



# Solstice Cloud Security Brief and Deployment Considerations

## Overview

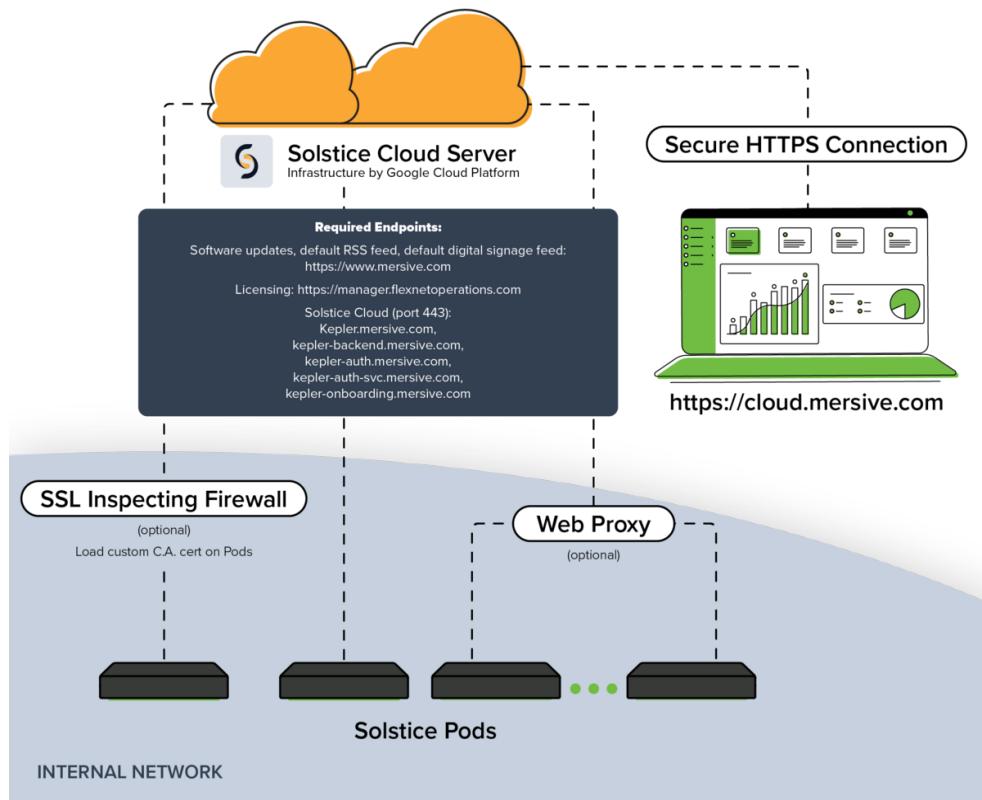
Solstice Cloud is a secure cloud-based management and analytics portal that empowers organizations to manage, analyze, and optimize their Solstice-enabled meeting and learning spaces by sending and receiving data from Solstice Pods deployed in those spaces.

Solstice Cloud users can access the portal from anywhere that has internet access. Solstice Cloud includes critical management tools such as configuration templates, real-time email alerts, and scheduled software updates to provide management-at-scale for deployments of any size. Additionally, anonymized metadata is continuously collected from Solstice Pods to deliver AI-driven insights on room utilization and workplace collaboration.

The security, stability, and data integrity of Solstice Cloud are of paramount importance to Mersive. This document outlines specific security features that are part of Solstice Cloud's architecture, and is only intended as a brief introduction for IT and network security teams. More information can be found by accessing Mersive's secure dataroom under NDA. To gain access, please work with your local Mersive representative.

## Topology

Solstice Cloud is designed using standard cloud topology, as shown below. The topology involves three components: 1) a Solstice Cloud cloud server that is maintained on the Google Cloud Platform, 2) a front-end user interface that runs in a web browser, and 3) a fleet of Pods, deployed on the on-premise network. All communication between these components takes place over encrypted SSL.



