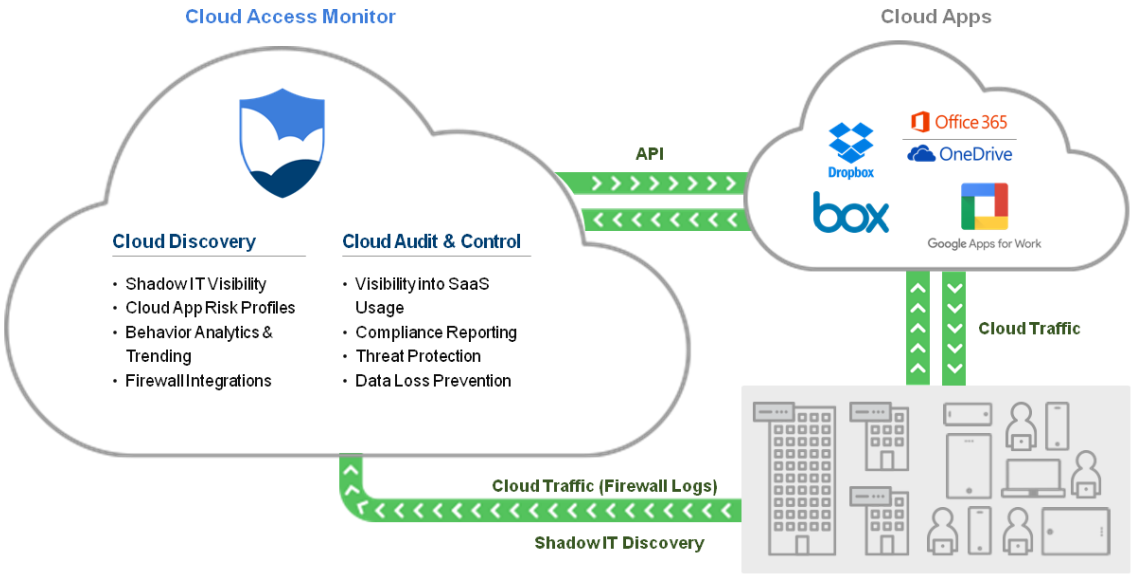
NETWORKWORLD
The Leader In Network Knowledge
www.networkworld.com October 14, 2016

ManagedMethods brings shadow IT and shadow data into the light

By Linda Musthaler, Principal Analyst with Essential Solutions Corp.

At the recent Gartner Security & Risk Management Summit, Gartner VP Neil MacDonald spoke about the technology trends for 2016 that provide the most effective business support and risk management. Cloud Access Security Brokers (CASBs) are number one on the list.

According to Gartner, companies' use of Software as a Service (SaaS) applications create new challenges to security teams due to limited visibility and control options. CASBs enable businesses to apply much-needed security policies across multiple cloud services.



SaaS is more than a trend; it's a global movement. In its IDC 50th Anniversary Transformation Everywhere presentation (opens a PDF), IDC claims that by 2020, penetration of SaaS versus traditional software deployment will be more than 25%, and packaged software will shrink to 10% of new enterprise installations. That means that 90% of new software installations will run from the cloud.

As Gartner's MacDonald alluded, there are two problems with SaaS applications that traditional security solutions do a poor job addressing. One is the limited visibility into the cloud apps, and the other is limited control over what happens inside a cloud app. This is the gap that CASB products intend to fill.

The visibility problem, also called shadow IT, refers to the IT department not knowing about or not sanctioning the use of various cloud apps. In this case, individual users, small workgroups and even entire departments engage with a SaaS provider and sign up for service—without IT involvement. Given that IT is ultimately responsible for data security, having people use unknown apps creates a number of problems for the organization. For instance:

- A SaaS app might not meet the business's security and compliance requirements.
- Some SaaS apps are too risky for business use.
- Data might elude disaster recovery plans if IT doesn't know where it is.
- The company could overpay for software licenses if multiple services in a category such as file sharing are used.

Even if a SaaS application is officially sanctioned for the company's use, there can be a problem with controlling what goes on within that application. This

is called shadow data, and it introduces problems like:

- Employees or other users putting sensitive or regulated data in the cloud without proper controls such as encryption
- Workers sharing files with inappropriate people, inside or outside the organization
- Disgruntled workers deleting files

SaaS app providers generally do a poor job of helping customers get the visibility and control they need. Traditional tools like firewalls – even next generation firewalls – might be able to report who is going to what cloud app, but they can't provide the depth of visibility and control that businesses need. And thus the CASB market was born.

Today the CASB solution market is relatively mature, with many vendors' solutions already three to five years old. While many CASB vendors focus on large enterprises, ManagedMethods is targeting small-to-medium sized businesses (SMB) and organizations like school districts and state and local governments. These types of organizations are enthusiastically embracing SaaS applications and they need help with shadow IT and shadow data.

ManagedMethods' solution is called Cloud Access Monitor. It is designed to uncover shadow IT through cloud discovery from the network, and help customers understand what cloud apps people are trying to use and the potential risk they present. Cloud Access Monitor provides additional layers of reporting for compliance, visibility and understanding, and then puts additional layers of data security and threat protection around the cloud apps. In particular, Cloud Access Monitor is integrated with four of the leading SaaS applications: Office 365 and OneDrive; G Suite (previously called Google Apps for Work); Box; and Dropbox.

Cloud Access Monitor can address many use cases, but the company says the two primary ones are cloud discovery and cloud audit and control.

In cloud discovery, the tool examines HTTP traffic to determine what cloud apps a person or group is using, which apps are used the most, which ones present risk to the organization, what apps people are uploading data to, from which locations people are accessing apps, and so on. The goal is to gain visibility and insight into what's happening with the cloud as it pertains to network traffic.

Using this insight, a company can determine which cloud apps it wants to sanction and which ones it wants to block. It can gain bargaining power to negotiate a site license agreement with its preferred applications. The company can account for data in the cloud for leak prevention and disaster recovery plans. Knowing what apps are in use, and by whom, is the first step to being able to take control.

The second major use case for Cloud Access Monitor is to take control of shadow data. Cloud Access Monitor is able to uncover what is going on inside a sanctioned cloud app, looking at who has access, what data they have sharing permissions to, who they are sharing the data with outside the corporate domain, whether there is sensitive or regulated data in the app, whether there is malware present, and more. Customers can get proactive alerts or can direct specific actions to happen when a situation is non-compliant with a policy; for example, drop a user's connection to the app if he is trying to download excessive data.

The four core SaaS apps supported grant OAuth permission into those accounts to gain visibility, discover all the data at rest, analyze that data for compliance reporting, scan for malware, and put in policies for data loss prevention.

For example, a retail organization may be using Google Drive (G Suite) and have a policy monitor to scan for malware as files are uploaded to Google Drive and scan data at rest, which provides for threat protection. They also prevent any associate or employee of the firm from deleting specific files and files of a certain size.

In another common use case, school districts using cloud applications in classrooms need to scan the data at rest in those apps for profanity, offensive remarks, threats and generally inappropriate behavior inside the data.

Cloud Access Monitor can be deployed on premise as a virtual appliance or in the cloud. If on premise, ManagedMethods can use a SPAN or tap and collect data passively. Otherwise the product can ingest data from firewall log files, so there is no impact to the network from deploying this solution. ManagedMethods says it can work with pretty much any firewall, but it has special partnerships with Check Point and WatchGuard to allow integration into their cloud management consoles and their threat protection layers.

As the use of SaaS applications continues to increase, organizations need a way to regain visibility and control over what their users are doing in the cloud.