T-Mobile Netherlands

Secure and cost-effective Managed Cloud Services
for AWS from T-Systems

About T-Mobile Netherlands

T-Mobile Netherlands is one of the largest Dutch telecommunications providers, serving more than 5 Million customers and offer an extensive portfolio of mobile network, fixed line and internet services for the consumer and business market. The company prides itself in offering simple and easy access to their services for their customers and having one of the largest 4G coverages for the consumer market, which covers the entire country.
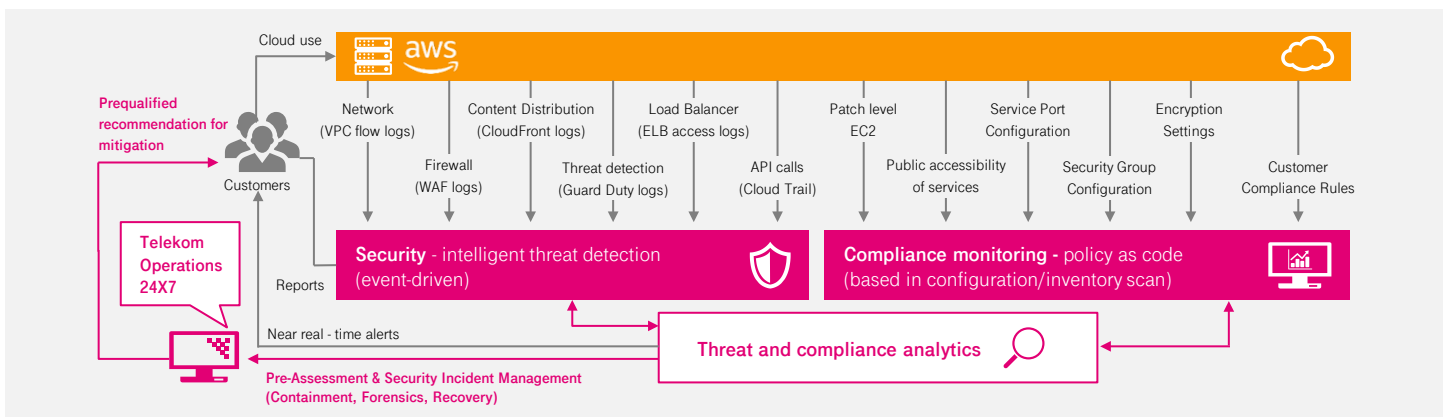
The Problem

T-Mobile Netherlands identified an intrinsic need to move numerous applications from a Company Data Center to the Cloud. They wanted a Landing Zone solution which could integrate with their existing on-premise network, could grow when future application migrations were identified and would enable the ability to save costs compared to their current hosting providers. With the limited time and existing experience available to support such a platform, they wanted to ensure enhancements to the platform could be provided using proven and established mechanisms, with assurance from a 3rd party that this can be performed in a secure and compliant manner. They needed the ability to keep track of costs in a simplified way and the ability of key internal stakeholders to be notified of important events.

The Solution

The proposal to T-Mobile Netherlands was to have a Landing Zone solution consisting of multiple core components to deliver the necessary functionality. A new Master Billing Account (and AWS Organization) was established, owned and configured by T-Systems,

which is not accessible by T-Mobile Netherlands and enable some of the central security features, such as T-Systems deployed SCPs and an Organizational CloudTrail. It provides T-Systems the ability to segregate the responsibilities of managing and supporting the accounts from the customer specific usage and ensure that central, T-Systems specific features of the security configuration (such as enabled Regions, CloudFormation Stacksets, IAM Policies and Roles) can't be modified or deleted in the individual accounts by the customer. This also made sure that Operational tasks, manual or automated could be seamlessly performed on each of the accounts. A DynamoDB table, hosted in the T-Systems DevOps Account ensures that a central source of truth for the accounts is maintained, including important technical information (such as product version, activated regions, support settings, etc.). This enable new features to be automatically deployed, with no impact to the customer solutions, or the agreed SLA's.

As part of the T-Systems managed service, each account is delivered with a Telekom managed module configuration. This is a security-oriented product developed in-house at T-Systems to ensure that the core security guidelines are met, and a set of Deutsche Telekom internal Privacy and Security requirements are established. The client get an Admin user account, with the ability to develop their solutions as intended and the necessary guardrails that ensured they were operating within agreed parameters. Another important feature of this module is the CloudTrail configuration, which is logging all API Service calls in an S3 bucket on the T-Systems Security account and is therefore integrated with the internal monitoring toolsets that the T-Systems Operations team uses. This way, if an event such as a root login happens, the event is forwarded to the Operations team via a 3rd Party incident Management software. They would then start an investigation of the event and if necessary, advise the relevant T-Mobile Netherlands contact.

Let's power higher performance

The entire technical configuration of the accounts enables T-Systems to provide the necessary support to ensure the right information is logged, highlighted, reported and addressed. With the Foundation Package included in every account, some of the most important security services are included in the process highlighted in the diagram above.

