OverOps

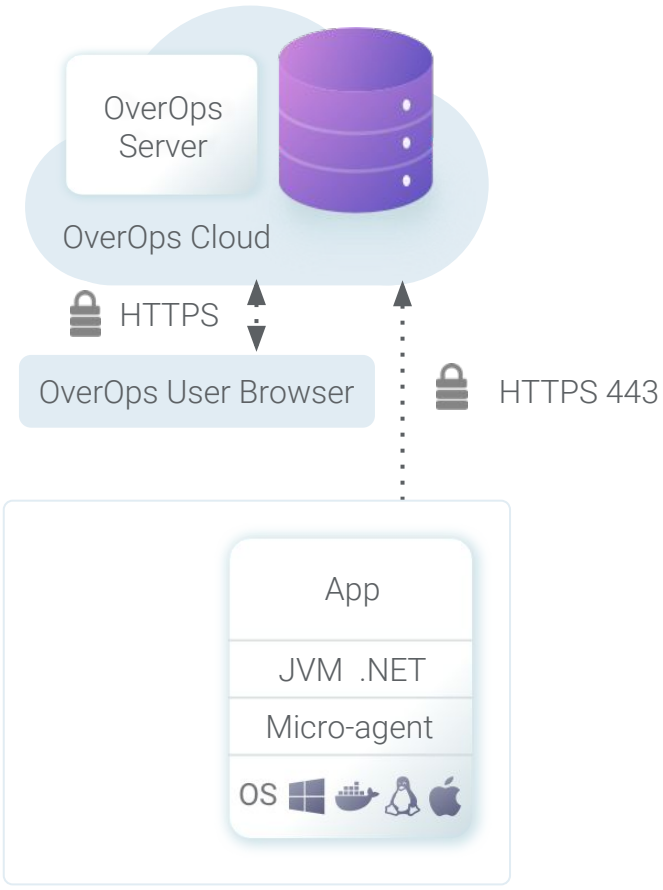
OverOps Architecture:

Built for Production & the Enterprise

SaaS

Powered by AWS.

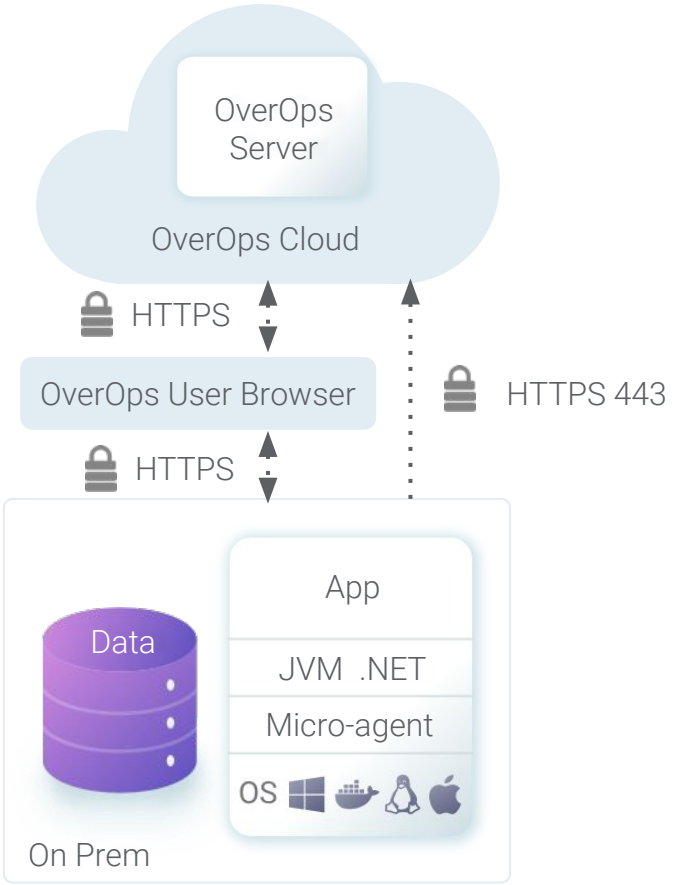
Based on AWS infrastructure, all collected data is redacted for PII and privately encrypted using your own 256-bit AES keys.



