ManagedMethods

WHITEPAPER

Bring Visibility and Control to SaaS Applications: Cloud Security Made Easy

Software as a Service (SaaS) is now a mainstream aspect of cloud computing and a standard way of work for organizations of all sizes and every industry. SaaS removes the need for organizations to install and run applications on their own computers or in their own data centers—but they do need to bring their own security to protect data and maintain compliance with internal policies and regulatory requirements. ManagedMethods' Cloud Access Monitor makes cloud security easy.

Businesses Are Getting SaaS-Happy

Small and mid-sized businesses, educational institutions, and state and local government agencies all run their operations these days using Software as a Service applications. The 2015 Gartner Cloud Computing Hype Cycle places SaaS on the verge of the "Plateau of Productivity," meaning that SaaS is mainstream today.[1] With tens of thousands of applications now available via the cloud, there's an application (or dozens) for practically every need and every niche. The research firm IDC says that 90% of new software deployments will be SaaS by 2020.[2] It's simply the preferred way of work today for most small and medium businesses.

Some of the most popular types of SaaS applications are for office productivity, collaboration and file sharing. Consider how many companies have embraced using just these four SaaS applications to enhance their productivity:

Office 365	As of March 2016, Microsoft claimed to have 60 million monthly active Office 365 commercial customers. The software vendor has seen 50,000 small business customers added to Office 365 each month, and it has had 340 million downloads of its Office Mobile applications, up from "just" 100 million downloads six months earlier.
Google G Suite	Google revealed at the end of September 2016 that its public cloud (Google Cloud) already has a billion active users, and 2 million businesses currently pay for G Suite and its family of applications, which includes Gmail, Docs, Drive and Calendar.
Dropbox	200,000 businesses use Dropbox Business, and more than 500 million people use Dropbox.
box	More than 66,000 businesses use Box for content sharing and collaboration.

[1] Gartner, Hype Cycle for Cloud Computing, 2015

[2] IDC 50th Anniversary Transformation Everywhere presentation, 2014

Those phenomenal usage figures show that a lot of organizations have gotten on the SaaS bandwagon, and more continue to join each month.

Certainly, the business advantages of SaaS are significant. There's no infrastructure to install and maintain; applications are updated frequently with new features and security patches; the pay-as-you-go model hits OPEX budget rather than CAPEX; and perhaps best of all, organizations increase their business agility when they can deploy applications in mere minutes. With these kinds of advantages, it's no wonder the use of cloud applications continues to increase on average 20% year-over-year.[3]

SaaS with a Side of Risk

While there's quite a lot to appreciate about the SaaS business model, there are some drawbacks as well—primarily concerns over data visibility and control. When data goes to the cloud, many organizations lose track of where it goes, who has access to it, and what people are doing with the data. Internal as well as external threats like malware can pose a danger to company data, and the organization can't even see the threats to know how to mitigate them. This lack of visibility into what's happening with the company's data in the cloud is a huge business risk. What's more, numerous regulatory requirements mandate the security and privacy of many types of business and personal data. Doing nothing to address the risks and compliance mandates is irresponsible and untenable.

When it comes to SaaS, there's a distinct division of responsibility for data in the cloud. The SaaS provider takes responsibility for providing a stable and secure infrastructure—the servers, the storage and the application software itself. The provider ensures that data is backed up and replicated for disaster recovery. Most, though not all, SaaS providers have the means to encrypt customer data at rest. However, much to many organizations' surprise, the customer is responsible for addressing all other levels of risk to the data and for adding appropriate security measures that will fully protect the data and enable the company to meet compliance requirements.

> **"Cloud access security brokers (CASBs) provide information security professionals with a critical control point for the secure and compliant use of cloud services across multiple cloud providers."**
>
> ***Gartner Inc***

Legacy security technologies that operate on organizations' networks aren't adapted to work in cloud environments. A firewall – even a NextGen firewall – might be able to provide details on the user traffic going to the SaaS application, but it can't say what those users are doing with the data, and whether the data is threatened by malware or other types of zero-day attacks. Legacy threat monitoring and prevention tools like virus scanners and data loss prevention (DLP) systems are great on a network but don't operate in the cloud. Clearly, businesses need a better way to monitor and control what is happening with their data within cloud applications.

