OpsGenie

Security in OpsGenie

Security in OpsGenie

OpsGenie is a modern incident management platform for operating always-on services, empowering Dev & Ops teams to plan for service disruptions and stay in control during incidents. OpsGenie collects and tracks data for each incident throughout its entire lifecycle. The secure handling of this data is OpsGenie's number one priority.

Security Framework

OpsGenie security is based on the ISO 27001 Information Security Standard and Cloud Security Alliance (CSA) Framework, which includes:

- Policies & procedures
- Personal security
- Asset Management
- Access Management
- Physical Security
- Cryptography
- Operations security
- Communications security
- System development and maintenance
- Supplier security
- Security incident management
- Business continuity management
- Compliance

Security is the responsibility of all employees of OpsGenie, and each employee must complete regularly scheduled security training. The Chief of Security and Reliability Officer defines and implements the security program at OpsGenie. This program is reviewed with the executive team regularly to ensure the latest security measures are in place to keep customer data secure.

Policies & Procedures

To provide the foundation of the information security framework, OpsGenie defines and implements a set of policies, procedures, standards, and guidelines. These documents are reviewed regularly and updated as needed.

Personal Security

Security begins with the employee at OpsGenie. Each employee goes through a thorough security process, which includes the following:

Background Checks

Information Security is addressed at the recruitment stage and background checks are performed on all OpsGenie staff. Criminal and reference checks are performed prior to hire. The contract with each employee contains their responsibilities for information security as an employee of OpsGenie.

Training & Awareness

An information security training and awareness program is in place so employees can perform their functions in an efficient and effective manner.

In addition to technical security education, product and technology education featuring security-related topics is given to developers. We also have a technical badge earning system which is a platform for the company to recognize employee achievement and motivate the team to develop new skills. Incidents and vulnerabilities that may affect security are reported through management channels as quickly as possible by employees.

Termination or change of employment

Terminated employees are removed from all systems. All access to any OpsGenie management systems, tools & platform is disabled the day the person leaves the company.

Employees who leave OpsGenie on their own or through termination are required to return all company assets, including but not limited to: laptops, computers, files, keys, and access cards on their last day.

Customer Data Protection

OpsGenie Security focuses on protecting customer data from unauthorized access and implements the following controls:

Data Classification & Handling

OpsGenie classifies customer data and establishes the most appropriate way of handling, storing, retrieving, and disposing of this data according to its classification. Customer data is classified at the highest level.

Data Encryption in Transit and At Rest

OpsGenie uses the best practice encryption algorithms for cryptographic controls to ensure the security of data and the environment that data is stored in.

OpsGenie uses AWS KMS (AES-256 algorithm) or other industry-standard methods for encryption to encrypt data at rest. TLS is used in transit as well. Encryption Keys are managed by using AWS services coupled with industry-standard methods.

Applications use a layer between application business logic and database resources. This intermediate layer ensures that one customer is not able to access another customer's data. Data in databases are designed to be segmented for tenants.

Credit Card Information Security

OpsGenie uses Stripe as a third-party payment processing service. Credit card information is sent directly to Stripe in an encrypted form and processed securely. OpsGenie does not store, collect and process credit card information of customers. Stripe is PCI compliant and our use of their service preserves that PCI compliance.

Systems & Communication Security

The security of our infrastructure and networks is crucial. Providing a secure network environment is one of the important goals of our security program. Within OpsGenie infrastructure, public-facing networks and private networks are isolated from each other to protect customer data.

TLS1.2 protocol is used for transferring all customer data. Also IP restriction is used for accessing AWS.

Public networks are protected against global threats including DDOS spoofing & port scanning with multiple levels of firewall. Network systems are managed by the designated operators with a specific business need. The Development and maintenance section of this document describes how the changes are applied.

OpsGenie uses multiple security tools to configure and asses vulnerabilities and intrusion detection.

Wherever feasible, OpsGenie adopts serverless services provided by AWS by hardening security of these services. Adopting serverless allows OpsGenie to increase the overall security of out applications and systems.

Authentication & Authorization

To prevent the exposure of customer data due to unauthorized access, the authorization of users in OpsGenie is set based on the least privilege. Users are only provided with access to the network, systems, applications, and network services that they have been specifically authorized to use. Access to the system is audited, logged, and verified.

The access rights of users are reviewed according to their job responsibilities at regular intervals (at least annually) by management.

