



CASE STUDY

SECURITIES REGULATORY ORGANIZATION SECURES ACCESS TO AWS

BACKGROUND

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

To more efficiently operate, the organization wanted to migrate to Amazon Web Services (AWS).

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.



QUICK FACTS

A securities regulatory organization that performs heavy data analytics and data science.

INDUSTRY

Financial Services

CHALLENGES

Automate AWS deployment without breaking compliance

Reduce compliance data collection and report preparation time

Isolate production, QA and development

SOLUTION

Appgate SDP

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

FINDING THE RIGHT SOLUTION

Having successfully used Appgate SDP to secure access to its on-premises datacenter, the organization turned to Appgate 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 SDP for AWS was a natural extension.

Appgate SDP 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 APPGATE SDP

Appgate SDP 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 SDP, 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 before Appgate SDP 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.

