AGAT

SphereShield

Secure your
Skype for Business
deployment

COMPLIANCE
- Data Leak Prevention
- Data Governance and eDiscovery
- Ethical wall policy engine

ACCESS CONTROL
- Multi Factor Authentication
- MDM/EMM Device Verification
- Account Lockout Protection

THREAT PROTECTION
- User and Network Behavior Detection
- Anti Malware Anti Virus
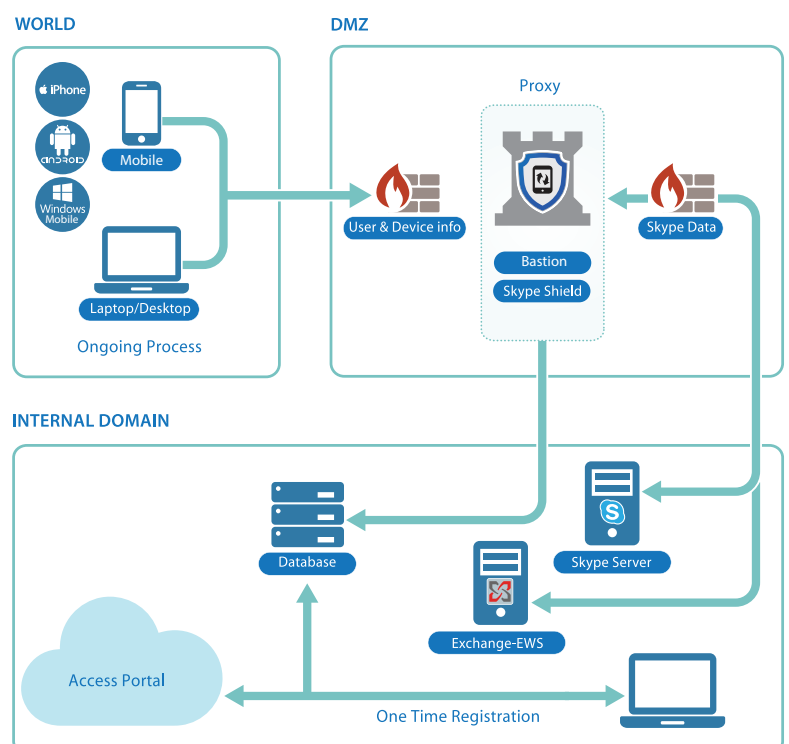- Auditing and security Events

SphereShield

Key Features:

- Federation Ethical wall
- Two Factor Authentication
- Account lockout Protection
- MDM conditional access
- Data Leak Prevntion
- eDiscovery
- Risk Engine
- Anti Virus/Anti Malware

Skype for Business tunneling into the network

Smartphones and personal computers can connect to Microsoft Skype for Business server using the Skype for Business client. While connected, sensitive information is exposed by Skype & Exchange servers, requiring the organization to take precautions. Companies realize that securing Skype connectivity is as important as obtaining remote access because smartphones can be used as a tunnel into the corporate network. SphereShield is specially designed to address the complex security and compliance needs of Skype for Business.

Skype Shield Typical Architecture

WORLD

iPhone

Android

Windows Mobile

Mobile

Laptop/Desktop

Ongoing Process

DMZ

Proxy

User & Device info

Skype Data

Bastion

Skype Shield

INTERNAL DOMAIN

Database

Skype Server

Exchange-EWS

Access Portal

One Time Registration

Product Features (Desktop & Mobile)

Two Factor Authentication

Requiring the device as the second factor in addition to credentials. Blocking authentication to Skype for Business and Exchange (EWS) by only knowing valid credentials.

DLP engine

Apply content rules policy on data such as preventing Social Security numbers, credit card numbers ID numbers from used in Skype for Business. Available as a stand-alone DLP engine or as an adaptor to commercial vendors such as Symantec, McAfee, and ForcePoint.
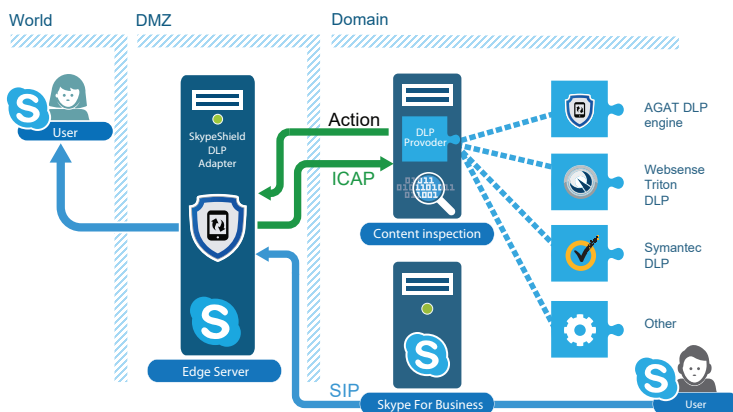
Block DDoS Attacks & Prevent Account Lockout

Prevent account lockouts resulting from Distributed Denial of Service (DDoS) and brute force attacks on Skype for Business servers for all SIP and HTTP authentication channels. Monitor failed login and device pre-authentication in the DMZ.

