# Performance and Security Monitoring in the Public Cloud

**Sneha Mirajkar** SMirajka@cisco.com
**Vittalkumar Mirajkar** Vittalkumar_Mirajkar@mcafee.com
**Narayan Naik** Narayan_Naik@mcafee.com

## Abstract

As business workloads move to public cloud, organizations must continue to maintain data and application security, optimize performance, and resolve issues as quickly as possible. However, getting access to large incoming traffic data in the public cloud can be a challenge and so is building strategies to access or tap traffic that is moving between cloud instances and then decide on a strategy for data filtering and grooming to help the security and performance monitoring layer to work efficiently and cost-effectively.

This paper, in addition to exploring the pros and cons of different approaches to security and performance monitoring in the public cloud, also provides an insight into how a filter-scanner sitting in the cloud instance and a security layer between cloud instances can provide the required security not only to the incoming traffic but also to the resting data, without compromising on the performance, mimicking the private cloud capabilities.

In a public cloud, traffic moving between different application and databases, referred to as east-west traffic is more difficult to intercept. When an organization uses a public cloud, the underlying infrastructure is completely transparent and seeing data is even more challenging. By embedding a network filter-scanner inside each cloud instance that is spun up, the filter-scanner can access all the data generated, eliminate all unnecessary info like duplications, erroneous data and more, in that instance and deliver it to security and performance layer, which then analyzes data packets/payload for anomalies and patterns in the data to enforces the business logic, i.e. ACLs to allow the request further or deny the same, creating incidents and reports to postmortem later, achieving security and performance at full strength in public cloud, preserving the benefits of cloud computing. Along with on-demand scalability, reduced time to resolution and easy operation on public cloud, which till now was limited to private cloud.

## Biography

Sneha Mirajkar is a Senior Software Engineer at Cisco, with 12+ years of experience in software testing and extensive hands-on in test automation using Python, AWS, web-services. She has expertise in AWS applications.

Vittalkumar Mirajkar is a Software Architect at McAfee, with 12+ years of testing experience ranging from device driver testing, application testing and server testing. He specializes in testing security products. His area of interest is performance testing, soak testing, data analysis and exploratory testing

Narayan Naik is a Software Engineer at McAfee, with 11+ years of experience in exploratory testing and performance testing. He holds an expertise in providing consultation to enterprise customers for features and compatibility of various security products and security solutions deployed. His areas of interest are inter-compatibility test areas, performance testing and encryption product lines.

# 1 Introduction

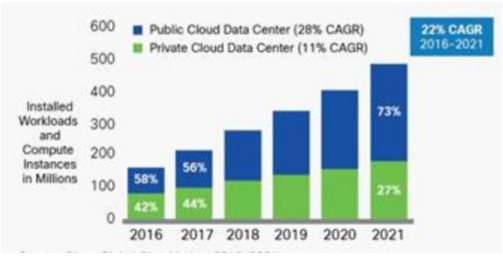
As workloads move to the cloud, organizations must adjust their strategies for accessing and monitoring traffic. They first need to tap traffic that is moving between cloud instances and then decide on a strategy for data filtering to help their monitoring tools work efficiently and cost-effectively. The solution proposed here, enables data processing to be done in the cloud and then delivered directly to cloud-based security tools. The best overall monitoring strategy for many organizations will be a hybrid approach that supports continued use of powerful customized tools, combined with newer cloud-native tools available. With this approach, security is maintained at full strength, while the organization continue their transitions to cloud computing without having to compromise on performance, thus having the benefits of a private cloud while working on public cloud infrastructure (Ixia 2019).

# 2 Increase in cloud adoption and its challenges

Public cloud, as indicated by the workloads and compute instances growth, is growing faster than the private cloud. Public cloud adoption is fueled by greater need for agility, cost consideration and increase strengthening of public cloud security. Enterprises might adopt a hybrid approach where some of the cloud computing resources are managed in-house and some are provided by an external provider. Cloud bursting is an example of hybrid cloud where many mission critical workloads and daily computing requirements are handled by a private cloud, but for sudden spurts of demand the additional traffic demand (bursting) is handled by a public cloud.