Access to information, applications, and systems is restricted by means of username and password. Tenants can configure SSO and disable password login. If the SSO provider supports MFA during login, indirect MFA login to OpsGenie is achieved, you can learn more here:

https://docs.opsgenie.com/docs/single-sign-on-with-opsgenie

OpsGenie supports SAML 2.0 and multiple SSO providers (Google, Okta, OneLogin, PingIdentity, Azure AD, and ADFS).

https://docs.opsgenie.com/docs/single-sign-on-with-opsgenie

Password settings are configurable and can be done by the customer. The settings details can be found here:

https://docs.opsgenie.com/docs/password-policies.

OpsGenie supports iOS and Android. The authentication method depends on tenant settings and can be password-based or SSO-based. After initial authentication, mobile applications are authenticated by using a token which is stored on mobile devices using native encryption.

Logging

OpsGenie maintains extensive logs specific to the application, operating system, and database layers. The responsible users and user groups monitor and review all log data.

Log information is protected against tampering and unauthorized access.
System administrator and system operator activities are logged, and access/change actions can be reviewed.

Protection from malware and malicious code

Servers and endpoint devices such as laptops and desktops are protected and monitored from malwares, malicious and unsafe codes or applications by deploying a set of protection tools.

Change Control

In order to prevent a breach of data, OpsGenie controls all changes in the production environment according to security requirements defined throughout this document.
All tests are documented and approved before deployment.

Penetration Testing

At OpsGenie, we annually engage a 3rd-party to conduct penetration and vulnerability testing of our platform including applications and infrastructures.

Development and maintenance

OpsGenie follows the Agile methodology for software development, which facilitates continuous development and deployment. OpsGenie does not deliver against the more traditional "point release" cycle. Instead, features and bug fixes are released to production when completed.

New features, configuration changes, and bug fixes in OpsGenie are handled as needed. A Continuous Delivery Model is used for delivery of software. A test driven model is used for development. All changes are verified with automated unit, integration, functional, performance, and security tests. Developers work together to review changes. There are multiple pre-production environments to test for accuracy and security.

OpsGenie complies with the OWASP Secure Web Application framework requirements, and tests for vulnerabilities regularly using vulnerability scanners.

Physical and environmental security

Data Center Security

OpsGenie is completely hosted on Amazon Web Services (AWS). As a customer of OpsGenie, the safety and security policies that AWS provide to us are also applicable to you, our customer. The AWS data center operations comply with a set of standards and regulations including ISO 27001, SSAE 16, PCI Level 1, FISMA Moderate Sarbanes-Oxley (SOX), and HIPAA (at the server level).

For more information about Data Center Security of AWS, please refer to the AWS Security White papers below.

https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

https://aws.amazon.com/security/

https://aws.amazon.com/compliance/shared-responsibility-model/

Working in Secure Areas

There are surveillance cameras and security in place to monitor the buildings. Employees have ID badges for entering the office. All visitors are escorted in the OpsGenie offices.

Business Continuity and Disaster Recovery

By design OpsGenie is always running, reliable & scalable. Providing committed SLAs and ensuring business continuity is important for OpsGenie.

Availability Zone Failover

OpsGenie runs on 3 different data centers in a single region by default. Unless all availability zones have an outage at the same time, OpsGenie will continue to be up & running.

Region Failover

OpsGenie uses more than two hosting regions. These regions are located away from each other. All data centers are online and serving our customers. In case of a regional failure in which all available zones have an outage, automated processes redirect customer data to the healthy region to help avoid any downtime.

For SMS, voice, and email sending capabilities, OpsGenie uses multiple providers to handle failover cases.

Replication of each region is continuously monitored and tested at regular intervals.

Backup

Data is backed up and continuously replicated to a different data center in a different region and backed up as encrypted files daily. Restore test of backups is tested at regular intervals.

Monitoring & Security Incident Response

OpsGenie is a heavily-monitored SaaS platform. Our monitoring solutions are able to notify us of vulnerabilities, threats, and incidents, and there are automated fixes within our monitoring solution. The IT Team assesses the vulnerabilities, threats, and incidents and then establishes remediation and mitigation. OpsGenie uses its own alerting & incident resolution capabilities as well.

Supplier security

The information security requirements are identified and included as part of the agreement/contract with the supplier or third party to minimize the any risk. The delivery of suppliers is monitored and reviewed regularly.

Compliance

OpsGenie complies with applicable legal, regulatory and contract requirements as well as industry best practices.

Customer data is stored for as long as it is needed to meet the operational needs of OpsGenie, together with contractual legal and regulatory requirements.

Cryptographic controls are used in compliance with all relevant agreements, laws, and regulations.

Regular technical compliance reviews, including penetration testing and IT health checks of all information systems, are taken to ensure continued compliance.