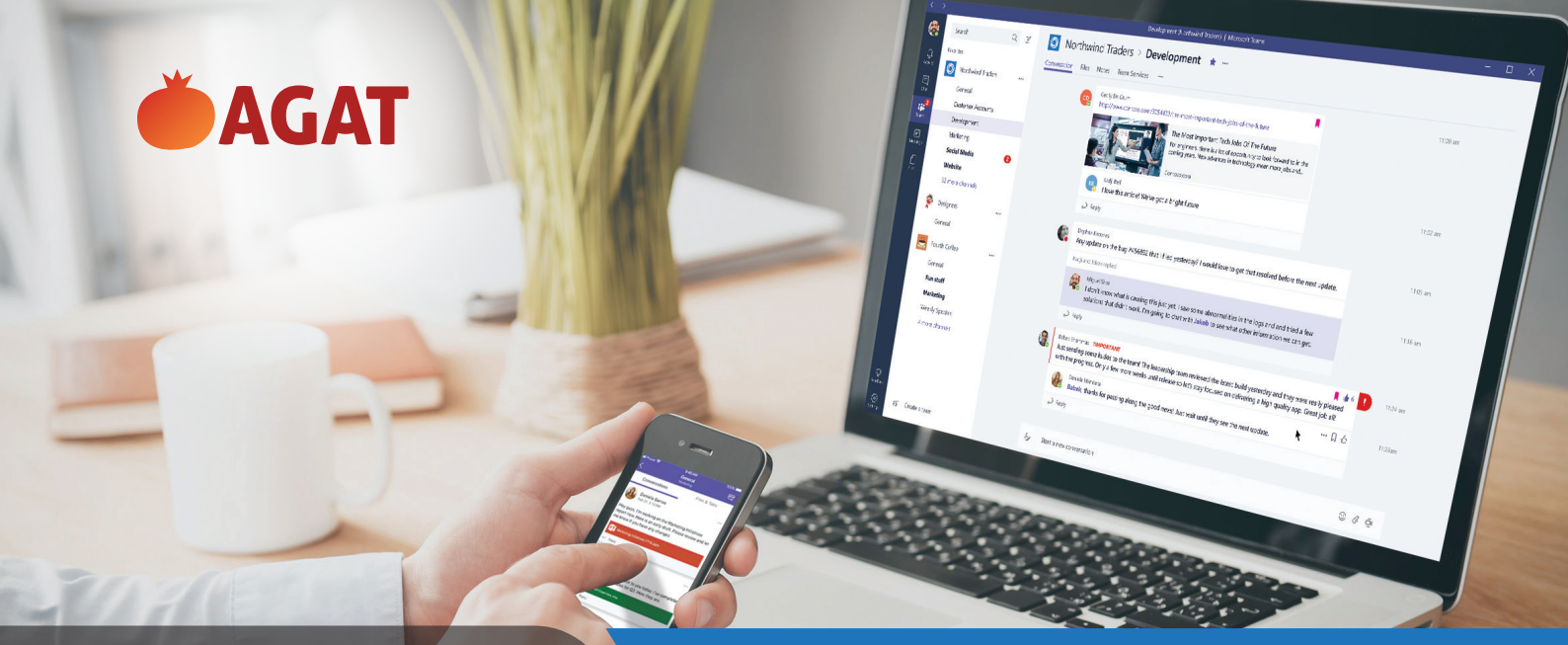
AGAT



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 Traffic

MDM CONDITIONAL ACCESS

Verify That Only Managed Devices Can Connect to Microsoft Teams

RISK ENGINE

Define Geo Location Rules and Display Live Map of Connections

ANTIVIRUS

Verify That no Malicious Code or Viruses are Uploaded to the Cloud

eDISCOVERY

Search and Export Information Easily and Fast

SphereShield offers advanced compliance and security solutions for Unified Communication services including Microsoft Teams.

Microsoft Teams offers an agile and easy-to-use unified communication platform. Yet, when using it, organizations need to take into consideration aspects of compliance and security. Microsoft Teams is an open platform that offers a vast range of collaboration options at the tip of the finger, anytime, anywhere and from any device. Utilizing such an accessible platform raises challenges with controlling communication to align with regulation, compliance, business needs, DLP and security.

The Main Challenges

While Microsoft Teams is an open platform that offers a vast range of collaboration options, it may raise some compliance and security problems.

Sensitive data might leak when two or more users are communicating. Therefore, preventing sensitive data from being passed through UC channels in real time is a main concern of companies that handle sensitive information. Many organisations already use DLP (Data Loss Prevention) products to contend with these threats, however most do not cover Microsoft Teams.

Managing a Unified Communication platform, requires addressing any collaboration between organizations or departments. To prevent compliance violations or conflict of interest, and accomplish your business strategy you may want to restrict specific users / groups / domains communication with each other, and their communication capabilities.

Team's accessibility anytime, anywhere and from any device challenges compliance and security, as employees might access their account from unmanaged devices.

Inline Real-Time DLP Inspection

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.

Address end-user unawareness and control what they can share and with whom. DLP inspection can be done by utilizing existing DLP infrastructures of leading DLP vendors. This allows reusing existing company policies, knowledge and experience. SphereShield can be integrated with Symantec, McAfee and ForcePoint. SphereShield also offers a build in DLP engine.