Services like Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and others offer much less expensive multi-tenant services on shared infrastructure with elastic compute and storage capabilities. Public cloud adoption continues to expand rapidly with AWS S3 growing over by over 650% between 2006 and 2013.1 Predictions for public cloud workloads show it growing at least 400% from 2015 to 2020.2

While the overall cloud workloads and compute instances are growing at a Compound Annual Growth Rate (CAGR) of 26 percent from 2016 to 2021, for the same period Public Cloud is expected to grow by 28 percent where as Private cloud at 11 percent. By 2021, there will continue to be more workloads and compute instances (73 percent) in the public cloud as compared to private cloud (27 percent) (Cisco 2018).




Average Workload and Compute Instance Density = (Total Physical Servers * Virtualization Rate (% of Physical servers are virtualized) * VM density (Average VMs per virtualized physical server)) + Non-virtualized Physical Servers) / Total Physical Servers.

Figure 2.1: Public vs. Private cloud growth between 2016 to 2021

## 2.1 The most serious attacks include:

**Data breaches:** If your cloud provider suffers a data breach, you may suffer exposure of sensitive customer information that could lead to serious financial or legal consequences, as well as damage to your brand.
**Denial of service:** These attacks take advantage of vulnerabilities in Web servers, databases, or other resources to disrupt a cloud service, sometimes as a distraction while another attack is taking place.

**Insecure interfaces:** The connectors of digital services are the most exposed part of any system and are frequently targeted. If the mechanisms used to manage systems, move data, and conduct admin tasks are compromised, an attacker can get access to almost anything.
**System vulnerabilities:** In multitenant computing, vulnerabilities in one environment can lead to an attack on an adjacent tenant with shared resources. The source is often poorly implemented or unpatched software.

## 2.2 Public Cloud Vs Private Cloud, a quick look

Below table gives a quick comparison at a broad level between Public Cloud vs Private Cloud. (Sungardas 2019)

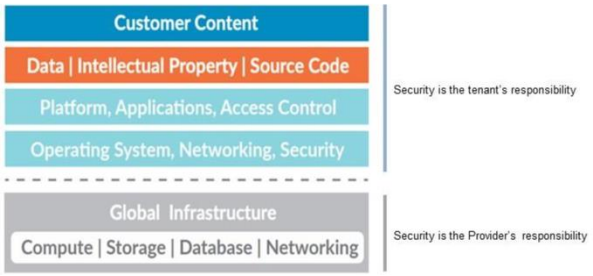
| | Private Cloud | Public Cloud |
|---|---|---|
| **Infrastructure** | Single-Tenant: Dedicated hardware and network for your business managed by an in-house technical team. | Multi-Tenant: Shared network hosted off site and managed by your service provider. |
| **Business requirement** | High performance, security, and customization and control options. | Affordable solutions that provide room for growth. |
| **Best use** | Protect your most sensitive data and applications | Disaster recovery and application testing for smaller, public facing companies. |
| **Scalability** | Can be managed in house. Extreme performance – fine-grained control for both storage and compute. | Depends on the Service Level Agreement but usually easy via a self-managed tool the customer will use. |
| **Support and maintenance** | Your technical administrators. | Cloud Service Provider's technical team. |
| **Cost** | Large upfront cost to implement the hardware, software and staff resources. Maintenance and growth must also be built into ongoing costs. CapEx. | Affordable option offering a pay as you go service fee.<br><br>OpEx – Pay as you go, scale up, scale down as needed, charged by the minute. |
| **Security** | Isolated network environment. Enhanced security to meet data protection legislation. | Basic security compliance.<br><br>Some may offer bolt-on security options. |
| **Performance** | High performance from dedicated server. | Competing users can reduce performance levels. |

## 2.3 Security considerations for Public cloud

As enterprises adopt public cloud, the potential attack surface expands to include attacks on the cloud provider, as well as the provider's other clients. Most providers employ strong security measures, but they

still face the same threats as traditional networks, the only difference is that, as a customer, you do not have as much control over what is done to safeguard against these threats.

In the current scenario, the public cloud is shared with multiple tenants. Thus, creating a larger need for securing moving traffic between the instances in public cloud (Johnson 2017).




Security is a shared responsibility by the user and provider, that requires constant attention and investment by both providers and organizations.

