Managed Security Services for your AWS environment

By AWS Premier Partner, T-Systems

AWS Security? Great! Where to start? Hmm...

AWS is the most secure cloud computing available today. It is also the only public cloud with its service offerings and supply chain vetted and accepted as safe for top-secret workloads. With the Shared Responsibility Model, you share your security and compliance with AWS.

But for those new to the model, the demarcation lines between responsibilities can be confusing. How do you define who is liable for what, and what policies and processes should you establish? And where AWS is responsible, your mantra should always be to verify this trust, but how?

When you add your complex data, applications, and compliance mandates to the mix, then begin reviewing numerous AWS security solutions, things can get daunting.

You can rely on T-Systems' Managed Security Services

Wherever you are on your journey with AWS, we can help you achieve and maintain the optimal security posture for your unique circumstances. Our comprehensive portfolio of security services for your AWS environments caters to the varying needs of all organizations.

As an AWS Premier Partner, we have extensive inside knowledge and experience of AWS security best practices. We can give you the strategic and tactical guidance you need, as well as practical, hands-on support 24/7.

Our approach to your security in AWS

We are much more than a managed security services provider; we are your strategic and collaborative partner. We will protect your critical assets and infrastructure in AWS with the same passion and care that we apply to our own.

We understand the importance of balancing security and the business— we measure and monitor often to continuously improve security function and enable the business to manage risk. We monitor how well we align agreed plans with core processes and what's going on in the business.

The increased use of the cloud also demands an increased level of security, especially in technologies that secure workloads, containers, and serverless applications . Our zero-trust approach to security and fault-tolerant solutions provides you, your stakeholders, and the regulators with the confidence and peace of mind you deserve. We enable you to implement all of the seven principals of the Extended Zero Trust Security model: zero trust networks, workloads, people, data, devices, visibility and analytics, automation and orchestration.

The highest level of visibility across your AWS estate, reached through consolidation, will guarantee you the security effectiveness needed to prevent sophisticated cyber attacks.

We bring together the capabilities of cybersecurity, business continuity and enterprise resilience. Embedding security across the business ecosystem and applies fluid security strategies to respond quickly to threats, so it can minimize the damage and continue to operate under attack. As a result, your business can introduce innovative offerings and business models securely across the entire value chain, strengthen customer trust and grow with confidence.

T· ·Systems·

Let's power higher performance

T-Systems AWS Managed Security Services Portfolio

To protect your AWS operating environment, our customizable portfolio of managed AWS solutions and services includes:

- Strategic guidance,designing and implementing security policies aligned with your Business strategies and growth.

- Determining the distribution of your security responsibilities based on your specific use cases

- Centralized Security Logging and Monitoring

- Continuous security monitoring and 24/7 reactive and proactive support

- Identity management and access control.

- Data Residency and Compliance Guardrails

- AWS compliance monitoring (CIS AWS Foundations, PCI DSS, HIPAA, HITRUST, ISO 27001, AND SOC2)

- End to End Protection of critical data streams

- AWS infrastructure vulnerability scanning

- Managed intrusion detection/prevention system

- A Landing Zone for the secure migration of complex environments and applications to AWS

- A 360° view of Security across the AWS Infrastructure.

- Security trainings for your non-technical teams Regular reporting and analysis of agreed security KPIs

- Fine-tuning your AWS environment (Well-Architected Reviews) to identify and eliminate gaps in your security posture

- Security audits

- Distributed denial of service (DDoS) mitigation

- Monitor, triage security events

- Regular alignment with your team so that business outcomes can be targeted, measured and met.

Our AWS security experts are here to answer your questions and would be glad to assist you. Get in touch today and take your next step to a secure and successful future with AWS.

T··Systems·

Let's power
higher performance