mersive
technologies inc

Kepler Security Brief and Deployment Considerations

2019

Kepler is a cloud-based monitoring and analytics service for enterprise Solstice deployments. It provides a real-time view of Solstice Pod status, usage statistics, and visualization tools that help administrators better understand how their meeting technologies are being used.

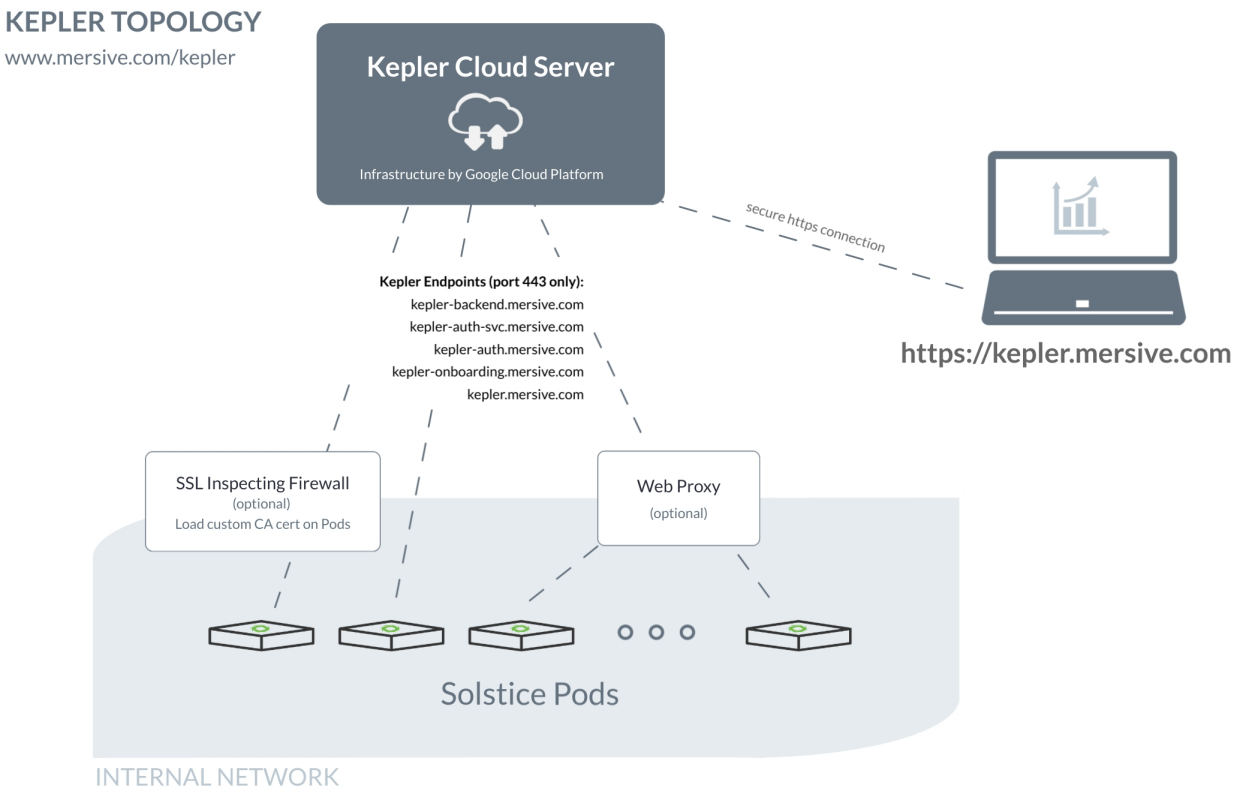
Kepler users can access the portal from anywhere that has internet access and provides management-at-scale for deployments of any size. It's tools include scheduled software updates and template-based configuration* with automatic provisioning to streamline the deployment process.

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

Topology

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

mersive
technologies inc



A dormant *Kepler 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 Kepler can use Solstice normally. Until a Pod is securely enrolled into a Kepler, that process cannot operate. When a Pod is enrolled in Kepler, a secure connection to the Kepler cloud is established between the Kepler producer and the users' Kepler account. Only then will this producer begin to read and transmit logging events from the Solstice application.

Security Assessment and Penetration Testing

Both Kepler and the Solstice Pod endpoint undergo 3rd 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.

mersive
technologies inc

In addition, the Kepler Server is scanned monthly for vulnerabilities to search for potential security regressions. In addition to these monthly scans, a full penetration test of Kepler 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 Kepler architecture. In overview, however, here are some of the security features to consider:

No Content Data Leaves the Enterprise Network. Kepler 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 Kepler. These messages are quite small and only should utilize 1-2 Mb of data per week.

GDPR Compliance. Mersive approaches privacy seriously and acts as a GDPR compliant data owner. All data stored in Kepler is de-identified, can be deleted on demand, and is only used according to our published privacy policy. (www.mersive.com/privacy-policy)

WebProxy Suport. The Pod can be directed to an on-premise web proxy server so that all Kepler bound traffic first passes through this Web Proxy. This ensures that Pods do not need direct internet access and instead, communicate to the Kepler through a managed firewall. Application specific traffic monitoring and other security protocols can be imposed on Kepler traffic at the Web Proxy server.

SSL Certificate Firewall Support. In addition to an Ethernet certificate that validates a Solstice Pod to a network authentication server, Kepler supports SSL certificate updates so that when a Pod communicates through the enterprise firewall it will present the correct certificate for authentication. 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 Kepler.

Enterprise Grade Encryption. All traffic between Kepler 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 Kepler.

Limited Endpoint Access. The Kepler system does not require general Internet access. Instead, either directly or through a managed Web Proxy server, the Solstice Pod only needs to reach a small set of destination URLs. In addition to a licensing server and our optional software updating portal, Kepler 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 to for access outside of the Kepler cloud can be used.