VALTIX

CUSTOMER SPOTLIGHT:

SPANISH NEOBANK MYINVESTOR SECURES AMAZON ECS SERVICE AND FARGATE WITH VALTIX DYNAMIC CLOUD POLICY

myinvestor

myinvestor

Industry:
Financial Services

Headquarters:
Madrid, Spain

Challenges:

· Maintaining agility while meeting stringent security needs

· Increase levels of security in AWS native services

· Security posture suffered because of potential security manageability

Outcomes:

· Zero time added to secure new workloads

· Consolidation of advanced security

· Dynamic policies tied to workload tags

Spanish Neobank MyInvestor Secures Amazon Elastic Kubernetes Service (ECS) and Fargate With Valtix Dynamic Cloud Policy

MyInvestor chooses Valtix to reduce business risk, simplify security, and gain efficiencies for their Kubernetes and serverless workloads

MyInvestor is a Neobank based in Madrid, Spain. Founded in 2017, MyInvestor offers a mobile app and website with a full range of financial services. MyInvestor is the largest fintech in Spain by volume.

Alejandro Delgado Ruiz had recently taken on a new challenge as MyInvestor's Chief Technology Officer (CTO). With strict regulations and the firm's reputation at stake, Alejandro knew he needed to focus significantly on improved security so the company could build on a solid foundation as they scaled. A potential security incident could threaten their business – there was no room for error.

MyInvestor has recently obtained its own banking license, so they fell under the same guidelines and regulations as their much larger, more established financial counterparts. They had to play bigger. At the same time, MyInvestor had to maximize the efficiency and effectiveness of its current resources.

Alejandro began his research process looking for a better solution. He wanted a cloud-first approach that would also keep up with advanced security requirements. He needed to protect containers, serverless, and data in AWS and wanted a common way to secure across each.

AWS Security Groups Fall Flat For MyInvestor

When MyInvestor started their Cloud migration journey with AWS, they leveraged security groups to define perimeter defense. These security groups would provide a "default-deny" approach to control inbound and outbound traffic to their resources.

However, they quickly found out that AWS security groups were challenging to manage. In practice, this became even more evident when deploying ECS clusters. The dynamic nature of the ECS cluster meant that you'd have to manage a lot of services' security groups and perform resource-consuming manual maintenance.

Héctor Martos Gómez, Infrastructure Specialist at MyInvestor, said: "Applying fine-grained restrictions using security groups in a dynamic environment would be a nightmare. Having to manually maintain an updated list of inbound and outbound allowed IPs for each service is a mess to manage."

Additionally, AWS security groups didn't provide the levels of security needed for inbound and outbound traffic inspection and control, such as FQDN or URL filtering.

When evaluating alternative solutions, Alejandro narrowed down his requirements.

- **The ability for security policies to apply dynamically to new workloads**
  Given the frequency of updates and new workloads in ECS and Fargate, they need a policy management approach that could be fully automated.

- **Advanced capability to secure egress traffic**
  Outbound traffic is the last line of defense in the case of a breach. MyInvestor needed the ability to filter outbound connections on known malicious domains, and the ability to restrict outbound connections to a whitelist of domains.

- **Intrusion prevention to block external threats with WAF plus IPS**
  A WAF was an obvious minimum requirement. Alejandro also realized they needed more, including the ability to prevent attacks on vulnerabilities through IPS.

- **Blocking ability for malicious IPs for both ingress and egress**
  The ability to block both inbound and outbound traffic from known malicious IPs meant that they could reduce their attack surface and raise the bar for a bad actor.

- **The ability to use Infrastructure as Code (IaC) tools**
  The ability to use Infrastructure as Code tools like Terraform enabled provisioning and management of the large-scale infrastructure they were building.

> *"It's all about visibility and control of inbound and outbound traffic within our environment."*
>
> **Alejandro Delgado Ruiz**, Chief Technology Officer (CTO)

Additionally, workloads were all within a cloud-native container and serverless environment, so they couldn't rely on endpoint agents, endpoint detection & response (EDR), or Cloud Workload Protection Platforms (CWPP). Alejandro needed one security approach that could provide consistent and pervasive protection for workloads and data.

Said Alejandro, "It's all about visibility and control of inbound and outbound traffic within our environment. You can never 100% guarantee an attacker can't get in, but you want to make it increasingly difficult. And once they are in, you want to take away the opportunity to exfiltrate data or establish command and control by limiting external access to only what's approved."

