Analytics

Security Measures Overview

At Procore, we're serious about protecting our customers' data, and have implemented numerous security measures to achieve that goal. In the spirit of transparency, some of those measures are described below.

Data Protection

Procore Analytics implements a layered data security approach. The following security measures are in place:

Transport Layer Security

All data in transit to the database is secured and encrypted via TLS 1.2 using the AES256 encryption standard.

Data Encryption

Azure Transparent data encryption (TDE) helps protect Azure SQL Database against the threat of malicious offline activity by encrypting data at rest. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.The encryption algorithm used is AES 256.

Azure SQL Database Firewall

All connection attempts pass through a firewall, only allowing trusted sources to establish a connection to the database server.

Authentication

All credentials require complex 16 character minimum passwords. Authentication controls are in place to validate all logins.

Auditing

All database actions are recorded and audit logs are stored for tracking database activity.

Threat Detection

Azure SQL Database Threat Protection is utilized to detect and respond to potential vulnerabilities, anomalous database activity, and SQL injection attacks.

SQL Vulnerability Assessment

Procore conducts vulnerability assessments on all tools to verify the effectiveness of security measures.

Data Hosted by Microsoft Azure

Microsoft hosts Procore Analytics data in Microsoft Azure's highly secure data centers.

Best-In-Class Service

Procore has a service-level objective for the 99.9% availability of its services. Individuals can email security@procore.com with any security-specific concerns or questions, or to identify specific vulnerabilities.