## Security Threat

### Account Lockout
Network account can be locked by an attacker simply sending authentication attempt while only knowing user name and not password (DDoS attack). Attack can be on multiple protocols (SIP/HTTPS), Multiple channels (sign in, Exchange, web api..) and multiple methods (basic, NTLM, SOAP) services

### Device Security Control
User can download SbB on a personal device which is not under MDM control and is not aligned with company security policy (jail broken for example) and bypass all MDM security layers by connecting to SfB server

### Communication Control
- Compliance and security require controlling modalities between communication participants
- No ability to define what is allowed to do and see - IM, file sharing, audio.. between federated users and internally
- Privacy issues related to presence
- Server info exposure

### Secure Authentication
Attacker can get access to SfB & Exchange by only knowing user name and password

## Solution

### Unified Monitoring & DDoS Protection
- Unified monitoring of all multiple authentication services and activate soft lockout protection to block external attempts from locking account
- Allow authentication to enter domain only from pre-registered device

### MDM Conditional Access
- Restrict registration only to managed devices
- Block devices as soon as they become out of compliant in case or removed from MDM control.
- Compliant with all leading vendors in the market including AirWatch, MobileIron, XenMobile, GOOD, MaaS360

### Ethical Wall
- Ethical wall engine with sophisticated policy rules
- Granular control on each activity based on parameters such as groups, domains, SIP, contact list
- Can be implemented to control external and internal communication

### Two Factor Authentication
- Two Factor Authentication (Skype & Exchange) by device enrollment
- Optional token authentication- RSA, Google authenticator, Microsoft Authenticator
**UNAUTHORIZED DEVICES**
- Control which devices can connect to company infrastructure

**DEVICE ACCESS CONTROL**
- Device enrollment process
- Filter by device type/ OS version

**ANONYMOUS TRAFFIC**
Allowing external guests required unauthenticated and anonymous requests to enter the network without inspection. Topology allow malicious traffic to get to internal servers and to overload internal servers with fictitious meeting requests

**APPLICATION FIREWALL**
- Application firewall in DMZ specifically designed for SfB traffic
- Protocol level sanitize- verify request structure and content
- Application level validate- validate meeting ID data
- Request rewrite- Verify all traffic entering the network is as expected and clean from malicious code

**CREDENTIAL THEFT.**
Domain credentials required by S4B can hacked while stored and used on device out of network control. Also users don’t have domain credentials when using smart card users

**APP CREDENTIALS**
- Authentication with specific SkypeShield credentials
- Soft token password
- Using smart card with PC to obtain sign in credentials for mobile

**SENSITIVE DATA LEAKING**
- Prevent sensitive information from being passed through Skype for Business to devices outside of company control.
- Require solution for all type of Skype for Business client

**DATA LEAK PROTECTION**
- Server side solution for inspecting content
- Build in DLP engine for blocking, modifying or masking sensitive information
- Request rewrite- Verify all traffic entering the network is as expected and clean from malicious code
- Group based rules
- IM notification
- Incident auditing
- Commercial DLP integration

AGAT Software is a security provider specializing in external access authentication and data protection solutions.

For additional information visit:

SphereShield.com
SkypeShield.com
AGATSoftware.com

AGAT Software, Har-Hotzvim Hi-Tech Park, Jerusalem, Israel | Tel: +972-52-5209860 | Email: info@agatsoftware.com