Check Point
SOFTWARE TECHNOLOGIES

THE ULTIMATE GUIDE:

6 STEPS FOR IMPROVING YOUR AWS SECURITY POSTURE

Amazon Web Services (AWS) has remained an undisputed leader in the cloud market space for a few years now – just in 2019, revenues gained from AWS stood at a whopping $35 billion. With more than a million users and almost 26% of software developers working on the platform, AWS boasts unparalleled penetration in the technology landscape.
However, increased usage has also led to a high number of touchpoints that can compromise security. Once every few months, a security breach resulting in huge losses is reported – bad news for businesses that rely on AWS more than ever before. With AWS offering many ways for businesses to protect themselves, why do violations continue to happen?

One of the biggest reason is because companies are unprepared to handle the latest generation of cyber-attacks, continuing to employ archaic security solutions in the face of sophisticated attacks. Such solutions tend to use manual and reactive remediation methods, which are difficult to scale across multiple clouds and AWS accounts. They also use a plug-the-hole approach, failing to look at problems in a holistic manner at the enterprise level.

Frustratingly, many security incidents happen due to misconfiguration of essential controls that can close the gates to these attacks. These controls can be established through continuous monitoring, visibility, and increased control of cloud security posture. The good news is that it's not hard to fix – and we've got you covered. In this e-book, we've put together the top six AWS security misconfigurations frequently encountered by users. Follow along to learn why these issues occur, their impact, and how to remediate them using our best-in-class solutions.

1

LOGGING NOT ENABLED ON CLOUDTRAIL S3 BUCKET

AWS CloudTrail is a service that monitors and detects unusual activities in AWS accounts. Often, companies with hundreds of AWS accounts depend on CloudTrail for investigation, compliance and auditing of cloud infrastructure.

CloudTrail's logs, contains sensitive information and is typically stored in an S3 bucket. Although the intention of CloudTrail records is to help administrators fix loose ends using this information, in the wrong hands these records can turn into dangerous tools for intruders.

To prevent and track unauthorized access to these records, administrators should set up logs on the S3 bucket access, allowing for audits and investigations in the event of a breach. Since logging for S3 buckets is disabled by default in AWS, this step is crucial configuration and is part of AWS customer's responsibility. While only a simple configurational change is required to enable logging, most cloud security teams forget to modify the default setting, providing no concrete method to determine unwanted access when it occurs.

HOW CHECK POINT HELPS

Enabling access logging on S3 buckets requires you to visit the AWS S3 console and click the 'enabled' checkbox for the target S3 bucket. This is a straightforward fix but when added to the many other issues and configurations that need to be tracked – especially across multiple accounts – this can slip through the cracks.

CloudGuard Dome9, Check Point's comprehensive platform to monitor cloud security, helps detect such misconfigurations automatically. The CloudGuard Dome9 service has more than 2000 built-in regulatory and compliance rules that are monitored across multiple frameworks such as CIS, HIPAA, and NIST.

In this case, CloudGuard Dome9 is offers posture check to identify disabled logging on S3 buckets. When it detects this misconfiguration, it will alert the cloud security operation team and continue to report this failing on every subsequent assessment, until fixed.

But CloudGuard Dome9 is not just a cloud posture and compliance monitoring solution. It also allows cloud administrators to auto-remediate misconfigurations, depending on the specific scenario and risk level, using CloudBots. For this issue, in particular, your security team can remediate in place through the cloudbot s3_enable_logging tool, or investigate before manually addressing the issue.

2

UNAUTHORIZED TRAFFIC FLOW TO AND FROM VIRTUAL PRIVATE CLOUDS

In 2019, the global virtual private cloud (VPC) market was valued at nearly $21 billion, and this is expected to grow rapidly at a compound annual growth rate of 23%. VPCs are powerful because they have the advantages of a private cloud (agility, scalability, private logical space, etc.) while still able to access the resources of the public cloud to which it belongs.

While VPCs offer many benefits, they sometimes can be exploited by nefarious parties to gain access to secure resources. Why? It's because VPC security is managed through permissions granted to security groups, and the default security group associated with an AWS VPC is not very restrictive. Although the default security group does not allow any inbound/ingress traffic to the VPC, it permits all outbound/egress traffic as well as inbound and outbound traffic between instances assigned to the security group.

This loophole creates a backdoor entry for some services in the VPC to gain unauthorized access to resources that they should otherwise not have permissions for.

HOW CHECK POINT HELPS

The ideal solution is to start from a point where no inbound or outbound traffic is allowed by the default security group. From that foundation of total security, the admin should then create multiple security groups, each allowing a certain level of permissions. Based on the AWS resources that the VPC needs access to, the corresponding security group can then be associated with the VPC.