MDM Conditioinal Access

Restricts access to the organization's Skype for Business server only to devices with MDM. Verifies Skype is used with a device that complies with the security policy. Compliant with all leading vendors in the market like MobileIron, Air Watch, MaaS360, BlackBerry, XenMobile, and Intune.
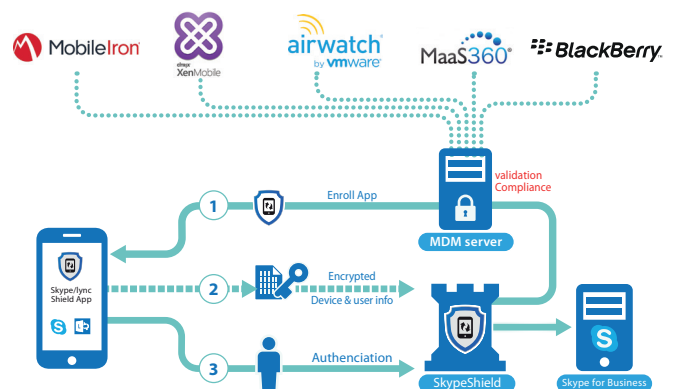
Federation Ethical Wall

Solves GDPR compliance, security and data protection requirements. Applies federation policies based on specific users, groups or domains/companies. Granular modality policy control handling IM, File transfer, Meeting, Audio, Video and more.
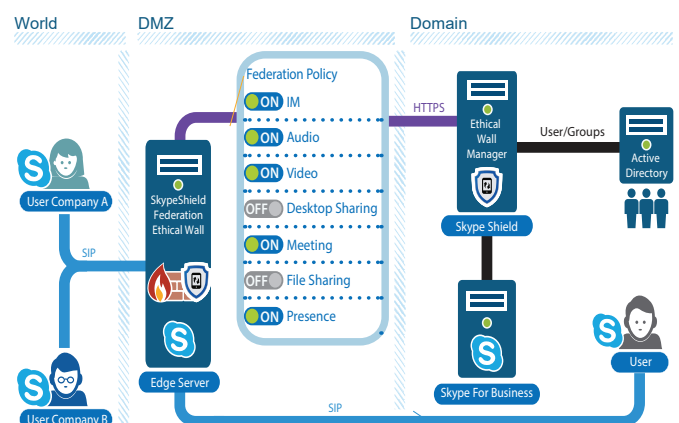
Device Access Control

Restricts the usage of Lync and Exchange only to registered devices. You can filter by device type and operating system version.

Smart Card Login

Offers a solution for organizations with a network policy requiring smart card login to allow authentication and use of mobile Skype for Business

RSA Token Authentication

Eliminate the need to use AD credentials for users of secure tokens wishing to connect Business servers from external devices and enable Two Factor Authentication based on the token.
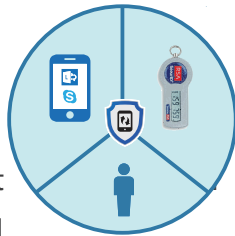
Exchange EWS Protection

Protect your Exchange Web Services (EWS) against account lockout and only allow access to EWS from registered devices (TFA). Block unauthorized access to emails using EWS.

Authorised Device

Non Authorised

EWS Protector

Exchange
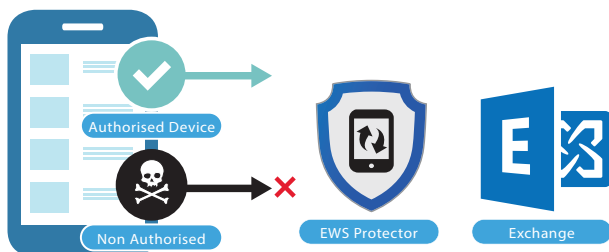
eDiscovery

Enable Skype for Business data governance as per GDPR regulations with advanced search capabilities that allow exportation or removal of conversations and the messages and files within.
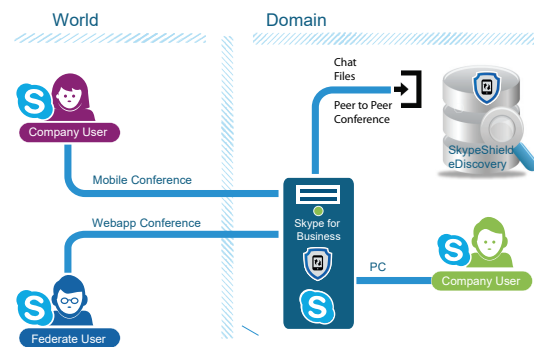

