SOC-2 Self-Assessment

As an organization that designs products, or as an individual engineer or designer, your models and designs are some of your most valuable assets. SimScale takes care of all security aspects for you and keeps your data safe so you can stay focused on your main goal: designing great products.

As we plan to have our security posture reviewed by an external auditor we are preparing for a SOC 2 Type 1 audit. This document summarizes the status quo of the SOC 2 trust service criteria as currently implemented by SimScale.

SOC 2

SOC is short for “System and Organization Controls” —and *de facto* an industry standard for software security and privacy. During the SOC 2 audit, an external auditor will carry out an extensive review of our processes (e.g. employee onboarding and offboarding, access review, various policies, disaster recovery exercises, software architecture, physical access, etc.) and ensure that they meet the mark.

The Type 1 audit is a point-in-time audit where the auditor verifies that the controls are satisfied at a specific point in time. We are planning to proceed to Type 2 afterward which is based on continuous monitoring during time periods of varying lengths.

Trust Service Criteria

The five SOC 2 trust service criteria are: security, availability, confidentiality, processing integrity, and privacy.

1. **Security**

   Protecting systems against unauthorized access.
2. **Availability**

   Ensuring that the system remains functional and usable.
3. **Confidentiality**

   Restricting the access of data to a specified set of persons or organizations.

   Ensuring that network communication is encrypted and cannot be intercepted by unauthorized personnel.
4. **Processing integrity**

   Ensuring that a system fulfills its purpose and delivers correct data.
5. **Privacy**

   Minimal processing and use of personal data in accordance with the law.

The following sections describe in detail how SimScale implements each trust service principle.

Security

SimScale believes that the best way to achieve a secure system is to follow best practices and industry standards, and not with obscurity (i.e. attempting to “secure” a system only by making it “difficult to understand”) or homegrown technology (e.g. custom encryption algorithms).

We have a designated team responsible for all aspects of security, such as infrastructure, software, and data.

Infrastructure security

SimScale's production infrastructure is hosted entirely on AWS (Amazon Web Services). Data processing is carried out in the Ireland region (eu-west-1), and backups are kept in a separate geographic region in Frankfurt, Germany (eu-central-1). Each region is composed of at least three "availability zones" (AZs) which are isolated locations, designed to take over in case of a catastrophic failure at one location. AZs are separated by a significant distance such that it is unlikely that they are affected by the same issues such as power outages, earthquakes, etc. Physical access to AWS is restricted by AWS' security controls. Furthermore, AWS monitors and immediately responds to power, temperature, fire, water leaks, etc.

Access to SimScale's production infrastructure is restricted to SimScale employees and contractors. All systems have controlled access and only a limited number of employees have privileged access. Access is only possible through a VPN (Virtual Private Network), or TLS (Transport-Level Security).

The production environment is separated from testing environments, using separate accounts and VPCs (Virtual Private Cloud) in AWS. This ensures that any defect in the test environment cannot impact the production system. The connection to the internet is controlled by dedicated gateways.

Organizational security

Since an organization is only as good as its people, SimScale takes great care when selecting and training its staff. All employees undergo a thorough selection process that has been designed to detect the best talent in the world for the job. Performance monitoring frameworks using Objectives and Key Results (OKRs) are implemented on an individual and team basis. The Human Resources department assists with individual L&D (Learning and Development) efforts.

SimScale’s employees are required to complete yearly security awareness training. The training is designed to increase sensitivity to physical security (hardware and media handling, office access control, etc.), digital security (e.g. secure passwords, two-factor authentication), social engineering attacks (“phishing”), and other security-related topics.

SimScale employment policy mandates that all hard drives must be encrypted. This is enforced by a remote monitoring tool. Additionally, Windows workstations require the use of malware detection.

Product security

SimScale is aware of how important it is to its customers that all data is handled securely. Therefore, several layers of protection ensure that the data is not accessible by unauthorized persons.

