Customer Assurance Package

Welcome Letter

We know it's about trust

This welcome letter provides an overview of our approach and commitment to information security. After reviewing the letter, we strongly encourage you to examine all attachments provided in the selected Customer Assurance Package. Visit **https://about.gitlab.com/security/** to learn more about GitLab's ongoing commitment to information security and privacy.

Customer Assurance Packages

We developed our Customer Assurance Packages (CAP) as part of the GitLab trust journey to ensure that customers have self-serve access to key security resources. GitLab offers and actively maintains two packages:

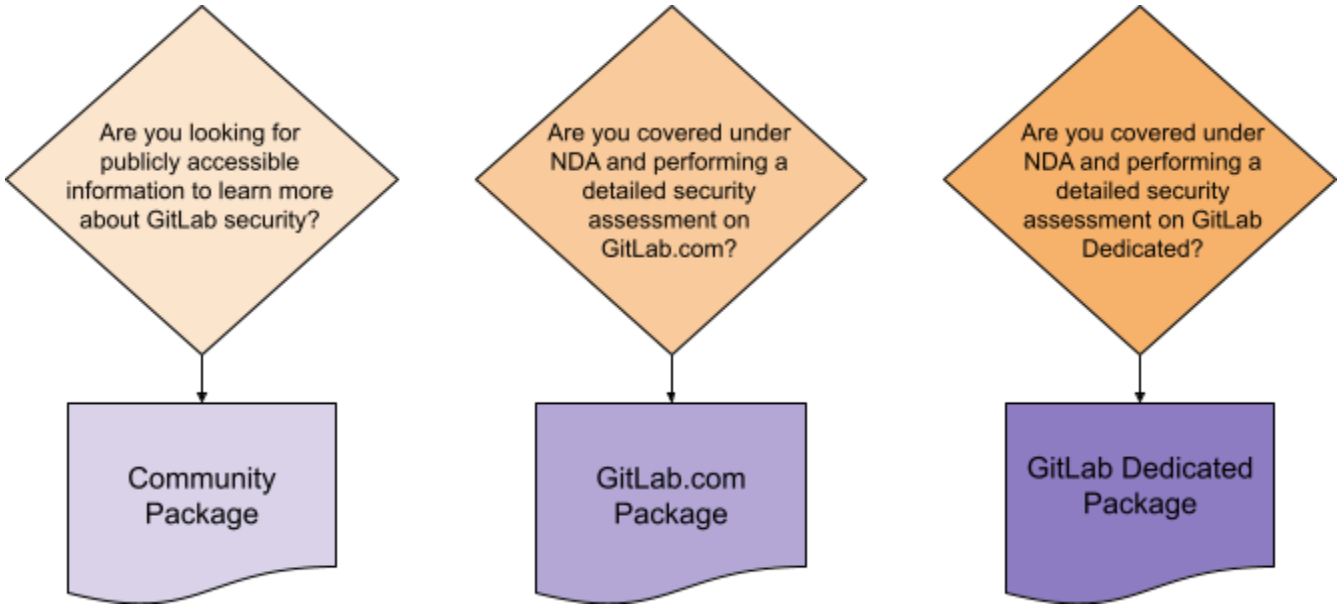
1. **Community Package:** The start of the trust journey, this package is a collection of publicly available documentation designed to introduce our approach to security.
2. **GitLab.com Package:** This package is designed to support both prospective and existing customers when completing security assessments on GitLab.com. *Due to the sensitive nature of the documentation, an NDA is required to be in place prior to sharing.*
3. **GitLab Dedicated Package:** This package is designed to support both prospective and existing customers when completing security assessments on GitLab Dedicated. *Due to the sensitive nature of the documentation, an NDA is required to be in place prior to sharing.*

GitLab Security Organization

At GitLab, we're committed to Information Security. It's our mission to be the most transparent Security organization in the world. Our Security organization is structured around four key tenets:

- **Secure the Product:** Our Security Engineering team ensures secure development and release practices.
- **Protect the Company:** Our Security Operations team prevents, detects, and responds to risks and events targeting the business and GitLab.
- **Assure the Customer:** Our Security Assurance team provides resources to help assure customers of the security of GitLab.
- **Lead with Data:** Our Threat Management team identifies, communicates, and remediates threats or vulnerabilities that may impact GitLab.

How to decide which package you need?



What's in the Customer Assurance Packages?

The GitLab Security Assurance team constantly works to provide our customers with greater confidence and visibility into GitLab information security practices by expanding and maturing our programs. One of our primary goals is to enable customers to meet their own regulatory requirements. See more details about our roadmap here: **GitLab Security Certifications, Reports, and Attestations**

Community Package Self attestations

- **PCI DSS Level 1:** Annual self assessment. Information security standard on the handling of credit card data.
- **ISO 20243-1:** Annual self assessment for GitLab.com and GitLab Self Managed. Guidelines that address specific threats to the integrity of software products throughout the product life cycle.
- **SIG Core:** Annual security questionnaire. Industry-accepted comprehensive set of questions used to assess third-party vendor risk.
- **CSA CAIQ Level 1:** Annual security questionnaire. Industry-accepted way to document which security controls exist in SaaS services, providing security control transparency.

- **FIPS 140-2 Attestation:** An attestation validating that all approved security functions within the GitLab FIPS package were configured to be conformant with all FIPS 140-2 requirements for transmissions, symmetric key functions and decryption, digital signature, message authentication, and hashing.
- And more!

GitLab.com Package

- **SOC 2 Type 2:** Annual third-party audit report that includes detailed testing results focused on non-financial reporting controls as they relate to *Security*, *Confidentiality* and *availability*.
- **SOC 3:** Annual third-party audit report that includes a synopsis of non-financial reporting controls as they relate to *Security*, *Confidentiality* and *availability*.
- **Google Cloud Platform (GCP) SOC 3:** Hosting provider's annual third-party audit report that includes a synopsis that is focused on non-financial reporting controls as they relate to *security*, *confidentiality* and *availability*.
- **BitSight:** Third-party security scorecard with ratings that provide data-driven, dynamic measurements of an organization's cybersecurity performance.
- **ISO/IEC 27001:** Annual third-party audit summary report that contains out of scope controls and any open non conformities (if applicable).International standard for information security management systems, cloud security and data protection.
- **External Penetration Test Report:** Third-party assessment of our application and network security postures by external security experts.
- **Business Continuity Report:** Annual exercise testing our Business Continuity processes and our capacity to recover after a business-impacting event.
- **TISAX**: Annual self assessment. Relative to the European Automotive Industry.
- And more!

GitLab Dedicated Package

- **SOC 2 Type 1:** Point in time third-party audit report that includes detailed testing results focused on non-financial reporting controls as they relate to *Security* and *Confidentiality*.

- **Amazon Web Service (AWS) SOC 3:** Hosting provider's annual third-party audit report that includes a synopsis that is focused on non-financial reporting controls as they relate to *security*, *confidentiality* and *availability*.
- **ISO/IEC 27001, 27017, 27018:** Annual third-party audit summary report that contains out of scope controls and any open non conformities (if applicable) to maintain certification. International standard for information security management systems, cloud security and data protection.
- **GitBITS:** One page product focused documents that can be quickly and easily consumed.
- And more!