



# SphereShield

For Zoom

## MAIN FEATURES



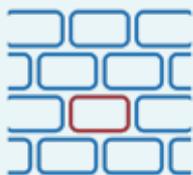
**RECORDING AI  
COMPLIANCE ANALYSIS**  
Audio & Video analysis for  
DLP and eDiscovery Needs



**Archive & eDiscovery**  
Compliance Archive.  
Search and Export  
Information  
Easily and Fast



**DATA LOSS PREVENTION**  
Inspect Content Passing  
Through Zoom to validate  
against DLP policies



**ETHICAL WALL**  
Control External and  
Internal Communications  
and permissions



**MDM/UEM/EMM  
Conditional Access**  
Ensure that only managed  
devices that are compliant  
with security policy can  
connect to Zoom.



**RISK ENGINE**  
GeoFencing and User and Entity  
Behaviour Analytics (UEBA)





SphereShield offers the most complete and advanced compliance and security solutions for all the major UCC (Unified Communications and Collaboration) platforms.

**ZOOM** is one of the most popular Unified Communications platforms in the market. Its success comes from a solution that is easy to use and rich with features. All this power and flexibility opens the door to various, nontrivial, compliance and security risks that can expose companies to regulatory fines and indirect financial losses.

## The Main Challenges

Zoom has been undoubtedly very successful, although its multiple communication and collaboration capabilities have raised many compliance and security concerns. Although it has improved by offering basic barriers as passwords or participant admission, it hasn't been able to provide a solution to automatically analyze the content of the conversations and what is being shared on the participants screens

Additionally, files and messages shared on conversations go without being inspected for data loss prevention or actual malware which means an open door for insider risk.

## Recording Compliance AI Analysis

SphereShield offers a unique capability to archive Audio & Video recordings (including on-premises archiving or VPS) and analyse its content. This is done by transcribing the audio conversation and analysing the on-screen video with OCR. Transcribe all recorded audio to 70+ languages with automatic language detection and speaker enumeration: which speaker spoke which words and when.

Search all meeting content by parameters such as dates, attendees, type (internal/external), text, audio, and more.

Also, inspect meeting audio and video by DLP policies with direct links to incidents.



## Archive and eDiscovery

Meet GDPR and other compliance requirements. SphereShield provides compliant archiving and an intuitive yet powerful eDiscovery engine. Perform advanced search by text, users, dates and more. Sphereshield can integrate with existing eDiscovery systems. Search for personal information and export user data.

## DLP Inspection

SphereShield for Zoom sets itself apart from the traditional Data Loss Prevention products by offering a complete solution that deals with several important limitations found in other solutions on the market. SphereShield offers inspection of Audio & Video, messages and files. This provides SphereShield with a unique capability to inspect existing recordings for DLP incidents with notifications and alerts. Choose between SphereShield's built-in DLP engine with custom rules available or integrate seamlessly with the major DLP vendors

## Risk Engine

SphereShield profiles Zoom usage for the sake of detecting anomalous behaviour.

By understanding the messages, files, hours, devices, IP addresses and other factors it can create and handle security events.

For example: location changes, impossible travelers (jumping from one location to another in a time that is not humanly possible) or users consuming large amounts of data.

Geo Fencing - Set Geo Fencing rules based on groups, domains or users. Allow, block or monitor access from specific countries. Get IP of all active users.

Shows map of all active users and detect when sign in is done from a location / IP that is blocked by geo fencing policy. Sends message when incident is detected

## Ethical Wall

SphereShield addresses many important regulatory issues by offering a flexible and granular control of who can communicate with whom and in what ways.

Address both internal and external users. Control which specific collaboration options to block and which to allow: Messaging, File-Sharing, Audio, Video, Screen-Sharing.

SphereShield allows users to create granular policies based on external traffic, users and groups

## Threat Protection | Conditional Access

-Threat protection – Anti Virus/Malware/Phishing: Analyze messages and files on Zoom meetings conversations. Get notifications and alerts.

-Conditional Access – ensure that users can only log on from a managed device . Integrates with the leading vendors such asBlackberry, MaaS 360, Airwatch and Citrix



## COMPLIANCE

- Ethical Wall | Data Governance
- Recording AI Compliance Analysis
- Archive & eDiscovery
- Data Loss Prevention



## SECURITY

- Threat Prevention | AntiMalware Antivirus
- Risk Engine | Geo Fencing & Behavior Anomaly Detection
- Conditional Access

### About AGAT Software

AGAT Software is an innovative security provider specializing in security and compliance solutions. AGAT's SphereShield product suite handles security threats related to authentication and identity as well as content inspection and data protection. Utilizing this expertise, AGAT developed SphereShield **to secure unified communications (UC) & collaboration platforms such as Microsoft Teams, Slack, Zoom, Webex and Skype for Business,**

For more information, visit <http://AGATSoftware.com>

For updates, follow us on [LinkedIn](#) & [Twitter](#).



AGAT Software, Har-Hotzvim Hi-Tech Park, Jerusalem, Israel  
Tel: +972-2-5799123, Mail: [sales@agatsoftware.com](mailto:sales@agatsoftware.com)