Trusted Cloud Provider FAQ

What is a Trusted Cloud Provider?

Built upon existing Cloud Security Alliance programs, the Trusted Cloud Provider program allows organizations to demonstrate their commitment to holistic security and serves as a reference point for customers looking to identify cloud providers that are aligned with their security requirements.

What qualifies a Trusted Cloud Provider?

- Have a current entry in the CSA Security, Trust, Assurance & Risk (STAR) registry.
- Have at least one current member of staff who has achieved the CSA Certificate of Cloud Security Knowledge (CCSK).
- Be a corporate member of Cloud Security Alliance and must volunteer at least 20 hours annually to CSA for activities such as research working groups, chapter events, blog posts and other work for the common good.

How do I know if we qualify?

CSA will notify current members if they qualify, or are near qualification, for the program. There is no application process for existing CSA members. New members will be made aware of their position during the onboarding process. For questions regarding your organization's status, reach out to membership@cloudsecurityalliance.org.

What do Trusted Cloud Providers receive?

Members of the Trusted Cloud Provider program receive a trustmark that will be displayed on the organization's entry in the STAR registry. Members achieving Trusted Cloud Provider status will also receive a copy of the trustmark logo graphics file for their own use.

CSA will announce each new Trusted Cloud Provider on social media and recognize the inaugural participants at CSA's premier annual conference, SECtember, to be held September 13-17, 2021. CSA will also periodically highlight Trusted Cloud Providers in educational campaigns and provide additional benefits in the future.

How do you verify volunteer hours?

CSA will internally verify participation in volunteer activities. The number of hours contributed are self-declared by the participant.

Do we have to renew our Trusted Cloud Provider status annually?

CSA will review your compliance with the Trusted Cloud Provider criteria prior to your company's membership renewal anniversary date. Compliant organizations will be renewed automatically.

How will we receive our trustmark?

CSA will email trustmark download information to the corporate member point of contact address on file. You may also contact membership@cloudsecurityalliance.org to receive the trustmark download information.

How do we use our trustmark?

When displayed on a website, the Trusted Cloud Provider trustmark should link to the member's CSA STAR registry entry so that interested parties can verify the accuracy of the status claim. You can find your company's STAR entry by searching https://cloudsecurityalliance.org/star/registry/ or you can contact star-help@cloudsecurityalliance.org for assistance.

The logo file includes a guide to further usage instructions.

What if I'm not a CSA member?

You must be a member of the Cloud Security Alliance to qualify for the program.
Contact membership@cloudsecurityalliance.org to confirm your organization's CSA membership status.

What is STAR?

The Security Trust Assurance and Risk (STAR) program encompasses key principles of transparency, auditing and alignment of standards. Companies who use STAR indicate best practices and validate the security posture of their cloud offerings through a listing in the STAR registry. STAR registry entry types include Level 1 Self-Assessment and Level 2 Third-Party Audit.

The Cloud Security Alliance STAR registry is the world's largest and most popular repository of cloud provider security statements. More information is available at www.cloudsecurityalliance.org/star.

How is being a Trusted Cloud Provider different from STAR?

The Trusted Cloud Provider program extends the credibility of organizations on the STAR registry by showing their extended commitment to holistic security through training/education and contributing to the community through volunteering and cloud security evangelism.