snyk

Business Continuity and Disaster Recovery Customer Overview for multi-tenant SaaS

Snyk Confidential V3:2023:CSA

As a provider of secure development tools, Snyks priority is to maintain a safe and secure environment for its service provision.

To ensure the highest level of security and resilience Snyk is continually investing in the overall information security program, resources and expertise that are required to ensure the continued service provision in adverse situations.

RESPONSIBILITIES

Snyks Resilience Director is the accountable owner for application and information continuity.
Individual components and tasks of the business continuity are owned by specific functions and teams, which are monitored and tested as part of our ongoing business continuity and resilience processes.

The following roles within the organization are responsible for reviewing and accepting the content of this policy and raising any issues they may see with any part of the programme at any time:

- VP of Engineering
- Business Resilience Director

BUSINESS CRITICAL INFRASTRUCTURE

Hosting

Snyk utilizes data centers managed by Google and AWS. Google and AWS have many years of experience in designing, constructing, and operating large scale data centers. This experience has been applied to the GCP and AWS platforms and infrastructure. The data centers are housed in nondescript facilities, and critical facilities have extensive setback and military-grade perimeter control berms as well as other natural boundary protection.

For additional information regarding specific security controls and the GCP & AWS compliance certifications see: https://cloud.google.com/security/ , https://aws.amazon.com/security/

Application Servers & Load Balancers

Snyk adopts a Cloud Native strategy by utilizing Kubernetes clusters, along with elastic load balancers hosted in Virtual Private Clouds, and does not manage or handle any hardware for maintaining its production environment. To keep the production environment running with high availability Snyk employs a combination of provisioning, redundancy, load balancing, and elasticity practices as described below.

Provisioning. The entire suite of Snyk's application host pools is provisioned by scripted automated infrastructure launching tools. This enables the building or relocation of a deployed environment to be as simple as a click of a button, while being managed as code for proper change management and audit purposes.

Redundancy. Each logical pool of application servers is fully redundant with at least three servers active at any given time. Servers do not maintain state, making the addition or removal of a server from the pool a trivial and automated task.

Elasticity. Furthermore, to prevent reduced or limited access to the various Snyk services, server pools automatically expand and shrink to meet request demands using Auto Scaling Groups, and traffic is distributed between the servers using elastic load balancers.

Multi Availability Zones. In addition to the numeric redundancy of deployed pools, each pool consists of servers in three availability zones, which translates to three physically separate locations across GCP's / AWS's data centre, enabling the continuity of Snyk services even in the unlikely event that one of GCP / AWS data centers becomes unavailable.

Database Servers

Snyk uses Google Cloud SQL / AWS RDS for database server management. To keep the production database reliably running, Snyk employs a combination of redundancy, hot-standby, snapshots, and point-in-time backups.

Redundancy & hot-standby. Each Google Cloud SQL / AWS RDS deployment includes a mirror replica setup as a hot-standby with data synchronized up to the speed of shipping data increments between GCP / AWS data centers. The Google Cloud SQL / AWS RDS service is set up for auto-failover allowing a seamless takeover of the hot-backup in case the master instance fails. Furthermore, the mirrored replica resides in a separate GCP / AWS availability zone, and availability zones are physically separate in GCP's / AWS's data centre, enabling the continuity of Snyk services even in the unlikely event that one of GCP / AWS data centers becomes unavailable.

Snapshots & point-in-time backups. Full database snapshots are taken daily and stored with a minimum retention of 90 days. Each snapshot is propagated to multiple GCP / AWS cloud storages in multiple availability zones and in multiple regions. Daily backups provide a last resort recovery in case of massive data corruption or loss.

Firewalls, Routing, and Networking

Snyk uses VPC in both AWS and GCP to enforce network routing, Akamai WAF has been used as an application layer firewall for both AWS and GCP.

