Staying Secure in the Cloud

CONSIDERATIONS FOR MIGRATING COMMUNICATIONS SOLUTIONS TO CLOUD SERVICES
Table of Contents

1. Overview .......................................................... 3
2. Introduction ........................................................ 3
3. Privacy vs. security .................................................. 3
4. What are we afraid of? ............................................... 4
5. Downtime .......................................................... 5
6. Data protection .................................................... 7
7. Data breaches ...................................................... 8
8. Service hijacking ................................................... 10
9. Loss of control .................................................... 12
10. Conclusion ........................................................ 13
11. Checklist of questions to ask your UCaaS provider .......... 14
12. Summary ........................................................ 15
1. Overview

When the transmission of data is involved, security is always a concern. That concern is understandably heightened when cloud services are involved. This white paper examines security considerations for migrating communication solutions into the cloud and offers insight into how the ShoreTel Sky service protects your valuable data.

2. Introduction

The benefits of cloud services are so compelling that organizations are now pushing critical business applications from their own in-house data room to the cloud, something which would have been unthinkable a decade ago. Along with this trend come valid concerns about who secures and controls an enterprise’s proprietary information, their content and the associated metadata.

As technology advances, so too does the ability for cyber-criminals to keep pace. The only comprehensively secure system is one which no one can access—so it’s crucial to strike the right balance between security and the delivery of services that satisfy business drivers and provide a superior user experience.

The threat level increases when services are combined. Separate points of entry increase vulnerabilities, as do user-accessible portals. A single point of failure can leave an organization open to a full system-wide hack.

As a premier Unified Communications as a Service (UCaaS) company, ShoreTel’s job is to deliver an environment that provides world-class availability, security, access control, and continual monitoring to ensure that your VoIP business phone service is uninterrupted and your data is safe.

3. Privacy vs. security

Security is much more than an IT department concern as business implications of a breach can be far reaching. Additionally, the increasingly mobile world creates access points that make systems easy to operate for the end user, but also creates the possibility of compromised privacy.

Although the terms are often used interchangeably, there is a difference between privacy and security.
• **Security** is the state of being free from danger—no one is maliciously corrupting your system (e.g., Target’s credit card system breach that compromised nearly 40 million credit and debit card accounts).

• **Privacy** is the state of being free from observation—no one is watching what you are transmitting (e.g., continuous monitoring and storage of mobile traffic).

In this paper we focus on security for your cloud-delivered UCaaS applications along with the services that store data and process your interactions.

### 4. What are we afraid of?

While cloud-based storage is a well-known offering, UCaaS is a relatively new paradigm. And while CIOs continue to express a concern for security, this has not slowed the adoption of cloud services.\(^1\) Synergy Research projects UCaaS subscribers will be only eight percent of the total enterprise IP telephony ports shipped in 2014, but forecasts growth of 113 percent for public and private cloud UCaaS business-suite subscribers by 2017.\(^2\)

Regardless of where the closet housing your data lives, whether on premises in your facility’s basement or in a data center located near Dallas, the primary objective of a communications system is to disseminate the information needed to run your business. And in industries from aeronautics to zoology, protecting data is a top priority.

We asked 1,200 people who run their company’s unified communication system (comprising both on-premises and cloud solutions)—CEOs, owners, CIOs, IT directors and managers—to rank their concerns around deployment of a UCaaS solution on a scale of one to five, with one representing least concern.\(^3\)

---

2. Synergy Research Group, “Cloud UC Services database” and “Enterprise Voice database.” Please note: Links require login. UCaaS includes only hosted UC subscribers, not total hosted VoIP subscribers.
As you can see from the survey results above, downtime, performance, and cost led the list, but a wide variety of security concerns were ranked as reasons for anxiety.

