The difference maker

The shared responsibility model of AWS places most of the burden of security and data protection squarely on the user. This can result in a challenging situation in which IT managers have neither the time nor personnel to implement the appropriate policies. And that can quickly lead to immeasurable security risks.

T-Systems provides support that makes all the difference in these types of situations. Drawing on a portfolio of comprehensive security services for AWS environments, we can practically eliminate critical security vulnerabilities.


Want to set up an AWS account? Nothing could be easier, at first. But with all those services and features, many give up before they reach the finish line. As a managed service provider, we help your company get the most out of all your services.
What’s included

- Security for the network configuration
- Protection of critical data streams
- Access control
- Use of encryption methods
- Constant monitoring
- 24/7 support

And best of all? You stay flexible and creative, and your cloud service is not limited in any way.

How do we do it?

A range of security components come into play to protect your AWS account. We ensure password requirements are met, regional guidelines are adhered to, and data protection classes are observed in S3 buckets. For complex solutions and environments with several applications, we provide what is known as a landing zone. The landing zone provides a structured AWS organization consisting of several accounts that serve various purposes.

A main user administration account ensures that individual users with specific IAM roles sign up for all sub-accounts and receive the necessary permissions.

SCPs round out the concept, limiting access to services such as CloudTrain and AWS Config at the account or organization level.

Every business is different

What do you do, for instance, when someone is responsible for running their own development or production environment? In this case, a separate compliance audit for one or several accounts is conducted to determine whether there are any flaws in the infrastructure, which components or configurations should be checked, and which actions to eliminate non-compliant components are necessary.

As required, we can train your employees to enhance their knowledge and ability to assess and handle security incidents themselves.

Our fault-tolerant, scalable solution ensures that basic security concepts such as multi-layer protection and the principle of least privilege are part of the main solution architecture.

Our operations team provides a complete 360° view of the network, operating system, and AWS API layers. We’re able to detect intrusions and initiate countermeasures practically in real time. This agile and well-architected approach makes implementing other more complex features a simple matter of modular upgrades.

With our help, your enterprise IT gets the foundation it needs for a secure future.