StarLeaf

Security Whitepaper

July 2018

Contents

Introduction

Business applications delivered from the cloud should be compelling for all companies–no matter their size or geographic spread. The cloud offers on-demand services, 24x7 support, a pay-as-you-go/pay-as-you-use pricing model, and will effortlessly scale to meet spikes in demand. So while service availability, high-performance, and security are key considerations, the real benefit of the cloud is a financial one. Placing infrastructure, the system core, in the cloud at geographically dispersed Points of Presence (PoPs) provides access to its rich functionality over the Internet. For end users this means that there is little or no capital investment in on-premise infrastructure. Costs are reduced further with no management burden placed upon internal IT resources.

However, when considering business video for mainstream communication, security, performance and reliability must be assessed.

In this paper, we look at the common security flaws and the areas of risk that exist today. We explain how StarLeaf eliminates risks, to ensure an open and secure environment for all internal and external video calls. Also, we outline how the StarLeaf Cloud guards against service downtime to provide resilience and high availability on a 24x7 global basis.

Security risks when endpoints are placed outside of firewalls

The first area of concern is the positioning of endpoints outside of a company's firewall. This is common practice as it provides the easiest way to enable video calling with other organizations, and external bridging services. Many end users omit to change default logins, which then allows hackers easy access to the equipment. Furthermore, these endpoints can be maliciously targeted for 'denial of service' attacks. Placement of endpoints outside of firewalls also exposes any vulnerability in the software, to allow hackers to do irreparable system damage.

Historically, video conferencing equipment has been of a proprietary nature, and deployed in such low volumes that it has avoided the attention of Internet hackers. Today, there is growing evidence that this is no longer the case; as companies increase their deployments of both software clients and personal devices, alongside increased use of video conferencing rooms, hackers are taking notice and beginning to target the equipment.

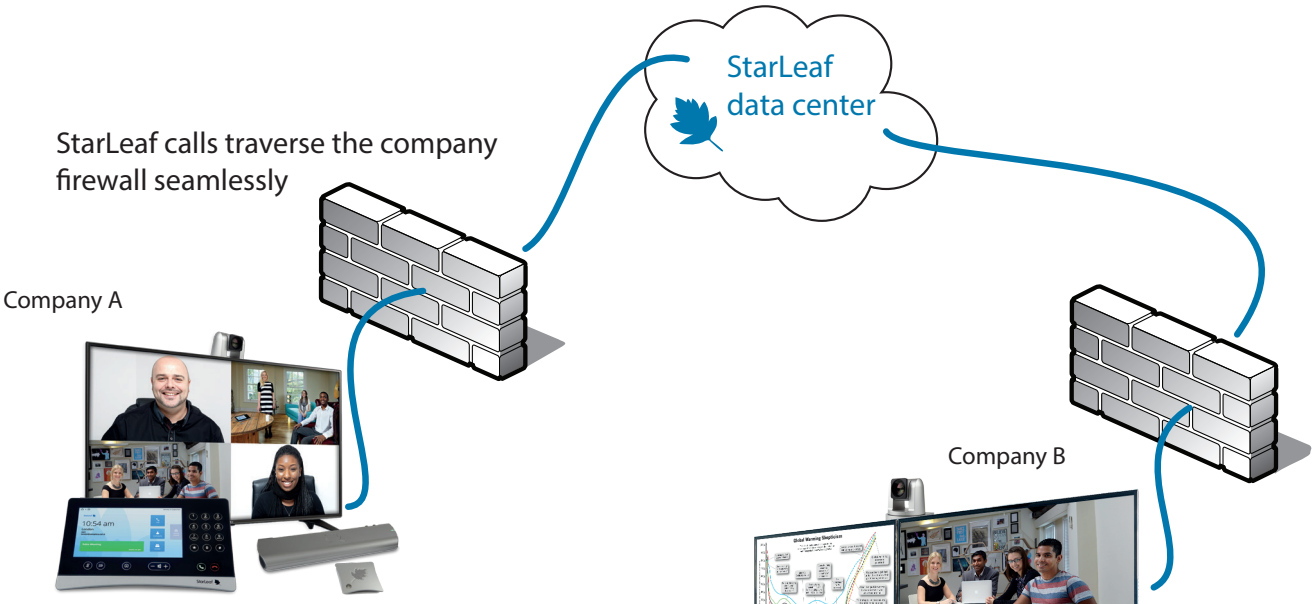
A new problem for endpoints that are outside of firewalls is H.323 spammers. This problem manifests itself as multiple nuisance calls to H.323 video endpoints. The spammers are actually looking for 'dial-tone' for the purpose of commiting toll fraud. While these criminals are unlikely to be successful in commiting toll fraud through an H.323 video endpoint, the resulting inconvenience and the need to decommission equipment will definitely result in financial loss.

