masterSAM

Protecting Cloud Resources

White Paper

DISCLAIMER

Silverlake MasterSAM Pte Ltd. ("MasterSAM") does not make any representation or warranty, express or implied, as to the accuracy, timeliness or completeness of this document or the information contained herein and none of such parties shall have any direct or consequential liability for the information contained in, or any omissions from, this document.

The information contained herein is subject to change without notice. MasterSAM reserve the right to amend or replace the information at any time, and undertake no obligation to update or correct the information set forth herein or to provide the recipient with access to any additional information. This information may not be modified, redistributed or reproduced by the recipient whether such information is in electronic or hard copy form.

The information contained herein is preliminary and does not purport to contain all the information that interested parties may desire. Neither the receipt of this information by any person, nor any information contained herein constitutes, or shall be used or relied upon as constituting, the giving of advice by MasterSAM to any such person.

By downloading / receiving this document, the recipient acknowledges and agrees that the recipient will not modify, distribute or reproduce the document in whole or in part and will use this document solely for the purpose of evaluating the recipient's interest in the Products.

1. ABSTRACT

Interest in cloud adoption is very active today and increasingly, businesses from certain industry verticals opt for cloud for data management, storage and analysis. While a cautious approach to cloud adoption can improve an organisation's security, it can also potentially bring about some risks which organisations should comprehend and respond to. The response to these risks is recommended to be an on-going process, from the time of provisioning till the operations and resources go on cloud.

As organisations inch towards onboarding more services to the cloud, the problem translates more to managing the accesses to the data and specific data sets. Consciously evaluating the security implications while shifting resources to the cloud help in ensuring risks of sensitive data exposures are minimised. Security and risk management leaders must understand and leverage the increasing overlap of cloud, identity and data security, as well as best practices regarding cloud security[1].

Additionally, organisations need to consider the risks to cloud resources, just as they would in an on-premises environment. This involves continual monitoring of the cloud resources and understanding that it is a shared responsibility between the organisation, cloud service provider, etc. Cloud providers handle the security *of the cloud*, while tenants are responsible for security *in the cloud.*

2. THE CHALLENGES – CLOUD THREAT ACTORS

MALICIOUS CLOUD SERVICE PROVIDER (CSP) ADMINISTRATORS

A CSP administrator, with a malicious intent, could leverage on his privileged credentials or position to access, modify or delete important information stored on the cloud platform. Or, he may use his elevated privileges to modify the cloud platform to gain entry into other connected networks, thus compromising the security posture of the setup.

MALICIOUS CUSTOMER CLOUD ADMINISTRATORS

Just like a CSP administrator, a malicious customer cloud administrator could also potentially jeopardise the security posture by misusing his privileged credentials to tamper with the sensitive data stored on cloud.

CYBER CRIMINALS OR STATE ACTORS

A cyber-criminal could intentionally leverage on a shortcoming in the cloud architecture or configuration to obtain sensitive data or consume the cloud resources at the victim's expense. Or, in the likes of Password spray attacks, a cybercriminal could exploit weak cloud-based authentication mechanisms to obtain user credentials[2]. Once such a threat actor gains access to compromised credentials, he gains full access to cloud resources, proving to be detrimental to the organisation. - Some common mistakes we fall prey to is if we do not configure security groups and Network Access

[1] "You've Got Cloud Security All Wrong — Why Identity and Data Security Are Paramount in a Cloud World", David Mahdi, Steve Riley, 20 October 2020

[2] CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121
https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

Control Lists (NACLs) properly, allowing global access from anywhere. One should also refrain from leaving a bucket policy public, allowing data to be copied out by anyone. Else, we just make it very easy for a cyber criminal to play his act.

Other than the earlier-mentioned threats, it is also possible that a credential compromise occurs unintentionally. By 2022, at least 95% of cloud security failures will be the customer's fault, Gartner estimates, citing misconfigurations and mismanagement.[3]

3. CLOUD RESOURCES TO PROTECT

Having thus far discussed the kind of challenges and threat actors, it is integral to understand what are we really trying to protect here – what kind of cloud resources are we looking at.

