CloudGuard Dome9 on AWS

Case Study | Centrify

HOW CENTRIFY ENFORCES CONTINUOUS COMPLIANCE AND SECURITY BEST PRACTICES ON AWS

Centrify ZERO TRUST SECURITY

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.

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.

THE SOLUTION

CloudGuard Dome9 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 Dome9 now monitors Centrify's entire infrastructure (Quality Assurance, Development, and Production environments).

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 noncompliant. Also, when policy violations did occur, Centrify needed automation capabilities built into their existing workflow process.

THE SOLUTION

The Compliance Engine from CloudGuard Dome9 continuously monitored Centrify's cloud infrastructure and helped detect policy violations. Also, when a policy violation occurred, CloudGuard Dome9 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).

CHALLENGE **03**
NETWORK VISIBILITY

Centrify needed a solution that could deliver a more finegrained 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.

THE SOLUTION

CloudGuard Dome9 provided comprehensive visibility of their security groups, policies, IAM roles and permissions. CloudGuard Dome9 integrated seamlessly into Centrify's account and was able to provide instant visibility within days with the appropriate level of permissions.

IMPLEMENTATION

Getting CloudGuard Dome9 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 Dome9 platform. The representational state transfer (REST) application programming interface (API), single sign-on (SSO) nature of CloudGuard Dome9 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.

"I totally would recommend CloudGuard Dome9. The main reasoning would be to save time 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

DESIGNED BENEFITS

- 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 Dome9
- 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 Dome9 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 Dome9 can automatically remediate misconfigurations to limit security exposures and maintain compliance.

ABOUT CHECK POINT SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

CONTACT US
Check Point Software Technologies Ltd.
959 Skyway Road, Suite 300
San Carlos, CA 94070
USA +1-800-429-4391
www.checkpoint.com

For a free security assessment or trial, please contact:
US Sales: +1-866-488-6691
International Sales: +44-203-608-7492

CDCCS12172018