What's more damning is that the tools used to identify vulnerable systems are readily available. **Using the same tools, and in seconds, StarLeaf's security expert was able to identify 150,000 exposed and vulnerable H.323 Cisco/Tandberg, Lifesize and Polycom endpoints.**

StarLeaf removes the risk with seamless firewall traversal

StarLeaf removes the need to place endpoints on the public Internet. Instead, all StarLeaf endpoints are designed to connect from within the end user's private network, behind the resident firewall. This provides easy and direct business-to-business video calling, without compromising on security. This is made possible by StarLeaf's firewall/NAT traversal solution. StarLeaf hardware and

software endpoints automatically connect out through firewalls, requiring only a single port to connect securely to the StarLeaf Cloud. This one connection is further secured by TLS (Transport Layer Security – cryptographic protocol that provides communication security over the internet) which handles all client to server communications; signaling, media, software upgrades, etc.



StarLeaf user initiates call to a partner company. Media and signalling are both encrypted when the call is set up.

The risks associated with automatic answer

There is a real and serious security risk when endpoints are set to automatically answer incoming calls. Unfortunately, some video systems have automatic answer set as a default by the manufacturer. Even when it is not, users typically set endpoints to auto answer because it is simply easier for the end user.

Furthermore, users may think they have switched everything off when they physically switch the TV screens off. Yet this is not the case; unless the video system is shut down, automatic answer will remain on, allowing anyone to purposefully or accidentally dial into the video conferencing room and remain unseen.

StarLeaf does not allow automatic answer

Knowing the risks associated with automatic answer, by default, StarLeaf users and administrators do not have access to auto answer. Instead, StarLeaf's ease-of-use ensures that anyone can make and receive calls, and, in times of absence there is video mail that enables video messages to be left.

Authentication, encryption, and recording devices

Understanding the security risks has allowed StarLeaf to engineer an entirely secure cloud-based video conferencing system. The issue of authentication is often overlooked in video conferencing, because you can see the person at the other end. Consequently, you may think that this is the only authentication you need. Not so when you consider the possibility that someone can intercept your call and remain unobserved, this is best described as a man-in-the-middle attack. This is made possible because existing video conferencing devices do not guarantee that the communication channel is secure from end-to-end. It is entirely feasible for a hacker to negotiate a separate and independent connection with each of the attendees. This can be achieved through standard off the shelf hardware or the use of malicious software, devised and written by the hacker.

Once a call has been intercepted, the hacker is free to remain on the call unobserved, and, in addition can record the video conference, capturing all video, audio and data.

Where a call is being recorded using the Starleaf recording feature, all participants in the call will be aware that they are being recorded.

StarLeaf authentication

Authentication with the StarLeaf cloud service requires a signed certificate that all StarLeaf endpoints (hardware and software) have burned into them at the point of manufacture. All StarLeaf Cloud servers also have signed certificates that are required by the StarLeaf endpoints to guarantee that they are connected directly to a genuine server. Consequently our secure and encrypted connection cannot be negotiated by anything other than an authorized StarLeaf device, thus preventing a man-in-the-middle attack.

The shortfalls in encryption for video users

Video systems use the Advanced Encryption Standard (AES) to encrypt the media, to prevent unauthorized persons from listening to or seeing your interactions. However, most video systems do not also encrypt the signaling. These unencrypted signals make it possible for hackers to see the conference ID and PIN numbers, providing them with all that they need to gain access to meetings that take place on a bridge/MCU.

StarLeaf encryption locks out the potential for attack

Every call made by a StarLeaf endpoint is authenticated and encrypted, both media and signaling. When you call from StarLeaf to any other video device it WILL use encryption if the recipient device supports it. Encryption cannot be disabled on StarLeaf calls.

Passwords

Key to the StarLeaf system is that all passwords, sent on the network, are never sent in plain text, only in industry standard PBKDF2 (Password-Based Key Derivation Function) hash format.

Existing Security – the closed network

There are many user organizations that acknowledge the weaknesses of the traditional video architecture, and have therefore decided to run a closed network. While this may achieve the goals of keeping the network secure, it vastly reduces the value of the investment made in the technology, by isolating anyone inside the network.

In this case, many organizations deploy a firewall traversal strategy, often predetermining a white list of approved IP addresses–those pre authorized to connect into the company. This is a sound strategy, but one that requires constant maintenance. Particularly when you consider that many home broadband connections get new IP addresses on a daily or weekly basis. A VPN connection provides a solution to this high-maintenance situation, and allows for both hardware and software based video devices to connect to the network. However, this approach requires the end user to master the intricacies of VPN connectivity from their laptop, access and navigate the video dial plan and in some cases download and install the video software. Most executives, remote and home workers would consider this set-up too difficult, cumbersome and complex for them to use video. Therefore, scaling video communications into the hands of those that need it most creates an increased cost and management burden for IT support.