**Figure 2.2: Public cloud shared responsibility model**

## 3. Data security approach in public cloud:

The approach we are presenting here to handle the authorized upload of files which may/may-not be malicious, is by getting complete transparency to cloud data. In order to achieve this, a simple customized **network scanner** is deployed as a component in each of the cloud instances spun up. How does this work? The **cloud filter platform** gets access to data in public cloud through the **network scanner**. The **network scanner** makes copies of all the data passing through the cloud instance. The captured data is filtered and sent to a **cloud filter platform,** that aggregates data from multiple sources, processes as necessary to remove duplicates and unnecessary info, isolates data of interest and delivers it to security solutions located in the cloud. A centralized, web-based interface is used to manage the **cloud filter platform** across the entire enterprise that is using the public cloud. Customized filtering policies are configured for policy enforcement.

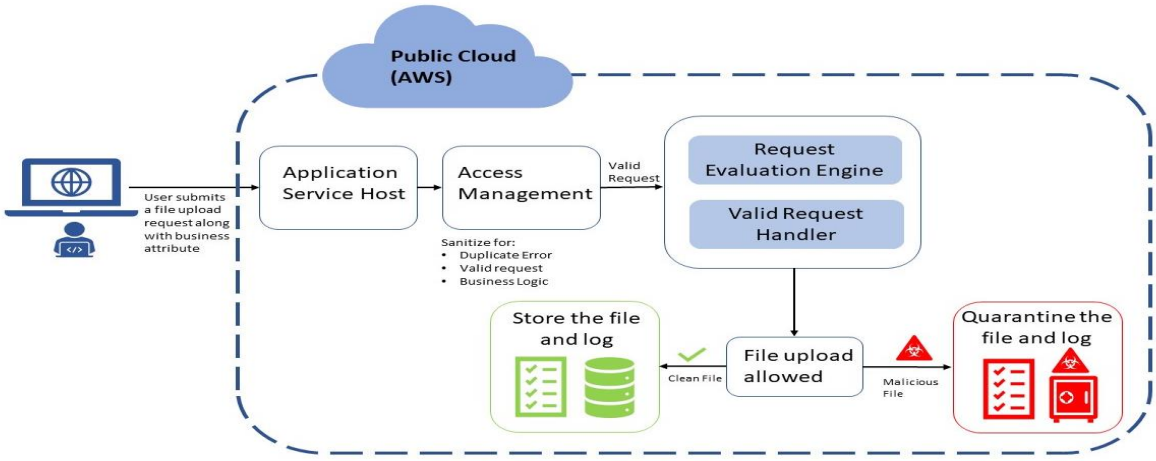



Figure 3.1 Data security approach in public cloud

## 4. Implementation of the suggested approach in public cloud:

The test environment chosen here is with AWS public cloud. The user end point is mobile device (A laptop connected to public network), the vendor storage is Dropbox and an AWS hosted cloud filter platform.

The proposed solution consists of establishing a 3-way handshake between the end point, cloud vendor and cloud filter platform. The 3 main entities being the public end point, the vendor storage and lastly the cloud filter platform.

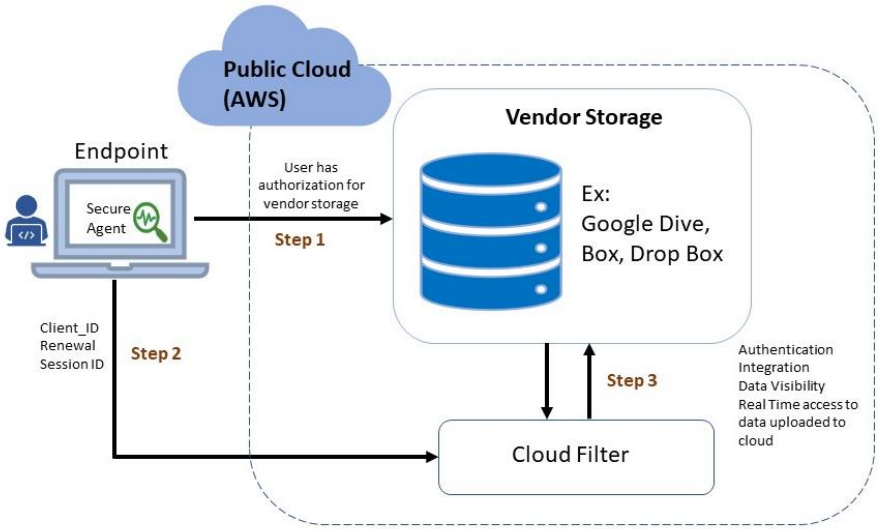



Figure 4.1 Three-way handshake.