SkypeShield Application Firewall

A module sanitizing non-authenticated requests to avoid any traffic passing through into the network without verification. Also, firewall verifies meeting ID before allowing request to go through and blocks unverified access. The Firewall also performs session termination and rewrites requests allowing only legitimate traffic to reach internal servers.
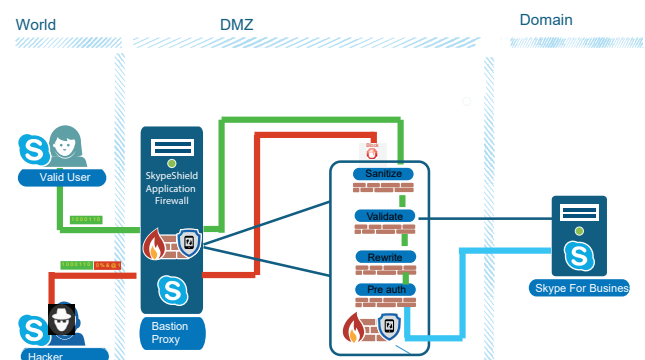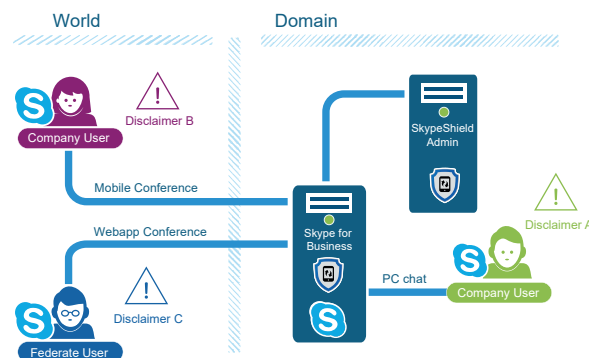
Risk Engine

Define Geo location (Geo-fencing) rules. Display live map of connections. Pro le user behavior and create security alerts when detecting suspicious changes related to location, devices, data capacity, activities.
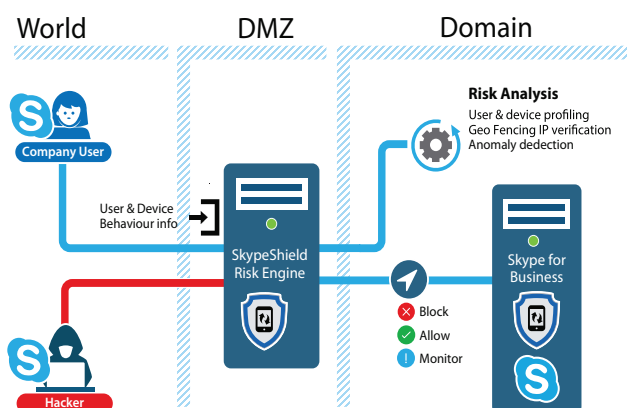
Disclaimers

Multiple context based disclaimers can be shown in conferences or conversations, based on domain, user type and more.

Active Directory Credentials Protection

Defining dedicated Skype for Business credentials that are different from the Active Directory credentials to address the risk of hacking network credentials.

About AGAT

AGAT Software is an innovative security provider specializing in security and compliance solutions. SphereShield - AGAT's product suite handles security threats related to authentication and identity as well as content inspection and data protection. Utilizing this expertise, AGAT has developed a solution for securing Microsoft Skype for Business with specific unified communication requirements. The solution can be implemented for On-Premise or for cloud as a Cloud Security Access Broker (CASB) SphereShield also offers a solution for securing Microsoft SSO infrastructure (ADFS) allowing authorized users to continue accessing cloud-based services even when their account is under DDoS attack SphereShield platform is integrated with leading security platforms (MDM, DLP, SIEM, Anti-Virus) such as Symantec, McAfee, MobileIron, IBM, VMWare, Citrix, BlackBerry, F5, ForcePoint, Kaspersky Labs and RSA.

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