platform.sh

Security assurance plan

For updated and additional information, please visit

https://platform.sh/trust-center/

Table of content

1. Introduction

1.1 Purpose of the document

This document constitutes the Security Assurance Plan (SAP) and describes the provisions in terms of information system security that Platform.sh undertakes to implement to meet the customer's security requirements throughout the duration of the contract. The SAP defines in particular the security organization put in place, as well as the technical and organizational measures implemented.

2. Security management

2.1 Information security policies

Platform.sh has created and enforced numerous internal information security policies and procedures to ensure that employees comply with rules and guidelines related to information security. These policies and procedures are designed to cover core aspects of information security: **confidentiality, integrity, and availability**.

Some of the internal policies and procedures include:

Anti-malware and software update policy	Business continuity and disaster recovery plan
Cryptographic controls and key management policy	Data breach policy
Data destruction policy	Data retention policy
Engineering and Operations Change Management	Firewall implementation reference
Firewall policy	Logging and monitoring policy
Password policy	Password reset policy

Payment Card Industry Data Security Standard (PCI DSS) policy	Risk management policy
Security hardening process	Vendor management policy
Vulnerability scanning and penetration testing policy	Vulnerability severity and remediation policy

2.2 Security incident management

The Platform.sh global Platform-as-a-Service (PaaS) is monitored, maintained, and secured in a follow-the-sun manner 24 hours a day, 7 days a week, and 365 days a year. Security Operations Center (SOC) activities are shared amongst the Platform.sh Support, Operations, Security Operations, and Crisis teams. In addition, should Platform.sh become aware of a security incident — such as an active or past hacking attempt, virus or worm, or data breach — senior personnel including the Chief Technology Officer (CTO) are promptly notified.

The security incident response procedures include isolating the affected systems, collecting forensic evidence for later analysis including a byte-for-byte copy of the affected system, and finally restoring normal operations. Once normal service is restored a root cause analysis is performed to determine exactly what happened. A Reason for Outage report may be provided to the customer upon request that summarizes the incident, cause, and steps taken.

Platform.sh cooperates with relevant law enforcement and depending on the type of incident the root cause analysis may be conducted by law enforcement rather than Platform.sh personnel.

Platform.sh endeavors to notify affected customers within 24 hours in case of a personal data breach and 72 hours in case of a project data breach.

Under the European General Data Protection Regulation (GDPR), Platform.sh is required to notify our supervising authority within 72

hours of a discovered breach that may result in a risk to the rights and freedoms of individuals. Our supervising authority is the French Commission Nationale de l'Informatique et des Libertés (CNIL).

2.3 Continuous improvement

The continuous improvement process implemented by Platform.sh uses feedback from several activities to inform decision making regarding improving our PaaS and the processes that support it. Activities providing feedback to continuous improvement include:

Risk assessments carried out by Platform.sh	Internal audits carried out by Platform.sh
External audits carried out by third parties	Support and security incidents
Daily administrative activities	

3. Security in human resources

3.1 Contractual aspects

3.1.1 Employees and contractors

In order to provide appropriate protection of its information assets, Platform.sh ensures that background evaluations of employees and contractors are conducted prior to granting them access to sensitive Platform.sh information. All background checks honor country employment practices. The activities conducted as part of the background evaluation are proportional to the sensitivity of the individual's position.

New employees sign an employment contract that defines their responsibilities with regard to the company's personal data. These clauses apply both during the term of this contract and after its termination.

Platform.sh employees are obliged to safeguard the availability, confidentiality, and integrity of personal data. It is forbidden to send customer data or the company's personal data outside Platform.sh. All data on Platform.sh systems is by default considered confidential.

3.1.2 Third-party service providers

Platform.sh performs a thorough due diligence process for all its third-party providers. Platform.sh decided to adopt the EU Commission's official, standardized template of an Article 28 DPA. By adopting the EU Commission's template, as suggested by Article 28(7) of the GDPR, we assure the strictest data protection coverage. We also use the official, standardized, module-based SCC templates as required by the European Commission, and choose the appropriate module based on the parties' relationship.

