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

The **AWS Well-Architected Framework** provides a consistent approach to building cloud architectures that can scale over time. By aligning your approach to the Shared Responsibility Model with the **five 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.

Operational excellence
Establish automated, repeatable processes to deploy resources

Security
Bring security measures in early to lead design and proactively assess risks

Reliability
Safeguard against disruptions and manage capacity for improved availability

Performance efficiency
Accommodate workloads with the right amount of computing

Cost optimization
Take a consumption approach to keep costs lower than data centers

Continuously safeguard your AWS investments with Trend Micro Cloud One™ – Conformity

Securing what you build in the cloud is not a one-and-done scenario. It's an ongoing process that should adapt over time. Conformity provides 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

10101101110101110
100011011011
1010110

Knowledge Base rules and guidance keep your environments safe

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

600+
out-of-the-box rules to verify that you're aligned to the AWS Well-Architected Framework

60+
AWS services are auto checked to ensure your cloud infrastructure is configured to best practice

Conformity key features ensure fast remediation

Real-time threat monitoring
Instant alerts and remediation steps to ensure critical systems are always secure, reliable, and optimized

Open source auto-remediation
Automatic triggers start remediation once a failure has been discovered

Conformity API
Integrate Conformity in the CI/CD pipeline and live AWS environments

Workflow integration
Customizations, access levels, and channel communication options bring Conformity into workflows

490M+
daily AWS Well-Architected Framework checks

840M+
misconfigurations found per day

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

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

Amazon Simple Storage Service (AmazonS3) buckets are a powerful and a popular AWS 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 Conformity:
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 Conformity:
Keeping hackers out of your Amazon S3 bucket

This time you're the same engineer, but you have Conformity.

Conformity identifies the risk in real time and notifies you that your Amazon S3 bucket is publicly readable and not encrypted.

Conformity 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.

Sign up for a free trial of Conformity!

Whether your AWS exploration is just taking shape, you're midway through a migration, or you're already running complex workloads in the cloud, Conformity can help. This solution offers full visibility of your AWS infrastructure and provides continuous cloud security and compliance posture management based on the AWS Well-Architected Framework. Let us do the heavy lifting so you can focus on innovating and growing on AWS.

Try it in your environment today!

Ready to subscribe?

Get Conformity in the AWS Marketplace

Resources to learn more

Conformity Knowledge Base