Check Point helps with this process in multiple ways.

First, the CloudGuard Dome9 platform offers posture check to determine default security groups associated with VPCs that allow any traffic. In such cases, administrators can choose to remediate manually, or through the cloudbot sg_rules_delete. This bot cleans up all ingress and egress rules from the default security group.

In addition, turning on the 'tamper protection' feature of CloudGuard Dome9 aids in setting up guardrails around your network policies – specifically, to determine if there is any change to the last known and approved state. For instance, if the security groups are modified, the system will automatically revert these changes to the earlier preferred state.

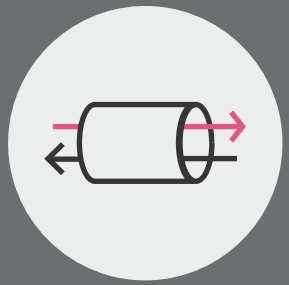
Finally, the CloudGuard Dome9 Clarity tool provides powerful cloud-security visualization that help with Cloud Security Posture Management (CSPM). Clarity offers a real-time topology map of security groups, interrelationships between security policies, and a visualization of traffic flow between security groups. These visuals make it easy to diagnose over-exposed cloud assets and operational issues caused by misconfigured policies.

3

UNRESTRICTED ACCESS TO SSH PORT 22

Port 22 has been reserved for SSH admin logins since 1995. The critical nature of port 22 means that no unauthorized service, resource, or IP address should be able to connect to this port because of the apparent risks involved in owning superior administrative privileges.

However, AWS default security groups allow traffic between instances within a security group, adding complexity and risk to this scenario. This means that a server configured to use the default security group can unintentionally gain backdoor entry to port 22.



HOW CHECK POINT HELPS

Similar to the various solutions described above that can be employed for VPC protection, Check Point's multiple product features help address the port 22 access issue, as well.

For starters, the CloudGuard Dome9 platform can determine if default security groups are not restrictive enough on inbound or outbound traffic and alert administrators through assessment reports. Additionally, CloudGuard Dome9 runs specific safety checks for port 22.

When an alert is received, cloud security administrators can then manually intervene or remediate using the cloudbot sg_rules_delete, removing all ingress and egress rules on the default security group. Cloudbot sg_single_rule_delete can achieve the same, one rule at a time.

CloudGuard Dome9's tamper protection is an additional module that helps you to maintain your security groups from within CloudGuard Dome9 and achieve full segregation of duties between your operational and security teams. Once enabled, any change that I done in AWS consule will be reverted, allowing security teams to establish guardrails around network security of your AWS environment.

It's also recommended to create a separate security group with the sole intention of accessing port 22. This way, if any other security group other than this one obtains permissions for port 22, tamper protection's active protection, feature can prevent this from happening.

Seeing and understanding the dangers in your network security can be challenging, but CloudGuard Dome9 Clarity is a powerful tool that renders intelligent visibility and situational awareness of network security in a cloud environment. It helps visualize the complete topology of all security groups, indicating any unintended traffic flow to open ports (not just port 22). The graphical representations make it easier to catch vulnerabilities that might otherwise go unnoticed.

4

CONFIGURATION OF IAM POLICIES AT A USER LEVEL

Unlike the three AWS security risks that we've discussed so far, this issue is not a problem created by default AWS configurations. Rather, this is the result of a complacent approach adopted by many organizations that have not fully considered the risk implications.

The general recommendation is to grant access to AWS resources through IAM policies assigned to particular IAM groups or roles. This means that belonging to a group or role automatically determines whether you have the permissions to perform certain operations or not.

However, many businesses make the mistake of administering IAM policies at a user level. As the number of users grows, this becomes a laborious and unsustainable method. Over time, it becomes difficult to monitor which users have access. How big is this problem? According to a survey by OneLogin, 20% of breaches in companies happen due to failures in de-provisioning ex-employees, with over 50% of user accounts found to be active even after the employees left the company.

HOW CHECK POINT HELPS

CloudGuard Dome9's Privileged Identity Protection is designed to function as an extra layer of defense over IAM services. It provides a complete view of all IAM users and roles, allowing administrators to manage permissions at a granular level. That means that if a certain policy which is expected to be attached to a group or role is found paired with a user instead, Privileged Identity Protection makes it easier to spot and fix the issue.

The feature also aims to minimize the impact of security issues by performing access management based on the Principle of Least Privilege. This effectively means that all users are granted basic, minimal privileges by default. Then, all sensitive operations and services are added into a restrictive policy list using IAM Safety, an application part of Privileged Identity Protection.

For example, if you identify 'Delete S3 bucket' as a sensitive operation, you can add it to the restrictive list. Then, if a user wants to perform this operation, they need to elevate their permissions just-in-time on IAM Safety for a short period of time (say, 15 minutes). Once the action is complete, they demote themselves back to the original permission state.

