GRANULATE™
An Intel Company

Security Overview

Our Security Commitment

Security

Granulate is built with security in mind and undergoes ongoing rigorous security testing

Privacy

We offer best-in-class data protection and settings that protect your infrastructure data

Compliance

Granulate's policies and products are compliant with GDPR privacy regulations

Commitment To Highest Security Standards

Secure Operations

- Granulate adheres to carefully controlled workflows that ensure that all business is executed based on established security guidelines. These workflows include carefully structured reporting lines, data access controls, segregation of duties, security monitoring, and internal audits.
- Granulate Security policies are designed to adhere to the strict guidelines set by Intel Corporation and internationally recognized security standards- SOC 2 Type II, ISO 27001 and HIPAA.

Secure Software Architecture

- Granulate architecture is designed around the goals of redundancy, security, and "always on" availability.
- Our security design relies on industry best practices such as encrypted transmissions, cross-site scripting prevention, firewalls, regular security updates and security assessments to ensure the security of your data. Auditing, access restrictions and secure decommissioning of data storage complement the design.

Secure Data Centers

- All performance data that are collected on the customer side are securely transmitted to our servers in the cloud and processed behind firewalls.
- Granulate runs on the Amazon Web Services (AWS) cloud-computing service and benefits from Amazon's secure, world-class data centers, which are certified for ISO 27001, PCI-DSS Level 1, and SOC 1 / SSAE-16.

Commitment To Highest Security Standards

Security Measures

Data Hosting & Storage

- Granulate runs in the Amazon cloud (AWS) cloud infrastructure. AWS security measures provide a high degree of data protection. AWS guarantees physical access controls, hypervisor protection, and secure decommissioning of instance data.

Permission & Authentication

- Direct access to AWS services by our employees is carefully regulated based on multi-factor authentication. Permissions are granted on a "need based access" policy following a thorough approval process.

Failover & Backups

- For high availability purposes we leverage AWS standards, best practices and failover solutions.

Monitoring

- All systems we run are subject to permanent health and security monitoring.

Security Testing

- The attack surfaces of our services are minimized based on automated vulnerability scans, regularly conducted internal security assessments.

Incident Response

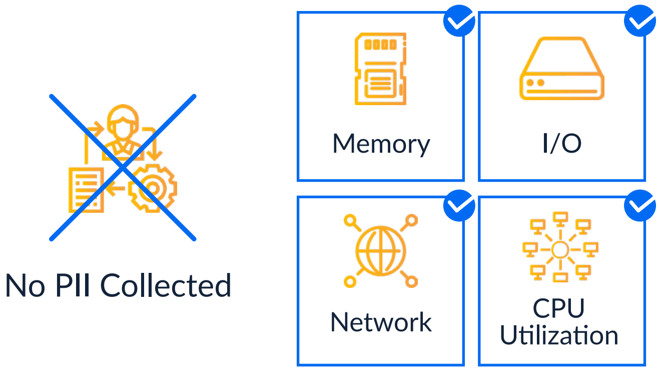
- We continuously monitor the security of our hosting environment. In case of security incidents, we thoroughly evaluate detected problems and the underlying root causes as described in our Incident Response Policy.

Training & Awareness

- All Granulate employees undergo annual security-awareness training.

Data Collected

Granulate Agent Collects Resources Data



The Following Data is Sent From the Agents

Resource	Data
Memory	Allocation Patterns Per Process Access Patterns Per Process - Reads/Writes, Random/ Sequential etc
Scheduler	Per Process Per Core
I/O	Access Patterns Per Process- Reads/Writes, Random/ Sequential etc
Network	Per Socket Metadata - Window Size, Recieve vs Send Ratio Over Time, Long/Short Lived, Congestion Control, RTT

Data Storage

- Granulate offers two different types of deployment models: SaaS and On-Premise.
- SaaS - Data is stored in AWS data centers.
- On-Premise, your monitoring data remains in your own data center.

