stack overflow FOR TEAMS

Security FAQs

Stack Overflow was built by developers for developers. So with our single tenant solution for your own technical teams, we're bringing you enterprise-grade security that will allow your team to share proprietary knowledge with confidence.

How we keep your data secure

Stack Overflow was built on transparent knowledge - which is why we want to ensure you have the most up-to-date information regarding our security measures for for the premium tiers of Stack Overflow for Teams.

General security measures

Q What is the difference between hosting yourself or in the Stack Overflow Enterprise Managed Cloud?

If you decide to host data in your own data center, this changes who has physical access to the servers.

Q Is client data encrypted?

The Enterprise and Cloud Hosted Business plans on Stack Overflow for Teams require the use of HTTPS in order for our clients to communicate with the site.

Q Who has access to login details?

Stack Overflow doesn't store usernames or passwords that are owned and managed by your organization because we require you to configure a SAML 2.0 Identity Provider (IDP) in order for users to access the site. To successfully log in and an account from a configured SAML 2.0 IDP, we require a unique ID, an email, and a full name.

Q Which Security certifications do you have on an organizational level?

We operate according to Support Privacy Shield and GDPR. We also have SOC 2 Type I and Type II reports.

Want to speak to a Stack Overflow for Teams expert about your security needs?
Contact the team: sales@stackoverflow.com

stack overflow FOR TEAMS

Security measures for hosting on your own premises

Q Where is Stack Overflow Enterprise customer data stored?

With Enterprise you have a choice between hosting the application in your own data center or cloud service.

Azure cloud security measures

Q Where is customer data stored on the Business and Enterprise plans of Stack Overflow for Teams?

For Cloud Hosted Business and Enterprise Cloud option, we use Microsoft Azure Cloud, which means you'll have world class infrastructure and security of the platform as your backbone. Our Enterprise plan includes SOC II certification along with other robust security measures.

Q How do you separate my Team's data from public Stack Overflow data?

Each Enterprise instance of Stack Overflow for Teams is isolated in its own Virtual Network within our Azure Cloud Subscription. This means that the infrastructure for your Team is not shared among our customer base and we provision each customer's infrastructure in such a way that traffic and data never cross customer boundaries.

Q Can issues on on other Cloud Hosted Business and Enterprise clients' instances affect my data?

Isolated Cloud infrastructure is provisioned for each customer, including networking and databases. There is no interaction between customer environments.

Q What encryption is used on Azure?

For Cloud Hosted, we utilize SQL Transparent Data Encryption (TDE) to encrypted data at rest. Data in transit is encrypted using TLS 1.2 using a SHA256 certificate with a 2048-bit key.

Q Who has admin access at Stack Overflow?

Access is restricted to Site Reliability Engineers for Stack Overflow for Teams Cloud Hosted and Enterprise plans who have been trained on the information security policies and guidelines in place. This includes guidelines for Data Loss and Leakage Prevention which aim to prevent customer data from ever leaving the provisioned Cloud environment.

Q Where can I learn more about Azure Cloud?

Since we run and manage the Enterprise and Cloud Hosted Business plans through a SOC II and ISO27001 certified Azure Cloud, you can learn all about it in detailed specifications published by Azure Cloud on the security of its public cloud platform and infrastructure.

Want to speak to a Stack Overflow for Teams expert about your security needs?
Contact the team: sales@stackoverflow.com