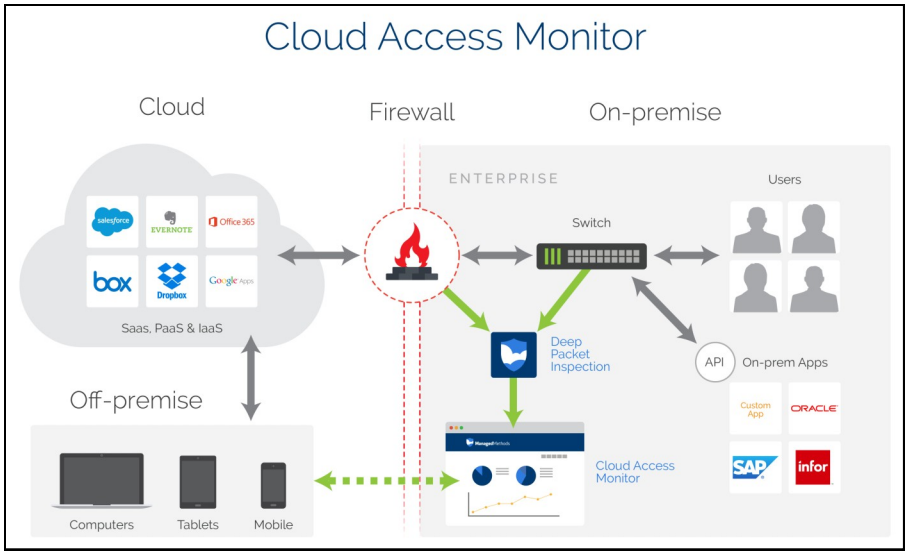
NETWORKWORLD
The Leader In Network Knowledge
www.networkworld.com May 11, 2015

Cloud Access Security Broker keeps usage data on-premise as you discover, analyze and secure cloud applications

By Linda Musthaler, Principal Analyst with Essential Solutions Corp.

Companies today are dealing with a whole different cloud economy compared to just a few years ago. SaaS applications are now available for 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. Practically every business unit relies on cloud-based productivity applications that have become integral to their mission.

Of course some workgroups and workers have become a bit too enthusiastic about using cloud applications, going so far as implementing tools outside the purview of the IT department, giving rise to what many call Shadow IT. Consider these statistics from various industry reports:



- The Ponemon Institute reports that an average of 50% of cloud services are deployed by departments other than corporate IT. What's more, an average of 44% of corporate data stored in cloud environments is not managed or controlled by the IT department.

- The average number of SaaS applications in use within enterprise organizations is 923—up 21% since 2014, according to Skyhigh Networks.

- A Cloud Security Alliance survey says only 8% of companies know the scope of Shadow IT within their environments. 72% of survey respondents say they don't know how pervasive the problem is but they would like to know.

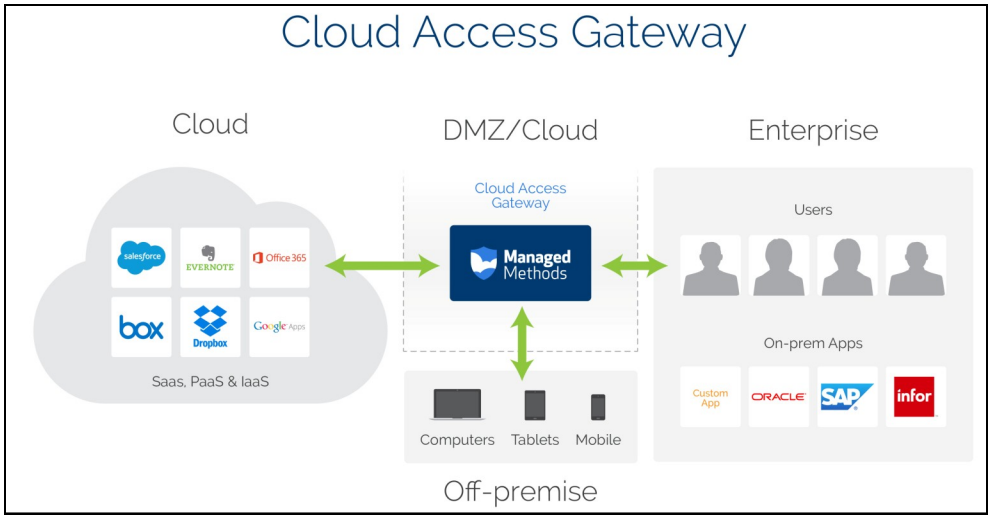
And they should know how pervasive the problem is. Left unchecked, Shadow IT can put companies at risk due to insecure or non-compliant data handling and storage practices. For example, one industry study found that among users of cloud-based file sharing applications, 34% have uploaded sensitive information, such as personally identifiable information (PII) or payment card information to one of these services.