3.2 Security awareness

As a part of the onboarding process, and annually thereafter, Platform.sh employees undergo security awareness and secure coding training.

The security awareness and secure coding programs include the following topics:

Security incident procedure	Social engineering
Phishing	Malware
Physical security	Network security
Password management	Use of confidential information
Data breach	Security by design
Risk assessment	Attack surface

Threat modeling	Development and security
Change management	Testing

4. Endpoint security

Workstation security

All Platform.sh employees are required to comply with the acceptable use policy, password policy, and remote working security recommendations for prevention and mitigation of data loss as well as loss of the computer and mobile device.

All employee workstations are required to have the following in place:

Password protected / Auto-login disabled	Full disk encryption
Screen saver enabled and configured to lock after 10 minutes	Firewall enabled and configured for as limited access as needed
Company approved antivirus solution	Utilization of a password manager for non-Single Sign On (SSO) applications

Infrastructure host security

The Platform.sh PaaS utilizes a proprietary malicious activity monitoring solution that logs, monitors, and alerts on host and container activity related to:

Privilege escalation	Privilege escalation via administrative syscalls
Filesystem tampering	Network access

The malicious activity monitoring solution is PCI DSS compliant and reviewed annually by third party auditors.

5. Access control

5.1 Platform.sh access management

Customer data is protected by limiting internal access and preventing unauthorized access by implementing security measures such as encryption of data in transport and at rest. Customer data is only accessed internally for support reasons at the customer's request, or to fix or prevent an outage. Additionally, access control lists of Platform.sh employees with access to customer data are reviewed monthly.

Data disclosure

Customer data is not disclosed to third parties unless legally obligated to do so under certain circumstances such as a law enforcement request.

5.2 Customer access management

Customers have multiple ways to manage access to the environment(s) they host on Platform.sh. Granular access can be managed and scoped to include:

Organization-level access permissions, including:	• Billing • Plans • Users • Project create/list • Admin • Viewer
Project-level access permissions, including:	• Admin • Viewer
Environment-level permissions	• Admin • Contributor • Viewer
Source integrations for GitHub, GitLab, Bitbucket	

5.3 Connection protocol

`Data in transit`

Data in transit between the world and Platform.sh is always encrypted as all of the sites and tools which Platform.sh supports and maintains require Transport Layer Security (TLS) or Secure Shell Protocol (SSH) to access. This includes the Platform.sh Console, Accounts site, git repositories, documentation, and help desk.

Data in transit on the controlled internal networks of the PaaS (for example, between the application and a database) may or may not be encrypted, but is nonetheless protected by private networking rules.

Regarding customer applications, data in transit between the world and customer applications is encrypted by default. Only SSH and Hypertext Transfer Protocol Secure (HTTPS) connections are generally accepted, with HTTP requests redirected to HTTPS. Users may opt-out of that redirect and accept HTTP requests via routes.yaml configuration, although that isn't recommended. By default HTTPS connections use an automatically generated Let's Encrypt certificate or users may provide their own TLS certificate.

Data at rest

All volumes that contain customer application data are encrypted at rest by default using encrypted storage (typically using an AES-256 block cipher). Some Dedicated Gen 2 clusters and the FR-3 region do not have full encryption at rest.

Customers with specific audit requirements surrounding data at rest encryption, may contact support with questions.

5.4 Access review

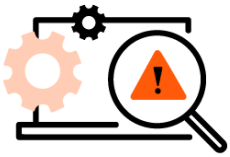
Role-based access control and the principle of least privilege are used to define and grant employee access to the PaaS and its underlying services and components. Access control lists of Platform.sh employees with access to customer data are maintained and monitored. All changes to access control lists go through an approval process by the system owner and are monitored and reviewed on a monthly basis. Additional alerting exists for changes to sensitive groups.

6. Physical security of premises

The Platform.sh PaaS service is entirely cloud native, as such, it is the responsibility of the individual Infrastructure-as-a-Service (IaaS) providers involved in the delivery of the PaaS service for maintaining the physical security of the data centers where the PaaS regions run.

Compliance information pertaining to the IaaS providers upon which the Platform.sh PaaS runs can be found on their respective websites or linked from the Platform.sh Trust Center website.