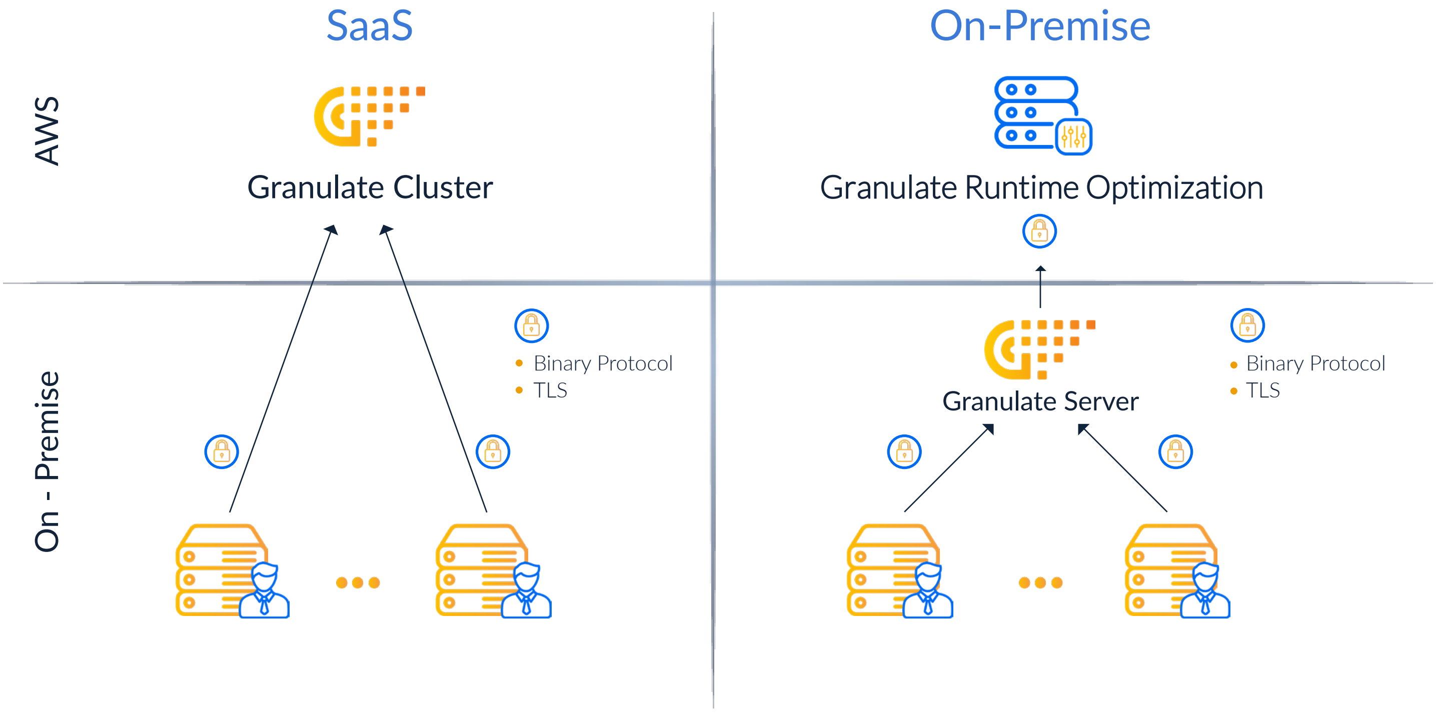
SaaS

On-Premise

Customer Infrastructure
(On-Premise)

