Cryptzone™

CASE STUDY

Cryptzone Provides Security for New AWS Environment

QUICK FACTS

A Securities Regulatory Organization that performs heavy data analytics and data science on sensitive financial data.

Industry

- Financial services

Challenges

- Automate AWS deployment without breaking compliance
- Reduce compliance data collection and report preparation time
- Isolate production, QA and development

Solution

- Cryptzone's AppGate®

Benefits

- Purpose-built for the AWS environment
- A Software-Defined Perimeter that dynamically creates a secure, encrypted network segment of one tailored for each user session
- Granular control of per-instance access with a full audit trail for compliance
- Immediately detects new cloud server instances, and automatically adjusts user access
- Single SSH key for each virtual private cloud to simplify and enhance security

Background

This securities regulatory organization analyses massive volumes of financial data across multiple markets to detect potential fraud, overseeing up to 75 billion market transactions every day.

Its team of developers and analysts utilized its datacenter to near capacity during the work week from 8am-5pm. However, nights and weekends, the datacenter was completely underutilized. To more efficiently operate, the organization migrated to Amazon Web Services (AWS). It not only reduced costs, but also delivered technical benefits by offering a rich set of big data analysis tools available in AWS. This helped the DevOps team, responsible for building financial data analysis models, become faster and more productive.

The Challenge

Within this highly regulated industry, the organization needed a solution for secure access to network resources in AWS and the ability to easily demonstrate compliance with financial regulatory requirements.

More specifically, the organization had a challenge with its SSH key management. For every AWS instance created, a developer needed to create a new SSH key. The organization runs over 30,000 EC2 instances daily with 80% having a lifespan of five or fewer hours. It created a huge burden for the users.

Furthermore, to comply with regulations, the organization needed to show who had access to what instances, the data on the instance, and when. An IP-based network security solution only shows what IP had access to a resource. Using an IP solution meant they were unable to demonstrate fine-grained logs of who had access to what and when.

Requirements

The organization needed to ensure secure access and compliance to AWS resources. It required a solution that automated AWS instance deployment without breaking compliance, reduced compliance data collection and report preparation and isolated production QA and development.

Furthermore, the organization has applications that need to access servers and a DevOps team that needs access to these servers. Trying to maintain different SSH keys for each application in each virtual private cloud quickly becomes a scaling problem and makes it difficult for the DevOps to remember which file to use for which server.

Finding the Right Solution

Having successfully used Cryptzone's AppGate to secure access to its on-premises datacenter, the organization turned to Cryptzone to help with its migration to AWS. It knew that traditional network access control solutions or cloud-native tools were unable to meet its needs. Using AppGate for AWS was a natural extension.

AppGate is purpose-built for the AWS environment and draws on user context to dynamically create a secure, encrypted network segment of one that's tailored for each user session. It dramatically simplifies the cloud resource user access problem and eliminates IP-based over-entitled network access.

Benefits of Cryptzone's AppGate

AppGate enables organizations to adopt a Software-Defined Perimeter, a network security model that dynamically creates one-to-one network connections between users and the data they access.

Adopting a Software-Defined Perimeter ensures that all endpoints attempting to access a given resource (whether in the cloud or on-premises) are authenticated and authorized prior to accessing any resources on the network. All unauthorized network resources are made inaccessible. This not only applies the principle of least privilege to the network, it also reduces the attack surface area by hiding network resources from unauthorized or unauthenticated users.

Identity-centric, highly granular access control

Using AppGate, the organization gained an identity-centric, highly granular access control solution. Every user obtains a dynamically adjusted network perimeter that's individualized based on their specific requirements and entitlements. This ensures that the context of the user and the device is evaluated in real-time before AppGate provides network access to the user-authenticated instances and services in the AWS environment.

Adapt in real-time

With simple policies in place, network access automatically adapts in real-time to changing conditions on the client side as well as on the cloud infrastructure side. Every new instance that is added or removed is automatically traced and added or removed from the access filter, without needing to change policies. It becomes an automation-driven network access process that's easily audited.

Overcome SSH key management challenges

AppGate was also able to overcome the challenges with SSH key management across the large-scale environment. Instead of the organization requiring separate SSH keys for each application – which had become a headache to manage and an impediment to productivity – AppGate delivered a single SSH key for each virtual private cloud. AppGate now dynamically grants access to EC2 users based on policies. This simplifies and enhances security, while ensuring development teams can be highly productive.

Full audit trail for compliance

AppGate also overcame the organization's compliance challenges. It applies policy enforcement to all instances when deployed, eliminating the SSH management issue. Policies are automatically adjusted based on user attributes. AppGate provides detailed logs of user access and activities to efficiently feed audit request data needs and reduces audit scope.

Reduce compliance reporting burden

AppGate leverages identity, not IP addresses, and user context to automatically create an individualized network perimeter for each user. This dramatically reduced audit preparation time because AppGate is people-based, not IP-based. As a result, there is far less need to cross-correlate which IP address represents which people saving the organization time and money.

About Cryptzone

Cryptzone reduces the enterprise attack surface by 99% by providing identity-centric network security and compliance software for hybrid environments. Using a distributed, scalable and highly available Software-Defined Perimeter model, Cryptzone protects critical data from internal and external threats, while significantly lowering costs. In cloud environments, including AWS and Azure, Cryptzone provides user access control, increases operational agility and improves regulatory compliance. More than 450 companies rely on Cryptzone to secure their network and data. For more info, visit: www.cryptzone.com.

Cryptzone™

Americas +1 888 272 2484 | **EMEA & APAC** +44 118 900 1236 | www.cryptzone.com | sales@cryptzone.com