

Cloud Threat Defense – a Threat Protection and Security Compliance Solution

Deepak R Bharadwaj
McAfee Software India Pvt Ltd.
Bangalore, India
Deepak_Bharadwaj@McAfee.com

Anamika Bhattacharya
McAfee Software India Pvt Ltd.
Bangalore, India
Anamika_Bhattacharya@McAfee.com

Manivannan Chakkaravarthy
McAfee Software India Pvt Ltd.
Bangalore, India
Manivannan_Chakkaravarthy@McAfee.com

Abstract— According to Cloud Security Alliance (CSA), over 70 percent of the world's businesses now operate on the cloud. However, like any new technology adoption, cloud computing adoption opens new forms of security risks. This paper explores security issues related to cloud computing and proposes a cloud-native scalable security solution for the cloud. The paper investigates some of the key research challenges of cloud security solutions to secure the dynamic cloud environment and provides a practical solution to overcome the challenges that the cloud providers and consumers face securing their data and valuable assets.

Keywords— cloud computing, cybersecurity, security threats, security controls, threat defense

I. INTRODUCTION

Cloud computing is an information technology paradigm that delivers scalable on-demand computing services like compute, storage, network, software and many more over the internet. More and more organizations are now entrusting their IT resources and processing to the cloud. This trend is likely to grow in the coming years. To illustrate, Gartner predicts [1] that cloud data centers will process 92 percent of workloads by 2020. Cloud workloads are expected to increase 3.2 times in that same span of time, Cisco forecasts [2]. As organizations start migrating to cloud the security teams must re-think their security strategies to secure their applications, workloads, and data on the cloud.

II. CLOUD vs TRADITIONAL: UNDERSTANDING THE DIFFERENCES

The Traditional multi-tiered architecture consists of the presentation tier, middle tier, and data tier where each tier runs its service on a dedicated server and is by design more static in terms of both hardware and networking configurations.

Cloud by default provides ease of scalability, dynamic provisioning, Failure Resiliency, and geo-availability hence application development and architecture also must go through a paradigm shift to adopt and leverage the flexibility and features of the cloud.

Adoption of **Service Oriented Architecture** and **Serverless Architecture** are picking up as applications become more cloud-native rather than lift and shift migrations of traditional applications to the cloud.

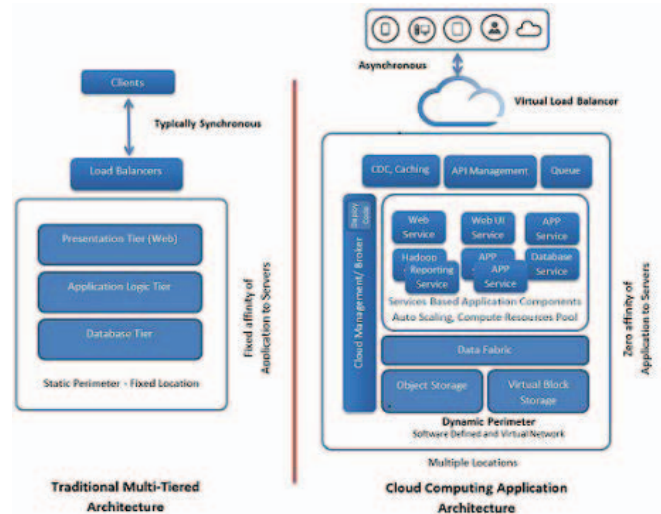


Figure 1. Cloud vs Traditional architecture [3]


With cloud services, the traditional endpoint focused security operations tools do not work as the perimeter and security gradually move away from the endpoint to cloud security controls and much of the insights are lost.

III. SECURING CLOUD

A. Shared Responsibility model

With a shared responsibility model on the cloud, it is imperative for an organization to monitor, identify and remediate on any potential threats and misconfigurations on their cloud assets.