Other than streamlining access to sensitive operations and services, this approach by IAM Safety has the advantage of auditing all user activities.

5

MULTI-FACTOR AUTHENTICATION (MFA) NOT ENABLED FOR AWS ACCOUNTS

According to Microsoft, adding multi-factor authentication for user accounts makes it 99.99% less likely for them to be compromised. And Google agrees as well. Strong, long passwords are no longer sufficient to ensure safety because in many attacks such as phishing, keystroke logging, etc. the attacker is already in possession of the exact password.

Adding MFA, in the form of a time-sensitive token, creates an added layer of protection to minimize invasion into AWS accounts. Examples of MFA forms include virtual MFA devices, Universal 2nd Factor (U2F) security keys, hardware fobs, etc.

Whenever a user attempts to log into the AWS account, they will have to key in the username and password, along with an authentication code from their MFA device (for example, a smartphone app). The random token is generated just at the moment of login and is valid for a short period of time only, which makes it more difficult to hack into a user account.

HOW CHECK POINT HELPS

Often, multi-factor authentication is not enabled for all users, putting some users at risk. It's fairly easy to identify the list of users who do not have MFA configured; on the IAM console, when you select a user, you can view whether the checkbox against 'MFA Device' is selected or not. But remembering to perform these audits routinely can be challenging.

CloudGuard Dome9 delivers MFA related checks for you in a consistent and automated fashion, frequently iterating through the user list and flagging anyone who does not have it configured.

As an additional benefit, CloudGuard Dome9 has its own inbuilt MFA-likemechanism, that it offers as part of Privileged Identity Protection. The method of using the IAM Safety application to elevate permissions for limited time to perform certain restrictive operations (as discussed in the earlier section) is a form of multi-factor authentication in itself.

Using this premise, logging into an AWS account could be categorized as a restrictive action. This ensures that even when attackers have the knowledge of a user account's password, they cannot log in without the second factor – access to IAM Safety and the privilege to temporarily promote themselves – required for authentication.

6

LAMBDA FUNCTIONS HAVE ADMINISTRATIVE PRIVILEGES

AWS Lambda has quickly gained popularity in the cloud-security industry due to its versatility and flexibility. This serverless service, which is only charged for the specific compute time, allows developers to abstract away their business logic from the underlying infrastructure. Rather than provisioning servers, developers can directly use Lambda to invoke a piece of code.

Due to its excellent performance, cost efficiency, scalability, and ease of integration with other AWS services, Lambda has found many takers. However, if Lambda functions are assigned administrative privileges, they could inadvertently end up gaining permissions to confidential AWS resources. This also creates a weak backdoor channel for infiltrators to penetrate.

With a surge in the use of AWS Lambda service by many customers, it's important to address this issue.

HOW CHECK POINT HELPS

The rule of thumb for Lambda (or any other) service is that it must only be given access to the resources that it needs – not less and not more. CloudGuard Dome9 for Serverless protects your Lambda Functions by validating what permissions are being used by Serverless Lambda functions and generating the exact IAM profile that follows the Principle of Least Privilege. Once allied, this IAM profile will ensure that the Lambda service has the absolutely minimal privileges that it needs.

This can be designed easily using CloudGuard Dome9 for Serverless module , allowing admins to control access of their serverless functions.

Beyond Lambda, this principle can be extended for all critical actions and resources by adding them into a restricted list and making them available only when a service or user promotes their access level in the IAM Safety application.

In 2019, a record-breaking 7.9 billion records were exposed in data breaches, representing a 33% increase over 2018. In this new environment, companies of all sizes can no longer afford to ignore the problem. Resolving frequently occurring issues and misconfigurations in your existing cloud environment will provide you an excellent head start. But that is not enough – choosing a robust security platform that minimizes manual errors is essential for staying protected.

In a daunting cloud-security environment, Check Point's Dome9 platform is the answer, mechanizing manual processes to reduce errors and save time, and visualizing data in a way that makes problems instantly visible. Our features include:

- Agentless, cloud-native security architecture which guarantees the implementation and enforcement of pre-configured regulatory and compliance policies
- End-to-end posture management and compliance lifecycle with continuous monitoring and remediation-in-place packaged together
- Sophisticated protection against intrusions and identity theft using IAM Safety, Tamper Protection and Serverless Security features
- Powerful visualization of cloud assets, including network traffic and security group relationships, which helps detect vulnerabilities in real-time
- Easy and quick integration with existing AWS accounts with the ability to secure your cloud environment in under five minutes

To learn more about how Check Point can immediately improve your security posture, visit https://www.checkpoint.com/products/cloud-security-orchestration/.