Antithesis Security Policy

[Information Security](#)

- [Motivation](#)
- [Definitions and Terms](#)
- [Security Thesis](#)
- [Security Goals](#)
- [Organization](#)

[Security Requirements](#)

- [Personnel](#)
- [Consumer and Regulatory Compliance](#)
- [Data and Workload Isolation and Architecture](#)
- [Service Hardening](#)
- [Access Controls and Privilege Management](#)

Information Security

Motivation

Antithesis provides the most valuable and comprehensive testing environment available for our Customers. Antithesis relies on the trust of our Customers to provide these services. At Antithesis, security is a fundamental design consideration of our offerings and is organized around a few core principles.

We believe that the most robust security architecture is that which is simple to explain, implement, and maintain. To that end, we base our architecture around a small set of clear and powerful security boundaries. Every mechanism has a clear purpose and is designed in a testable manner.

This document lays out the basic security goals of the Antithesis Platform. These goals are the

standards against which Antithesis holds everything we build and the policies we set out. Additionally, this document describes the essential measures that Antithesis takes to implement our security goals.

Definitions and Terms

Administrator Privilege: Administrator Privileges are the technical permissions to change or configure how a system or service works, as opposed to merely accessing or using it. This includes root privileges on any servers, as well as the ability to deploy a server in the first place.

Authorized User: A fully authenticated user that has specific permissions for a certain, scoped action.

Customer: An organization that has engaged Antithesis to provide its services. A Customer corresponds to at least one Tenant.

Cloud: Hardware, accessed over the internet, operated by a third party.

Endpoint: Workstation or laptop used by Authorized User(s) to interact with our system.

Security Regression Review: A targeted review of updates to existing security components intended to ensure no regression against the standing security policy.

Tenant: A Tenant is the basic unit of isolation, security and otherwise, within the Antithesis Platform. Each Antithesis Customer is allocated one or more Tenants, reflecting the Customer's isolation preferences. Antithesis may, at its discretion, build further security boundaries within a Tenant as a pragmatic matter.

TCB: Trusted Computing Base; software, application, and service components which are responsible for maintaining security goals. Software that is not part of the TCB is untrusted, and cannot compromise any security goal even if it is deliberately malicious.

Trusted Third Party: A third party who, if they acted maliciously, could compromise any of our security goals

Security Approach

The Antithesis security approach is premised upon the idea that security responsibilities should be built into the fewest possible pieces of software. Each piece of this limited set of security aware components is built to fill a small, auditable, and testable function within the overall security architecture. This set of components, together with the portion of Trusted Third Party software that sits on a security boundary, is collectively referred to as the Trusted Computing Base or TCB. Every other piece of software produced by or *used* by Antithesis, not only has no security responsibilities, but is fundamentally untrusted. This means that even if such non-TCB software components were malicious, they would not be able to harm any of our Security Goals. Consequently, Antithesis can maintain a high velocity of development and innovation on the vast majority of the Antithesis Platform consisting of non-TCB software, and so long as all

modifications to the TCB are stringently reviewed and audited, the overall security of the Platform cannot be impacted.

Any software responsible for maintaining the boundary between Tenants must necessarily comprise a portion of the TCB. Consequently, since we want the TCB to be as small and as easy to scrutinize as possible, the vast majority of the Antithesis Platform is comprised of components that only deal with a single Tenant. This means that Antithesis essentially maintains a parallel copy of our entire infrastructure for every Tenant, in stark contrast to the common industry approach of packing multiple customers into a single global system. We believe that this additional infrastructural burden is well worth it, because it means that the set of all trusted components is small, rarely changing, easy to fortify, and easy to audit.

The TCB is most robust when its features are pared down to provide as minimally configurable a set of security boundaries as reasonable. The focus of the TCBs is on making the important security boundaries (between Tenants) very strong rather than on offering limitlessly configurable access control within those boundaries.

Security Goals

Isolation: Any user or service without permissions for a Tenant will not be able to inspect or disrupt the operations of that Tenant.

Confidentiality: Only Authorized Users of a Tenant and authorized Antithesis employees should be able to read Tenant data.

Integrity: Only Authorized Users of a Tenant and authorized Antithesis employees should be able to write Tenant data.

Availability: The availability of our products and services to a Tenant should not be compromised by actions of unauthorized individuals, or failures of another Tenant's systems. This further implies that Tenants must be isolated from a performance standpoint, and that excessive load on one Tenant cannot result in an outage of another.

Erasure: On the authorized request of a current or former Tenant, Antithesis should be able to reliably and permanently delete all Tenant data and/or encryption keys required to decrypt all Tenant data.