Once the data is uploaded to the cloud vendor by the authorized end point, the polling agent (part of message queue) updates the queue with the delta of the changed values in the cloud vendor storage at the end of the scheduled polling time, this contains the metadata json of newly added files.

The metadata will be consumed by the scanner/filter for analysis, identifying potential malware (VirusTotal 2019), invoking the corresponding quarantine action. The non-malware metadata is then consumed by the downloader for the files to be downloaded and scanned for violations against given set of rules (Google 2019), (StackArmor 2019), calling for corrective actions such as updating the administrative contacts of the violations and access restrictions.

In the above approach, the performance is not compromised as the malware detection scan is executed on the file metadata, thus not waiting for the file to be downloaded. Secondly, for the policy violations, scans are triggered on the downloaded files and not the actual files, this leads to no variations in the performance of the cloud eco-system. Furthermore, with increase in the frequency of the API calls made to the cloud vendor to fetch more data, performance can be improved, since the data can be processed much faster to have more substantial results in given time.

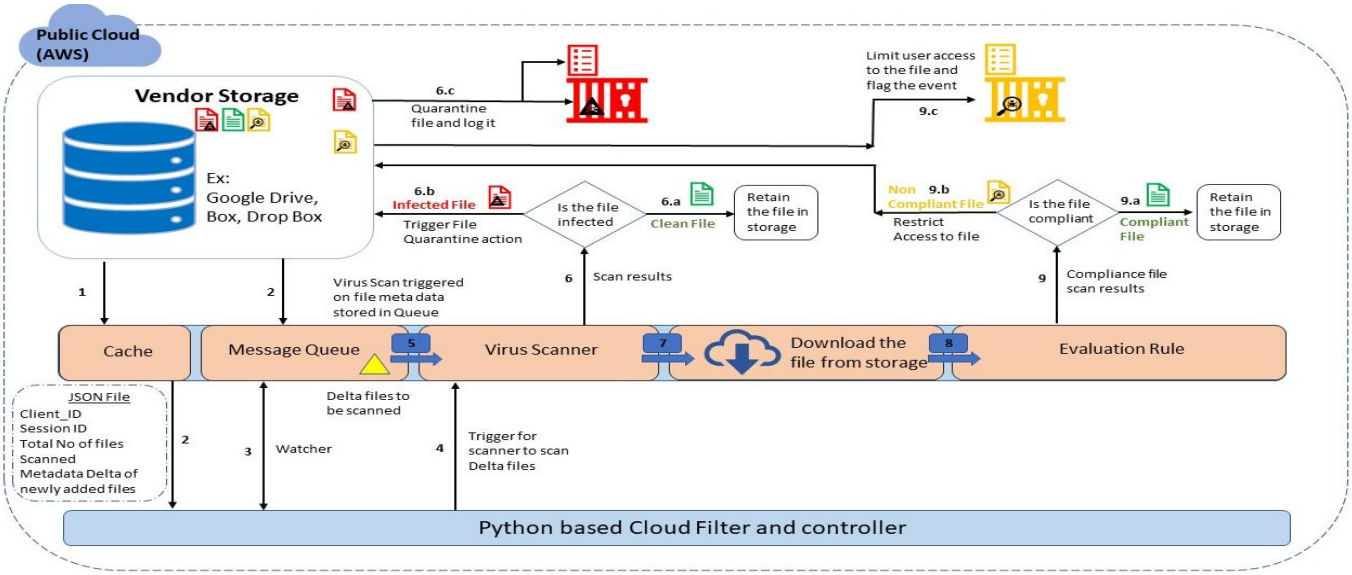



Figure 4.2 The workflow of file analysis and corrective actions

Advantages:

- With the flexibility and on-demand scalability, data collection and filtering can be automatically initiated each time a new vendor is launched.
- Reduced time to resolution – threat identification and issue resolution is in real time.
- Increased security in public cloud.
- Performance can be hiked since container technology is used for filtering and processing in the cloud instance.
- Custom policies to decide on the course of corrective measures.

