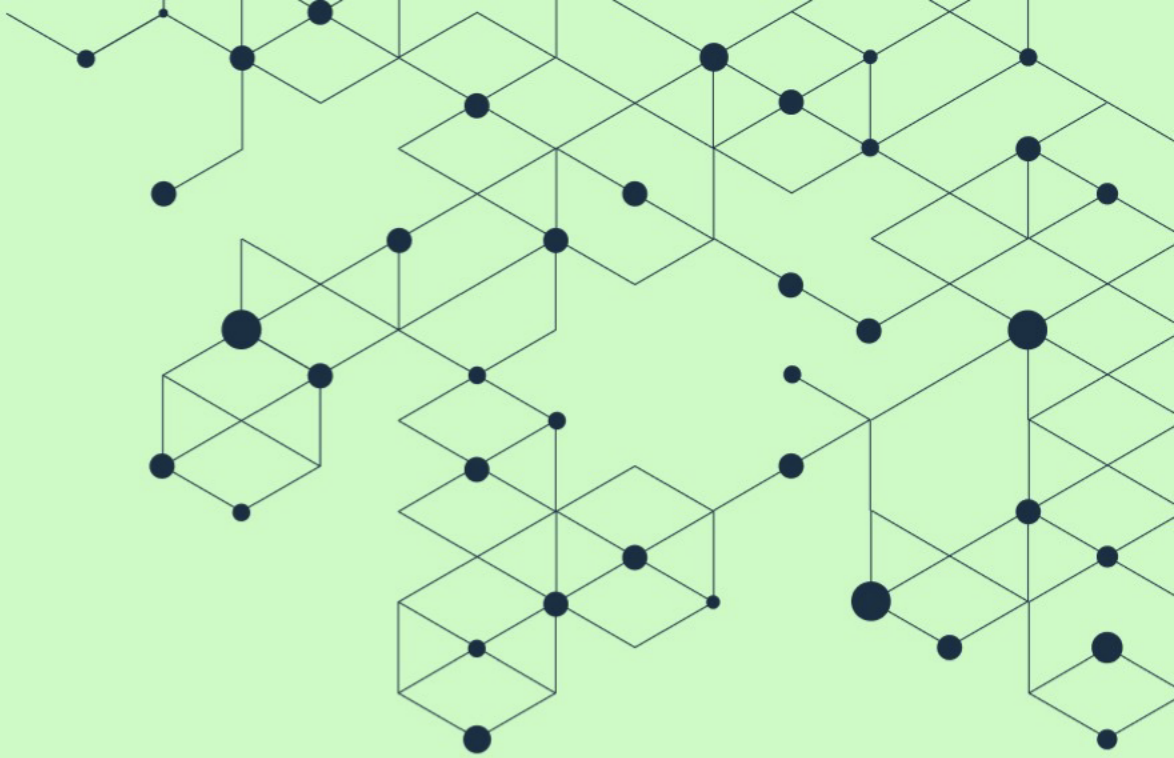


Stairwell

Security at Stairwell

White Paper

01-Aug-2022

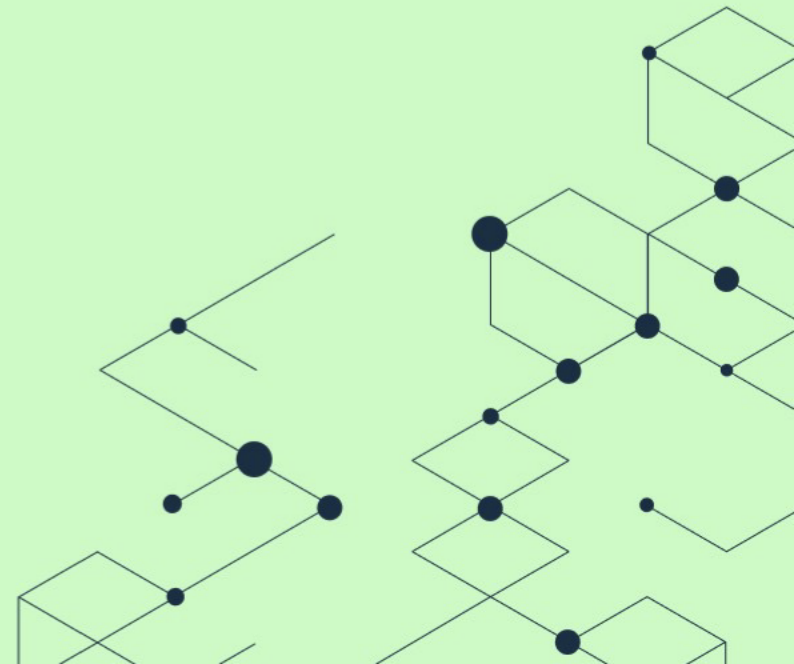


Table of contents

Introduction

Stairwell helps organizations take back the cybersecurity high ground with solutions that attackers can't evade. The Inception platform empowers security teams to outsmart any attacker by providing continuous contextual threat analysis, detection, and response.

This white paper outlines Stairwell's approach to security and compliance for Inception, including details on organizational and technical controls regarding how Stairwell protects your data.

Our people

Stairwell has created a vibrant and inclusive security culture for all employees.

The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training, and in the performance evaluation process.

Employee background checks

Before they join our team, and where local labor law or statutory regulations permit, Stairwell will conduct a criminal background check on the employee. Other types of background checks may be conducted depending on the sensitivity of the employee's position.

Security training for all employees

All Stairwell employees undergo security training as part of the onboarding process and receive ongoing security training throughout their Stairwell careers.

When a new employee signs their offer letter, they also sign a confidentiality agreement and, during onboarding, agree to our Code of Conduct, which highlights our commitment to keeping customer information safe and secure.

Depending on their job role, additional training on specific aspects of security may be required.

Employee competency

Every role at Stairwell is defined in a job description that includes the role's responsibilities for information security.

Employees are not only evaluated on their specific job duties but how well they met their information security-related expectations as well.

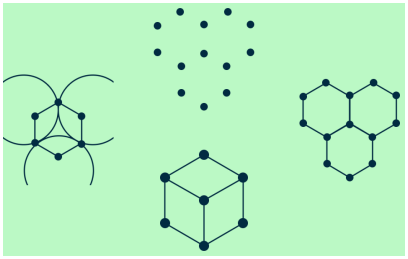
Compliance specialists

Stairwell has a dedicated compliance team that reviews compliance with security laws and regulations.

As new security and privacy standards are created, the compliance team determines what controls, processes, and systems are needed to meet them.

This team facilitates and supports independent audits and assessments by third parties.

Our processes



We know that our customers rely on Stairwell's products and services to help secure their companies.