Routing. Snyk uses GCP'S / AWS's VPC firewalls to enforce network routing, and follows these guidelines:1) Access is granted using the principles of Least Privilege.2) Thin external environments with general internet connectivity precede internal environments with impactful web services and databases.3) Production environment is hosted completely separate from any other non-production environments on GCP / AWS. This further reduces side effects impacting these environments such as temporary routing misconfigurations.

Firewalls. WAFs are used to reduce the chance of a disaster by further restricting routed traffic based on application level attack patterns. Common attack vectors such as SQL injections, cross-site scripting, and other attacks are filtered at the WAF level and never reach the web server.

Networking. All Snyk DNS entries point to a CDN, load balancer, or other reverse proxy. This means that traffic routing to all core application servers are either non-accessible from the web, or accessible by strictly knowing their IP which is otherwise held confidentially. By these means, the impact of a DOS (denial of service) or DDOS (distributed denial of service) is limited to the CDN or load balancer's ability to grow in scale to absorb the attack. In addition, Snyk uses the services of Akamai, which on top of acting as a reverse proxy, employ request level filtering for all traffic and thereby protect against Web Application and DoS attacks.

DNS

Snyk uses Akamai for DNS services. Using Akamai DNS makes it easy for Snyk to manage traffic globally through a variety of routing strategies that include: Latency Based Routing, Geo DNS, and Weighted Round Robin. Combined with DNS Failover, Snyk's customers get routed to the closest available Point of Presence (POP) for the fastest possible response times.

DATA BACKUP, RETENTION and RESTORE

Snyk holds great value in maintaining the highest standards of data security. A detailed outline of the backup, retention and restore policies is listed below.

Data Backup

Snyk employs several separate methods of data backup, each with the ability to address different types of disasters or unavailability.

Hot Standby. At any given time every database has a mirrored database server acting as a hot standby, deployed in a separate availability zone, with automatic failover in case the master becomes unavailable. This guarantees the continued availability without data loss in case the master database server becomes unavailable or in the unlikely event the entire datacenter of the master server becomes unavailable.

Snapshots. Snyk stores a full copy snapshot of the entire database. The copies are propagated into multiple storage buckets across multiple availability zones and regions, making them available for use even in the unlikely event that one of the data centers becomes unavailable. Snapshots are used as a last resort to restore a database to a time where it is known to be consistent and coherent. Snyk retains 7 daily backups and 13 weekly backups.

Data Retention

The table below outlines our data retention policies

Type	Data retention period
Postgres Database daily snapshots	Minimum 90 days
Production application log files	Minimum 90 days
Production audit logs	Minimum 90 days

snyk

Data Restore

Snyk replicates data to a testing environment in order to carry out data restoration drills on a Production like environment. During these restoration drills, various levels of restores from a Compose snapshot are practiced.

The purpose of the drill is to evolve the skill set required in the restoration process. The drills are executed by either the Cloud Platforms team or a cross set of engineers within R&D.

SOFTWARE

Most of Snyk's Intellectual Property is embedded within the application itself, and includes the user experience, architecture, and deep analysis of the package management life cycle for each ecosystem. Snyk maintains all efforts to keep access to the code restricted to the core engineering team that owns the application or service.
Irrespective of the Intellectual Property embedded in the code, it is also clear that some company wide disasters may occur by the introduction of improper code, be it with malicious intent or not.

Distributed Code Repository

Snyk uses Git as their distributed version control system, and Github for a central host and management of said repos. This means that at any given time full replicas of the codebase exist, both on Github and on employees' computers. The implication of this is that there is practically no chance of accidental loss of the codebase. Even if Github as a hosting provider were to become unavailable, setting up another remote host can be undertaken quickly.

To help make sure that only relevant personnel have access to the codebase, a few of the key features of Github are employed:

- Sensitive company repos are always private
- Access to the company repos is by invite only
- Authentication of users on Github requires MFA (multi factor authentication)
- Github access is fronted by Okta for authentication

Quality Control

Since the most likely root cause to reduce service availability to customers is the deployment of new malfunctioning code, Snyk employs the following quality controls:

- Every new feature mandates writing automated tests to validate it.
- Every changeset committed needs to be explicitly approved by a member of the code review committee before it can be merged back into the main branch.