Valtix Enables Dynamic Security With Tag-Based Policy

Alejandro found Valtix on the AWS marketplace after researching solutions that could provide cloud-native network-based security. After signing up for the Valtix Free Tier and going through the initial steps, he knew he'd found something unique and well-aligned with his needs. Alejandro requested a meeting, and after going through an introduction with the Valtix team and an architectural discussion, he was excited about the possibilities for how the technology could enable their business to achieve its goals.

Said Alejandro, "I could see immediate power in the ability to be able to create tag-based policies through the Terraform provider, and apply those policies on the resources of the workloads that have those tags. These tag-based policies will allow us to group resources with similar a whitelist of outbound domain restrictions. For new resources, tag-based policies enable agility as we can secure by simply adding the appropriate tag."

In comparing Valtix to other solutions, he briefly considered whether a traditional NGFW appliance would meet their requirements. He knew a virtual appliance would introduce even more operational challenges, however.

After going through full proof of concept, the value became even more obvious. Some of the key strategies that Valtix enabled included:

- **Security delivered fully as a service**
  Valtix drastically simplified their security infrastructure and drove efficiency. Instead of having to think about deploying a WAF or other security controls for each workload, security could be defined as policy associated with workloads identified through tags – saving tons of time with the provider. The result: security just works, thus creating a force multiplier for MyInvestor's team to play bigger than their team size.

- **Centralized Security of Ingress and Egress**
  Valtix enabled a centralized security model across accounts that guaranteed traffic would be protected, thus reducing risk. All workloads would be deployed into private subnets. Valtix policy would define application of security and routing to the public internet. This meant that traffic could be inspected and policy applied no matter what type of workload (containers, serverless, etc.). As a result, DevOps teams could move faster with less risk that a simple vulnerability or misconfiguration could result in a security incident.

- **Tag-based Security Policy**
  Combining tag-based policy with the other values provided by Valtix enabled a new level of business agility. With their previous approach, it might take a day or two to deploy security fully. When you multiply this effort times many app updates and deployments, valuable time was wasted. With Valtix Dynamic Multi-Cloud Policy (™), Alejandro's team was able to virtually eliminate the effort required to secure new apps to zero.

- **Policy-as-Code**
  The ability to create and manage policy as code with the Valtix Terraform provider closed the loop on Infrastructure as Code, being able to create and manage policies using resource outputs from the infrastructure.
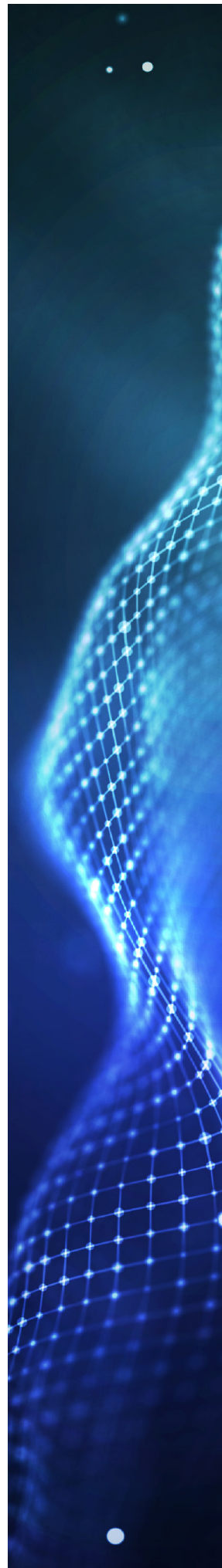
Almost immediately, Valtix showed quantifiable business benefits for Alejandro, which was critical for his business case.

• **Business agility**

DevOps focuses on deploying containers at speed with which the business desires. Security adds no additional time to daily and weekly builds.

   • *Quantified Value: Millions saved*

• **Resource efficiency and tools consolidation**

Alejandro collapsed multiple disparate services into a single platform with Valtix. Cloud networking, traffic routing, and security is applied all now run through Valtix and is defined via policy.