Organization

Security Lead: Ben Collins

Security Committee: The Committee is comprised of the Security Lead, the leads of Finance, Legal, and one member of the founding team. The Committee is responsible for overseeing and enforcing this security policy.

Security Reviews: The Security Committee is responsible for conducting an annual audit to

ensure that Antithesis, as a company and online software provider, is compliant with this security policy. In addition, material changes to TCB components will be subject to Security Regression Review before deployment, except in emergencies (and in the latter case, must be reviewed as soon as possible post facto). Antithesis will also perform a security review before introducing any new Trusted Third Party into our architecture.

Data Confidentiality Reviews: Any process that performs cross-Tenant data analysis can potentially compromise confidentiality and must be subject to a data confidentiality review prior to such analysis occuring.

Tenant Access Review: The Security Committee is responsible for maintaining a procedure for reviewing Antithesis employees who request access to particular Tenants. This review is responsible for verifying both that the employee needs the Tenant access for some purpose and that any agreements with the Tenant's associated Customer permit the employee's access.

Updating the Security Policy: This policy will be reviewed at least yearly and more frequently if recommended by the Security Committee. If the Security Committee approves updates material to Antithesis Customers, those Customers will be made aware of the updates through standard channels within 30 days. Antithesis is not obligated to provide advance notice of changes, either proposed or implemented.

Availability: The Security Policy will be available either on the public website or upon request from a current or prospective Customer.

Breaches of Security: The Security Committee is responsible for maintaining a procedure for reviewing potential breaches or vulnerabilities which may compromise our systems or customer data. Employees are expected to notify Management and the Security Committee promptly upon the discovery of any suspected vulnerability or breach. The Security Committee, then, is responsible for making sure that the vulnerability is mitigated and for investigating how to prevent similar incidents.

Notification of Security Breaches: The Security Committee is responsible for notifying any Customers impacted by a known security breach. Antithesis will notify any affected customer that a breach has occurred in no less than 72 hours from the confirmation of such breach, unless Antithesis has reason to believe that the breach was the result of the actions of a rogue employee of a customer. In this case, Antithesis will take steps to mitigate the vulnerability before notifying such customer, and will provide such notice within 72 hours of the mitigation of the vulnerability.

Security Requirements

Personnel

Antithesis' Employee handbook and training will make clear policies around the handling of Client data, including an obligation that each Employee read and agree to be bound by this

Security Policy. Antithesis will also provide annual training to each Employee with regard to the Security Policy, including any new or additional requirements. Just as the technical mechanisms will disallow cross-Tenant information sharing, Antithesis Employees are prohibited from violating the principle of confidentiality.

In practice, compromise of an Endpoint (workstation or laptop used by Authorized User(s) to interact with our system) can compromise confidentiality, integrity or availability. Each Tenant assumes responsibility to secure the Endpoints used by their own users. Antithesis engineering and professional services employees all run modern, fully-patched and hardened distributions of Linux and do not use root accounts under normal circumstances.

Data Storage, Handling, and Transmission

The Tenant boundary is again the most important for ensuring the integrity of client data. Antithesis takes all steps to ensure that Tenant data is never accessible to services which are not part of the Tenant or the TCB.

Communications between Endpoints and platform components must always be encrypted using an appropriate protocol that provides confidentiality and integrity. Communications between platform components must either be secured by encryption, by Cloud platform networking restrictions, or both.

Tenant data is stored and manipulated on various ISO 27001 certified third party compute providers, including Amazon Web Services and Google Cloud Platform. Consequently, these Cloud providers are Trusted Third Parties. When data is transferred between providers, into providers, or pulled from providers, secure channels will be used. Tenant data is handled with security best-practices, including but not limited to encryption at rest for long-term storage.

Consumer and Regulatory Compliance

Antithesis does not request, accept, or handle personal data or personally identifiable information. This policy is enforced through contracts with Customers. Accordingly, regulations governing proper handling of personal data (GDPR, HIPAA, CCPA, etc.) do not cover Antithesis's systems.

Antithesis personnel must not disclose, market, or otherwise contact Antithesis Customers outside of their work on behalf of Antithesis, either electronically or through other media, using information gathered through the provision and management of Antithesis services.

If one of the stated policies in this document is in conflict with a governmental regulation, the issue must be presented to the Security Lead for investigation and resolution.

To the extent the results of Antithesis' testing demonstrate a flaw or bug with respect to any open source software comprising a portion of the Customer's software, Antithesis may disclose such flaw or bug to the author of such open source software within thirty (30) days of discovery, unless a longer time frame is requested by the Customer, in which case the Customer and Antithesis shall work together in good faith to ensure disclosure of such flaws and/or bugs, but

wiithout jeopardizing the Customer's ability to address such flaws and/or bugs prior to such disclosure. In the event that Antithesis' testing finds a flaw or bug in any non-open source third party software, the Customer and Antithesis will work together in good faith to determine the appropriate disclosure of such flaws and/or bugs to the applicable third party, but without jeopardizing the Customer's ability to address such flaws and/or bugs prior to such disclosure. In the event of a conflict between this Security Policy and a Customer contract with respect to onward disclosures of open source software security flaws, the Customer contract shall control in all respects.

