HOW CENTRIFY ENFORCES CONTINUOUS COMPLIANCE AND SECURITY BEST PRACTICES ON AWS

Centrify

Customer Profile

Centrify is a leading cybersecurity company that serves more than 5,000 organizations around the world.

Challenge

- Filtering capabilities and real-time updates when moving SaaS applications to AWS
- Continuous compliance automation and validation of various frameworks
- Identify misconfigurations and remediation through network visibility

Solution

- Check Point CloudGuard Posture Management
- Check Point CloudGuard Posture Management Compliance and Governance
- Check Point CloudGuard Posture Management Clarity

Resaults

- Improved management and situational awareness of cloud assets through a single pane of glass
- Automated continuous compliance, helped detect policy violations and perform auto-remediation
- Seamless integration into Centrify's account providing real-time visibility of cloud assets and configurations

> "I totally would recommend CloudGuard Posture Management. The main reasoning would be to savetime and headaches if you're trying to properly secure your environment and get a handle on your external [SaaS] footprint."
>
> - Felix Deschamps, Principal DevOps Architect at Centrify

Overview

Centrify

Centrify is a leading cybersecurity company that serves more than 5,000 organizations around the world. Its security platform is credited with converging Identity as a Service (IDaaS), Privileged Access Management (PAM), and Enterprise Mobility Management (EMM) into a single solution.

As organizations move to Amazon Web Services (AWS), they need to control access to their resources, such as Amazon Elastic Compute Cloud (Amazon EC2) instances, and validate users are who they say they are. Centrify validates access to resources, that the devices being used are trusted endpoints, and helps to establish role-based access.

Premise

Recently, Centrify made the decision to move all software-as-a-service (SaaS) applications to AWS. Centrify went through a Well-Architected Security Review with AWS in order to become an AWS Partner Network (APN) Advanced Technology Partner. Members of the Centrify team met with Solutions Architects at AWS to discuss options for optimizing their SaaS environment. They discussed their needs and developed a shortlist of five leading AWS security automation solutions for Centrify to explore.

Upon further technical review, the DevOps team found that most of the solutions available on the market provided metrics, but did not give the team a way to efficiently monitor or control their security and compliance. In summary, they were looking for three main use cases for infrastructure security.

Check Point
SOFTWARE TECHNOLOGIES LTD

January, 2020

Business Challenge

Challenge 01 Cloud Inventory Management

New application deployments resulted in the creation of security groups (SGs), IAM roles and policies as part of the built-in infrastructure automation. There were also various Amazon Simple Storage Service (Amazon S3) buckets created to host tenant data, configuration, logging information etc. Due to the dynamic nature of SaaS environments, when things changed, the Centrify IT team had to spend countless cycles to stay up to date with their environment and assets.

Challenge 02 Cloud Compliance

Establishing compliance on the cloud was a top priority. Given the rapidly scalable nature of their AWS environment, Centrify needed to be able to check whether they were compliant with various frameworks at all times. Misconfigurations or policy changes could immediately make them non-compliant. Also, when policy violations did occur, Centrify needed automation capabilities built into their existing workflow process.

Challenge 03 Network visibility

Centrify needed a solution that could deliver a more fine-grained view of the security infrastructure and help identify misconfigurations. This instant visibility was critical to minimizing security holes that could open up the attack surface. Centrify also had assets and policies across multiple accounts and regions, and needed a purpose-built tool to synthesize and visualize this information from a single pane of glass

SOLUTION

The Solution 01

CloudGuard Posture Management helped them improve inventory management and situational awareness, providing a single pane of glass to manage coverage for all of Centrify's dynamic cloud assets. The ability to filter and get immediate information for any instance or object in their environment was key. CloudGuard Posture Management now monitors Centrify's entire infrastructure (Quality Assurance, Development, and Production environments).

The Solution 02

The Compliance Engine from CloudGuard Posture Management continuously monitored entrify's cloud infrastructure and helped detect policy violations. Also, when a policy violation occurred, CloudGuard Posture Management would immediately push a notification via email/ SNS that could trigger an automatic response (such as create a Lambda Function or Amazon CloudWatch alarm for a quick response).

Implementation

Getting CloudGuard Posture Management integrated with the DevOps teams existing systems was "fairly quick," according to Felix Deschamps – the Principal DevOps Architect at Centrify. After only a few days, the team had all their SaaS applications on-boarded to the CloudGuard Posture Management platform. The representational state transfer (REST) application programming interface (API), single sign-on (SSO) nature of CloudGuard Posture Management simplified the process, making it easy for Centrify to establish the right level of permissions to their systems without exposing what was more than necessary.

Results

- Automated responses to events which simplify workflow and remediation.
- Configuration of account access without requiring explicit keys
- Flexibility in the level of permissions granted to CloudGuard Posture Management
- Centralized view of security and compliance posture
- Granular control over security groups and compliance policies
- Built-in security and compliance bundles that can be customized
- Faster time to value – up and running very quickly
- Seamless integration with existing SSO tools

CloudGuard Posture Management is an innovative SaaS platform that delivers visibility across your security and compliance posture. Users can continuously check their environments against business and regulatory requirements, with automated alerts on any changes. Further, CloudGuard Posture Management can automatically remediate misconfigurations to limit security exposures and maintain compliance.

For more information, visit: https://www.checkpoint.com/products/

Check Point
SOFTWARE TECHNOLOGIES LTD

January, 2020