A dormant *Solstice Cloud Producer* process is resident on each Solstice Pod that is independent of the Solstice application itself. In this way, users that do not want to make use of Solstice Cloud can use Solstice normally. Until a Pod is securely enrolled into Solstice Cloud, that process cannot operate. When a Pod is enrolled in Solstice Cloud, a secure connection to the cloud is established between the Solstice Cloud Producer and the user's Solstice Cloud account. Only then will this process begin to read and transmit logging events from the Solstice application.

## Security Assessment and Penetration Testing

Both Solstice Cloud and the Solstice Pod endpoint undergo third-party penetration testing. As an on-network IoT device, the Solstice Pod is tested twice a year, both as part of a complete bench-test and in-situ on an enterprise network. The results of those tests are made available to partners under NDA.

In addition, the Solstice Cloud Server is scanned monthly for vulnerabilities to search for potential security regressions. In addition to these monthly scans, a full penetration test of Solstice Cloud takes place once a year. The results of the penetration tests are uploaded to the secure dataroom and can be viewed under NDA.

## Security Features

Given the nature of today's security landscape, we do not overtly publish all of the details related to security features that have been built into the Solstice Cloud architecture. In overview, however, here are some of the security features to consider:

- **No Content Data Leaves the Enterprise Network.** Solstice Cloud receives only de-identified event data to allow administrators to monitor room usage and analytics. No screen content, files, or visual information is ever shared with Solstice Cloud. These messages are quite small and only should utilize 1–2 Mb of data per week.
- **GDPR Compliant.** Mersive approaches privacy seriously and acts as a GDPR compliant data owner. All data stored in Solstice Cloud is de-identified, can be deleted on demand, and is only used according to our published privacy policy. ([www.mersive.com/privacy-policy](http://www.mersive.com/privacy-policy))
- **Web Proxies are Supported.** The Pod can be directed to an on-premise web proxy server so that all Solstice Cloud-bound traffic first passes through this web proxy. This ensures that Pods do not need direct internet access and, instead, communicate to Solstice Cloud through a managed firewall. Application-specific traffic monitoring and other security protocols can be imposed on Solstice Cloud traffic at the web proxy server.
- **Support for SSL-Inspecting Firewalls.** In addition to an Ethernet certificate that validates a Solstice Pod to a network authentication server, Solstice Cloud supports SSL certificate updates so that a Pod will present the correct certificate for authentication when it communicates through the enterprise firewall. Administrators can generate an SSL certificate and install it on their Solstice Pods so that the firewall SSL inspection ensures only valid devices are communicating to Solstice Cloud.
- **Enterprise Grade Encryption.** All traffic between Solstice Cloud components is encrypted using a 2048-bit, RSA-based cipher algorithm. All weak ciphers have been removed from the SSL layer to ensure that only RSA-based ciphers are utilized. This encryption applies to all

configuration traffic and any event logging that can be transmitted to Solstice Cloud.

- **Limited Endpoint Access.** The Solstice Cloud system does not require general internet access. Instead, the Solstice Pod only needs to reach a small set of destination URLs, either directly or through a managed web proxy server. In addition to a licensing server and our optional software updating portal, Solstice Cloud only requires access to five endpoints. Outbound traffic to other locations (shown in the topology diagram of this document) can be blocked, and firewall rules that monitor for access outside of the Solstice Cloud cloud can be used.

## Disaster Recovery

The Solstice Cloud application is hosted on the Google Cloud Platform. The application front end is hosted on a global Google content delivery network. The application back end runs in a containerized environment with Kubernetes clusters in multiple zones. The application is deployed and configured via code, allowing for a repeatable redeployment in case of disaster. Primary data stores include Google Cloud SQL and Google Cloud Storage. Google Cloud Storage has been designed for at least 99.99999999% annual durability. Google Cloud SQL instances are backed up daily, with backups stored in multiple regions.