Solstice Conference Security Overview

Introduction

With Solstice Conference, Mersive introduces a new category of room system that can be used with a wide variety of video conferencing services. Solstice Conference enhances meeting productivity by allowing onsite participants to share an unlimited amount of content while allowing remote participants to experience that same level of content-rich collaboration as if they were onsite.

With a one-step start, Solstice launches the appropriate conferencing software, joins the host to the call, and wirelessly bridges room audio and video devices to the host laptop to support the video conference when needed.

Since meeting content requires an added level of security beyond meeting audio and video, Solstice Conference was designed and built with security as a top priority, like all Mersive products. This document outlines important considerations surrounding the security profile of Solstice Conference.

System Architecture

Solstice Conference consists of two system components that work together to support meeting connectivity and collaboration for onsite and remote participants:

1. The Solstice Pod handles all in-room wireless content sharing and wireless connectivity between room audio/video devices and the meeting host's laptop. All data is streamed over the local network only.
2. The meeting host's laptop creates a single connection to the cloud via the video conferencing application installed on the host laptop.

This system architecture leverages existing components with known security profiles, creating no new security exposure. The Solstice Pod is hardened with multiple layers of security capabilities (listed in the General Security Profile of the Solstice Pod section). Existing video conferencing software applications each have their own security profile and are provisioned by IT or installed by individual users according to the IT policy.

Beyond the security profiles of these two components, Solstice Conference includes security capabilities beyond those offered by traditional video conferencing room systems (see Specific Security Features of Solstice Conference section).

General Security Profile of the Solstice Pod Endpoint

Third-Party Penetration Testing

The Solstice product suite, including Solstice Conference, undergoes extensive penetration testing twice a year. The results of these tests are loaded into a secure data room and are made available to our partners and customers under NDA. In addition, Mersive will publish a response memo that details any changes that will be implemented in response to those findings.

Same Enterprise Security Model as the Solstice Pod

When acting as a room system in support of Solstice Conference, the Solstice Pod still provides all the security features that have been built into the product over the past 5 years. These features are detailed in our ‘Security Features of the Solstice Pod’ document. This document is available in the secure data room and can be viewed upon request. Each of these features apply to ensure that the Solstice Pod endpoint, even when being used in conjunction with video conferencing software, remains secure. At a high-level, these features include:

- 2048-bit, RSA-based encryption to all data in transit and at rest
- User authentication for runtime connection that includes a rolling proximity key
- Counter brute-force attack mechanisms including automatic back-off
- Attack detection and logging mechanisms that can be tied to automatic email alerts
- Ability to disable configuration traffic on less-trusted network interfaces (e.g. guest networks)
- Support for secure certificate installation and authentication for both network authentication and SSL-based communication
- Command whitelist enforcement to detect and ignore unknown and potentially dangerous payloads

Specific Security Features of Solstice Conference

Local Content Sharing is Isolated to the Local Network

When using Solstice Conference, users who share content from the Solstice-enabled room are not sending their content directly through the cloud. Instead, that content only traverses the local network and is encrypted in transit. Only when the room display is shared to remote users is that content sent through the video conferencing infrastructure in the cloud. This limits security exposure by retaining privacy for local meetings, or when users in the room are sharing content amongst one another. The security of the video conferencing application only needs to be relied upon when the room display is shared to remote users.

Device Connections Live Behind the Security Firewall of the Solstice Pod

Traditional room systems may involve IoT devices (e.g. audio or IP-enabled cameras) that are directly connected to the enterprise network. This can potentially expose hundreds of endpoints that are independently configured to the enterprise network. Solstice Conference allows users to connect audio and video devices directly to the secure Solstice Pod platform. The Pod’s security layer then sits between these A/V devices and the enterprise network. Because Solstice Cloud is used to manage and monitor both the Pod and the connected devices, a unified approach to security policy compliance and configuration can be applied to Solstice Conference enabled rooms.

No Video Conferencing Endpoint Exists when Not in Use

Because Solstice Conference leverages the meeting host’s device, there is not a persistent video conferencing endpoint that maintains a connection to the cloud. Dedicated video conferencing room systems are “always on” and maintain an open connection to the video conferencing cloud infrastructure. This creates a potential vulnerability as a discoverable endpoint that can be exploited. In the case of Solstice Conference, it is only when an active video conferencing call is in progress that the room system is connected to the cloud.

Remote Content Sharing is Limited to a Single Cloud Connection

Solstice Conference only creates a single connection from the room to the cloud regardless of the number of onsite users that are sharing content. This single connection can be easily monitored by the enterprise firewall and the ability to shut down this connection is an important security distinction from other video conferencing room systems. Traditional video conferencing systems require a new user connection from the enterprise network to the cloud each time a user needs to share content from their device with others in the meeting. Each of these individual connections must be monitored independently and create a new potential vulnerability.

Direct Conferencing Analytics and Monitoring

Each time Solstice Conference is used, information about the conferencing session is relayed to the Solstice Cloud for real-time monitoring and analysis. This information contains important security management information including the conferencing software used and its release version. This helps administrators detect the use of insecure video conferencing software or versions that may be out of date and need to be managed.