Enterprise 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 Stack Overflow for Team’s Enterprise version.

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 Stack Overflow Enterprise application requires 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 Enterprise expert about your security needs? Contact the team: sales@stackoverflow.com
Security measures for hosting on your own premises

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

Where is Stack Overflow Enterprise customer data stored?
For the Enterprise Cloud option, we use Microsoft Azure Cloud, which means you’ll have world class infrastructure and security of that platform as your backbone, including SOC II and ISO27001 certified infrastructure.

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.

Can issues on other Enterprise clients instances affect my data?
No. The whole infrastructure is set up to isolate applications, networks, and ultimately your data from other customers. We provision a separate Virtual Network in our Azure Cloud Subscription for each customer.

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.

Who has admin access at Stack Overflow?
Access is restricted to Site Reliability Engineers for Stack Overflow Enterprise 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 your provisioned resource group in our Azure Cloud subscription.

Where can I learn more about Azure Cloud?
Since we run and manage the Stack Overflow Enterprise Managed Cloud service through a SOC II and ISO27001 certified Azure Cloud, [you can learn all about it in detailed specifications](https://example.com) published by Azure Cloud on the security of its public cloud platform and infrastructure.