Gigamon®   ManagedMethods

Joint Solution Brief

Enabling Comprehensive Visibility and Monitoring of Cloud Application Usage

The Challenge

Cloud application (SaaS) usage is on the rise. Business units are adopting SaaS applications at an increasing rate. Sensitive data moves freely between the enterprise and the cloud. IT security teams are struggling to maintain control, and to prevent data loss and reduce risk. Sanctioned and unsanctioned cloud application usage has created additional risk of internal/external data leaks, malware attacks from suspicious cloud providers and, the danger of Shadow IT spinning out of control.

Integrated Solution

- ManagedMethods' Cloud Access Monitor and Gigamon's Unified Visibility Fabric™ provide IT security groups with visibility and insight into all cloud application usage
- Easy, efficient, and scalable deployment model ensures rapid time-to-value and full visibility of cloud applications being used by your company

Key Benefits

- Provide adaptable traffic visibility: Aggregates network traffic to gain in-depth visibility across the enterprise into cloud application usage. Forward traffic from multiple external links to the same ManagedMethods deployment for analysis
- Scalable deployment: intelligently distribute large traffic flows across multiple ManagedMethod platforms
- Enforce policies to ensure data privacy on cloud application usage
- Monitor cloud access to identify sensitive data leaving the organization

Introduction

Companies today are dealing with an entirely different cloud ecosystem compared to just a few years ago. It's no secret that cloud application (SaaS) usage is on the rise in today's business world. SaaS applications are available for most of the core business functions throughout an enterprise. It's relatively easy for business units within the company to implement new applications themselves, without IT involvement, and their use is on the rise. Sensitive data moves freely between the enterprise and the cloud while IT security teams struggle to maintain control, prevent data loss, and reduce risk. The use of both sanctioned and unsanctioned cloud applications has created an intensified risk of internal/external data leaks, malware attacks from suspect or infiltrated cloud; Shadow IT is in danger of spinning out of control.

To detect the use of these SaaS applications, enterprises need to monitor network traffic and identify the applications being utilized. This hits a further complication: on average, 25-35% of traffic on today's corporate network is SSL encrypted and many security and analytics tools can't decrypt that traffic, or hit performance issues when they do[1]. With Gartner predicting that 50% of all network attacks will be encrypted by 2017[2], this presents a blind spot that needs to be removed to control Shadow IT.

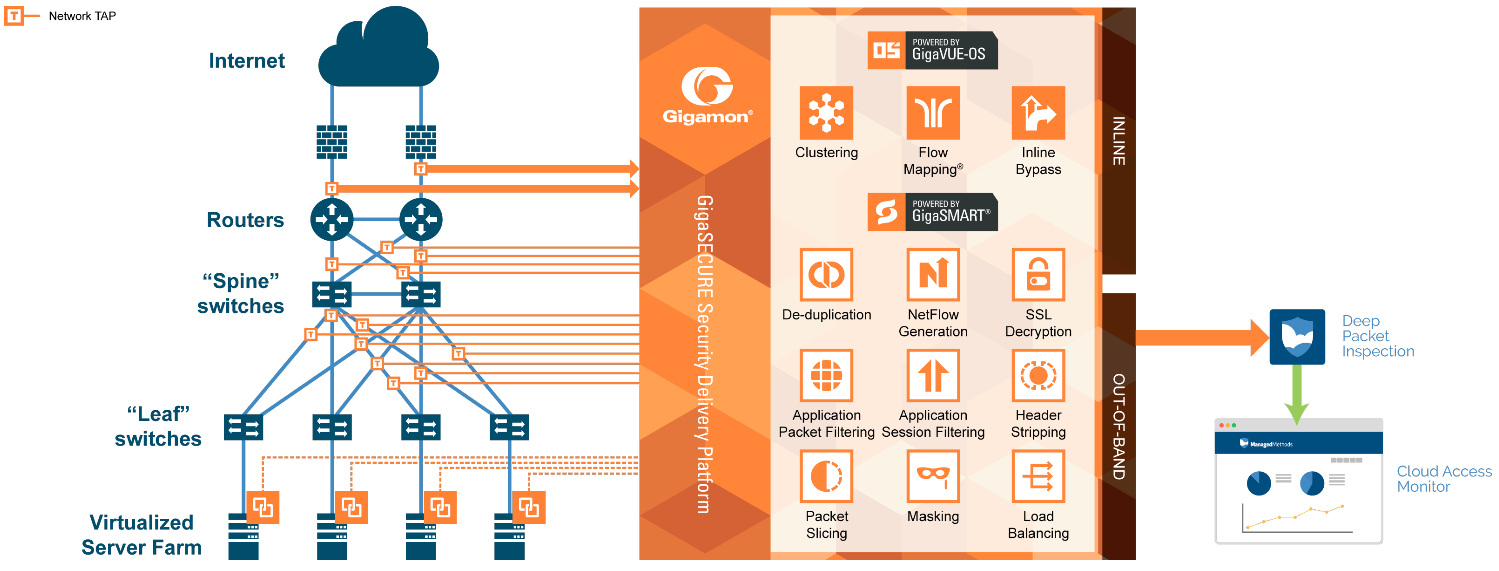
Gigamon Visibility Fabric and ManagedMethods Cloud Access Monitor

Visibility today means insight into infrastructure blind spots. The integration of Gigamon's GigaSECURE® platform and ManagedMethods' Cloud Access Monitor provides IT security groups with visibility and insight into all traffic and cloud application usage on the network. Rather than try to pull data from a SPAN port, or firewall, which will drop traffic when the device is running near capacity and may drop packets well before then due to contention, the GigaSECURE platform provides an efficient way to tap into any external links from the company's network. Any link at headquarters or from remote locations, can be tapped and the traffic delivered to a ManagedMethods monitor where SaaS applications can be identified.

The GigaSECURE platform can also be used to decrypt SSL encrypted traffic and forwarded to Cloud Access Monitor for analysis.

[1] Pirc, John W. "SSL Performance Problems." NSS Labs. 2013. Accessed October 27, 2015. https://library.nsslabs.com/sites/default/files/public-report/files/SSL%20Performance%20Problems.pdf

[2] Gartner "Security Leaders Must Address Threats From Rising SSL Traffic". Published: 9 December 2013



ManagedMethods Cloud Access Monitor is a Cloud Access Security Brokers (CASB). It analyzes traffic leaving your network, telling you who is using cloud applications, which apps they are using, what data they are sending, which devices they are using and where they are doing this (on-site or off).

With this information, IT can assess the risk to the business of the applications being used and react appropriately to enforce corporate policy while maintaining business continuity.

ManagedMethods and Gigamon have collaborated to offer customers one of the most flexible deployment options, coupled with robust performance. The combined solution ensures traffic is analyzed to show unsanctioned use of cloud applications and services that could potential expose an organization to security risks and data loss.

About Gigamon

Gigamon provides the GigaSECURE® Security Delivery Platform to enable the management of increasingly complex networks. Gigamon technology empowers infrastructure architects, managers and operators with pervasive visibility and control of traffic across both physical and virtual environments without affecting the performance or stability of the production network. Through patented technologies, centralized management and a portfolio of high availability and high-density fabric nodes, network traffic is intelligently delivered to management, monitoring and security systems. Gigamon solutions have been deployed globally across enterprise, data centers and service providers, including over half of the Fortune 100 and many government and federal agencies.

Learn More

For more information on the ManagedMethods and Gigamon solution, contact:

ManagedMethods

www.managedmethods.com

Gigamon®

www.gigamon.com