- Every changeset committed to the code base is verified against an elaborate test suite of automated checks. Upon failure of one of the tests, the commit is rejected.
- Code is first deployed in a QA environment, where other members can test it before promoting the changes to the Production environment.

Deployment Roll Back/Forward

In the event that code that has passed all the aforementioned quality control measures still impairs the functionality or availability of Snyk's services, Snyk's deployment tools allow for one click roll back to the previously working version.
Debugging is then performed using readily available logs and debugging tools. Post bug fix, a root cause analysis of how the bug passed the quality control measures is performed. Actions are documented with owners and dates. Updates to processes and technology are made accordingly.

DISASTER AND INCIDENT MANAGEMENT

Snyk has implemented an incident management policy and associated processes in line with ISO/IEC 27001:2013 which is externally reviewed on an annual basis, as part of its ongoing certification process.

At a high level the policy and processes define 5 stages as follows:

Preparation - Define and refine processes, train skills, identify and repair gaps in logging or monitoring capabilities

Detection and reporting - Monitor events, identify concerning patterns and raise alerts. Route these alerts to the right people, quickly and reliably, waking up the right on-call if needed

First response / Triage and escalation - First impressions - how bad is it and who is needed immediately to help contain and remediate? Is there a customer or security impact? Are lives or facilities at risk? Prioritize the incident and escalate as needed

Containment and remediation - Confirm the blast radius, stop it getting worse, then make it better. Get customer service levels back to an acceptable baseline as quickly as possible.)

Post-incident actions - Stand down the response team, close the incident and schedule a retrospective. Replace temporary fixes with permanent ones. Have a retro and build a Root Cause Analysis. Spin off any actions into team backlogs or new projects, they're not for incident management

Key Personnel

In the case of an incident Snyk has implemented a clear division of roles and responsibilities to handle the operational responses needed during such an event.

The individual teams that may be involved in creating an Emergency response team (ERT) as well as a Disaster Recovery Team (DRT) are as follows:

- **Engineering** - Directly respond to incidents involving our production systems
- **CIS** - Directly respond to incidents involving our Corporate IT systems and support comms systems
- **InfoSec & Risk** - Directly respond to cybersecurity attacks and data breaches, facilitate processes generally
- **Procurement -** Directly respond to supply chain incidents
- **People** - Directly respond to incidents impacting people and facilities
- **Legal** - Escalate to regulators and help reduce the legal risk of any communication or action
- **Customer Success** - Manage communications and impacts with customers
- **Marketing** - Help craft public communications to manage the reputational impact

In addition to the above, specific roles within the incident management/ERT team are as follows:

Incident Lead

This person takes over responsibility and decision making for the incident. They will primarily focus on communication throughout the incident and help facilitate the necessary fix and next steps. They have the authority to make final decisions and can (if necessary) overrule the group to ensure momentum is maintained.

They are also responsible to ensure everything that is useful and needs to be preserved to help with post mortem, is preserved. All communication goes via the lead.

Tech Lead

This person takes the responsibility for the technical investigation into what's wrong, why and how we can fix it. They work alongside the Incident Lead to ensure a fix is reached in a timely manner.

snyk

Incident Investigator/s

This person/s takes responsibility for learning from an incident. Ensuring we take the opportunity to learn as much as possible from what happened. They are accountable for a post incident report (aka post mortem document), and group engineering weekly discussions. They may also run retrospective sessions and/or interviews to build an understanding. They will make recommendations of actions to team lead(s) or directors who then become accountable for converting to actions (or not).

Emergency Response

Triggering Events. Key triggering events that would lead to activation of a disaster recovery plan are as follows:

- Total loss of availability of Snyk application website (https://app.snyk.io)
- Total loss of availability of Snyk corporate website (https://snyk.io)
- Total or partial loss to services available in the platform within the production environment, resulting in customer impact
- Total or partial data loss in the production environment

This list is not exhaustive; Any anomalous condition that may result in or lead to a service degradation or outage will trigger the incident management processes to ensure intervention to avert disruptions or restore service to operational status.

