Trimble Secure Development Lifecycle

Trimble's Secure Development Lifecycle (TSDLC) framework comprises tools and processes that embed and operationalize security practices to ensure our solutions meet consistent security levels. These include security measures on our systems and networks such as identity and access management, vulnerability management, intrusion detection solutions and many more.

Equally important, Trimble teams monitor and manage technology infrastructure and environments. Using the TSDLC framework, we review our cloud infrastructure and processes according to industry best practices. We continuously execute 24x7 security monitoring, vulnerability scanning, intrusion detection, dynamic and static analysis and open-source analysis of our solutions. We perform application security assessments using Trimble specialists as well as third-party security experts.

Our TSDLC tools and processes, along with our continuous monitoring, management and appropriate incident response, provide you with confidence in the security of our solutions.

Availability of Trimble solutions

Availability

We continually monitor the performance of our solutions to prevent possible incidents that would impact system availability. We consolidate views from log parsing, infrastructure monitoring and application performance management (APM). Please see your organization's Trimble Service Level Agreement (SLA) for complete details regarding each solution's target availability.

Disaster recovery

Trimble ensures all its cloud-based solutions have disaster recovery plans in place that support disaster prevention and recovery. Trimble aims to provide a robust recovery plan while taking all possible steps to prevent a disaster. Our prevention and recovery plans:

- Reduce the likelihood of a disaster.
- Implement contingency plans to restore partial or full service as soon as possible after an incident has occurred.
- Document a clear communication strategy to keep customers and any other relevant parties informed of the situation as it develops.

Infrastructure

Amazon Web Services

Trimble hosts its cloud-based solutions and customer data through Amazon Web Services (AWS). As the world's leader in cloud infrastructure, AWS is designed to deliver a flexible, reliable, scalable and secure cloud computing environment with high-quality global network performance.

AWS provides secured data centers all around the world. These data centers are protected from unauthorized physical access and environmental hazards by a range of security controls. The AWS platform offers exceptionally high security compliance, including certifications such as ISO27001, SOC 2 and FedRAMP.

Cloud security

Cloud and data security are shared responsibilities between the cloud infrastructure provider and the client using the cloud solution. In Trimble's case, this means we trust Amazon Web Services to manage the security of the cloud infrastructure, and Trimble teams are responsible for the security in the cloud environment.

Hosts are hardened with automatic (Linux) and scheduled (Windows) patching, isolated VPC, data encryption and robust vulnerability management practices that include penetration testing, role-based access control and security groups.

Trimble utilizes managed services such as AWS Shield. We have an in-house 24x7 Security Operations Center team for monitoring alerts using top-tier endpoint detection and response solutions and other security engineering tooling. Read more about AWS cloud security in AWS Whitepapers & Guides

Data management

Access control

For multi-tenant cloud-based solutions, Trimble logically segregates each customer's data within the applicable AWS environment. Each customer organization is assigned a Globally Unique Identifier (GUID) that isolates it from other accounts. The customer's end users are then attached to the correct account by the customer's admin. The customer's admin can only set up users in their organization's specific account with their assigned GUID. This structure drives the segmentation of data and security controls across the application.

Trimble products are built with a role-based security model. This model allows administrators at various levels to control access to data within each customer organization. Users are placed into specific groups and inherit the access permissions granted to their assigned groups. Trimble restricts access to its premises and customer data and protects its source code repositories by using, among other measures, multi-factor authentication to access production systems.

Data encryption

All customer data is encrypted at rest. Encryption in transit is enforced for the data in transit, providing industry-standard levels of security for data transmission over the internet.

- Trimble leverages AWS technology to achieve Server-side encryption for our document store and other storage volumes encryption.
- Transport Layer Security protects all Trimble HTTPS endpoints. Our web services force secure transport using HTTP Strict Transport Security (HSTS).
- For our commercial cloud offerings, data in transit and at rest encryption uses the AES256 standard.

Single sign-On

Single Sign-On (SSO) is an optional integration feature that allows users to integrate Trimble applications with their SSO provider. Trimble Single Sign-On requires a standard SAML 2.0 connection setup on both parties. It allows users to authenticate to Trimble solutions without having to enter credentials within each application. Trimble supports all other technology providers as long as they can set up a standard SAML 2.0 connection.

Multi-factor authentication

Multi-factor authentication (MFA) is a security feature that is available to all Trimble customers. This feature requires users to validate their authentication using two or more items of evidence. All Trimble administration tools require MFA. MFA works by entering a username, password, and code provided by an authenticator service such as Google Authenticator.

Data backups

Trimble actively maintains data backups so that in the event of data corruption, inconsistency or loss, we can restore data as quickly as possible. Backups are maintained separately from the primary data repository but within the same geographical region.

Trimble maintains internal targets for Recovery Time Objective (RTO) — the maximum time expected to restore the system to operation — and Recovery Point Objective (RPO) — the maximum expected loss of data in the event of a disaster.

Data retention

Data is retained for a standard period of time after a Trimble customer's contract termination or expiration unless otherwise agreed in the applicable customer contract. At the end of that period, the customer data is purged from the database, and documents are removed from the file store. The database information will still be part of previous database backups for the duration of the standard backup retention period. Please see your Trimble contract for more details.

Data extracts

During the applicable data retention period following contract termination or expiration, our cloud-based customers may request a copy of customer data in the form of a Microsoft SQL Server Database (database extract) and an archive of project documents stored as part of the customer's account.

Compliance and security best practices

Vulnerability scanning

Trimble uses vulnerability scanning tools to proactively expose, remediate, and manage security vulnerabilities in our cloud-based systems.

Third-party component analysis

Like most software products, many of Trimble's software solutions include underlying components from third-party suppliers that are necessary building blocks for the software. Trimble uses third-party component analysis tools to scan these components to check if there are newer versions or patches available, check for any known vulnerabilities, and confirm licensing compliance.

Intrusion detection

In a world of increasingly sophisticated cyberattacks, Trimble employs intrusion detection tools to detect attacks on our cloud service endpoints (points of access) and our internal systems.

Static source code analysis

Static code analysis is the analysis of computer code directly, i.e., without actually executing programs. Analysis of source code is a useful method of detecting security threats in the system before it is deployed and released.

Dynamic code analysis

Dynamic analysis is typically used in association with static code analysis and looks at a “live” or “staged” system as opposed to the code directly.

Anti-virus

Many Trimble applications provide features that allow customers to upload files and data in various forms. Trimble employs anti-virus scanning tools to check data as it is uploaded to assist in the removal or the quarantine risky or suspicious data.

Cybersecurity awareness

A prerequisite for developing secure solutions is understanding the threat landscape in which the service is operating. At Trimble, threat modeling is one of the core guiding principles used to design and develop our solutions.

Within Trimble, we regularly update our knowledge about cybersecurity topics and share awareness about cybersecurity threats among all parties responsible for managing and developing our solutions. As a baseline, all employees attend mandatory cybersecurity training sessions. Solution architects and developers participate in specialized cybersecurity training sessions addressing threats specific to the products developed by Trimble.