7. Operational safety



7.1 Flow filtering

7.1.1 Web Application Firewall (WAF)

Enterprise and Elite projects on Platform.sh come with a web application firewall (WAF) at no additional cost. This WAF monitors requests to customer applications and blocks suspicious ones. It helps protect customer applications from attacks such as distributed denial of service (DDoS) attacks.

Protections applied by the Platform.sh WAF include:

CRLF injection prevention	Request smuggling
Header injection	Response splitting
HTTP protocol enforcement	Uniform Resource Identifier (URI) syntax
File upload limit	File extension restriction
Disallowed requests and headers	Slowloris DDoS attack prevention

7.1.2 IP Filtering

IP flow filtering is a shared responsibility between Platform.sh and our customers. Some highlights of Platform.sh's responsibility regarding firewall security:

- Only a small number of ingress ports are allowed open to customer environments, e.g., 22, 80, 443
- Using Infrastructure-as-Code-based configurations, only approved ports and services are open across the internal infrastructure of the PaaS
- Hosts are deployed using Infrastructure-as-Code-based firewall configurations that enforce pre-approved ports and services by host role
- Infrastructure-as-Code firewall configurations are reviewed and approved by Platform.sh Security and Operations teams twice a year per PCI DSS requirements
- A comprehensive vulnerability management program has been designed to maintain the security of the PaaS infrastructure, e.g., secure development, vulnerability scanning, network segmentation testing, penetration testing, and patch management
- The vulnerability management program is compliant with PCI DSS requirements and is audited by a third party annually

IP filtering options available to customers' include:

- The use of routes (INGRESS) to define which application(s) are exposed to the internet
- The use of HTTP access control IP filtering (INGRESS) to control access to their environments
- The use of customizable outbound firewalling options to limit outbound traffic using the outbound key in the

applications .platform.app.yaml file (EGRESS) (elite and enterprise customers only)

- The use of relationships (INTERNAL) to allow multiple services to communicate with each other internally
- How the customer defined configurations above become a part of the running configuration for their environment can be summarized as follows:
    + Our customers describe (in their configuration files) a direct graph of services. Something like "this application is connected to this database and this queue", or "this other application is connected to this queue and this cache", or "this application is able to receive HTTP requests from this domain". This is what we call describing the "relationships". We dynamically transform this directed graph into pairwise stateful firewall rules (realized by IPTables). If there is a relationship between container A and container B, container A gets an outbound rule allowing the IP of B, and container B gets an inbound rule allowing the IP of A.

7.1.3 Intrusion Prevention System (IPS)

Currently, the PaaS does not offer the possibility to activate/deactivate Intrusion Prevention System (IPS) on demand. On Platform.sh's side, there is no automatic IP or range blocking. Blocking IP's (or not) is usually left to the appreciation of the on-call engineer based on the specific circumstances. Customers have the option to apply HTTP access control for their environments at any time.

7.2 Hardening configurations

System and service hardening is a security best practice, and several steps have been taken to harden the services that make up the

Platform.sh PaaS solution. Some examples of the hardening practices in use by the PaaS are:

- A hardened kernel, e.g., only required modules are enabled, KASLR, PTI
- Kernel Common Vulnerabilities and Exposures (CVE) are reviewed weekly and security patches are deployed according to policy
- Unprivileged user namespaces are disabled
- Administrative capabilities are dropped within the container environment, e.g., cap_sys_admin, cap_net_admin
- The host file-system is designed to be read-only
- Operations are performed without using root and are fully automated. All operations are logged
- Only the services required to support customer workloads are enabled at the host level
- Only the specific services required by a customer application are enabled within its containerized environment
- The software images used by the services are updated regularly using a reproducible build system which ensures the latest packages, and their dependencies, are used. The build system uses GNU Privacy Guard (GPG) signed packages that are validated at build time
- The grid and dedicated infrastructure undergoes third-party network segmentation testing twice a year and penetration testing annually

7.3 Applying security updates

The Platform.sh Rule: **Update Early, Update Often**

Platform.sh periodically updates container images for the latest security updates from upstream providers. (PHP versions, Ruby versions, MariaDB versions, etc.). These do not always happen immediately but when a security vulnerability is identified and released it tends to be fairly soon after.

