Cloud Access Monitor

Cloud Access Monitor can tell a company what cloud applications are being used, by whom, when, and how often. It looks at all client devices, not just users, under the presumption that workers today use multiple devices to access applications for work.

Cloud Access Monitor's inspection goes deep

A unique and key feature of Cloud Access Monitor is that it applies deep packet inspection (DPI) technology to analyze the cloud activity data. DPI provides the ability to look at all the information going to or between cloud applications, not just log entries, to take the discovery further and conduct granular analysis that goes much deeper than what can be done with logs alone. ManagedMethods utilizes DPI for all of the benefits it provides.

Greater visibility

There is visibility into the actual payload of network traffic, whereas log data simply provides source and destination details. This enables an organization to craft more meaningful policies to secure the information going into cloud applications. For example, say a group of workers is using Evernote and there is a concern about putting sensitive information into this cloud service. ManagedMethods' Cloud Access Monitor can look at the content that is getting uploaded to this application and check for the presence of specific information such as Social Security numbers or other PII.

Low overhead

The process of gathering packet information from a SPAN port has low overhead as compared to turning on logging on egress devices. Data can be collected 24x7 without impacting end user performance. By comparison, the process of capturing log files can actually choke older generation firewalls if done for too long a period of time, and so it's recommended to log files for an hour or so during non-critical times and then turn logging off. This can create gaps in the data for application monitoring.

Data availability

Gathering packet data is non-intrusive to network operations and the network data is immediately available for analysis. This aids in near real-time monitoring for specific concerns, such as the size of messages going into SaaS applications. In contrast, having to upload log files to a third party vendor location for post analysis is not quite as timely.

Compatibility and ease of use

ManagedMethods' packet capture technique works with any firewall or network switch and does not require an additional log processor. What's more, this process is well understood by network administrators because SPAN ports are used by many other products.

See the risk that cloud applications pose to the business

The reason for gathering and analyzing this data is to understand the risk that various cloud applications can pose to the business. The Cloud Access Monitor dashboard, shown in Figure 2, displays information about what cloud applications are in use, which ones have known vulnerabilities, and how risky the applications are to business users.

