4Sight Communications
www.4sightcomms.com
info@4sightcomms.com

Securing your Journey to Teams

Microsoft Teams has emerged as the leading platform for enterprise communications and collaboration. The benefits of Teams include the built-in integration with other Office applications (in both the product and offer structure), tools that enable better workgroup collaboration, and flexibility in call control and voice services deployment.

If you are considering a Teams deployment or have already taken the plunge, there are a number of considerations that you will need to evaluate. Teams is a departure from previous Microsoft UC platforms (Skype for Business, Lync), as it is fully contained in the Microsoft cloud. While this makes it easier to deploy (no more complex premises hardware), you will still have to decide how you deploy voice services and how you properly secure your network. Ribbon makes this process both simple and cost effective.

For voice services, Teams offers two options –Microsoft's Phone System and Calling Plans or a 3rd party SIP Trunking provider, which is known as Teams Direct Routing. The table below provides a comparison between the two approaches.

500,000+
More than 500,000 organizations use Teams

91%
91 Fortune 100 companies use Teams

44+
In 181 markets with support for 44 languages and growing

10,000+
150 organizations have 10,000 or more active users

	Microsoft Calling Plans	Teams Direct Routing
Geographic availability	Mainly North America and UK with limited availability elsewhere.	No geographic limitations depending on the capabilities of the service provider.
Pricing	Generally flat rate per employee.	Allows for ease of call aggregation across employee groups, ensuring greater flexibility and generally making it more cost effective.
Session Border Controller (SBC) required?	No.	Yes. However, in combination with lower voice costs, the TCO of including an SBC is minimal.
Survivability/High Availability	Reliant upon the components and design of the Microsoft network.	More flexibility in the deployment means that elements such as hardware redundancy (HA) and link failover can be easily implemented.
Best For:	**Smaller enterprises (< 25 employees)**	**Mid to large enterprises**

For most enterprises, Direct Routing will be the obvious choice, providing you flexibility, cost efficiency, and geographic coverage. Moving forward you will need to decide who will provide you voice services. This provider will develop a design and provide pricing tailored to your enterprise's requirements. There are many service providers and system integrators that are deeply imbedded in Microsoft telephony solutions. They will be invaluable in a successful implementation.

Obviously no implementation could be successful without planning for and implementing a top-to-bottom security policy. The vulnerabilities typically focused on in voice networks – toll fraud and denial of service attacks – have huge economic consequences if not protected against properly. The latest data from the Communications Fraud Control Associations says that toll fraud cost enterprises upward of US$6 billion per year.

The following section discusses, in greater depth, some of the components that help make a Teams implementation secure.

Session Border Controller (SBC)

Whether you purchase your own SBC or have it included within the deployment from your Teams implementation partner, it is a vital, required component within your network. At a high level, an SBC is part firewall, protecting the network from IP-based attacks; part traffic cop, policing traffic to prevent overloads and directing it over shorter distances to save money; and part peacemaker, ensuring that networked devices from different vendors all speak the same language, allowing high quality of voice conversations to be maintained. Microsoft requires a certified SBC to be present in any Direct Routing implementation.

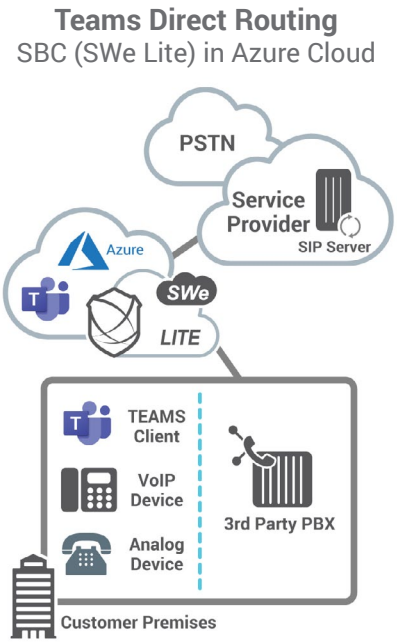
Going a step deeper, let us discuss some of the key benefits of an SBC relating to security:

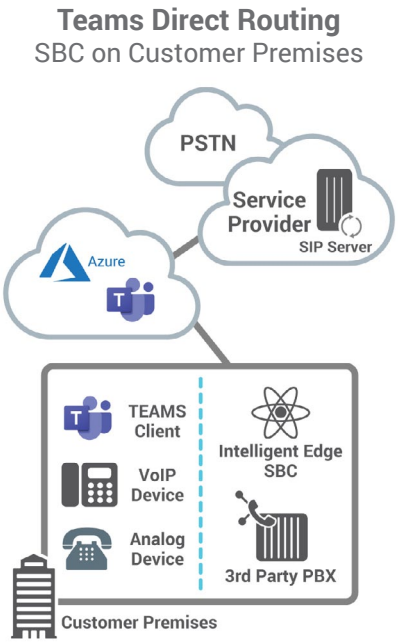
Toll Fraud Protection. IP telephony scams can come in many forms. In most cases, hackers gain access to corporate voice networks to make free international calls, which can cost the enterprise tens of thousands of dollars. A primary defense is deploying an SBC to hide the enterprise's network topology from the outside world. Another layer of protection – an overarching analytics engine – is needed, to analyze traffic, look for patterns, and cut-off attacks as they happen, minimizing the likelihood of similar future attacks.