An essential part of software security is “defense in depth” which means that there are multiple layers of protection. In case one layer is breached, the next layer helps to contain the breach and mitigate its consequences. This can be achieved by isolating software components from each other, such that the breach of one component does not affect adjacent software. SimScale’s service-based architecture provides natural isolation between components. Additionally, we use container virtualization as a means for further encapsulation of the code we’re running. AWS' VPC (Virtual Private Cloud) provides another layer of isolation from the internet on the network level. The implementation of a “zero trust” security model provides one more layer of defense with respect to the public internet.

As a general principle, all of SimScale's data is encrypted while being transported across networks and when stored ("in transit and at rest"). In case of unauthorized access to the data, an attacker would only see undecipherable garbage which cannot be decrypted without the corresponding keys. The encryption methods employed by SimScale are industry standard and deemed unbreakable by contemporary standards. Data at rest (virtual filesystems, relational databases, and object storage) is encrypted using industry-standard AES-256, while data in transit is encrypted with TLS ≥ 1.2.

There are two ways for a user to log in to SimScale: Single sign-on (SSO) and username plus password. Single sign-on can be used by organizations to fully manage access to SimScale and, for example, to ensure that former employees no longer have access after the offboarding period. We support Google and Microsoft Active Directory SSO using OAuth. If no SSO is used, the default login method is username and password. To protect against brute-force attacks, we use rate limiting together with a slow password hashing algorithm which naturally slows down the speed at which such an attack can be executed. SimScale does not store passwords in clear text, but only cryptographic hashes. This means that SimScale does not know the passwords of any users, and no passwords can be reconstructed from our databases.

SimScale is sponsoring a public bug bounty program hosted by Intigriti. The objective of the bug bounty program is to receive security-related bug reports from trusted "white hat hackers" before the vulnerability is actively exploited in a malicious way. This program has already contributed and keeps contributing to SimScale's product security. All security issues undergo a triaging process and are escalated based on their criticality.

SimScale uses various automated scans to detect software vulnerabilities. Processes are in place to find and upgrade vulnerable components. All teams are monitoring the vulnerabilities in their services and are committed to reducing them. The progress is supervised with team-level Key Performance Indicators (KPIs) and goals.

Access control

We regularly keep track of and review the list of employees who have access to which systems and remove access where applicable.

Offboarding processes ensure that former employees cannot access internal systems anymore after the termination of their contract. Thanks to the VPN, SimScale can centrally restrict access to internal networks.

MFA

Multi-factor authentication (MFA) adds another layer of security on top of classic password authentication. In addition to username and password, the user requires another individual token of access. Stealing or guessing the password is not enough for an attacker to gain access to a system, because the second factor would also need to be stolen. Usually, the second factor is a physical device, such as a mobile phone which has been paired with the authentication system. SimScale employs MFA to protect access to the infrastructure provider (AWS) and the version control systems, among other systems.

Availability

Redundancy

Hosted on a cloud infrastructure, SimScale implements a service-based architecture where many dedicated software components operate isolated from one another, but in a coordinated way, much like a complex machine where individual parts can be replaced independently from one another.

As a general rule, SimScale's services are redundant, meaning that there is always more than one instance available. In case of a crash, or overload, the spare takes over, and the faulty instance is replaced automatically, to restore the original count of running services. This happens 24/7 without any human intervention.

The same is true for the deployment of new versions of SimScale's services. During the release of a new version, the running instances of a service are replaced one by one, while SimScale's engineers have taken great care during the preparation of the update that the old and the new version can run at the same time. In case of an unexpected problem, the system can be restored to the previous state without any downtime.

Performance monitoring

SimScale uses a number of performance monitoring systems, such as New Relic, Prometheus, and CloudWatch. New Relic is used to monitor application performance, such as server response times and user interface speed. Prometheus collects server-side metrics like CPU and RAM usage.

Additionally, SimScale monitors the performance of databases with AWS tooling.

Different alerting channels notify the developers in case the performance of the system has regressed, for example, due to increased response times, or increased error rates. To enable the root cause analysis of bugs, SimScale collects system logs from all parts of the system. These logs can only be accessed by authorized users.

SimScale is planning to offer a public status page as part of the SOC 2 certification process.

Backups and disaster recovery

To reduce the risk of simultaneous failure, SimScale backs up the data from object storage to a different AWS region with very limited access.