Shining a Light on What's Happening in Cloud Applications

This need for visibility and control is addressed by a classification of products and services collectively known as Cloud Access Security Brokers (CASB).[4] At the 2016 Gartner Security & Risk Management Summit, Gartner VP Neil MacDonald spoke about the technology trends that provide the most effective business support and risk management. CASB was number one on the list.[5] MacDonald says that companies' use of SaaS applications provides new challenges to security teams due to limited visibility and control options. CASBs enable businesses to apply much-needed security policies across multiple cloud applications.

CASB tools are designed to be security, visibility and policy

[3] Gartner press release, January 2016

[4] The term Cloud Access Control, or CAC, is used by analysts with the company 451 Research but we'll use CASB, as it seems to be more common.

[5] Gartner press release, June 2016

enforcement points placed between cloud services and the consumers of those services. There are two main functions of CASB solutions:

1. Monitoring
2. Policy enforcement

The monitoring portion of the solution provides visibility into the cloud applications in use by members of an organization. At a basic level, a monitoring tool performs application discovery to report on which cloud applications are in use, by whom, when, and how often. Companies are often surprised to see the extent of previously unknown cloud applications in use. Many businesses underestimate their use of cloud applications by 80% or more. Those applications that are outside the purview of the IT department – the workgroup that is often responsible for data security – are generally known as "shadow IT."

More advanced CASB monitoring functions include delving into specific SaaS applications to watch what is happening with the data to determine if the actions comply with a company's security policies, and whether there are threats present that could pose risk to the data. For example, the CASB service might watch for events where users upload sensitive data in the clear to a file sharing application in violation of company policy.

The enforcement portion of the solution allows an organization to enforce policies on the application activities and to apply security measures to protect the data. The enforcement capabilities of a CASB tool are intended to bring to cloud applications the typical types of control measures that legacy applications in a data center provide. In the example above where a user attempts to upload sensitive data, an enforcement rule can prevent that action from happening.

ManagedMethods' Cloud Access Monitor: Cloud Security Made Easy

ManagedMethods' CASB solution focuses on the ways that small and medium-sized organizations work today. Cloud Access Monitor delivers the most efficient and cost effective way to gain visibility into how data is stored, accessed and shared in cloud applications like Microsoft Office 365, OneDrive and Google G Suite, and to discover and control unsanctioned shadow IT applications.

Cloud Access Monitor is one solution that can be deployed in multiple ways, owing to the way an organization prefers to work.

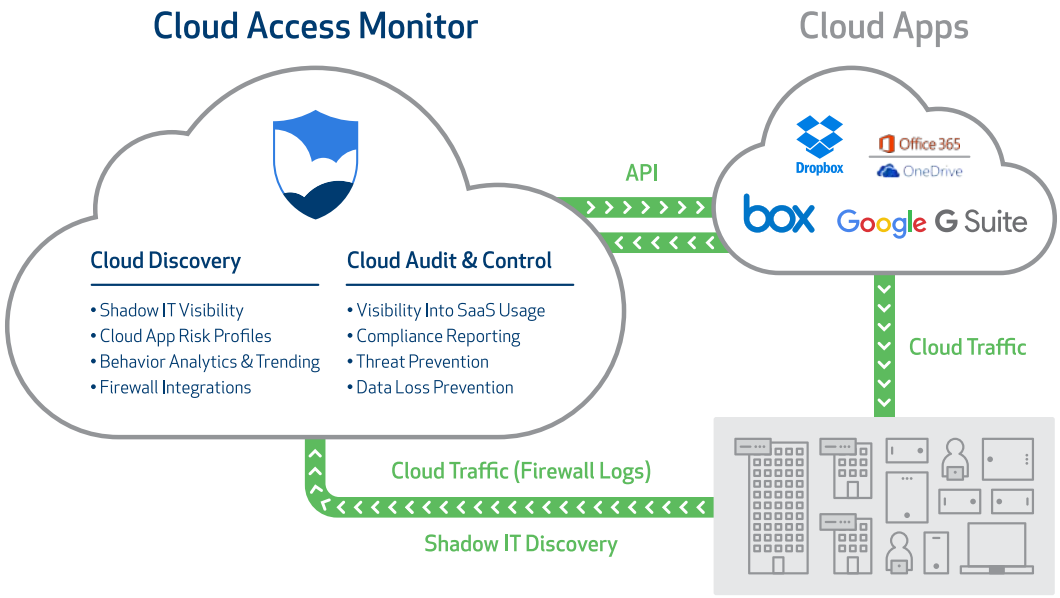

Figure 1: The architecture of Cloud Access monitor

It can be deployed as an application program interface (API) product with any of a number of sanctioned applications. In another deployment model, Cloud Access Monitor can be used to analyze network traffic and logs to discover and report on shadow IT applications. Or, more beneficially, both aspects of Cloud Access Monitor can be deployed together to provide full visibility over shadow IT and control over sanctioned cloud applications.