Further functionality of the managed services includes a 24x7 Service Desk availability and a Billing Dashboard made available to ensure full visibility of costs, including any incurred by the Services T-Systems provides.
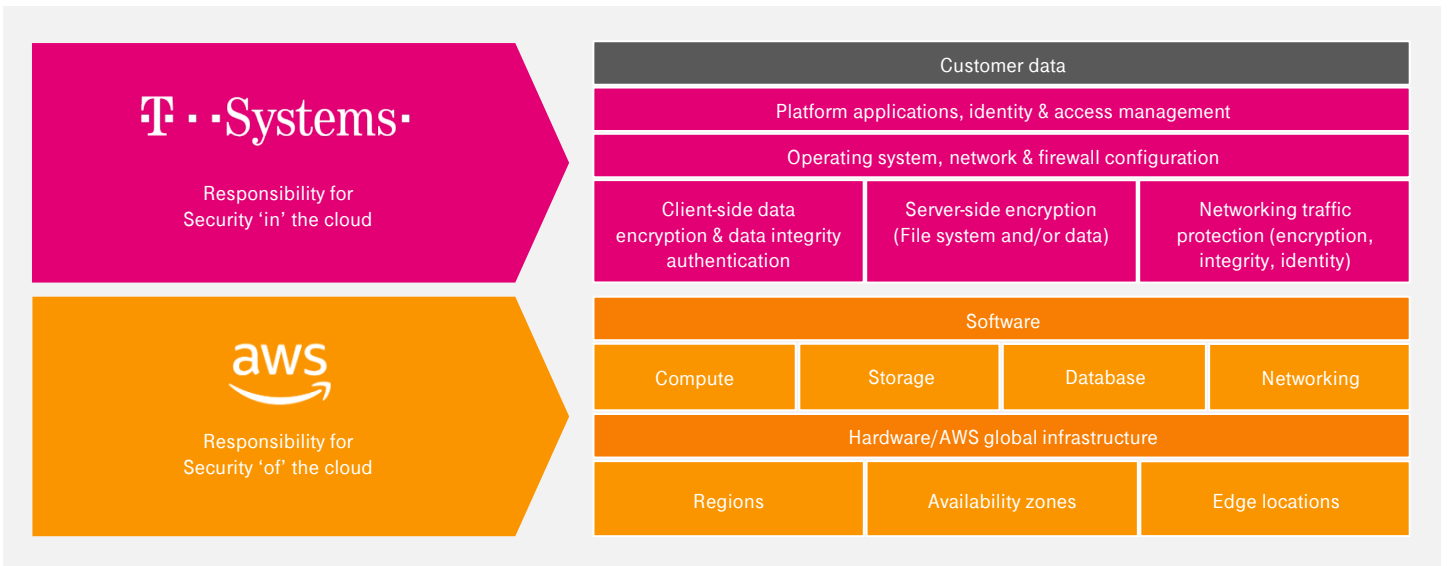
Results and Benefits

The ability to quickly procure the necessary accounts with the T-Systems DevOps process, seamlessly integrated with the Monitoring and Reporting toolsets and a 24x7 Service Desk enabled T-Mobile Netherlands to increase their agility of developing new solutions in the cloud and reduced the time-to-market for projects from 6-9 months to 2-3 months. Additionally, it gave T-Mobile Netherlands the peace of mind and group-wide approval from potential internal blockers to utilize the platform to its full potential. The easily accessible Billing dashboard provided them a way to keep track of costs and find quick remediation methods if needed.

Next Steps

Due to the scalable architecture of the Landing Zone, additional application domains could be established if required. A set of AWS Accounts, containing the Telekom managed module would be created, one for the non-production workloads and the other for production. If an application is critical, or contains very sensitive information, T-Systems offers an additional, advanced Service Module, which contains integration of further security services, such as WAF, CloudFront, VPC FlowLogs, amongst others.

"We required a managed service provider to provide us with a secured environment On AWS within a matter of days to run Reporting during our merger activities. This happened over the Christmas holidays. T-Systems delivered!"

David Logan
Manager, Network & Infrastructure Ops - T-Mobile Netherlands

As is the case with the Foundation Service, with the Advanced Service all the logs are being centrally stored in the T-Systems Security Account and used by our Monitoring Software to alert, auto-remediate and report on important events. With the advanced module, more in-depth coverage of the pillars from the responsibility matrix are addressed, in addition to the ability to provide Managed EC2 and Managed RDS components. A Cost Optimization component would also ensure that continuous review of spend would be reported and if necessary, remediated. The integration between the Service Providers, as well as the ability to centralize their operation has been identified to be of major importance to T-Mobile Netherlands. A central, T-Mobile Netherlands operated Service Management Software would be used to log and track any incidents, assets and changes on the platform. This way, the customer would have visibility over all the Service Providers and have full visibility of ticket resolution. To enable this, the current automated forwarding of events via API would be updated to utilize this toolset as the new Target and the T-Systems Operations team would then start resolving any incidents in the new solution.

T··Systems·

Responsibility for Security 'in' the cloud

Customer data		
Platform applications, identity & access management		
Operating system, network & firewall configuration		
Client-side data encryption & data integrity authentication	Server-side encryption (File system and/or data)	Networking traffic protection (encryption, integrity, identity)

aws

Responsibility for Security 'of' the cloud

Software			
Compute	Storage	Database	Networking
Hardware/AWS global infrastructure			
Regions	Availability zones		Edge locations

T··Systems·

Let's power higher performance