**Downtime**

A sudden influx of customers, an unexpected hurricane or a denial of service attack—all are issues that can cause a shutdown of operations until the problem is resolved. Performance and uptime have a direct effect on the bottom line, so it’s no surprise that companies are wary of anything that impacts these core requirements. Consistent monitoring can help narrow the impact point of origin and bring you back online.

The ShoreTel Sky system consists of multiple components: the network, soft-switch clusters, carriers and databases. To ensure that we meet the high level of availability that our customers require, we continually improve our network with the most advanced routers and switches available. Our network architecture is designed so our core and distribution routers are redundant and have no single point of failure.
This starts with the data center. ShoreTel employs a Tier III (with Tier IV capabilities) data center committed to 100 percent uptime with a true 2N power and cooling design. With a 2N design, the entire primary system could fail without even a blip of downtime registered by customers.

Additionally, ShoreTel maintains a “lights-out data center”—the entire system is prewired with a fiber interface (and a copper backup) connecting all racks. Because all wiring is already in place, nothing more than a simple patch is needed when adding or changing equipment and access is strictly controlled.

The data center also includes full Uninterruptible Power Supply (UPS) backup systems and uptime guarantees with systems in place for environmental control and continuity. UPS units are located inside both the primary and backup data center facilities where ShoreTel Sky hosts servers. Municipal electricity powers the buildings, which powers the
UPS system. The primary UPS is monitored daily as are performance results. Facilities are equipped with generator backups that automatically supply power in the event of a commercial power failure. Environmental equipment, including HVAC, UPS, PDUs, generators, as well as adequate lighting and fire suppression, are also present at each facility.

Redundancy

Loss of data is not always the result of intentional actions. Natural disasters or other simple errors can be the root cause—the key is redundancy, redundancy, redundancy.

ShoreTel deployed a north/south data center alignment, with locations in Dallas and Chicago, allowing full redundancy across the continental U.S. for both the primary and redundant data center. The centrally located region of the data center provides optimum end-to-end latency of less than 60ms—the time it takes for a packet to travel the network from creation to destination.

Securing your assets isn’t solely reliant on best-of-breed firewalls and replicating data across data centers in near real time, although ShoreTel has also implemented redundant storage capacity. Failover options are implemented to provide for the best redundancy possible—whether an existing MPLS circuit backup for each customer edge node, or a ShoreTel provided QOS-enabled private point-to-point access. To further ensure uptime, ShoreTel also interconnects via MPLS by examining a customer’s existing connectivity options to create a generic routing encapsulation tunneling protocol that can establish a backup path for egress and ingress voice traversal.

Data protection

Security and data protection concerns are embodied in government requirements for specific verticals, such as Sarbanes–Oxley/Dodd-Frank for financial, HiPAA for
healthcare, and PCI compliance for financial transactions and retail. All cloud providers are subject to numerous state and federal information security and privacy laws and regulations.

**Compliance**

ShoreTel Information Security Policies are organized in accordance with ISO 17799, Information Technology – Code of Practice for Information Security Management, an international standard and are in compliance with other regulatory and compliance mandates where applicable. (ISO 27001 compliance testing is now in progress.)

It is critical for a cloud service data center to meet high standards for security and availability. As such, the ShoreTel Sky data center is compliant with SAS-70 and SSAE-16. As part of the Sarbanes-Oxley (SOX) law, SSAE-16 (and the older SAS-70) standard state that a company has the proper processes in place for how transactions could potentially impact other organizations.

To meet the Information Security Standards of our customers, ShoreTel will have secured certifications for the following by the end of 2014:

- **CPNI**: Customer Proprietary Network Information is the data collected by communication providers regarding consumer calls.
- **ISO 27001-2013**: An information security standard specification for information security management systems (ISMS).
- **HIPAA/HITECH**: Health Insurance Portability and Accessibility Act and Health Information Technology for Economic and Clinical Health focus on protecting an individual’s health and medical care information.
- **PCI-DSS**: Payment Card Industry Data Security Standard applies to financial institutions, merchants, online retailers, and all that provides services to these companies.

