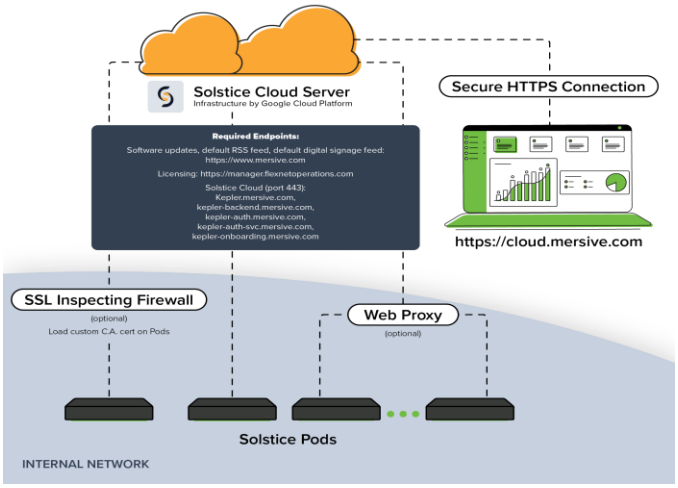
Solstice Cloud Security Overview

Solstice Cloud has expanded from analytics to include management capabilities, allowing administrators to easily deploy, organize, monitor, and update Solstice Pods at scale. Due to its cloud architecture vs. the existing on-premises Dashboard, managing Pods may pose security concerns for some customers. However, security, stability, and data integrity were key credentials when building Solstice Cloud.

Solstice Cloud Topology

Standard cloud-topology with three components:

1. Cloud server hosted on the Google Cloud Platform
2. Front-end user interface that runs in a browser
3. Fleet of Pods deployed on the on-premises network



Security

Routine penetration testing

- Annual (or more) penetration testing by independent, third-party to validate security of the Solstice Pod and associated cloud systems.

Pods do not require general cloud access

- Only a small number of cloud endpoints are required and can be easily added to firewall rules. Those endpoints are available from Mersive and won't change.

Web proxies are supported

- Proxies are supported if you don't want to allow direct cloud access from on-prem devices. If enabled, all Solstice Cloud traffic will pass through the specified web proxy.

Enterprise grade encryption

- All Solstice Cloud traffic is encrypted with industry standard 2048-bit RSA-based cipher.

Support for SSL-inspecting firewalls

- If using a firewall that inspects encrypted traffic, simply upload the CA cert to each Pod.

Privacy

No content data leaves the internal network

- No screen content, files, or visual information ever leaves the Pod

No personally identifiable data is collected

- Solstice Cloud does not collect any personally identifiable data about Solstice users. The data collected is best described as metadata about meetings or configuration state of Pods.

GDPR compliant

- Solstice Cloud is fully compliant with GDPR's guidelines and is classified as a Data Controller. Please see the privacy policy (www.mersive.com/privacy-policy) for more details