However, these updates aren't automatically propagated to individual projects as that would involve potential customer downtime. Instead, the latest available version of every requested container is loaded on each deploy to a given environment. After a deployment customers are always guaranteed to be running the latest Platform.sh-provided version of a container.

If customers use Platform.sh-provided Let's Encrypt TLS certificates, their site is automatically redeployed approximately once every two months to ensure it always has an up to date certificate. That also ensures container versions are up to date at the same time.

7.4 Remote Connections

Platform.sh secures remote access to its infrastructure in several ways:

- Virtual Private Network (VPN) must be established to one of the Platform.sh managed regional endpoints
- VPN establishment requires successful multi-factor authentication
- Access authorization for the administrator is validated by the destination host as a part of our proprietary remote access protocol
- Remote administration requires access to proprietary tooling

- Remote administration activity is fully logged

Customer remote access is secured in the following ways:

- Three methods to connect:
    + Platform.sh Command Line Interface (CLI)
    + Application Programming Interface (API) token
    + SSH via Public Key authentication
- All data encrypted in transit by default
- Granular individual remote access management defined in three ways:
    + Organization-level
    + Project-level
    + Environment-level
- Mandatory SSO dashboard access with a third-party identity provider (IdP), including Google and OpenId Connect (elite and enterprise customers only)
- Multi-factor over ssh (elite and enterprise customers only)

7.5 Logging

Application logs

Application logs are those generated by the host application or application server (such as PHP-FPM). These logs are immutable to customers to prevent tampering. They are also secured behind key-based SSH so that only the customer and our relevant teams have access.

System logs

Platform.sh records routine system logs. Customer-specific system logs or the customer environment are not accessed unless one of the following situations applies:

1. There is a request to do so by the customer,
2. To fix a problem or outage,
3. To prevent an outage, or
4. To comply with a legal obligation.

Access logs

There are two main types of access logs: Web and SSH.

Web access logs

Application access logs are immutable to customers to prevent tampering. These logs are secured behind key-based SSH so that only the customer and our relevant teams have access.

SSH access logs

SSH access logs are securely stored in our infrastructure and aren't accessible to customers. These logs can be accessed by Platform.sh support personnel as part of an audit, if requested.

Access by customers and Platform.sh support personnel to customer environments is logged. However, to protect customer privacy, only the connection itself is logged, not what was done during the session.

Vendor data sharing

All data collected and shared with vendors has been identified and is monitored including to which geographical destinations such data is transferred. All vendors have been assessed for security and GDPR compliance. Relevant Standard Contractual Clauses (SCCs) and Data Processing Agreements (DPAs) are in place where applicable.

Log shipping

Customers can ship application and service log files to external 3rd party endpoints and services supporting syslog protocol to surface and identify issues on all their applications running on Platform.sh in a single log repository of choice.

The supported external endpoints are:

- Splunk, New Relic & Sumologic on the Grid and Dedicated Generation 3 (both via CLI and from within the Console)
- Datadog, Loggly, LogDNA, Parpertrail & Logz.io on the Grid and Dedicated Generation 3 (both via CLI and from within the Console)
- Rsyslog on Dedicated Generation 2 (only via CLI)

Fastly log shipping

When customers use a Fastly content delivery network (CDN), forwarding CDN logs to a third-party service can help diagnose caching issues, and therefore improve their site's overall performance.