Disadvantages:

- Restricting access to the uploaded files until the scan is completed may come with additional cost of implementing access restrictions.
- Increased cloud expense – Cloud capacity must also support traffic collection and filtering.
- Tool costs – containerization using the latest version of Docker will need constant upgrade.

## 5. Results:

Cloud filter and scanner does not have any impact on the response time of the file up loads from endpoint to cloud storage. Cloud filter does not live intercept the network traffic but performs scan operation on metadata and policy evaluations on mirror imaged data, since there is no withholding of live data, network performance impact is almost Nil, however the overall system security is drastically increased with this approach.

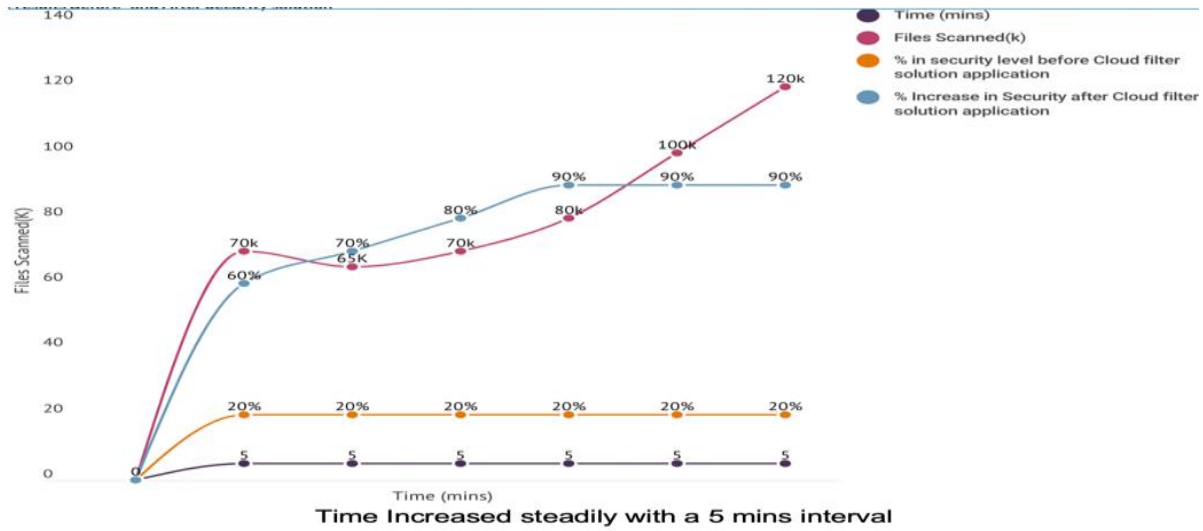



Figure 5.1 Result graph With and Without potential security risks.

## 6. Conclusion:

Security and performance management in the public cloud has been a major concern. Of the multitude of security concerns in public cloud, one of the most prominent being malware detection and policy violations. These can be achieved by deploying the approach discussed in this paper. The complete solution is built using open source tools and readily available virus information database ex: virustotal.com

The possible trade-offs here could be handling the additional logging and spike in CPU usage based on the data handled.

## 7. References:

Cisco. 2018. "Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper." Nov 19. Accessed May 2, 2019. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf/index.html.

Google. 2019. *Cloud Data Loss Prevention.* Accessed April 5, 2019. https://cloud.google.com/dlp/.

Ixia. 2019. *Security and Performance Monitoring in Public Cloud.* Accessed May 2, 2019. https://www.ixiacom.com/resources/security-and-performance-monitoring-public-cloud.

Johnson, Stephanie. 2017. *Only YOU Can Secure Your Data in the Public Cloud (In My Best Smokey the Bear Voice).* Oct 23. Accessed May 4, 2019. https://blog.paloaltonetworks.com/2017/10/can-secure-data-public-cloud-best-smokey-bear-voice/.

StackArmor. 2019. *Data Loss Prevention (DLP) on AWS S3.* Accessed May 15, 2019. https://stackarmor.com/data-loss-prevention-with-stackarmor-threatalert/.

VirusTotal. 2019. *https://www.virustotal.com.* Accessed 2019. https://www.virustotal.com.

www.sungardas.com. 2019. *The Difference Between Public and Private Cloud.* Accessed May 10, 2019. https://www.sungardas.com/en/about/resources/articles/difference-public-private-cloud/.