   • *Quantified Value: Millions saved*

• **Risk reduction**

Enabling a default deny approach to security means that only what needs to be opened to the internet gets exposed through Valtix cloud gateways. This approach mitigates inadvertent exposure through known vulnerabilities and reduces the possibility that a zero-day will yield a major incident.
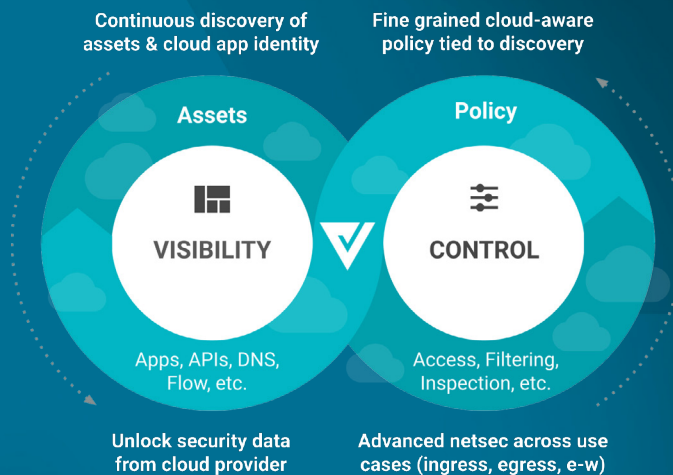
   • *Quantified Value: Priceless*

Meet Valtix Dynamic Multi-Cloud Policy™

Clouds Are Dynamic. Security Policy Must Be Too.

According to Gartner, by 2025, 99% of cloud security failures will be within the customer's control. When it comes to cloud network security, failures happen when policy is fragmented across accounts or clouds. They also happen when policy is tied to IP addresses that inevitably change. Cloud teams need a cloud-native model of tag-based policy that works multi-cloud.

Only Valtix Delivers Dynamic Security Policy

• Connects continuous visibility and control to discover new cloud assets and changes, associate tag-based business context, and automatically apply the appropriate policy to ensure security across dev, test, production, and compliance workloads.

• Powers Valtix security gateways so they just work in the background, invisible to cloud teams.

• Ensures that critical security gaps don't emerge and that the business stays secure and resilient.

Continuous discovery of assets & cloud app identity

Fine grained cloud-aware policy tied to discovery

Assets

Policy

VISIBILITY

CONTROL

Apps, APIs, DNS, Flow, etc.

Access, Filtering, Inspection, etc.

Unlock security data from cloud provider

Advanced netsec across use cases (ingress, egress, e-w)

Plans for the Future

While ingress and egress were a great start, Alejandro wasn't done. Segmentation (East-West) was on the near-term roadmap. The flexibility of the Valtix platform combined with Dynamic Multi-Cloud Policy would enable them to become more strategic about security in the cloud. Alejandro felt confident that Valtix would provide a foundation for MyInvestor going forward, while also maintaining agility.

Said Alejandro, "For any fast-moving startup, time and talent are two of the most important things. With Valtix, we're able to provide powerful protection for our AWS deployment, but do so efficiently and at the speed of an agile startup. I couldn't be more excited about the future of our partnership with the Valtix team."