Knowing the extent of the Shadow IT problem is half the battle; the other half lies in doing something about it. This has given rise to a category of solutions that Gartner calls the Cloud Access Security Broker (CASB) market. CASB tools are designed to be security, visibility and policy enforcement points placed between cloud services and the consumers of those services.

ManagedMethods is a new entrant in the CASB market. ManagedMethods' products help companies monitor and control the use of cloud applications (SaaS) and reduce the potential risk of Shadow IT. What's interesting about ManagedMethods in a teeming CASB

market is the solution can do its data collection and analysis entirely on-premise, if desired. The solution can be installed on-premise as an appliance or as a software offering, or it can be delivered as a SaaS solution with on-premise data collection. This makes it a good choice for companies that are reluctant to or prohibited from sending activity information outside the organization.

ManagedMethods has separated its full solution into two products, Cloud Access Monitor and Cloud Access Gateway. The company learned through early research that many prospective buyers prefer to start their implementation with monitoring cloud application usage and getting a thorough understanding of what is going on. Then, later, these customers grow into the need for the security gateway that adds policies and protections for cloud usage. The Cloud Access Monitor product is generally available now, and the Cloud Access Gateway product is slated for release in the second half of this year.



The Cloud Access Monitor product is used by security teams to discover and monitor all the cloud applications being used by the organization. Many other CASB solutions use log files to discover cloud applications, but ManagedMethods passively captures traffic as it comes in or goes out of an enterprise network. The solution looks at data coming off of a switch or a firewall, giving the ability to analyze the traffic in real-time with no intrusion and no latency. Then ManagedMethods applies deep packet inspection (DPI) to analyze the data at a more granular level.

The monitor product can tell the company what cloud apps 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. The application analysis includes an editable risk score so that companies can see at a glance which cloud apps pose the most risk to the business.

The deep packet capture is a key component of ManagedMethods' solution. It provides the ability to look at all the information, not just log entries, to take the discovery further and conduct granular analysis that goes deeper than logs can. For example, let's say a company is concerned about employees putting sensitive information into Evernote. ManagedMethods can look at the content uploaded and check for the presence of information such as Social Security numbers or other PII. Coupled with the policy engine of the Cloud Access Gateway, this content information can help the company set protections for that sensitive information, such as encryption or tokenization.

ManagedMethods doesn't have to look at all traffic and file contents, though. It filters for certain protocols that are used by cloud applications. This vastly reduces the required processing power.

The second piece of the solution is said to be coming to market in a few months, and this is the gateway service. ManagedMethods says it will have a full suite of features and functionality for controlling the use of cloud applications and adding policies and security. They say it will include encryption, tokenization, authorization control, policy management, content filtering, malware detection and prevention, and integration with single sign-on, among other capabilities. The idea is to have a comprehensive set of capabilities to bring to the cloud the types of controls that companies are accustomed to having in their data centers.

As cloud usage and especially Shadow IT continue to grow, companies need something like a CASB tool to regain knowledge and control of the applications their workers are using.