Figure 1 above shows the architecture of the different approaches to ManagedMethods' CASB product.

Let's look at each of these deployment modes and their benefits.

API Connections into Specific Sanctioned Applications

Most organizations have a list of officially sanctioned cloud applications that they have evaluated and purposefully chosen, and workers are directed to use them. Among the most commonly used sanctioned applications are Microsoft Office 365, which provides a suite of productivity tools that most knowledge workers are accustomed to using; Microsoft OneDrive for file storage and sharing; Google G Suite (previously known as Google Apps for Business/Education/Government) for email and document creation and sharing; and the file sharing services Dropbox and Box.

ManagedMethods has an API integration into each one of these SaaS applications, which means Cloud Access Monitor operates as if it is actually part of the application. This is something that no legacy security product or cloud access proxy gateway can do. This level of integration provides the ability to monitor and control/enforce what happens inside the application, regardless of whether a user has come in from the company network or not. Even mobile workers who don't go through their corporate network to get to sanctioned cloud applications have all the security measures of Cloud Access Monitor applied to their work. API connectivity into an application provides "anytime, anywhere" visibility.

If someone attempts an action inside a sanctioned application that violates a company policy, Cloud Access Monitor can respond to protect the data. For example, say an employee is attempting to move files from the company version of Google Drive to his own private copy of Google Drive, and this violates the company policy of where business files can be stored. Cloud Access Monitor can detect the activity and respond in various ways: send an alert to the security administrator, prevent the copy activity, warn the user that his activity is against policy, and so on. The control/enforcement response is up to the company's security administrator.

Cloud Access Monitor can answer any number of questions pertaining to the sanctioned applications. For example, who has access to specific files in a shared repository? Are people sharing data inappropriately with others both inside and outside the organization? Are files infected with malware being uploaded to a company file share? Are students using profane or otherwise unacceptable language on their school accounts? Has any sensitive information such as personal health information (PHI), credit card numbers or Social Security numbers been uploaded inappropriately? According to a Ponemon Institute study, 88% of workers say they handle sensitive information.[6] How is this data protected if it's put into cloud applications? This is the visibility gap that Cloud Access Monitor shines a light on so that appropriate controls can be applied.

Legacy security solutions won't work inside cloud applications, so ManagedMethods partners with various security vendors to integrate their capabilities into Cloud Access Monitor to further protect the data within sanctioned cloud applications. Through these integrations, Cloud Access Monitor can detect and act upon potential harmful malware or external threats and gain deeper visibility into application usage and encrypted traffic. For example, an integration with Check Point Software adds data loss prevention capabilities.

[6] Ponemon Institute, "Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations," August 2016

Network Analysis for Cloud Discovery

Many organizations have a need to know all the unsanctioned cloud applications being accessed by their employees. Although people have the best intentions to use these applications to get their work done, they don't realize they are contributing to the management problem of shadow IT. The Ponemon Institute reports that an average of 50% of cloud services are deployed by departments other than corporate IT.[7] A Cloud Security Alliance survey says 72% of respondents say they don't know how pervasive the problem of shadow IT is but they sure would like to know. [8]

Cloud Access Monitor is used by security teams to discover and monitor all the cloud applications being used by the organization. Many other CASB solutions only use log files to discover cloud applications. Cloud Access Monitor can consume log files or passively capture traffic via a network SPAN or TAP. By monitoring data coming off the switch or the firewall, ManagedMethods' solution has the ability to analyze the traffic in real-time with no intrusion and no latency, and then apply deep packet inspection (DPI) to analyze the data at a more granular level.