DoS and DDoS Defense. Denial of service attacks can cripple your network, causing you lost business and high levels of customer dissatisfaction. To combat DoS/DDoS, SBCs use specialized policing software to deal with high traffic volumes and protect the core network from attacks.

Encryption. A well-constructed Teams implementation will design in media and signaling encryption to prevent eavesdropping by bad actors. An SBC can perform encryption and decryption depending on what the endpoint or network element requires.

Malformed Packet Protection. An attacker may attempt to send malformed packets to cause an application or service to crash, or otherwise exploit a vulnerability that provides unauthorized access. An SBC maintains full session state information and is therefore able to detect and respond to attempts to send malformed packets over the network.





In addition to security and fraud protection, implementing an SBC has a number of other benefits. First, since an SBC is a connector between networks and network elements (phones, PBX, cloud-based Unified Communication servers) it enables you to execute a phased approach to Teams deployment. This is particularly relevant if you intend to keep your current PBX or UCaaS service as the underlying call control while using Teams for collaboration and messaging.

Second, an SBC gives you flexibility to change SIP trunking vendors at any time. Since you own the SBC that terminates the SIP Trunks, moving vendors is not a huge burden.

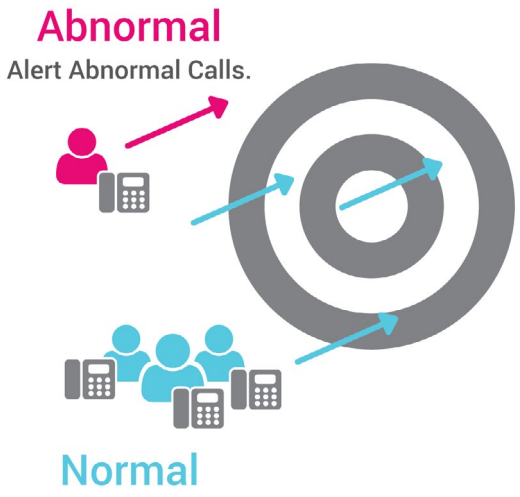
Last, an SBC is an investment in your network infrastructure. It will future-proof you against incremental investments should you change course. Additionally, cloud-based SBC implementations (such as the Ribbon SWe Lite in the Azure Marketplace) have nearly infinite session capacity, ensuring you do not grow out of capacity as your business expands.

Ribbon SBC's are built on a carrier grade, battle-tested architecture that can be found in thousands of enterprises globally. Ribbon SBCs are fully certified by Microsoft. This has important benefits, including that Ribbon SBCs are part of the Microsoft test cycle as new Phone System features are introduced. Customers are also guaranteed support from Microsoft when using certified SBCs, and our support organizations work together closely to quickly resolve issues. Ribbon SBC's can be deployed as physical appliances, virtually on universal CPE, or cloud-based in Microsoft Azure (SWe Lite).

Analytics – Fraud Protection

Communications fraud costs enterprises billions of dollars per year. In order to meet their objectives (generally financial gains), bad actors often cover a broad set of call scenarios – from PBX hacking, to subscription fraud, to Wangiri (one ring and cut) and other use cases. With the variety and inherent complexities of SIP and VoIP protocols, Teams environments will benefit greatly from the added value of behavioral analytics and anomaly detection to deter or eliminate the various types of fraud attacks.

Most UC fraud activities are traced to a few behaviors in calling destination and traffic patterns. Identifying the patterns can be as simple as noting the destination or as complex as requiring historical analysis of traffic. The most successful attacks tailor the fraud to mimic actual user or network behavior. This allows them to go unnoticed for the most amount of time and generate significant costs to the unsuspecting organization. Bad actor attacks may be focused on specific items.



Ribbon's solution for toll fraud protection - FraudProtect - gives you valuable insights and mitigation policies by using network behavioral analytics and customizable incident detectors to stop fraud before the bad actor(s) can do any damage.

FraudProtect provides you with the insights and tools needed to identify and stop the UC fraud in your network. FraudProtect will help you by identifying repetitive calling patterns and flagging them as anomalous activity. This is done in real-time based on destination detection and other criteria. Fraudulent calls are quickly identified and terminated, mitigating the potential for expensive toll charges.

Network Behavioral Analytics

FraudProtect models your network traffic patterns to establish a baseline "normal" activity. From here, anomalies and devia-tions from the established baseline are graded for fraud likeli-hood and reported to you for mitigation.

As it learns more, the FraudProtect behavioral model will include variations for seasonality or changes due to business growth. It will continue to add these to the baseline to refine the predictive process.

Incident Detectors

As an additional layer of fraud detection, FraudProtect has a customizable toolset called incident detectors. This allows you to create undesired activity flags modeled to your specific requirements. These detected incidents can trigger an alert or automate a network response to stop fraud in your network.

Ribbon FraudProtect works with Ribbon SBCs and other network elements, including third party devices, to provide you with a comprehensive solution set for your Teams implementation.

At 4Sight Communications, we are passionate about Unified Communications. We work with our customers to reimagine the world of business communications and collaboration. We drive progress, innovation and creativity at a rapid pace with the shared goal of helping businesses stay ahead of the curve when it comes to taking advantage of the latest technology. This is how we can ensure that business will be done more efficiently and effectively.

For more information, please contact your designated account manager or request more information at info@4sightcomms.com.