EMA IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

EMA CASE STUDY

aviatrix®

Fortune 500 Bank Unifies Network Operations and Cybersecurity in the Cloud with Aviatrix Distributed Cloud Firewall

Solving Network Operations Was Step One

When the manager of cloud networking and security for a Fortune 500 bank adopted the Cloud Networking Platform from Aviatrix®, his initial aim was to solve cloud networking complexity in his Azure environment. His team was especially challenged by managing networking across multiple VNETs and Subscriptions.

“Prior to installing Aviatrix, troubleshooting was very interesting,” he said. “We would have multiple tabs open and try to trace where the problem was and where it wasn’t.”

Aviatrix offers deep visibility via the Aviatrix CoPilot® management solution, which offers monitoring and troubleshooting capabilities based on the telemetry it collects with its data plane software. Aviatrix CoPilot quickly simplified network operations for the bank’s team, the cloud networking and security manager said.

“The best part of the Aviatrix platform is that with a team of three people, we can support the entirety of our Azure environment. Combined with Terraform for automation, it just keeps things connected and working well,” he said.

aviatrix®

Distributed Cloud Firewall Changes the Game

Aviatrix expanded its solution last year with the introduction of its Distributed Cloud Firewall, which leverages Aviatrix data plane elements to create distributed security inspection and enforcement points across a cloud network. It also integrates with a cloud provider's native security tagging and security grouping capabilities to enforce security policies and impose controls at a granular level. Aviatrix Distributed Cloud Firewall brings intrusion detection, threat prevention, URL filtering, microsegmentation, and other capabilities to the entire cloud network. Users can manage Aviatrix Distributed Cloud Firewall centrally, like a single firewall, via Aviatrix CoPilot, the same console that manages its overall Cloud Networking Platform.

"Aviatrix was brought in to be a networking solution to simplify cloud networking," the bank's manager of cloud networking and security said. "The reality is, it's a security solution. In this day and age, our concern is having a bad actor getting inside [the cloud network]. We have to move away from perimeter security and get that security closer to the resources."

Aviatrix Distributed Cloud Firewall allows the bank to deploy security capabilities in all its cloud landing zones.

"We now have eyes directly in front of the application because Aviatrix is in the data path," he said. "We have full visibility with security from the source all the way through the network, not just an ingress/egress capability."

The bank now has default enforcement of all security policies out of the box for every new resource spun up in Azure. Cloud administrators must reach out to the cloud networking and security teams to request exemptions to security policies, which is a far cry from the early days of the cloud when cloud administrators would circumvent most security policies without even trying.

"Our cybersecurity team absolutely loves this ability because now we block everything until it is approved," the cloud networking and security manager said. This enables a least privilege, zero trust approach that meets corporate and regulatory requirements.

EMA CASE STUDY

Extending Distributed Cloud Firewall to Kubernetes

Aviatrix enhanced the power of Distributed Cloud Firewall even further with its recent introduction of Aviatrix Distributed Cloud Firewall for Kubernetes. While the original version of Distributed Cloud Firewall focused on securing virtual machines within a cloud environment, this new version extends security to containerized applications in Kubernetes clusters.

Aviatrix Distributed Cloud Firewall for Kubernetes addresses a very painful problem for cloud native security. The existing Kubernetes ecosystem has robust solutions for securing connections within Kubernetes clusters, but there are fewer solutions for securing connections between clusters or between clusters and other services, such as traditional applications, API-based services, and other non-containerized entities. Securing these connections is essential because many cloud native applications need to connect with a variety of resources. Aviatrix Distributed Cloud Firewall for Kubernetes addresses this gap.

Enabling a Multi-Cloud Future

While this Fortune 500 bank is in a single cloud today, the cloud networking and security manager believes that Aviatrix has futureproofed his organization for its inevitable multi-cloud future.

"We know we will grow into multi-cloud, and we know we are positioned to do that very quickly [with Aviatrix]," he said. "It simplifies how you do your work. When you absorb everything that it is capable of, it simplifies everything and allows your team to focus on other things."

4403.040524