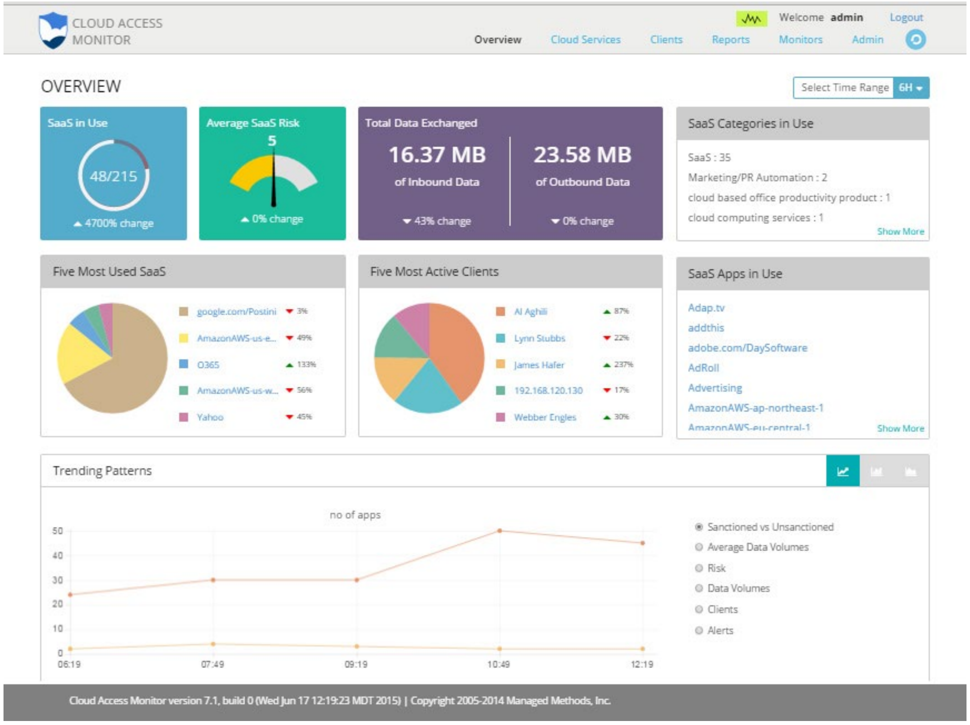

Figure 2: Sample view of the Cloud Access Monitor dashboard

The vulnerabilities information on the dashboard comes from a third party database of vulnerable sites. ManagedMethods draws on this database to look for any problems or known issues by application or website. The risk assessment information is a combination of data from ManagedMethods' own risk analysis team and information provided by a customer's own security team. ManagedMethods does basic risk analysis for cloud applications and we allow our customers to modify the risk posture based on each customer's own perception of an application. For example, ManagedMethods might ascertain that a cloud storage service has sufficient controls for typical enterprise use to be considered low risk, but a pharmaceutical company with very confidential intellectual property may view this service as quite risky. This customizable risk score enables a company to see at a glance which cloud applications pose the most risk to the business.

Cloud Access Monitor also looks for anomalies in usage data to highlight, say, sudden increases in SaaS usage or data going out the door. This can trigger an alert that directs the company to look into the details of the anomalous behavior.
Features, functions and benefits of Cloud Access monitor

The table below summarizes the main features and benefits of using Cloud Access Monitor to put an end to shadow IT.

Feature/Function	Benefit
Cloud application monitoring – Identify the outbound and inbound cloud traffic, with a focus on categorizing the services that exchange data with enterprise assets	Gain visibility into the cloud services that are actually in use
Application risk assessment – Identify and quantify each SaaS app's security risk profile	Quickly assess the level of risk that SaaS apps pose to the organization
Monitor for specific concerns – Custom monitoring for size of messages to SaaS, content of the messages	Quickly catch activities that could be signs of malicious or prohibited behavior
Anomaly detection – Detect anomalies in usage and data exchange based on observed baselines	Quickly catch activities that could be signs of malicious or prohibited behavior
Scheduled and on-demand reporting – Get reports of user activity and SaaS usage	Distribute reports to people who need to see the level of cloud activity
Take action – Contact a user using unsanctioned applications or send a command to a firewall to block specific SaaS applications	Shut down risky activity that is against company policy
Monitor off-premise usage – Monitor off-premise usage of SaaS apps through a lightweight client extension	Gain visibility on cloud services in use even when employees are not on the company network
Cloud traffic archival – Archive records of traffic going to/coming from cloud services	Facilitate regulatory compliance and forensic analysis

Conclusion

There's no doubt that enterprises get a lot of value from utilizing applications deployed in the cloud. It's possible to be fully up and running in a SaaS application in mere hours—or even minutes, depending on the application. Line of business departments, collaborative workgroups and individuals are eager to pull out the corporate credit card and get started quickly, often without consulting the IT or information security teams beforehand. Despite good intentions to increase productivity, these workers unwittingly create a range of problems with their use of shadow IT.

ManagedMethods shines a light on shadow IT and helps companies get control of their data and applications once again. Cloud Access Monitor discovers what applications are in use, continuously monitors them, categorizes them, and evaluates them for risk. More importantly, the IT team is able to get the information necessary to develop appropriate policies, set company-wide standards for approved applications, and apply the necessary controls to safeguard data and reduce risk.

ManagedMethods uniquely gives companies choice and flexibility of how to deploy this solution. Customers choose if they want to deploy Cloud Access Monitor fully on-premise, hybrid on-premise/cloud, or fully cloud-hosted. This flexibility allows organizations to deploy CASB as they need or want to have it, keeping their private log and activity data on-premise if they so choose.

If you suspect you have a shadow IT problem – and most companies do – please contact ManagedMethods to get a free trial of Cloud Access Monitor. Let us give visibility to your cloud usage and control issues and help you reduce your risk.
About ManagedMethods

ManagedMethods Mission

ManagedMethods mission is to provide customers with an easy to use, efficient and effective Cloud Security Solution. We believe in the basics.   You cannot secure what you do not know exists. Shadow IT is a real problem, but it does not need to be. With our products, companies can easily monitor and control the use of Cloud Applications (SaaS) and reduce their cloud risk.

Founded in 2013 by veterans of enterprise software performance and security tools, ManagedMethods products are focused around the growing use of Cloud applications and services that are at the core of today's mission critical business functions.