Secure external calling for closed networks

The StarLeaf Cloud allows an organization to securely open their network to external video calls. As the StarLeaf network is fully owned and operated by StarLeaf with known Points of Presence, StarLeaf customers only need to open their firewall to a single IP or DNS name further enhancing their security. Then users on the Internet, be they customers, vendors or remote employees, can communicate securely from remote locations into the corporate network. If ever there is a security breach, such as theft of a home user's equipment or a mobile worker's laptop or iPad, that worker's StarLeaf account can be either removed or have its credentials changed immediately to disable any unauthorized calls into or out of the organization, all without impact to any other users.

Private Direct Media

Uniquely amongst end-to-end cloud video conferencing service providers, StarLeaf allows for private direct media. This means that where the media for a call can be routed directly between the two endpoints in a point-to-point call, it will be. In this case, the media for that call will not leave the customer's own network.

External penetration testing

StarLeaf commissions regular penetration testing from expert third parties on both the StarLeaf Cloud and StarLeaf Portal. This testing not only ensures that there are no major problems on the StarLeaf Cloud, but also that all known issues can be prioritized by the development team.

The most recent round of testing, carried out by CNS Group, concluded in June 2016 and reported no major or critical issues against the StarLeaf Portal. The remaining low priority issues have also been mitigated or are now prioritized against future StarLeaf releases.

In addition to regular commissioned testing, StarLeaf also has an active bug bounty program, encouraging freelance security researchers from around the world to find and report possible security issues to StarLeaf. Details of this program can be found on the StarLeaf website.

Data center security

Any service based applications that are delivered from the cloud, need to provide high and continuous availability, backed-up by system engineered redundancy. Without adequate provision of redundancy, an end user may experience temporary or prolonged loss of service.

The StarLeaf Cloud solution is fail-safe. Its data centers all benefit from physical security as well as system redundancy throughout. All StarLeaf data centers are supplied with at least two independent, generator backed, power feeds. This ensures that the failure of either of these power feeds will not lead to a service outage at that data center. All StarLeaf data centers are provisioned with at least two independent network feeds. This ensures that the failure of either of these network feeds will not lead to a service outage at that Point of Presence.

Consequently failover to standby servers occurs in the event of any abnormal outages or component failure. In addition, StarLeaf has deployed virtualization technology that allows for the migration of both services and individual customer dial plans in times of system failure. All StarLeaf systems are backed-up daily, thereby ensuring customer configurations are protected and up-to-date.

Furthermore StarLeaf has multiple geographically dispersed Points of Presence (PoPs) – and it is possible for all users to be moved between them as required to protect against any catastrophic local events that prevent access to a whole data center.

Where possible, StarLeaf data centers adhere to the relevant local standards for compliance. For example:

- Payment Card Industry Data Security Standard (PCI DSS)
- FIPS (Federal Information Processing Standard) 140-2 Encryption
- SOC3 Systrust for Service Organizations
- BS EN ISO 9001:2008
- ISO/IEC 27001:2005

Monitoring

The entire StarLeaf Cloud is monitored 24/7 by StarLeaf's in-house Network Operations Team. A plethora of metrics are continuously monitored to ensure the smooth-running of the system. Wherever possible, potential service issues are anticipated and resolved in advance.

For example, while the service would continue to run if there was a hardware failure, the automatic monitoring of the system would alert the StarLeaf Network Operations Team to the failure and mitigation actions would be undertaken.

Disaster planning

- If the possibility of a disaster affecting a data center is identifed (for example a forecast extreme weather event) StarLeaf will take action in advance to mitigate risk
- Where a risk is identified, StarLeaf will move the customers hosted in the at-risk location to another data center in advance of the at-risk event
- Customers will be notified of these actions

Disaster recovery

- The StarLeaf Cloud is fully backed up and backup data is held securely in multiple locations
- In the exceptional case of failure at any one of its data centers, where an unplanned event causes loss of access to a StarLeaf point of presence, customers will be restored from a backup to an alternate data center
- StarLeaf endpoints will automatically connect to the new data center with no user input required

Conclusion

We are faced with a dilemma when it comes to video communications. The wider we open ourselves up to communicating with video the greater the benefit, but also the greater the risk. We don't want anyone eavesdropping on our communications or making unsolicited calls. StarLeaf makes it easy to open up the world of video without opening up any vulnerability and as a cloud-based solution it can be considered totally secure with both media and signaling encrypted.

StarLeaf

Get in touch to find a solution for your business communications

email - hello@starleaf.com

EMEA	North America	CALA	ANZ	APAC	FRANCE
London, UK	San Jose, USA	Sao Paulo, Brazil	Sydney, Australia	Hong Kong	Paris
+44 (0) 330 440 1847	+1 408 689 0448	+55 (11) 3051-7578	+61 2 8188 4700	+852 2178 2030	+33 (0) 1 84 88 46 62