Security information and event management (SIEM)

The Platform.sh PaaS infrastructure logging, monitoring, and response features include:

- Ingress network activity (HTTP/SSH) is logged in a central location for monitoring, reporting and incident response
- Egress network activity from customer environments is not logged due to privacy constraints
- Administrative activity within the PaaS infrastructure is fully logged in a central location
- Platform.sh Operations, Security Operations, and Crisis Team maintain 24x7x365 on-call response to alerts from purpose-built monitoring tooling

- Our logging, monitoring, alerting, and response practices are PCI DSS compliant and audited by a third party annually

7.6 Service Supervision

The Platform.sh PaaS has the following service supervision features:

- 24x7x365 follow-the-sun monitoring of all critical PaaS components
- SOC activities are shared amongst the Platform.sh Support, Operations, Security Operations, and Crisis teams
- Incident management is guided by a best-of-breed SaaS solution that is integrated with multiple enterprise systems
- Root cause analysis is performed and reviewed after each incident
- Service outage response procedures are formally tested and reviewed throughout the year and at least annually

7.7 Data Backup, Data Retention, and Data Restore

Backups of environments running on Platform.sh PaaS have the following features and options:

- Backups include the environment's complete data but exclude code. To restore code to its previous state when the backup was taken, use Git commands such as revert.
- Backups include all persistent data from all running services and any files stored on mounts. The snapshot is stored internally and can't be downloaded.

- Only for active environments can backups be created and restored. Inactive environments must be activated in order to have backups created.
- By default, creating a manual backup causes a momentary pause in site availability so that all requests can complete. This means the environment is backed up in a known consistent state. The total interruption is usually only 15 to 30 seconds. Any requests during that time are held temporarily, not dropped.
    + To avoid this downtime, the use of live backups are recommended.
    + For consistent backups, the scheduling of backups during non-peak hours is recommended.

Data backup locality

Customer application and data, including backup data, does not leave the region. Each region has its own storage cluster that holds customer application data. The only time the data is copied from the storage cluster is during the backup process. The backup is stored in object storage in the same region as the storage cluster and application.

Dedicated backups and retention

Platform.sh takes a byte-for-byte snapshot of Dedicated Gen 2 production environments every 6 hours. Backups are retained for different durations depending on when they're taken.

Backups are created using snapshots saved to IaaS block storage volumes. A block storage snapshot is immediate, but the time it takes to write to the storage service depends on the volume of changes.

- Recovery Point Objective (RPO) is 6 hours (maximum time to last backup).
- Recovery Time Objective (RTO) depends on the size of the storage. Large block storage volumes take more time to restore.

These backups are only used in cases of catastrophic failure and can only be restored by Platform.sh. A support ticket must be opened to request a restoration.

The restoration process may take a few hours, depending on the infrastructure provider in use. In the ticket, customers can specify backups of files, MySQL, or both. Uploaded files are placed in an SSH-accessible directory on the Dedicated Gen 2 cluster. MySQL is provided as a MySQL dump file on the server. MySQL dump files may be restored at any time. Platform.sh support will not overwrite production sites with a backup; customers are responsible for determining a "safe" time to restore the backup, or for selectively restoring individual files if desired.

Customers are free to make their own backups using standard tools (mysqldump, rsync, etc.) at their own leisure.

Backups for Dedicated Gen 2 environments are retained based on when they were taken.

Grid backups and retention

On Grid environments, non-Production environments can have up to 4 manual backups. Other important backup details, like RPO and the number of available backups for Production environments depends on the schedule type defined below.

Schedule	RPO	RTO	Manual backups	Automated backups
Basic	24 hours	Variable. Recovery time depends on the size of the data being recovered.	2	2: daily
Advanced	24 hours		4	21: daily, weekly, and monthly
Premium	6 hours		4	44: hourly, daily, weekly, and monthly

The schedules available depend on the support tier. An upgrade comes at an additional cost. The exact cost depends on the size requirements of the storage environment.

Automated backups are retained for a specific amount of time depending on their type and backup schedule.

Log retention

Platform.sh logs and stores various types of data as a normal part of its business. This information is only retained as needed to perform relevant business functions. Retention periods vary depending on the type of data stored. If a legal obligation, law enforcement request, or ongoing business need so requires, data may be retained after the original purpose for which it was collected ceases to exist.

Account information

Information relating to customer accounts (login information, billing information, etc.) is retained for as long as the account is active with Platform.sh.

Customers may request that their account be deleted and all related data be purged by filing a support ticket.

System logs

System level access and security logs are maintained by Platform.sh for diagnostic purposes. These logs aren't customer-accessible. These logs are retained for at least 6 months and at most 2 years depending upon legal and standards compliance required for each system.