"With Valtix, we're able to provide powerful protection for our AWS deployment, but do so efficiently and at the speed of an agile startup."
Alejandro Delgado Ruiz, Chief Technology Officer (CTO)
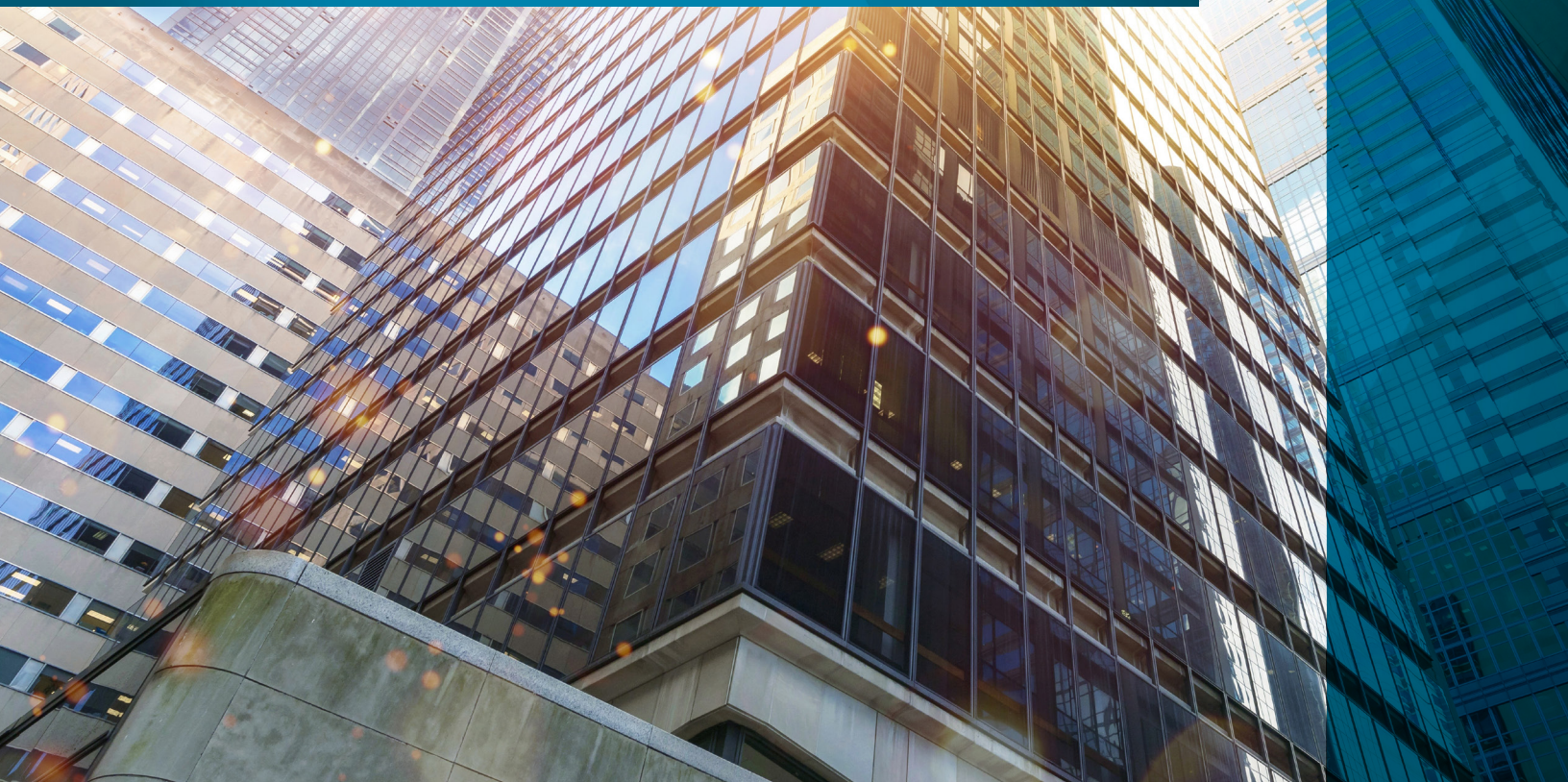
VALTIX

CUSTOMER SPOTLIGHT:

SPANISH NEOBANK MYINVESTOR SECURES AMAZON ECS SERVICE AND FARGATE WITH VALTIX DYNAMIC CLOUD POLICY

ABOUT MYINVESTOR

MyInvestor is a neobank for investment solutions powered by a neobanking license for additional mortgages, loans and remunerated accounts. It offers exclusive investment products with no minimum entry fees and the market's most competitive commissions. The company's mission is to help clients manage their wealth, placing the best investment products within their reach, independently of their acquisition power. With a business volume of more than 2.3 billion euros at December 31 st 2022, it is the largest fintech in Spain in terms of total volume (secured loan book plus deposits plus assets under administration).

ABOUT VALTIX

Valtix is on a mission to protect every workload, every app architecture, across every cloud. The first multi-cloud network security platform delivered as a service, Valtix was built to combine robust security with cloud-first simplicity and on-demand scale. Powered by a cloud-native architecture, Valtix provides an innovative approach to multi-cloud security enabled in minutes and with no infrastructure to maintain. The result: security that is more effective and aligned to cloud agility requirements. With Valtix, organizations don't have to compromise in the cloud. They can meet critical security and compliance requirements without inhibiting the speed of the business.

Join 4 of the top 10 pharmaceuticals and leaders across every industry and **sign up free** *in minutes.*

Ready to get started?
Schedule a demo at ***Valtix.com***

HQ - Santa Clara, USA
2350 Mission College Blvd #800 Santa Clara, CA 95054
650.420.6014 info@valtix.com