Shared Security Responsibility Model			
On-Premises	IaaS	PaaS	SaaS
Users	Users	Users	Users
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network	Network	Network	Network
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical


 Customer Responsibility Cloud Provider Responsibility

IaaS: Infrastructure as a service; PaaS: Platform as a Service; SaaS: Software as a Service

Figure 2. Shared Security Responsibility Model

B. Challenges with securing Cloud

- **Dynamic environment:** The elastic nature of environments on the cloud, makes timely ongoing visibility of virtual instances difficult.

Protecting of such environments require a continuous discovery, security assessment and proactively take actions to protect them.

- **Perimeter definitions:** Cloud workloads are often fragmented across several different geo-locations and environments, making it difficult to centrally manage assets
- **Loss of control on physical security:** As organizations lose control over physical security, the responsibility of protecting data and workloads at transit and rest falls into the lap of the customer.

Virtualized and multi-tenant nature of public cloud make it necessary that an organization is always up to speed with the latest vulnerabilities and take remediation actions when necessary.

C. Top Security Issues in Cloud

As per reference [4,5], the top security threats identified in the cloud are:

- Data Breaches
- Insufficient Identity, Credential, and Access Management
- Insecure Interfaces and APIs
- System Vulnerabilities
- Account Hijacking
- Malicious Insiders
- Advanced Persistence Threats
- Data Loss

- Insufficient due diligence
- Abuse and Nefarious Use of Cloud Services
- Denial of Service
- Shared Technology Vulnerabilities

To identify and mitigate the above security threats they can be categorized under the following categories:

1) **Poor Identity and Access Management:** Identity and access management are very important to answer the 5 W's(Who, what, when, where, why) of accessibility of resources. Poor Identity and access management can result in

- Account Hijacking:** If Cloud vendor console or API credentials are lost, a malicious actor outside of an organization can take control of the cloud environment.
- Data Breaches:** Poor access management of object storage buckets and data stores cause sensitive information to be made public, which has been one of the major causes of data breaches on the cloud.
- Malicious insiders:** Malicious insiders trying to take admin/root privileges, can result in loss of sensitive data and systems.
- Abuse and Nefarious use of cloud resources:** Account hijacking of a cloud account can result in the malicious user to use the compromised resources to launch DDOS, spam and phishing campaigns leaving the organization prone to legal liability
- Insufficient Due-diligence:** Organizations which handle data and fall under regulatory compliance laws, need to have a clear plan to migrate to the cloud, else this poses a security threat and legal liability.

2) Workload threats

- Advanced persistent threats(APT):** Malware and Advanced persistent threats once enter an environment, adapt to the security measures and over time gain a foothold in the environment and propagate itself laterally and once it reaches the intended goal, it will exfiltrate sensitive data. These threats are difficult to identify and remediate.
- Vulnerabilities:** With Cloud services being multi-tenant, vulnerabilities that include privilege escalation and VM boundary jumping can cause data breaches and leave the applications and workloads vulnerable.
- Insecure application services:** Insecure API's serving different service of an application can leave the application vulnerable to known attacks and result in application downtime or data breaches.

3) Network threats

- a. *DOS and DDOS attacks:* Poor network segmentation and firewall management lead to cloud resources being targeted by DOS and DDOS attacks which result in poor application performance and even application downtime.
- b. *Data exfiltration:* Poor outbound firewall controls leads to data exfiltration attempts by compromised workloads

IV. PROPOSAL-CLOUD THREAT DEFENSE

Cloud Threat Défense is an integrated cloud-native scalable solution focused on the endpoint and cloud security control logs to create a unified security operations tool that can bring visibility into threat intelligence, analytics, and proactive remediation assistance.

The aim of this proposal is to successfully demonstrate ways to identify trends, threats and intelligently suggest appropriate remediation actions by using Cloud native services to collect, aggregate and analyze logs across different sources.

A. Cloud Workload Defense Control Hierarchy

Based on Gartner guide for Cloud workload protection [5] Figure 3 below helps enterprises prioritize their security strategies for the public cloud.