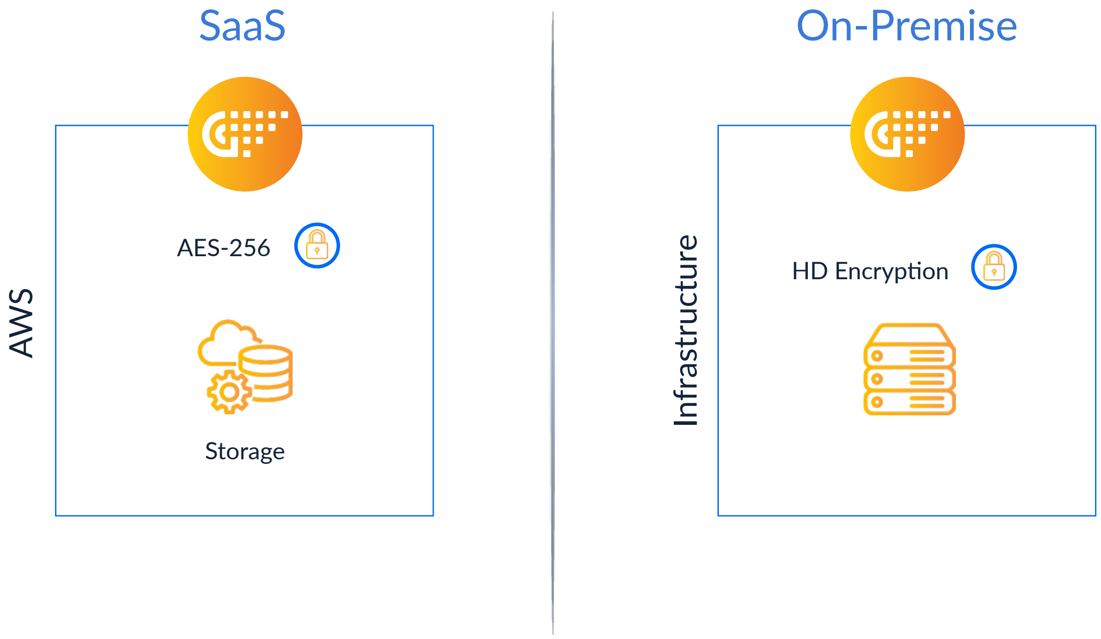
Data Transit

- All data exchanged between Granulate sAgent and Granulate Cluster is encrypted in transit.
- Data is sent using proprietary encrypted binary protocol.
- Granulate SaaS uses TLS 1.3 (SSL Labs Grade A+).



Data Encryption At Rest

- Granulate SaaS uses AWS storage with AES 256 encryption.
- Encryption keys are managed by Granulate using AWS Key Management Service (KMS).
- Managed customers must configure their own hard disk encryption and manage encryption keys on their own.



Communication Exchange

Secure Communication Between Granulate Components

- The Granulate sAgent communicates with the Runtime Optimization
- All communication between the sAgent and Runtime Optimization encrypted
- Granulate isn't able to initiate a connection to the customer's cluster

Types Of Communication

- Installation – Account Name, License Name, Installation Flags
- Agent Registration – License Key, Service ID
- Granulate License – License Status, Service ID, License Key, License Details, License Model
- Health Check – Service ID, Time Zone, Traffic Size, Update Window, Performance Data
- Metrics – Service ID, Monitoring Timeframes, Success & Failure Alerts, Performance Data
- Heartbeat – Service ID, Node ID, Source Information
- Updates – Service Updates, Version, Description, Download URL

Security Certifications

- Granulate services and data is hosted in Amazon Web Services (AWS) facilities.
- The services and facilities of AWS are certified against international standards:
  - ISO 27001 (Information Security Management System)
  - ISO 27017 (Cloud Services Security)
  - ISO 27018 (Personal Data Protection)
- Granulate services are designed to adhere to internationally recognized security standards - SOC 2 Type II, and HIPAA.
- Granulate is GDPR compliant.

Data Protection

Access Control

- Our customers individually control access to the data that Granulate has access to.

Monitoring & Audit Logging

- All systems operated by Granulate are subject to health and security monitoring, logging audit, and automated analysis of system logs.

Data encryption

- All electronic communication sent to and from Granulate over HTTPS relies on TLS encryption on the relevant ports.
- sAgent encrypts all data before they are sent to Granulate Server.
- Metric and transaction data is encrypted even while at rest, and each customer’s data is programmatically partitioned from the data of other customers.