Application logs

Application logs on each customer environment are retained with the environment. Individual log files are truncated at 100 MB, regardless of their age. When an environment is deleted, its application logs are deleted as well.

Data Restore

Customers have the ability to restore backups based on their unique needs. Key features and options include:

- Once backups of an environment exist, they can be restored from a previous point.
- The restore action requires an Admin role for that environment type.
- In the restore action, data is restored and the backed-up environment is deployed. This deployment uses the built app, including variables, from when the backup was taken. But code isn't restored, so any future (re)deployments use the current Git repository to build the environment.
    + Git commands such as revert allow for restoring code to its previous state when the backup was taken.
- It is possible to restore backups to a different environment than they were created using the CLI.

7.8 DR and reliability

Platform.sh tests incident management, disaster recovery, and business continuity plans and procedures throughout the year, and in accordance with the requirements of PCI DSS and SOC 2 Type 2.

Planning and testing takes into account the following activities:

- Business Impact Assessment (BIA)
- Risk management activities
- Lessons learned from previous incidents

Results of the testing are reviewed for lessons learned, post-test action items are captured and tracked for remediation, and the final reports are reviewed by third party auditors on an annual basis.

7.9 Shared responsibility matrix

Platform.sh and customers share the responsibility for ensuring an up-to-date and secure application environment. The customer is responsible for achieving and maintaining their own certifications and compliance.

The following is a general allocation of responsibilities between Platform.sh and the customer. For more guidance on responsibility for specific certification requirements, refer to the relevant documentation (such as PCI Compliance) to access the relevant shared responsibility matrix.

Responsibility	Platform.sh	Customers
Physical and Environmental controls	We use third-party hosting and thus these requirements are passed through to those providers (such as AWS).	N/A
Patch Management	Platform.sh is responsible for patching and fixing underlying system software, management software, and environment images.	Customers are responsible for maintaining and patching application code uploaded to Platform.sh, either written by them or by a third-party.
Configuration Management	Platform.sh maintains the configuration of its infrastructure and devices.	Customers are responsible for the secure configuration of their application, including Platform.sh configuration and routes managed through YAML files.
Awareness and Training	Platform.sh trains its own employees in secure software development and management.	Customers are responsible for training their own employees and users on secure software practices.

Capacity Management	Platform.sh is responsible for capacity management of the infrastructure, such as server allocation and bandwidth management.	Customers are responsible for ensuring their application containers have sufficient resources for their selected tasks.
Access Control	Platform.sh is responsible for providing access control mechanisms to customers and for vetting all Platform.sh personnel access.	Customers are responsible for effectively leveraging available access control mechanisms, including proper access control settings, secrets management, SSH key management, and the use of two-factor authentication.
Backups	Platform.sh is responsible for backing up the infrastructure and management components of the system. On Dedicated Gen 2, Platform.sh also backs up application code and databases on behalf of customers.	On Platform.sh, Professional customers are responsible for all application and database backups.
Managed CDN and WAF	If a customer's plan includes a managed CDN and/or a managed WAF, Platform.sh is responsible for setting up and maintaining the included measures. See more details about each at their respective documentation pages.	If a customer's plan does not include a managed CDN or managed WAF, the customer is responsible for setting up and maintaining such measures.

8. Compliance

8.1 Audits and technical tests

Platform.sh is **compliant with major security and privacy standards** that ensure customer privacy, including the European GDPR, German BDSG, Canadian PIPEDA, the Australian Privacy Act, California's CCPA, TX-RAMP, and HIPAA. A SOC 2 Type 2 audit over Security, Privacy, and Availability as well as a PCI DSS Level 1 audit for regions hosted on Amazon Web Services, Microsoft Azure, and Google Cloud Platform is conducted by third party auditors annually.

Platform.sh understands the need for application owners to ensure the integrity and standards compliance of their applications, as such, care must be taken in the scoping and execution of application testing. Only certain types of testing and testing scopes are permitted due to the potential for adverse impacts to other clients which would violate our terms of service.