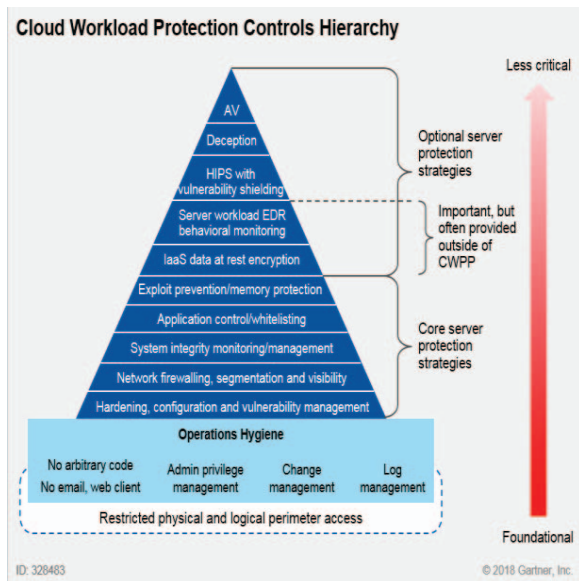


Figure 3. Cloud Workload Protection Controls Hierarchy [6]

B. Approach

Traditional workloads tend to be long-lived hence a full stack security solution with a large footprint might be an acceptable solution, whereas cloud servers tend to be immutable and installation of security solutions with a large

memory/disk footprint, kernel dependency tends to consume the computational resources and is a bane to the quick agile deployment workflows on cloud.

The above-mentioned solution architecture proposes that a different approach for the cloud security, which is more of detection based rather than prevention i.e., it is rather easy to replace the vulnerable/compromised servers than to fix them.

The solution is built using the two concepts on the cloud servers i.e. Immutable servers and Zero-Trust.

1) Immutable Servers

The solution utilizes the concept of immutable servers as one of the remediation actions. The basic premise is that rather than changing the existing server when a potential threat is identified, it's better to create a new one with pre-defined security controls and policies as it minimizes the challenges for configuration management and improves the reliability of the infrastructure.

2) Zero-Trust

The solution continuously analyses the configurations, user access logs, network logs, endpoint logs to provide us the ability to enforce the Zero Trust concept to cloud security i.e. "never trust, always verify".

With immutable servers on the cloud, we can take additional steps to lock down configurations, workloads, applications, and users to the least privilege, known and accepted usage patterns.

In the above solution, any deviation from the preconfigured policies it is assumed to be out of compliance without further decision making, which automatically triggers the configured remediation actions like network isolation, termination or revoking of privileges as applicable to the resource.

C. Cloud Threat Defense- Proposed architecture

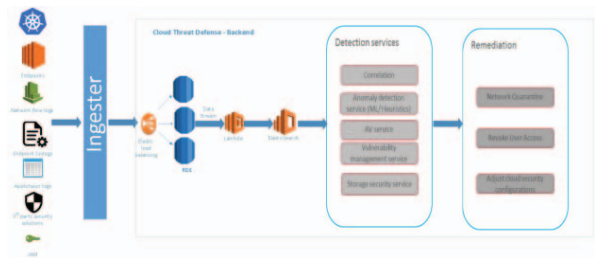


Figure 4. Cloud Threat Defense – Architecture

The solution collects the logs from the various sources like user access logs (CloudTrail logs), NetFlow logs, endpoint auth and syslogs, application logs, container logs and security vendor logs/events which is ingested with some more context added like geo, network segments, image ids, cloud tags etc. to the hosted solution backend.

The logs available at the backend are continuously analyzed by the detection services to find the anomalous activities and take necessary remediation actions.

D. Cloud Threat Defense – Security Model



Figure 5. Cloud Threat Defense – Security Model

1) **Discover Assets**

Cloud Threat Defense discovers cloud workloads, access logs, network logs, syslog and the logs from antimalware endpoint security solutions. It utilizes cloud-native services including but not limited to like CloudWatch, CloudTrail, VPC, AWS Lambda, Kinesis, S3, Redshift, and Machine learning to create a data lake upon which Analytics and Machine learning can be plugged in to identify trends and threats on Endpoint and cloud services.

2) **Assess Security Posture**

Cloud Threat Defense assesses the Cloud workloads that are spawned in terms of the firewall controls on the network segment it is in, known vulnerabilities based on the OS/kernel versions and on the status of third-party anti-malware solutions deployed.