Relational databases are backed up on a daily schedule.

SimScale is currently planning a rehearsal of disaster recovery in Q4 of 2022. In this exercise, a clone of the production environment will be recovered from scratch using backups, and tested for soundness.

Incident handling

Whenever an incident occurs, SimScale follows an internal incident response plan. For critical issues, the response team will follow an iterative response process designed to investigate, contain exploitation, eradicate the threat, recover system and services, remediate vulnerabilities, and document a post-mortem with the lessons of an incident.

Customers and users can report outages via regular support channels (for example via the website, or using the live chat feature in the workbench). SimScale's internal communication systems have dedicated channels for incident escalation.

Confidentiality

Except if you are on the Community plan, other users won't be able to see your content, unless you grant access explicitly. SimScale engineers may use your data to provide support and when necessary to fix bugs.

Access controls

All employees and contractors are contractually bound to confidentiality, which persists after the termination of the work contract.

As part of a “clean screen” policy, all computers used by SimScale staff must automatically lock the screen after a certain period. This is enforced by a centralized monitoring solution.

All data is subject to the “principle of least privilege”, meaning that every employee only has access to necessary information.

Deletion

User data will be stored by SimScale up to 60 days after the termination of a subscription term, according to the terms and conditions. In this event, or when a user requests the deletion of data, the data is made inaccessible or physically deleted, depending on data type and storage location. For technical reasons, data may remain in backups after this point.

Processing integrity

Quality assurance

Product quality is very important to SimScale. There are many different facets, including:

- Accuracy of simulation results
- High performance of the user interface and simulation core
- Almost zero downtime

Several measures are put into place in order to keep product quality high:

- Code review: Every single code change is reviewed by a peer of the developer before it is accepted into the main code branch. It can only be merged if the reviewer agrees. It is usually necessary to add a test alongside, and the code review process ensures that this has been done as well.
- Continuous integration: Before code is accepted, it is built by our continuous integration environment and component-level tests, as well as integration tests, are executed. If the build fails, the developer is notified immediately and a fix is required before the code can be merged.
- Manual testing: Once the code has been merged, the change is deployed to a development environment, and in most cases tested manually by our QA team. Any substantial problems or regressions found are declared a release blocker and require a fix before the change may be released to the production environment.
- Automated integration testing: A large battery of automated tests is executed against the testing and staging environments and checks many common workflows for regressions of any kind. In case the tests fail, the QA team tracks the problems and forwards them to the developers.
- Validation and overnight tests: Since result accuracy is of paramount importance to simulation software, we use a special layer of integration tests to ensure the correctness of simulation results. As simulation errors can be caused by code changes in CAD handling and meshing, there are additional tests that protect the CAD and meshing stacks against regressions. Updates of third-party software are tested extensively before release.

Any code change is released only if all these steps succeed.

Furthermore, access to the code base is protected via multi-factor authentication (MFA), which poses another layer of defense against the malicious injection of code.

Since SimScale depends on third-party software, we regularly contribute to the quality assurance of our suppliers. Whenever SimScale becomes aware of regressions or bugs, they are reported upstream. In this way, SimScale is contributing to the quality, stability, and accuracy of other software in the scientific computing and engineering space.

Process monitoring

Where possible, SimScale uses software to enforce processes. For example, code review and having tests passed are enforced by the source control management tool.

Regular reviews on different levels (individual, team, department, company) foster alignment between all individuals and the company objectives.

Privacy

SimScale takes data privacy very seriously and complies with the rules of the European Union's GDPR (General Data Protection Regulation). GDPR grants a wide range of rights to SimScale's users, such as the right to be informed, the right of access, the right to rectification, the right to erasure, and others.

One fundamental rule of the GDPR is the principle of "data minimization", which ensures that we are not processing more personal data than necessary. As a result, the core simulation platform uses only minimal personal data for user authentication and essential communication (which is a name, contact email, and a password hash).

Privacy policy

We are aware that confidential handling of your data is essential to establishing trust. Therefore, SimScale's privacy policy ensures that the data of our users is protected according to the high standards of GDPR.