Our processes are designed to ensure reliability and continuous improvement by describing how things are done, providing the focus for making them better, and delivering successful outcomes.

Access control

Stairwell implements the principle of least privilege[1] across all information assets.

Employees are only provided with access to information assets they have been specifically authorized to use.

[1] "The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function." Committee on National Security Systems (CNSS) Glossary Working Group (2022). *CNSSI 4009: Committee on National Security Systems (CNSS) Glossary*. [online] CNSS Instructions. Available at: https://www.cnss.gov/CNSS/openDoc.cfm?6sTAdOUQfZWi4i9xLhu7Sg== [Accessed 5 Aug. 2022].

A formal user registration and deregistration process uniquely identifies each employee and enables the assignment of access rights, while a formal user access provisioning process implements the assignment or revocation of access rights for all user types to all information assets.

The use of privileged access rights is restricted and controlled, as is access to source code, development tools, and software libraries.

Users' access rights are reviewed at least quarterly.

Change and configuration management

All changes to information assets are subject to change management procedures, with a focus on separation of duties.[2]

For example, the same person may not initiate, approve, and execute a change, nor may a single person request, approve, and implement a change to access rights.

Stairwell establishes standard configurations for hardware, software, and services which are monitored and enforced by automated means to ensure that the configuration, including required security settings, are not altered by unauthorized or incorrect changes.

Secure development

Stairwell employs industry-standard practices for software development, including:

- Maintaining separate development, quality assurance, and production environments;
- Establishing secure coding guidelines for each programming language used;
- Defining security requirements in the specification and design phase;
- Maintaining secure repositories for source code and configuration; and
- Ensuring security in the version control process.

Third-party security

Stairwell is a "cloud native" company and relies on third parties, such as the Google Cloud Platform (GCP), to provide much of our computing infrastructure. As a result, our security is only as good as the security of our suppliers and we take their security as seriously as we take our own.

