CLOUDWIZE Glassbox

SECURING YOUR CLOUD ENVIRONMENT WITHIN MINUTES

KEY TAKEAWAYS:

THE CHALLENGE

Avoid Application-Targeted attacks by using WAF and ensuring there's no internet-facing ALB that's unsecured by WAF, at all times

THE SOLUTION

A customized set of rules to detect and alert on related policy violations, providing a simple query mechanism for any internet-facing ALB that's not secured by a WAF

THE RESULT

Faster process, within minutes the cloud environment was secured with no need for building or maintaining any scripts

INTRODUCTION

Glassbox is an enterprise analytics platform that automatically records, analyzes, and indexes every digital customer interaction.

Glassbox gives its partners a deeper customer understanding by helping them identify the reasons behind users' interaction (or lack thereof) with the partner 's platform in the way that the partner intended.

With a comprehensive suite of services, Glassbox can add transparency and clarity to every aspect of their partner 's online presence – from troubleshooting and testing to revealing why the new product isn't gaining the traction it deserves.

THE CHALLENGE

Looking to maintain and ensure high service availability, the Glassbox Cloud Operations team needed to reduce to a minimum the risk of being a target to Application-Targeted Attacks such as SQLI, XSS, DDoS, used by hackers to overload the system. The attackers do this by sending an endless, rapid stream of legitimate requests that lead to system unresponsiveness and failure.

A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between web applications and the Internet. It typically protects web applications from attacks such as cross- site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection.

In order to effectively manage their WAF, Glassbox had to conduct periodic reviews of their environment by following these steps:

1. Going through **every** ALB:
    a. Check its scheme to see whether it is internet-facing
    b. Check its security group rules
    c. Check its VPC ACL rules
    d. Check that it has the production environment tag
2. Going through **every** WAF:
    a. Check if all of the ALBs from the first step is attached to at least one of the WAFs

This was a long, time-consuming process that left the system unprotected for periods at a time. Since this process is manual, the risk of human error is relatively high.

Glassbox was looking for a consistent, effective and efficient way to keep their cloud environment secured, plus find a way to ensure all the internet facing ALBs and web-servers are covered by WAF.

THE SOLUTION

CloudWize's holistic platform allows cloud teams to regain visibility and control over their ever-changing cloud environment, helping them troubleshoot faster, prevent incidents from reoccurring, detect divergence from best practices, optimize cloud-related costs and ensure that all security and compliance policies are met.

We provided Glassbox with the ability to create a smart, customized set of rules, based on their specifications to effectively manage their WAF.

THE FIRST RULE:

The first rule involved three services:

- **ELBv2**

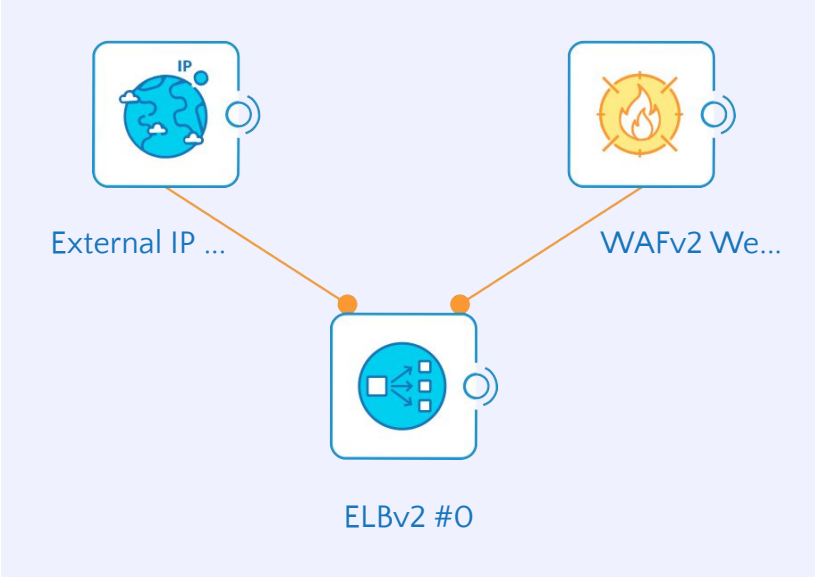
  Schema is"internet-facing"
  Type is "Application"
  Name contains the word "customer "

- **WAFv2**

  Attached to the ELBv2

- **External IP**

  IP Range is set to 0.0.0.0/0 and has network access to the ELBv2 in any protocol and port.



THE SECOND RULE:

Glassbox wanted everyone connecting with them via internet-facing ELBs with sensitive resources in their targeted groups, to authenticate themselves using OKTA. Therefore, a rule was set to assure the configuration of the system is properly architectured for this purpose.

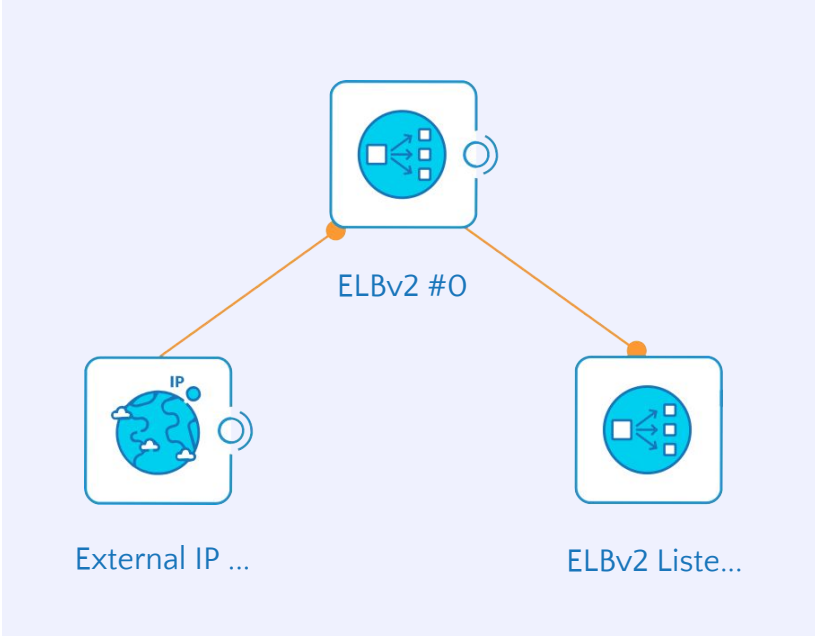
The rule consisted of the following: :

ELBv2:

- Has listener

  Issuer != .*okta.* OR Null

- Has access from 0.0.0.0/0 (The Internet)



This set of rules allowed them to not only identify symptoms and perform diagnostics of policy violations but also to monitor actual changes in their complex cloud architecture and zoom-in on the real root-cause behind symptoms, alerting on any changes related to security and compliance.

After setting up the rules, Glassbox conducted an initial architecture scan to detect breaches and see what needs to be fixed.

With the ever-changing nature of the cloud environment, a one-time scan isn't enough and the team must constantly monitor changes that can affect security and compliance status. Working with CloudWize, Glassbox started getting real-time alerts on deviations from their customized set of rules and policies.

THE RESULT

Within minutes of integrating CloudWize's platform, Glassbox created a full set of customized rules, ran the tests, and fixed detected breaches.

A task that took a whole day to complete with Cloudwize takes 5 minutes, and now there is only ongoing maintenance that is automated.

The time saved is translated to cost reduction and allows the team to focus on strategy.

"A task that once took me a whole day to complete was done in 5 minutes, and the ongoing maintenance is now automated, alerting me when my attention is needed!!

Moneer Monayer, Information Security Expert, Glassbox