Security And Complaince For Webex Teams

SphereShield for Webex Teams is a robust solution designed to help companies deal with issues of access control, compliance, and threat protection when deploying Webex Teams.

Ethical Wall | **DLP** | **Risk Engine**

eDiscovery | **Antivirus** | **MDM/UEM**

Highlights

- Ethical wall with granular communication control
- Prevent sensitive data being shared with wrong people or reaching the cloud
- Advanced communication capabilities (e.g., file transfer, desktop sharing, chat) control
- Control internal, external or guest communication
- Full visibility of communication, data and activity via eDiscovery module
- Admin portal with a variety of reports, auditing and eDiscovery tools

Ethical Wall To Allow you Control Communication

Restrict communication participants, and control or block specific options such as chat or file sharing, between different users. Granular control is offered based on groups, domains and users and applied dynamically based on the context of the communication. Specific policies can be applied to chat, teams and meetings depending on participant type (Employee, external or guest).

Use Existing DLP Infrastructure

SphereShield is leading in its field with an inline DLP inspection that is capable of blocking or masking all data that is defined as sensitive in real time, before arriving to its destination. Gain control over what they users can share. DLP inspection can be done by our built in engine or utilizing existing DLP infrastructures of leading DLP vendors. SphereShield can be integrated with Symantec, McAfee and ForcePoint.

Prevent Sensitive Data From Being Uploaded To The Cloud

Utilizing cloud platforms while making sure all sensitive data is not leaving the network may pose as a challenge for companies that have DLP concerns. SphereShield lets you keep your organization's delicate information secure on premise.

Risk Engine To Control Who Connects To Your Network And From Where

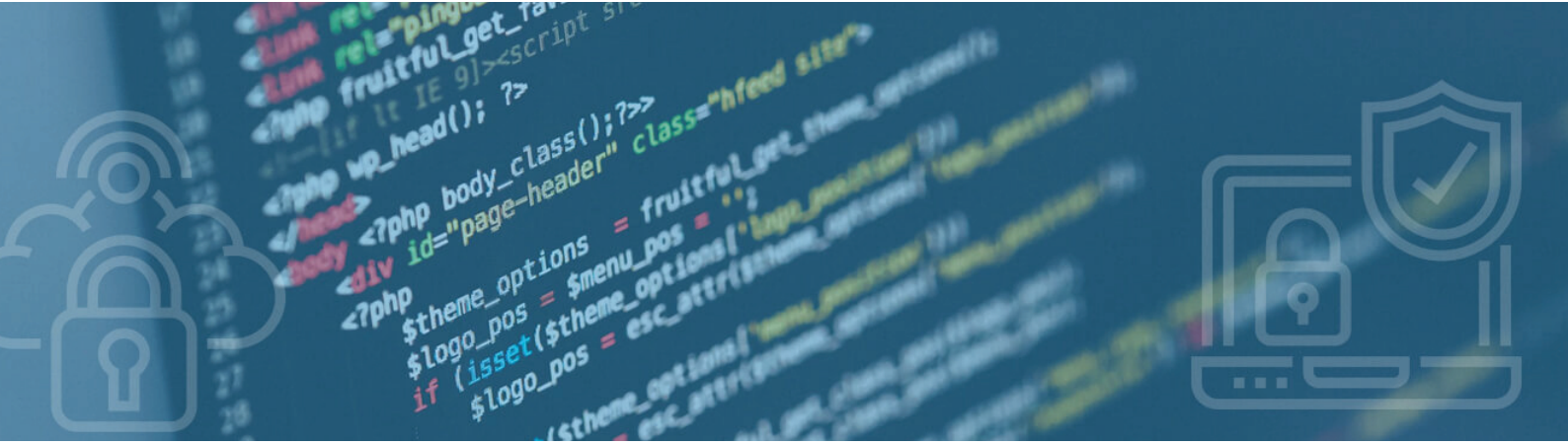
SphereShield Displays a live map showing locations from which parties are connecting helping you monitor where failed access attempts occurred. Users Receive security alerts in response to detection of suspicious changes in location, device, data capacity, and in reaction to atypical activity. In addition, you are able to block connection from specific locations or allow access from these locations only to specific groups / domains, by defining Geo-Fencing rules.

Search And Export Information Easy And Fast With eDiscovery

SphereShield's advanced eDiscovery module offers a search by text, user, dates and more. Users can see messages and file incidents in context, and archiving can be done on-site. SphereShield can also be integrated with existing eDiscovery and archiving solutions.

Keep Your Network Safe With Our Antivirus

Use SphereShield's Antivirus to scan files, or integrate it with leading vendors such as Kaspersky, McAfee, Symantec and more.



Featuring DLP and Antivirus integrations with leading vendoers

McAfee™ Symantec FORCEPOINT

KASPERSKY Fidelis™ Cybersecurity

About AGAT Software

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

AGAT's client base consists of government offices, banks, insurance companies and large industrial global corporations, including Fortune 500 companies.

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

AGAT

AGAT Software, Har-Hotzvim Hi-Tech Park, Jerusalem, Israel
Tel: +972-2-5799123
Mail: info@agatsoftware.com