Build in the cloud with confidence

While AWS provides secure cloud infrastructure, through the Shared Responsibility Model, you are responsible for securing the workloads, applications, and data that you run on AWS. That's where Trend Micro can help. Our services help you map to the AWS Well-Architected Framework so you can build viable cloud architectures and meet ongoing compliance requirements, keeping your environment secure and scalable.

Establish a strong cloud foundation with the AWS Well-Architected Framework

Benefit from a consistent approach to building cloud architectures that can scale over time. By aligning your approach to the Shared Responsibility Model with the six pillars of the AWS Well-Architected Framework, it takes any guesswork out of the process. Leverage consistent best practices and guidance for your architecture so you can focus on building great solutions in the cloud, fast.

Continuously safeguard your AWS investments

Securing what you build in the cloud is not a one-and-done scenario. It's an ongoing process that should adapt over time. Trend provides you with automated checks and clear remediation steps based on the AWS Well-Architected Framework—keeping you on top of the latest from AWS and best practices.

Achieve **complete visibility** into your AWS infrastructure through one pane of glass so you know who's interacting with your environment

Adhere to **best practices** to build securely and reliably, ensuring you make the most of your cloud investments

Keep your cloud builders up to date on the **latest AWS products and services**, as well as their best practice configurations for security and compliance

40M+

daily AWS Well-Architected Framework checks

6M+

Misconfigurations found per day

Trend cloud security key features ensure fast remediation

- **Real-time threat monitoring**
  Receive instant alerts and remediation steps to ensure critical systems are always secure, reliable, and optimized
- **Open-source auto-remediation**
  Automatically trigger start remediation once a failure has been discovered
- **Conformity API**
  Integrate into the CI/CD pipeline and live AWS environments
- **Workflow integration**
  Bring customizations, access levels, and channel communication options into workflows

Knowledge Base rules and guidance keep your environments safe

Trend delivers a robust educational toolset called Knowledge Base. Leverage detailed resolution steps to rectify security vulnerabilities, performance and cost inefficiencies, and reliability risks for what you have in the cloud.

10101101110101110
100011011011
1010110

600+

out-of-the-box rules to verify that you're aligned to the AWS Well-Architected Framework

80+

AWS services are auto-checked to ensure your cloud infrastructure is configured to best practices

Steer clear of security risks with just-in-time alerts

A data breach can happen in an instant. Trend delivers the latest information and tools to help you secure what you're accountable for in the Shared Responsibility Model.

Amazon Simple Storage Service (Amazon S3) buckets are a powerful and popular service secured by AWS. However, you are responsible for securing what you put in your Amazon S3 buckets, including configuration and encryption. What happens if you make a mistake?

Without Trend:

PII data breach due to misconfiguration

- You've activated an Amazon S3 bucket to store personally identifiable information (PII) about your customers.
- You're busy, and you've overlooked unique configurations for this bucket and encrypting the data.
- When your PII is made public, you don't receive a notification. Six months later, all your data has been hacked and shared.
- Your company has to report to its shareholders about this massive data breach and do major damage control.

With Trend:

Keeping cybercriminals out of your Amazon S3 bucket

- This time you're the same engineer, but you have Trend.
- Trend helps you identify the risk in real time and notifies you that your Amazon S3 bucket is publicly readable and not encrypted.
- Trend sends you a message with instructions from Knowledge Base on how to configure your Amazon S3 bucket so it's no longer public.
- You pat yourself on the back for protecting customer PII and upholding your shared responsibility efficiently.

Experience Trend in AWS Marketplace with free trials and always-free tiers.

Start for free