Approved Activities

- Vulnerability scanning of the web application. This may be performed as often as required without approval from Platform.sh.
- Web application penetration tests that don't result in high network load. This may be performed as often as required without approval from Platform.sh.
- Application level load testing that does not result in high network load. If the load test may result in the application to be down, we ask to open an urgent ticket as a courtesy 30 to 60 minutes before the load test begins. Typically application level load tests will trigger one or many NodePing alerts. Knowing that a load test is in progress will allow the on-call engineer to immediately snooze alerts.

Approved Activities by Prior Arrangement

For Dedicated customers, infrastructure penetration testing (but not load testing) is permitted by prior arrangement, however, it requires special advanced preparation. A support ticket request must be submitted a minimum of three (3) weeks in advance for us to coordinate this on behalf of the customer.

Prohibited Activities

- Vulnerability scanning of web applications which a customer does not own
- Denial of Service tests and any other type of load testing which results in heavy network load
- Social engineering tests of Platform.sh services including falsely representing a person as a Platform.sh employee
- Infrastructure penetration tests for non-Dedicated customers. This includes SSH and database testing.

Rate Limits

Please limit scans to a maximum of 20 Mb per second and 50 requests per second to prevent triggering denial of service bans.

Troubleshooting

If a vulnerability scan suggests there may be an issue with Platform.sh's service, please ensure the container is updated and re-test. If the problem remains, please contact support.

8.2 Legal and regulatory

Platform.sh strives to be good custodians of customer data. Customer data is not sold and many steps are taken to be transparent about how customer data is used. For more information on how personal data and cloud data privacy is handled at Platform.sh, please see our Privacy Policy.

Platform.sh has taken numerous steps to ensure compliance with the GDPR.

Platform.sh provides a PaaS solution that customers may use for applications requiring Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance as well as TX-RAMP Level 2 compliance. All HIPAA and TX-RAMP workloads will run on the US-4 PaaS region.

Platform.sh engages a third-party auditor to produce a SOC 2 Type 2 examination report that includes a review of controls relevant to security, availability, and privacy. The annual audit covers the Platform.sh PaaS product as well as the Blackfire Application Performance Monitor (APM) product.

Platform.sh has adopted the European Commission's June 2021 official, standardized DPA Clauses for controllers and processors in the EU or adequate countries, with minimal customizations allowed by law and specific to Platform.sh.

The European Commission's module-based standard contractual clauses (SCCs) for transfers of EU personal data to non-adequate countries are required. Platform.sh executes the appropriate SCC module with all applicable third parties (vendors) whose services we may use. Questions regarding SCCs may be directed to dpo@platform.sh.

8.3 Cooperation with Authorities

Platform.sh provides a PaaS in a cloud environment and operates worldwide. Thus, situations may arise where Authorities must seek customers' account records and customers' personal data from Platform.sh based on a valid legal process. These guidelines inform Authorities on how to submit such requests for personal data.

However, please note, Platform.sh will first attempt to redirect Authorities to request the personal data directly from the customer.

Platform.sh complies with the rules and laws of the relevant jurisdictions ("Applicable Laws") in which it operates, as well as the privacy rights of its customers. Accordingly, Platform.sh diligently reviews requests to ensure that they comply with the Applicable Laws, and only provides personal data when Platform.sh reasonably believes it is legally required to do so.

Platform.sh strictly evaluates and seeks to limit or object to requests pursuant to relevant laws, including those that are overbroad, seek a large amount of personal data, or affect a large number of users. Platform.sh also objects where there is insufficient justification to compel the release of the requested data under Applicable Laws.

In accordance with the EU Digital Services Act Package, French law, and the European Data Protection Board's requirements and recommendations, Platform.sh provides two reports on an annual basis outlining governmental authority requests and abuse reports received during that year.

Glossary

Capabilities

Starting with kernel 2.2, Linux divides the privileges traditionally associated with superuser into distinct units, known as capabilities, which can be independently enabled and disabled. Capabilities are a per-thread attribute.

Common Vulnerabilities and Exposures (CVE)

The Common Vulnerabilities and Exposures (CVE) program is a dictionary or glossary of vulnerabilities that have been identified for specific code bases, such as software applications or open libraries.