Data Retention

- Granulate stores and retains different types of monitored data from your environments (see section ‘Data Collected’ for relevant monitored data).
- The monitoring data is stored on the Granulate Server for a retention period of 2 weeks, billing data and anonymized aggregations of data are stored for a longer period of time.

Business Continuity And High-Availability

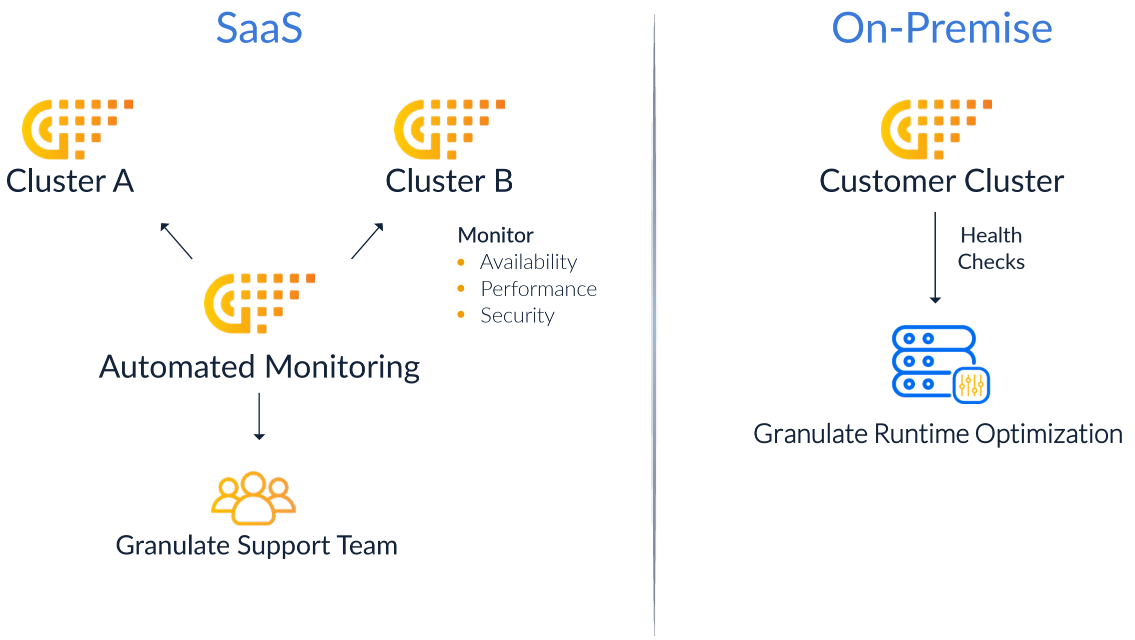
- Granulate sAgent is designed to ensure 99.99999% availability SLA of the customer’s infrastructure.
- Granuate leverages AWS fail-over mechanisms to ensure high availability of all services.
- Granulate optimization agents are completely autonomous and will continue to work properly even without network connection to the server.

Performance Improvments Guarantress

- Granulate's sAgent is built with internal high performance gain failsafe mechanisms to prevent performance degradation.
- The sAgent holds a performance gain threshold of 65% improvement, below this threshold the agent starts to automatically relearn for a 20 second timeframe to rise above the gain threshold.
- Following 3 consecutive failures to return to the 65% threshold, an alert is raised and the agents can be configured to deactivate automatically.

Infrastructure Monitoring

- Granulate constantly monitors the availability, performance, and security of all SaaS clusters.
- If a problem is detected, the Granulate support team is notified immediately.
- On-Premise deployment customers can also choose to monitor by sending regular health checks to Granulate Runtime Optimization .