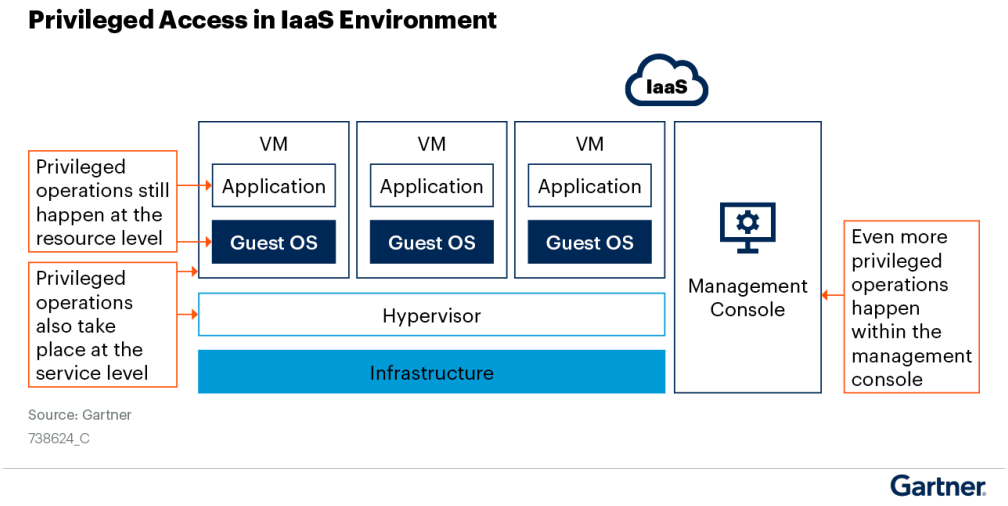
In a traditional **on-premise** environment, we would encounter the need to protect the below-mentioned:

- Users
- Applications
- Operating Systems
- Point of Accesses

In an **on-cloud** environment, we would encounter a few other cloud resources (*in addition to the above*) such as:

- Cloud Administrative Accesses
- Auto-scaled instances
- Containers

Managing privileged access from, for and in the cloud presents several unique challenges (see Figure 1-below). Privileged operations occur at multiple levels – resource level, service level and even more at the management console level – thus making it all the more integral for organisations to ensure the right action towards mitigating security, privacy and data residency risks.



[3] Source: https://www.csoonline.com/article/3208905/top-cloud-security-controls-you-should-be-using.html

4. HOW WE HELP

MasterSAM solutions protect any Privilege Access in the environments, including but not restricted to Operating Systems, Databases, Applications, Firewalls, VPNs, Cloud Hosting Provider and more. It does this by adhering to the **4A principle: Authorization, Authentication, Access, and Audit.**

Authorization

Users are granted the least privilege to access any environments. Access can be granted on a long term or short-term basis based on comprehensive workflow features. The workflows that are available includes:

1. One Level Approver
2. Two Level Approver (Serial or Parallel)
3. Three Level Approver (Serial or Parallel)
4. Emergency Workflow

When the access is not needed anymore, they will be automatically revoked without any human intervention. This will ensure that not only the least privilege is granted all the time for users to any environments, it also automates the revoking process so that there will not be any dormant access that are left over because of forgotten manual process.

Comprehensive matrix of what the users can request for can be configured easily. Users can be configured to only able to request for certain resources, and to have different resources to use different workflows. This allows some non-critical resources to be able to be granted long term access, while access to other critical resources need to be approved by three approvers.

Authentication

Users are authenticated before they can gain access to any environments. Authentication can either be done locally or via Active Directory.
For Active Directory authentication, all the security policies applied in the Active Directory will be enforced.
For local authenticated users, there are a lot of security policies that can be configured to further ensure user authentication will not be easily compromised:

1. Password Complexity, number of digits, upper case, lower case characters, and special characters can be enforced.
2. Enforce users to reset password after the next login to ensure the administrator do not have access to the credentials.
3. Dormant accounts will be automatically deactivated after 30 days.
4. Maximum and minimum password age.
5. Password History

Access

Users are able to access the environments seamlessly without much changes to operations. The autologin to the target resources will utilize the existing privilege account in the target resources to ensure maximum compatibility and also seamless integration with any target resources.
Autologin works out of the box for the following protocols:

1. RDP
2. SSH
3. Telnet
4. VNC
5. Client and Web Applications.

There are more than 100 readily available autologin connectors covering databases, firewalls, network devices etc. They can be applied directly into the solution to allow autologin to the target resources in a plug and play manner.