Content delivery network (CDN)

A CDN, or content delivery network, is a network or collection of servers in locations all over the world. Also known as a content distribution network, a CDN can refer to many types of content delivery services, such as load balancing and video streaming.

Dedicated Generation 2

Dedicated Gen 2 environments are managed virtual machine clusters with triple redundancy. Their dedicated architecture makes them differ from Grid environments. With Dedicated Gen 2 plans, Production and Staging environments are dedicated virtual machines, while Development environments run on the Grid, meaning shared redundant infrastructure. This difference means a few configuration options and tools function differently in the different environments.

Dedicated Generation 3

Dedicated Gen 3 provides a scalable solution as an additional option on top of existing Grid applications. It provides redundant configuration with a minimum of three Virtual Machine instances. Every service is replicated across all three virtual machines in a failover configuration (as opposed to sharding, allowing a site to remain up even if one of the VMs is lost entirely).

Block storage

IaaS providers make persistent block level storage volumes available for use with virtual machines. Block storage volumes behave like raw, unformatted block devices.

GNU Privacy Guard (GPG)

Allows for the encryption and signing of data and communications.

Grid

Grid environments are standard for Professional plans. They run on shared infrastructure and are lxc container-based.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a US federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

Intrusion Prevention System (IPS)

IPS proactively detects and prevents harm from malicious traffic. IPS protection identifies potential threats by monitoring network traffic in real time by using network behavior analysis.

Kernel Address Space Randomization (KASLR)

KASLR enables randomizing the physical and virtual address at which the kernel image is decompressed, and thus prevents guest security exploits based on the location of kernel objects.

Let's Encrypt TLS certificates

Let's Encrypt is a non-profit certificate authority run by Internet Security Research Group that provides X.509 certificates for Transport Layer Security encryption at no charge.

Namespaces

Namespaces are a feature of the Linux kernel that partitions kernel resources such that one set of processes sees one set of resources while another set of processes sees a different set of resources.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an established information security standard which applies to any organization involved in the processing, transmission, and storage of credit card information.

Platform-as-a-Service (PaaS)

PaaS is a cloud computing model that provides customers a complete cloud platform—hardware, software, and infrastructure—for developing,

running, and managing applications without the cost, complexity, and inflexibility that often comes with building and maintaining that platform on-premises.

Page table isolation (PTI)

PTI is a countermeasure against attacks on the shared user/kernel address space such as the “Meltdown” approach.

Security information and event management (SIEM)

SIEM technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources.

Security Operations Center (SOC)

SOC is an in-house or outsourced team of IT security professionals that monitors an organization's entire IT infrastructure, 24/7, to detect cybersecurity events in real time and address them as quickly and effectively as possible.

SOC2 Type 2

A SOC 2 report evaluates data systems using the American Institute of Certified Public Accountants' (AICPA) Trust Services Principles (TSPs). The TSPs are industry-recognised standards for cloud service providers, software providers and developers, web marketing companies and financial services organizations.

SOC 2 reports provide assurance to prospective and current customers about the security, availability, confidentiality and privacy of the information systems. A Type 2 report will then cover the design and operational effectiveness of controls over an extended period of time, usually six months to a year.

Texas Risk and Authorization Management Program (TX-RAMP)

TX-RAMP provides a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a State of Texas agency.

TX-RAMP Level 2 is required for cloud computing services that store, process, or transmit the confidential data of a state agency and the cloud computing service is determined to host moderate or high impact information resources.

Web application firewall (WAF)

A web application firewall (WAF) is a type of firewall that protects web applications and APIs by filtering, monitoring and blocking malicious web traffic and application-layer attacks — such as DDoS, SQL injection, cookie manipulation, cross-site scripting (XSS), cross-site forgery and file inclusion.

We hope this document has given you a clear and comprehensive overview of our security and privacy practices. We take these matters very seriously and we are committed to protecting your data and respecting your choices.

If you have any questions, concerns or feedback, please do not hesitate to contact us at hello@platform.sh. We would love to hear from you and address any issues you may have. Thank you for choosing us as your trusted partner.👍

platform.sh