SaaS

Cluster A

Cluster B

Monitor

- Availability
- Performance
- Security

Automated Monitoring

Granulate Support Team

On-Premise

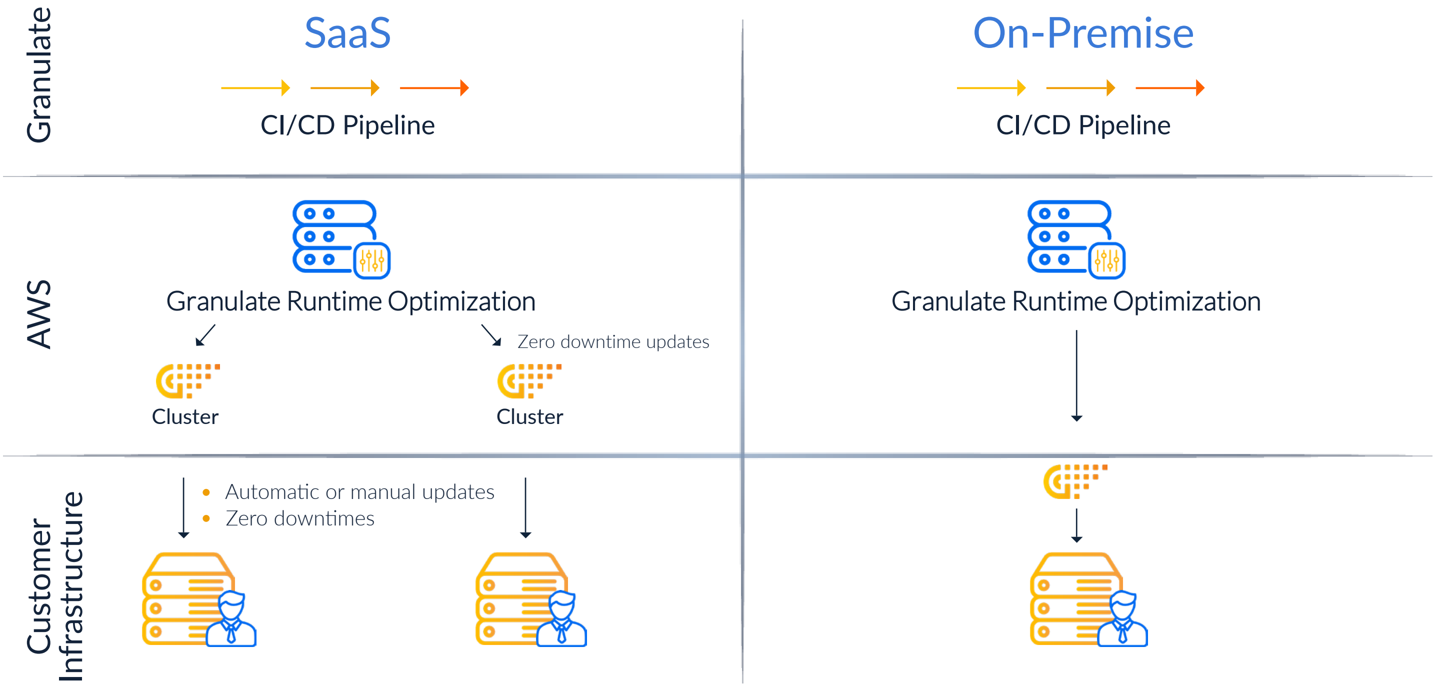
Customer Cluster

Health Checks

Granulate Runtime Optimization

Rolling Updates & Hot Fixes

- Using a fully automated CI/CD pipeline, Granulate is able to roll out updates and hot fixes within a few minutes.
- The Granulate architecture allows for zero-downtime upgrades of clusters and agents.
- Updates of Granulate sAgent and Runtime Optimization can be done both manually and automatically.



Granulate

AWS

Customer Infrastructure

SaaS

CI/CD Pipeline

Granulate Runtime Optimization

Zero downtime updates

Cluster

Cluster

- Automatic or manual updates
- Zero downtimes

On-Premise

CI/CD Pipeline

Granulate Runtime Optimization

For more information contact info@granulate.io

GRANULATE™
An Intel Company