Audit

All the activities performed by the user accessing the environments are recorded in human consumable screenshots. This is very different than the event-based format that is prevalent in syslog, event logs, and SIEM activities, where most of the time, the context of the activity is lost.
With the audit trail available in MasterSAM Analyst, the whole activity of the user can be played back, even the activities that does not make any changes to the system, but can give hint on what the user is trying to do. This gives additional advantage in forensics compared to event-based audit trail where only actions that leads to changes are usually recorded.

MANAGING CLOUD ADMINISTRATIVE ACCESSES

As seen in Figure 1, a significant number of privileged account activities happen within the management console.

Controlling Privileged Access to IaaS/PaaS/SaaS involves ensuring interactive access to cloud-based control panels. Several Privilege Access Management (PAM) tools support this use case by establishing an authorized administrator's session to an IaaS, PaaS or SaaS control panel. They also support various authentication mechanisms. Using these methods, PAM tools can control the level of access granted to the privileged user (through the use of security roles or groups). Some tools also support ephemeral just-in-time access, where a security token is created on the fly.[4]

Typically, cloud administrators perform their day-to-day tasks via two avenues:

1. Web Management Console (e.g., AWS Management Console, Azure Management Portal)
2. Command Line Interface / CLI (e.g., AWS CLI and Azure CLI)

The web management console is a web-based application that provides a user interface to manage cloud services. The management console is password authenticated.

[4] IAM Leaders' Guide to Privileged Access Management, Abhyuday Data, Felix Gaehtgens, Michael Kelley,February 2021

The command line interface is unified tool that enables cloud administrators to interact with cloud services using commands in a command-line shell. Depending on the public cloud provider, the authentication is based on a secret access key, username and password, or X509 certificate.

MasterSAM Star Gate's autologin feature is useful to secure access to the web management console and command line interface. The web console or command line interface is launched with MasterSAM AppSphere, and the credentials injected from our secure password vault, removing any password exposure to the end user.

MANAGING AUTO-SCALED INSTANCES

One of the advantages of hosting target resources on the cloud is the dynamic nature of deployment and provisioning. Servers and instances are able to be provisioned when need arises, and deprovisioned when the need passes. Even though these instances are short lived, they still constitute as a target resource in the environment and need to be protected by Privilege Access Management.

MasterSAM Star Gate is able to automatically protect any auto scaled instances to ensure full compliance with security best practices.

MANAGING CONTAINERS

Containers technology such as docker and kubernetes are becoming the de-facto standard for applications that are developed and hosted on the cloud. These containers are deployed in containers host instead of operating systems. The applications that is within these containers usually need some credentials to access external resources. MasterSAM's Application to Application Password Management (AAPM) feature enables the credentials within these containers to not be exposed as plain text, and managed in the same centralized place with all the other credentials.

5.CONCLUSION

Ungoverned cloud adoption or poor foundational practices put organizations at risk of security breaches, data loss, compliance issues and budget overruns. It is thus, important, to review the best PAM practices and capabilities and opt for a governance and monitoring based model to safeguard your cloud resources. MasterSAM provides security at every layer – Users, Applications, Operating Systems, Containers, Auto-scaled instances and at Cloud Administrative access level.

For more information, you may write to info@mastersam.com

---------- **END OF DOCUMENT** ----------

About Silverlake

Silverlake is a leading Technology Innovations, Banking, Financial and Cyber Security solutions provider in the ASIA Pacific region. Silverlake's business transformation itself is fueled by its relentless desire to delight its customers. Executing parallel efforts in pursuing technology innovations as well as keeping its more than three-decade legacy of deploying core banking at 100% success rate is paramount to the company's strategy. It's subsidiary business, Silverlake MasterSAM, is one of the global market players in Privilege Access Management and cyber security domain. Recognized as Top 25 APAC Compliance solutions providers, Silverlake MasterSAM, headquartered in Singapore, has offices in the Malaysia, Thailand, Philippines, Vietnam and IndiaFor more information, please visit www.mastersam.com.