[2] "The principle that no user should be given enough privileges to misuse the system on their own." Hu, V.C., Kuhn, R. and Yaga, D. (2017). Verification and test methods for access control policies/models. *Computer Security Research Center.* [online] doi:10.6028/nist.sp.800-192.

Stairwell conducts an assessment of the security and privacy practices of each third-party supplier to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide.

Once we have assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

We review each supplier's compliance with those contract terms as well as their overall performance at a frequency commensurate with the level of risk that the supplier poses to Stairwell's and our customers' objectives.

Data protection

Our customers need to know that the data they provide us and the services we provide are safe from unauthorized access or disclosure, modification or destruction, and disruption.

Stairwell relies on both organizational and technical measures to ensure the confidentiality, integrity, and availability of the information we process and the services we provide.

Some of those measures include:

- Classifying and labeling information in order to apply appropriate protections;
- Employing data leak prevention tools to identify, monitor, and detect the disclosure of sensitive information as well as block actions or transmissions that may expose sensitive information;
- Masking or transforming sensitive information (e.g., replacing values with their hash) to limit its exposure;
- Using cryptography to protect sensitive information; and
- Deleting sensitive information when no longer needed to prevent unnecessary exposure.

Data at rest

Stairwell uses Google Cloud's native encryption service to protect all stored information.

Data for storage is split into chunks and each chunk is encrypted with a unique data encryption key. These data encryption keys are stored with the data and encrypted with key encryption keys.

Encryption keys are managed by Google on Stairwell's behalf using the same hardened key management systems that Google uses for its own encrypted data, including strict key access controls and auditing. Data at rest is encrypted using AES-256 and automatically decrypted when read by an authorized user.

Google's *Encryption at rest in Google Cloud* whitepaper, dated July 2020, provides greater detail on the mechanics of Google's encryption and key management services.

Data in transit

Within Stairwell's virtual private cloud (VPC) and peered VPCs, all virtual machine to virtual machine (VM-to-VM) traffic is encrypted using Google's native encryption service.

Traffic passing over public networks is protected using Transport Layer Security (TLS) v1.2 or higher.

Incident management

We have a comprehensive incident management process that begins by providing employees with a simple, straightforward process for reporting observed or suspected information security events. These reports may be submitted with attribution to the employee or anonymously.

Stairwell's incident management process includes capabilities for the administration, documentation, detection, triage, prioritization, analysis, communication, and remediation of incidents.

Only competent personnel are allowed to handle the issues related to information security incidents; they are provided with numerous opportunities for professional development related to their incident management responsibilities.

No one is ever happy about an information security incident, but when one does happen, we do our best to learn from it, determine why it occurred (without assigning blame), and prevent it (or something like it) from happening again.

Vulnerability management

One advantage of being a "cloud native" company is that Stairwell doesn't have an "on-prem" environment to protect.

While "the cloud" can be more secure than standard on-premises environments due to default network topologies and configurations (VPCs, security groups, NACLs, and routing) making it harder for attackers to exploit hosts in the cloud, leaving hosts with known vulnerabilities can negate all of those benefits.

Stairwell uses automated tools to maintain an accurate inventory of assets and deploy new assets from templates and vetted images.

We regard our assets as immutable; patching live instances is rare as vulnerable assets will be removed and replaced with fully-patched assets.

We engage competent third parties to conduct planned, documented, and repeatable penetration tests and track the usage of third-party libraries and source code to support the identification of vulnerabilities. When discovered, we take appropriate and timely action to address vulnerabilities.

Logging and monitoring

One of Inception's key benefits is that it treats all files as suspicious and pre-preserves them, allowing you to detect compromises across past, present, and future states. So, we'd be remiss if we didn't apply the same level of protection to our own information assets. And, through our logging and monitoring programs, that's just what we do.

We record activities, exceptions, faults, and other relevant events to prevent unauthorized access, identify information security events that can lead to an information security incident, and support investigations.

We also continuously monitor our information assets for anomalous behavior and take appropriate actions to evaluate potential information security incidents. Abnormal events are communicated to the appropriate teams to improve our auditing, security evaluation, and vulnerability management processes.