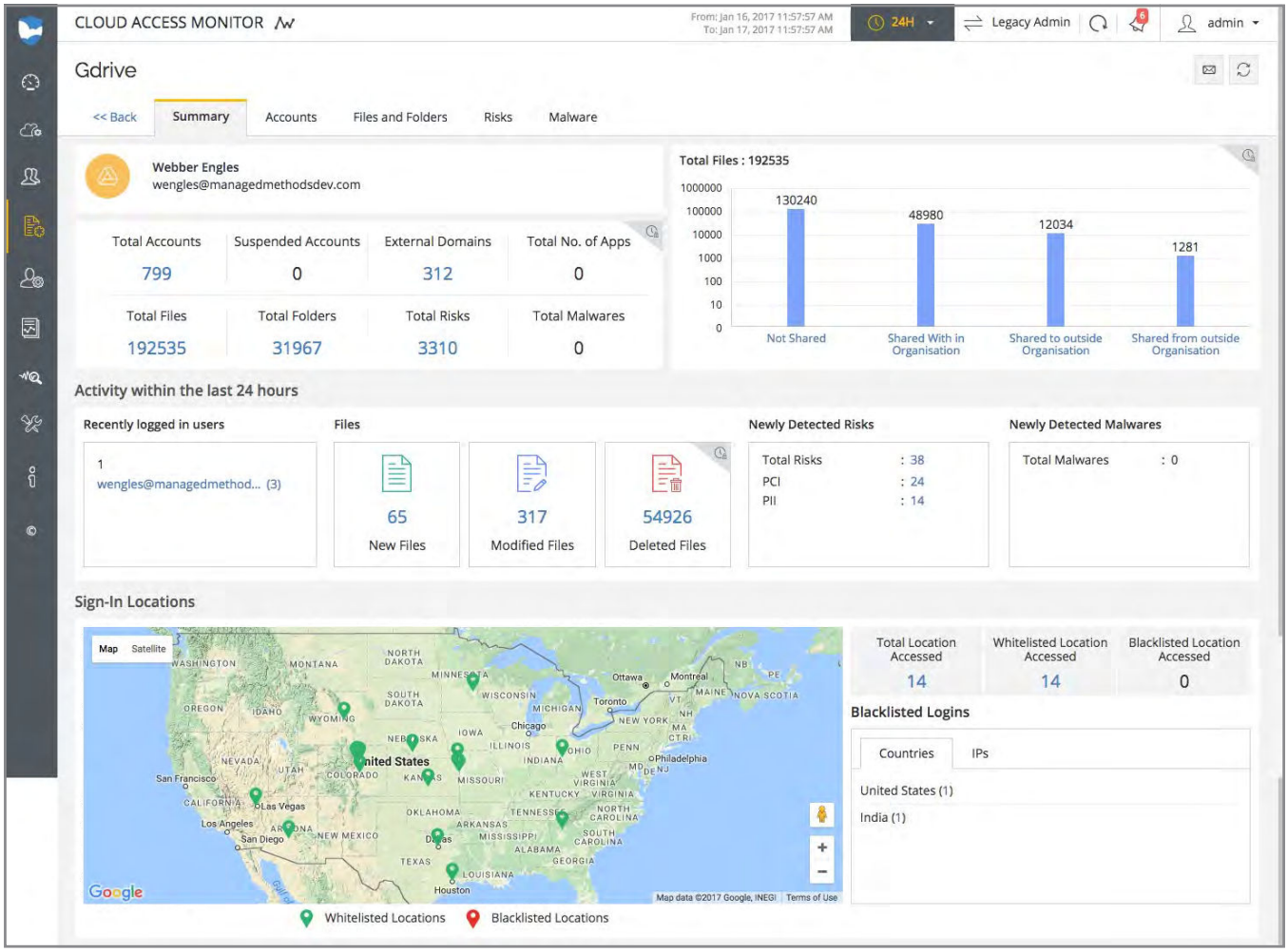

Figure 2: Cloud Access Monitor assesses risk from cloud applications

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

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

Using DPI, Cloud Access Monitor can check for the presence of information such as Social Security numbers, personally identifiable information (PII), or other forms of sensitive information going into cloud applications. Consider the example of a software developer uploading proprietary source code into an unauthorized file sharing application. This could be indicative of a foolish mistake on the user's part or an attempt to steal or sell intellectual property.

Data from the discovery process is used to assess the risk of each of these cloud applications. SaaS usage is viewed from both a security and a compliance perspective. 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 each application is for business use.