Data and Workload Isolation and Architecture

Pursuant to the core security goal of Isolation, Antithesis ensures that the only resources and tools available to multiple Tenants are in the TCB and vetted as such. Any other components are untrusted, and may only be deployed to Cloud resources which are specific to a single Tenant and only have network access, credentials, keys or ambient authority to interact with other resources specific to that Tenant, so that a malicious Tenant cannot compromise security goals with respect to any other Tenant. The tools that configure these deployments to ensure Isolation are part of the TCB.

Tenant data is stored and accessed only in cloud services such as Amazon S3 or Google BigQuery, where it is encrypted at rest and where access control configurations limit access to resources belonging to the Tenant, on Cloud resources specific to the Tenant, or transiently on Endpoints (for the purpose of reporting to Authorized Users of that Tenant).

Any system that processes Tenant data and produces non-Tenant data, (e.g. a test suite that evaluates new Antithesis Platform functionality against Tenant use cases and reports summary metrics), presumably is or has a component which is trusted. Accordingly it must be considered a part of the TCB and is subject to security review before deployment. Additionally this review must evaluate whether it meets our obligations to the Tenant(s) with respect to our use of knowledge derived from Tenant data.

Service Hardening

Antithesis develops *all* software components with attention to security best practices, and makes sure to patch security-critical dependencies in a timely manner. Nonetheless, Antithesis focuses its security auditing and secure development practices on TCB components, since these are the only components whose breach could result in a security compromise.

Antithesis relies on so-called *infrastructure-as-code* procedures for the deployment and maintenance of Cloud-hosted services. This allows Antithesis to easily track and replace resources in order to redeploy systems with updates and patches. Importantly, the infrastructure declarations have their changes tracked in order to simplify the review process. The absence of manually-deployed infrastructure makes it possible to reliably replicate our entire infrastructure for new Tenants. Because of its role in managing Tenants and Tenant boundaries, the infrastructure configuration is part of the TCB, and any changes to infrastructure declarations are subject to Security Regression Review before deployment, except those changes which

result from fully-automated systems which themselves are subject to security reviews.

Antithesis, according to industry best practices, fully locks down and secures its server operating systems. Only the minimum necessary set of applications and services are installed. Network-level access controls are used to restrict connections to necessary hosts on necessary services and log incoming requests. Given that servers can be deployed and replaced easily, Antithesis generally does not permit interactive user logins to production servers.

On those occasions where administrator action is necessary on a server, Antithesis makes sure to lock down administration using industry best practices. All administrator traffic is encrypted and logged.

Whether a server is involved in the TCB or wholly contained within a Tenant, Administrator Privileges are only granted on a “need to have” basis. The Security Committee is responsible for making sure that permissions are only granted to individuals who are already Authorized Users of the Tenant and who have demonstrated a need. Processes will be adopted that necessitate more than one person in the chain of approval for the granting of any new Administrator Privileges. The addition/removal of account access is auditable.

Access Controls and Privilege Management

In keeping with generally accepted best practices, Antithesis follows a principle of least privilege for all users and implicit users, including but not limited to personnel, Tenant compute resources, and internal services. Tenant access is restricted to short-lived temporary credentials which can be easily revoked when no longer needed.

Any Antithesis personnel who need access to Tenant resources must be approved by a representative of the Security Committee who is responsible for verifying that the access is required in order to maintain Antithesis systems or to perform services for a Tenant. Moreover, they must verify that granting access complies with any agreements with the affected Tenant.

Administrator Privileges in Tenant Cloud systems are restricted to pre-approved purposes (e.g. deploying updated infrastructure to Tenants or the TCB). No Antithesis personnel or other Users have Administrator Privileges associated with their “normal”, everyday accounts. Instead, Authorized Users wishing to exercise Administrator Privileges must manually and temporarily “escalate” their privileges for the duration of a login session. Such escalation is auditable and logged. Per recommended practice, so-called “root” accounts for Cloud providers are reserved for emergencies, require multi-factor authentication, and automatically notify Security Committee representatives upon access.

There are no services that make sensitive Antithesis or Tenant resources accessible to external users, including Customers. If and when Antithesis opts to create any such service, it will be designed with the principle of least privilege and other generally accepted best practices, and the Security Policy will be amended to account for it.