On-Prem Data

The ease of SaaS. The security of On-Prem.

Data is redacted for PII, encrypted locally and stored on your machine. Only the metadata is sent out to OverOps' cloud for analysis.



*Full on-premises also available.

A Simple JVM Agent
HotSpot, OpenJDK & Zulu. IBM J9. Versions 6-8.

No Changes to Code or Build
Install micro-agent & add an *-agentlib* argument to the JVM.

All JVM Languages
Supports .NET and all JVM languages & frameworks.

Fast. Secure. Scalable.

Less than 3% CPU Overhead

OverOps employs self-throttling at the JVM level, combined with continuous guidance provided by the analysis engine to limit the number of error snapshots taken.

No GC Overhead

OverOps runs at the native JVM-level and does not allocate Java objects at run-time. Collected information is placed directly in shared memory outside of the managed heap.

< 50mb/Hour Network Overhead

Error information captured by the JVM agent is placed into shared memory and sent for storage by the collector process. The size of event snapshots is capped at 50Mb per hour.

No Throughput Overhead

Since OverOps only reacts to errors, it does not affect normal code execution – even if a transaction is experiencing a high degree of failures (expected or unexpected).

256-bit AES Encryption

All source code and variable state collected is privately encrypted using a 256-bit AES Encryption key before leaving the production node. Only you have access to secret encryption keys which are not stored by OverOps.

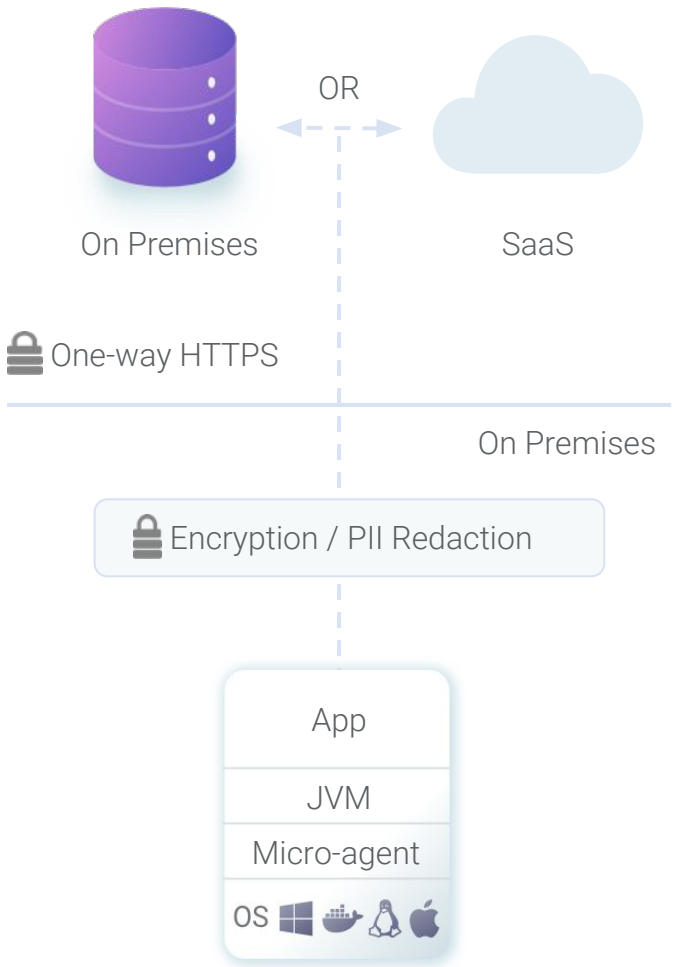
PII Redaction

OverOps redacts PII variable data before it leaves the production environment. Variable state is redacted based on configurable variable value patterns and code symbology: variable, package and class names. PCI and HIPAA-compliant.

Access Control

Robust support for two-factor authentication with OAuth (e.g Google Apps and GitHub), LDAP and SAML. Administrators can limit access to OverOps to a specific VPN or network. Communication between all components is made over outbound HTTPS port 443.

ISO 27001 Certified



Visit www.overops.com/architecture to learn more.