Protection against malware

An effective malware attack can lead to account compromise, data theft, and possibly additional access to a network.

Stairwell takes these threats very seriously and uses a variety of methods to prevent, detect, and eradicate malware, including internal use of the Inception platform.

Our technology

As mentioned earlier, Stairwell is a "cloud native" company and we take advantage of all that the cloud has to offer in terms of flexibility, efficiency, scalability, and security.

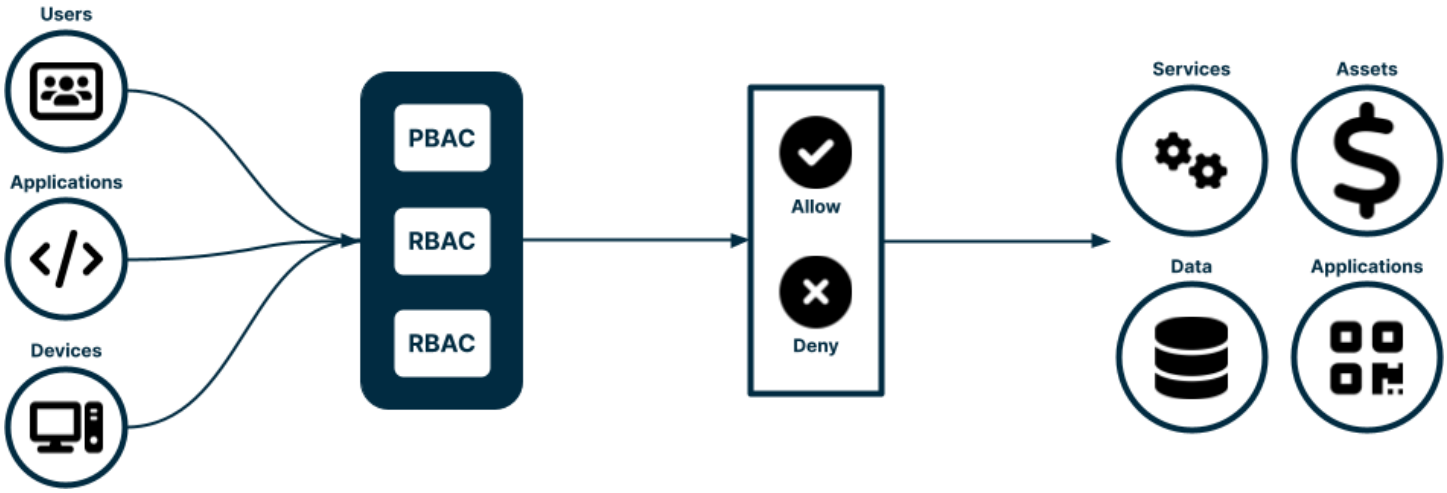
Zero trust architecture[3]

Stairwell has implemented a zero trust architecture to prevent unauthorized access to data and services while making access control enforcement as granular as possible.

Within our architecture:

- All data sources and computing services are considered resources;
- All communication is secured regardless of network location;
- Access to individual resources is granted on a per-session basis;
- Access to resources is determined by dynamic policy, and
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

We monitor and measure the integrity and security posture of all owned and associated assets and collect as much information as possible about the current state of our assets, network infrastructure, and communications and use it to improve our security posture.



Google Cloud Platform

The infrastructure supporting Stairwell's products and services is fully based on the Google Cloud Platform (GCP), Google's suite of public cloud products and services. The *Google security whitepaper*, dated January 2019, describes Google's approach to security and compliance for GCP.

[3] "An enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement." Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020). Zero Trust Architecture. *Computer Security Research Center*. [online] doi:10.6028/nist.sp.800-207.

Conclusion

Stairwell demonstrates its commitment to the people, processes, and technology described above through a rigorous compliance and certification program.

Our ISO/IEC 27001:2013 certificate is available here and our certification report is available on request.

Stairwell has been audited against the AICPA's 2017 Trust Services Criteria for Security and found to be SOC 2 compliant. Please contact us to request access to our complete SOC 2 Type II, report.

The protection of your data is a primary design consideration for all of Stairwell's products, services, and personnel operations.

We work across our organization and with our suppliers, partners, and customers to maintain the security and integrity of your data and the availability and reliability of our products and services.