AGAT

SphereShield
For Microsoft Teams

MAIN FEATURES

INLINE REAL-TIME DLP

Inspect Content Passing Through Microsoft Teams in Real Time

>

ETHICAL WALL

Control External and Internal Communications and permissions

>

Archive & eDiscovery

Compliance Archive. Search and Export Information Easily and Fast

>

CHANNEL MANAGEMENT

Move, Archive and Export Channels in Microsoft Teams

>

RECORDING AI COMPLIANCE ANALYSIS

Audio & Video analysis for DLP and eDiscovery Needs

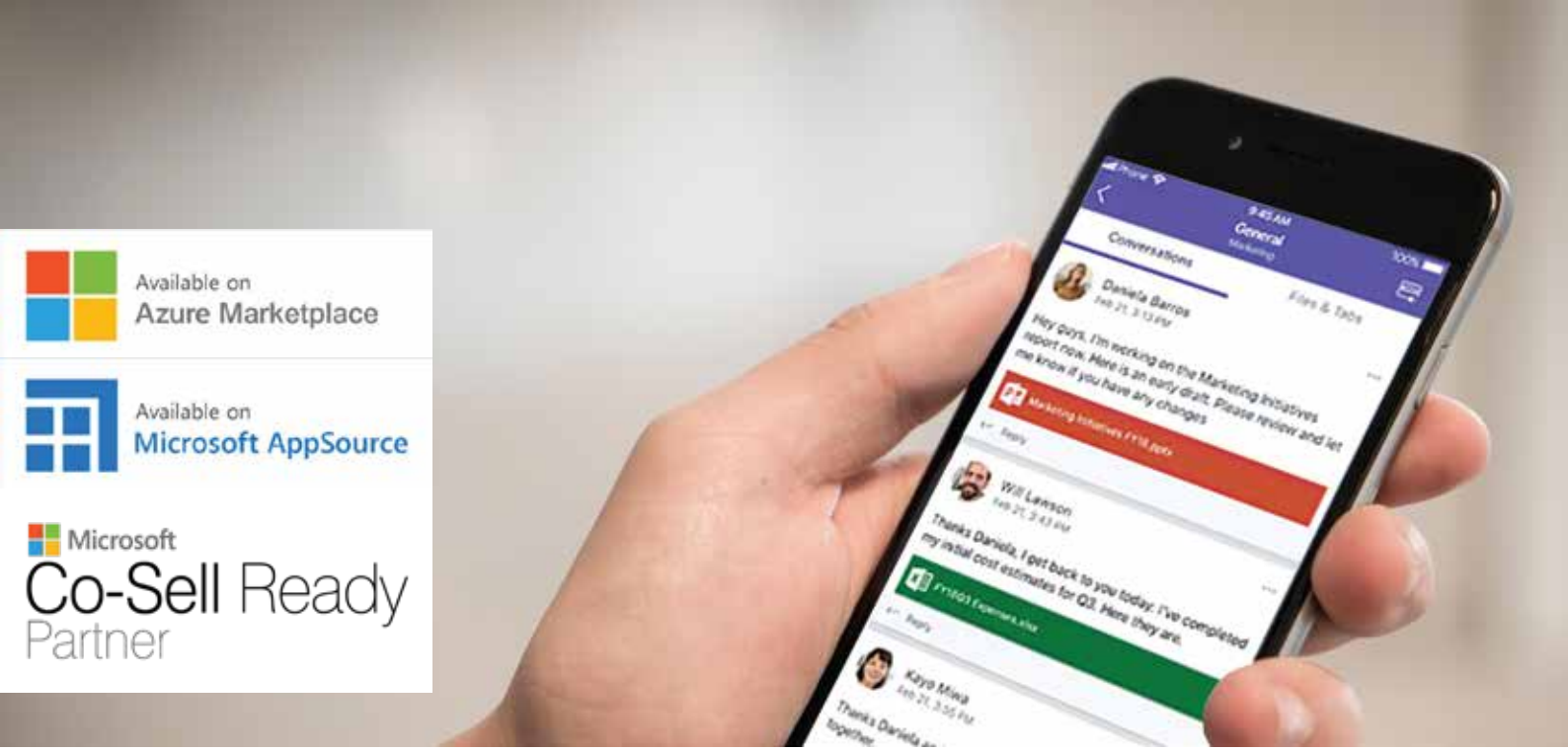
>

RISK ENGINE

GeoFencing and User and Entity Behaviour Analytics (UEBA)

>

Microsoft Partner



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

MICROSOFT TEAMS 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

Microsoft Teams has been very successful, although its multiple communication and collaboration capabilities have raised many compliance and security concerns.
External users and guests can freely message and share files within the company without an effective way to determine who can communicate with whom.
Additionally, information doesn't get analysed to determine whether it contains sensitive or even harmful content.

Microsoft Teams puts all of the company in a single environment without any specific team division or hierarchies. It erases barriers to communications that are sometimes necessary due to the nature of the organization or to comply with specific regulations.

Inline Real-Time DLP Inspection

SphereShield for Microsoft Teams 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 Real-Time inspection of messages, files and even Audio & Video* for the complete scope of Teams, Channels, Chats and Meetings. This means that SphereShield can prevent sensitive data from being sent to the cloud and reaching its destination even for a short period of time.
You can choose to either block, mask or just to be notified about the incident.
Choose between SphereShield's built-in DLP engine with custom rules available or integrate seamlessly with the major DLP vendors

SphereShield allows users to create granular policies based on external traffic, users, groups and Teams.Scan all the content used in MS Teams including Exchange, OneDrive and SharePoint.

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 external users and guests as well as internal communications between different Active Directory Groups, Azure Active Directory Groups, Users, Domains and Teams.
Control which specific collaboration options to block and which to allow: Messaging, File-Sharing, Audio, Video, Screen-Sharing.
Check This comparison Table to understand how SphereShield compares and adds value to Microsoft Information Barriers.

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.

Channel Management

SphereShield for Microsoft Teams provides multiple productivity tools with Channel Management. Channel Management helps your Teams environment evolve with your ever changing business. Move, Archive, Export, Copy & Merge Channels. Remove the clutter, increase productivity and archive when needed.

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. Capable to integrate with existing eDiscovery systems. Search for personal information and export user data. SphereShield provides a full data dashboard independent of O365. Supports files and messages as well as Audio & Video*

Risk Engine

SphereShield profiles Teams 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.

Additional Security Solutions

-Threat protection – Anti Virus/Malware/Phishing
-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

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