The "Full Enterprise": API Connections and Network Analysis

The two deployment models discussed above – integrated with one of the sanctioned SaaS applications like the four discussed above (Microsoft Office 365/OneDrive, Google G Suite, Box and Dropbox), or as a pure network analysis tool – can be combined for a much more powerful implementation of Cloud Access Monitor. The "Full Enterprise" deployment provides 100% visibility into an organization's use of cloud applications and threats that might be present.

Consider this example of how the two components of the Cloud Access Monitor product go hand-in-hand: A company is a Google G Suite shop and it has a next generation firewall. The company wants Cloud Access Monitor to analyze the network for what cloud applications people are using and to expose the shadow IT, and it also wants visibility into Google G Suite that the firewall can't provide. Meghan in the marketing department just logged into G Suite from the corporate network in Los Angeles. Cloud Access Monitor sees that login from both the firewall visibility as well as through the cloud application. Ten minutes later, Meghan's credentials are used to login from a coffee shop in New York City. This second login creates a conflict with what the network and the API in the cloud have seen, so Cloud Access Monitor can send an alert for someone to investigate what's going on. It could be a case of a compromised credential, with the potential for data loss or some other threat. Having the well-rounded perspective from the two halves of Cloud Access Monitor correlates the information and puts the whole story together.

Organizations are increasingly choosing this Full Enterprise mode to ensure they have the visibility and control they need from all angles of their SaaS applications.

ManagedMethods Delivers Rapid Deployment with No Impact on Users or Networks

Every organization needs data security, yet many hesitate to put more than the most basic level of security in place due to the perception that security solutions are very complex and thus difficult to install, operate and maintain. This perception is highlighted in a survey conducted by 451 Research in which 57% of respondents cite "complexity" as their number one barrier to adopting data security tools and techniques more widely. The cause cited as the number two barrier, "lack of staff to manage the solutions," ranked even higher than the perennial problem, "lack of budget."[9]

ManagedMethods has intentionally made Cloud Access Monitor quick and easy to install and use, regardless of the deployment configuration a company chooses. The solution can be installed on premise as a virtual appliance, in a public or private cloud, or as a hybrid combination of the two modes—and it's not a daunting task. Through API connections and integrations with numerous popular network security vendors, ManagedMethods makes cloud security easy.

For example, the shadow IT and cloud applications discovery from the network – with immediate visibility – can be setup

[9] 451 Research and Vormetric Data Security, "2016 Vormetric Data Threat Report," 2016

using out-of-the-box installations in less than an hour. No special training is required, and there is no need to re-architect the network. The API connections to the sanctioned cloud applications generally take 30 minutes or less per application. Cloud Access Monitor provides cloud security with no impact on users or networks.

In Summary

As organizations conduct more and more of their business using SaaS applications and services, they need to build an appropriate level of security and compliance around their data. SaaS providers don't provide adequate security, and legacy security solutions can't reach into the cloud. Only a Cloud Access Security Broker like ManagedMethods' Cloud Access Monitor can reach deep into sanctioned cloud applications to provide the visibility, control and policy enforcement that companies require.

Cloud Access Monitor uses application program interfaces to deploy right into several major cloud applications today, including Microsoft Office 365/OneDrive, Google G Suite, Box and Dropbox, and API connections into even more SaaS applications are coming soon. This mode of deployment brings enterprise-class security to cloud applications that companies use every day to run their businesses.

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 companywide standards for approved applications, and apply the necessary controls to safeguard data and reduce risk.

Every organization – large or small, public or private – is challenged by cloud visibility and control issues. Left unchecked, this lack of visibility can put companies at risk due to insecure or non-compliant data handling and storage practices. Whether an organization has 10 or 10,000 employees, the increased usage of cloud applications and services is becoming more of a security concern for IT teams. Knowing the extent of the problem is half the battle; the other half lies in doing something about it. Cloud Access Monitor accomplishes both.

About ManagedMethods

ManagedMethods offers the most efficient way to gain visibility into how data is stored, accessed and shared in cloud applications such as Microsoft Office 365, OneDrive, Google G Suite, Dropbox and Box, as well as to control unsanctioned Shadow IT applications. ManagedMethods' Cloud Access Monitor is the only Cloud Access Security Broker (CASB) that can be deployed in 30 minutes, with no special training, and with no impact on users or networks.