Assembly Points.
Assembly points at each company office have been determined.

Activation of Emergency Response Team. When an incident occurs the ERT are activated. The ERT will then decide the extent to which a disaster recovery plan (DRP) must be invoked. All employees are communicated to and provided with appropriate levels of guidance around the incident. The key activities of the ERT team are to::

- Respond immediately to a potential disaster
- Assess the extent of the disaster and its impact on the business, data center, etc.
- Establish and manage disaster recovery team to maintain vital services and return to normal operation
- Ensure employees are notified and allocate responsibilities and activities as required.

Disaster Recovery Team

The Disaster Recovery Team (DRT) will be contacted and assembled by the ERT. The team's responsibilities include:

- Restore key services within 4 business hours of the incident
- Recover to business as usual within 8 to 24 hours after the incident
- Coordinate activities with the disaster recovery team, first responders, etc.
- Regularly report to the emergency response team
- Collate any useful evidence and document recovery process for post mortem

Communication Strategy

Internal Communication. Upon initial identification of an incident, the ERT will notify all company personnel of the event using the company wide email distribution list as well as company wide slack channel. Specific incident slack channels are created in order to have a mechanism to audit and track incidents during their lifecycle. An incident workflow slackbot automatically sets up the entire incident workflow with key roles identified such as Incident Commander and Technical Lead, the current status of the incident, when the incident is closed, etc. After the incident, the Root Cause Analysis / Post Mortem is archived with the incident channel. At least hourly status updates will be sent using the same distribution list and slack channel until the business has been restored to usual.

Customers. In case specific customers are impacted due to the disaster, the Senior Customer Success Manager present will be the key personnel responsible to construct and deliver a message using their discretion for the medium (email, phone, other) and time of the notification.

Availability Dashboard. Snyk maintains a dashboard of services and their current status (operational/down) at all times at https://status.snyk.io

Root Cause and Containment

The DRT's first mission is the containment of the incident to prevent further spread of the damage. Immediately upon containment, the DRT will investigate the root cause of the incident and offer short term and long term remediation plans.

The DRT will produce a post mortem report containing the points as depicted below and deliver it to the appropriate level of leadership depending on the type of incident that has occurred. Lessons learned from the report will be incorporated into the company infrastructure and the disaster recovery training.

- Nature of the incident: what were the symptoms?
- Discovery: how discovered, and by what system/personnel?
- Containment: - Investigative steps taken to determine quickest containment route - Actual containment plan taken
- Root Cause: investigative steps to analyze root cause
- Remediation plan: short term and long term actions proposed

Self-reflection:

- How can the impact of the incident be reduced?
- How could containment time have been improved?
- What alternative containment plans should have been considered?
- How could the incident have been detected earlier?
- How could the incident have been mitigated automatically?

TESTING, TRAINING AND EXERCISES

Plan Maintenance

This document is to be updated annually to make sure it accurately represents the infrastructure and processes currently active in the company's portfolio. In addition, the document will be augmented with lessons learned after any of the following:

- A company initiated disaster recovery plan exercise
- Major infrastructure changes or additions
- Change to any of the related data security policies
- A real incident

Exercises

Disaster recovery plan exercises are an essential part of the Snyk continuous improvement process.

The aim of all exercises is to ensure Snyk identifies:

- What needs to be improved
- How the improvements can be implemented.
- Ensure emergency & supporting teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Disaster recovery plans will be performed annually. The scope of the disaster and simulated impacted infrastructure will be chosen based on the combination of likelihood of an incident and the readiness of the team to react.

COMPLIANCE

Snyk is responsible for ensuring appropriate continuity and availability controls as detailed in this document and externally validated as part of our ongoing ISO 27001:2013 compliance and ISAE3402 SOC2 Type II reporting.