3) **Identify Security Threats**

Cloud Threat Defense applies data analytics and machine learning on the data gathered from the above steps in the security model to identify potential security gaps and provide a risk score for the threats identified. It also proposes the appropriate remediation actions to mitigate and avoid similar security issues in the future.

4) **Remediate Security Issues**

Cloud Threat Defense provides corrective actions to remediate the issues identified and provides the mechanism to auto-remediate the issues by mechanisms like the isolation of

compromised resources, update the endpoint security solutions, auto-correct any insecure changes of firewall settings.

E. Cloud Threat Defense – Sample rules for Detection Services

Detection Methodology	Rules
Heuristics	Failed login attempts beyond a preset threshold
	Multiple RDP/SSH attempts from a high-risk Geo
	High Volume of Outbound connections/data flow from an established baseline
	Unusual login at a time not known as an established usage pattern for a user
	RDP/SSH attempt from a Geolocation not known as an established usage pattern for a user
Immutable policy	Attempts to make changes to sensitive system/boot configuration files
	Attempts to make changes to Windows firewall/Linux Iptables
	Attempts to install new applications, which are not whitelisted
Vulnerability	Continuous tracking of the latest NIST, CVE reports mapping vulnerable applications and libraries
Configuration checks	Changes to Cloud vendor firewall rules
	Changes to cloud configurations which fall outside of the known compliance policy
	Creation of new assets which have insecure access policies
Zero Trust	If a vulnerabilities/suspicious activity are detected by AV in a machine, then distrust all servers spawned from the same machine template
	If network anomalies found in a machine, distrust all servers under the same network firewall policy

Table 1. Cloud Threat Defense – Detection Services Rules

F. Cloud Threat Defense - Usecases

a) **Address Poor Identity and Access Management**

Based on the cloud access logs, one can classify, and aggregate incidents based on services accessed, users, location and number of attempts to access cloud services and resources to identify anomalous behaviors like:

- *Superhuman activity*: A user has logged into the cloud console or accessed resources from two different geo-locations

- *Usage Spike*: A user's resource consumption is out of the ordinary based on the user's previous behavior.
- *Data Breaches*: Log analysis should show access setting of any new or old resources to ensure that any sensitive data sources are not made public either by accident or malicious intent.

b) Address Workload Threats

Based on the Syslog/Windows Events Logs and the logs collected from the third-party security solutions, one can hone on:

- Malicious privilege escalation attempts.
- Malicious malware file creation and propagation paths.
- Failed attempts to take terminal access of sensitive resources.
- Attempts to change key configuration files

c) Address Network Threats

Based on the cloud network logs, one can identify:

- Lateral movement of malware
- Malicious attempts at port scans and brute force attacks
- Insecure firewall configuration and DOS/DDOS attempts of cloud resources.

G. Cloud Threat Defense – Value

- Remove the burden and complexity of installing, maintaining a typical centralized logs collection solution.
- Reduce alert fatigue on the number of logs created on the endpoint, Security vendors and cloud services by intelligently honing upon appropriate logs for threat hunting.

- Visualize the threats and logs collected across cloud services to easily identify vulnerable cloud services and cloud servers in a dynamic auto-scaled environment.
- Competitive services from cloud vendors like AWS GuardDuty only provide issues that can only be identified via cloud service logs but misses out on providing a holistic threat identification and deep analysis on the endpoint logs and security vendor logs.

V. ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper.

VI. REFERENCES

- [1] <https://www.gartner.com/en/newsroom/press-releases/2017-02-22-gartner-says-worldwide-public-cloud-services-market-to-grow-18-percent-in-2017>
- [2] <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html>
- [3] <https://www.linkedin.com/pulse/how-cloud-computing-application-architecture-different-muhammad-ahmed>
- [4] <https://cloudsecurityalliance.org/media/press-releases/csa-releases-top-threats-to-cloud-computing-deep-dive/>
- [5] <https://www.incapsula.com/blog/top-10-cloud-security-concerns.html>
- [6] <https://www.gartner.com/doc/reprints?id=1-4TZ49CB&ct=180326&st=sb>