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 sensetive information secure on premise.

Ethical Wall

SphereShield can define and apply communication policies that 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 are 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).

MDM/UEM/EMM conditional access

SphereShield allows verifying that only managed devices that are compliant with security policy can connect to Microsoft Teams. SphereShield can be integrated with the following leading MDM vendors: MobileIron, BlackBerry, MaaS360, Airwatch and XenMobile.

Compliance and GDPR

SphereShield offers Tools for complying with GDPR regulations.

eDiscovery

SphereShield helps you to meet GDPR and compliance requirements with a full on-cloud or on site data dashboard independent of O365. Easily Integrated with existing eDiscovery and archiving solutions.

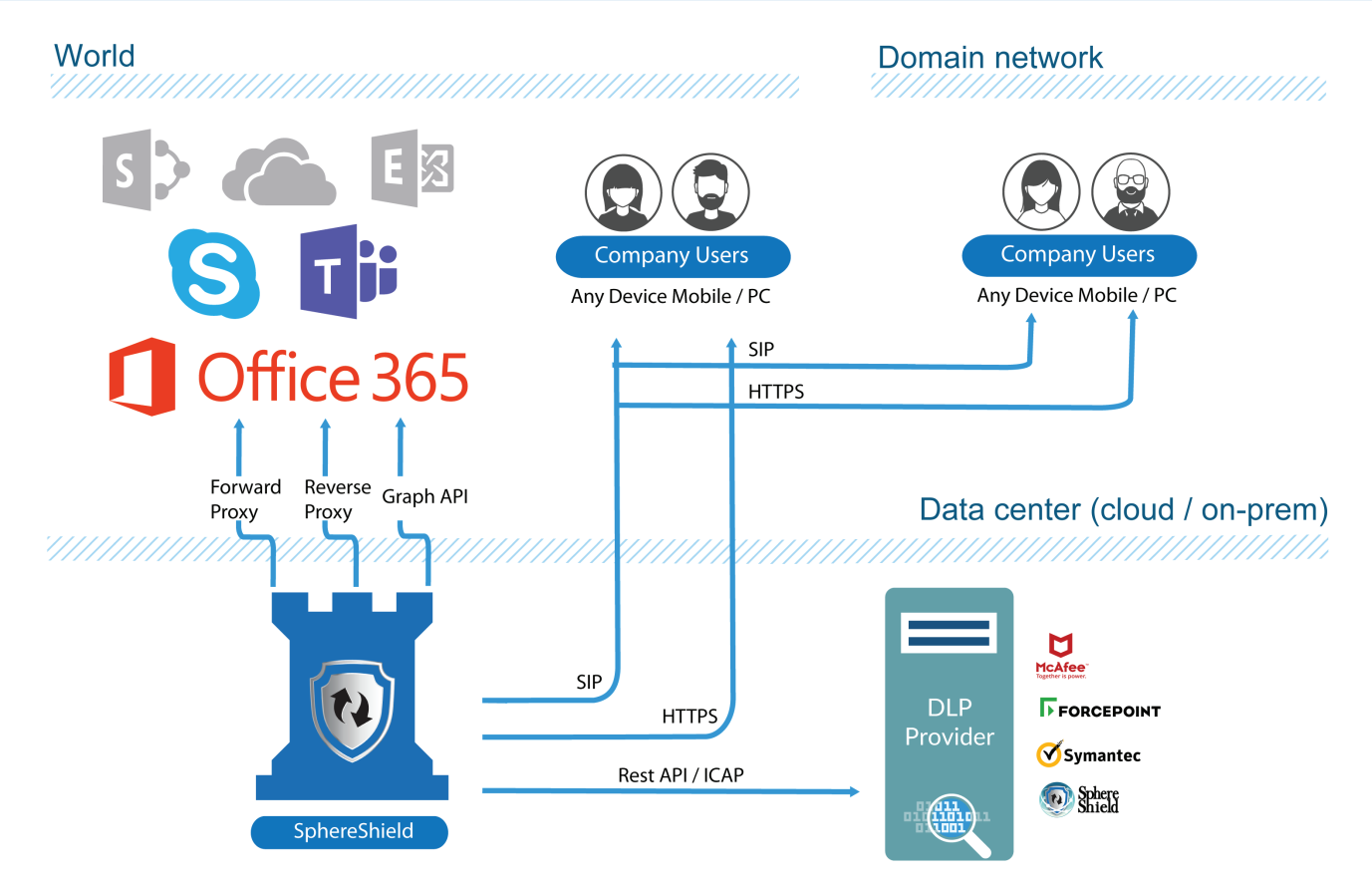
Risk Engine

Define Geo location rules and display live map of connections. Recieve security alerts in response to detection of suspicious changes in location, device, data capacity, and in reaction to atypical activity. Geo-fencing rules are defiened to block connection from specific locations or allow access from these locations only to specific groups / domains

Antivirus

Verify that no malicious code or viruses are uploaded to the cloud. SphereShield can be Integrated with Kaspersky, McAfee, Symantec, Sophos and more.

SphereShield for Microsoft Teams Topolgy



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 communication (UC) & collaboration platforms such as Skype for Business or Microsoft Teams.

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: info@agatsoftware.com