**Data breaches**

ShoreTel takes system security seriously, and utilizes industry best practices to constantly harden our operating system and ensure that the network is well-protected against known threats.

To protect our systems from attackers, we deploy the best breed of firewalls, intrusion detection and prevention systems. These measures provide protection against SYN or TCP Flooding, or other types of DDoS attacks. Our external-facing devices are tightly monitored and maintained in order to stay a step ahead of hacking threats.
The external-facing portion of the network is known as the Demilitarized Zone (DMZ). This is where customer access for phone and web services both originates and terminates. All data in this sector is encrypted because this is the only area exposed to an untrusted network (the Internet). The database, the most secure zone, houses all customer data. No Internet, or otherwise external traffic, can access this zone, which resides past the DMZ.

System infrastructure is separated into zones – protected by an intrusion prevention system (IPS) and firewall. The IPS exists between the customer and external zones. While the firewall allows authenticated customers to log in to dedicated web server ports, the IPS examines signatures of what the customer is sending. Each piece of malware has a particular pattern. If the IPS detects any data packets with such signature patterns, the communication is stopped.

On the customer end, communications are secured with robust authentication and encryption authorization credentials. Further, a setup or registration process can validate user information using digital certification. Ideally a solution will automatically detect when the system is accessed from outside the corporate firewall and automatically secure the session in progress.
The ShoreTel Sky voice architecture includes Session Border Controllers (SBC). SBCs enforce security, quality of service, and admission control mechanism over the VoIP sessions. SBCs provide firewall services to protect the IP Phone from possible attacks, act as gatekeepers, and function as point of demarcation between our upstream PSTN peering service provider networks.

**Insecure APIs**

Organizations often build their brands on the integration of third-party apps, a system reliant on companies sharing their APIs far and wide. Education around strongly built interfaces and consistent monitoring prevents far-reaching consequences.

For continued growth and success, it is crucial for a company to extract the full value out of their customer relationship management software and phone system. ShoreTel has a team specifically focused on helping customers integrate business process applications—such as Salesforce, NetSuite, and Bullhorn—which require authentication at the partner and user levels. Third-party companies can also apply through a vetted program and sign an agreement to ensure additional API and SDK security.

**Service hijacking**

Sadly, phishing scams and other fraudulent interactions still produce results. Any kind of connection from client to provider can provide an opening—so keep your credentials confidential. In a business environment, anything that equates to dollars lost is understandably a concern.

In the telephony industry, people tend to construct networks based on voice quality, not security. People tend to trust encryption via its default—which is a dangerous assumption. For example, the standard-issue default password provided with VoIP infrastructure becomes quite security risk if the PIN is never reset.

In fact, many don’t encrypt traffic at all. However, “securing” an infrastructure by assigning it a unique VLAN ID could potentially be an easy target for a hacker to crack in less than 10 seconds. As SQL databases break down into chunks and shuffle info, like IP addresses, out across networks, a lot of information is theoretically there for the taking.

The solution is in the ability to react quickly. As soon as an incident is discovered (ideally within seconds from a monitoring solution) ShoreTel’s team tracks down the point of compromise and mitigates it. At ShoreTel, constant monitoring by our IPS system detects attacks and quickly shuts them down to deplete the potential value for a hacker to waste his time and energy.
ShoreTel runs internal vulnerability scans against any systems containing (or accessing systems that contain) confidential data on a quarterly basis. Effective vulnerability management can reduce risk to a computing environment by verifying that systems or network devices are using current patch levels, are not running unnecessary services, and do not have default passwords.

**Toll Fraud**

The most common type of service hijacking in the telecommunications industry is toll fraud—when an attacker gains unauthorized access to your phone system to make long distance calls via your account. According to the Communication Fraud Control Association in 2013, worldwide phone fraud caused by compromising phone systems cost consumers approximately 46 billion dollars.

To minimize the damage any misappropriation of an account can cause, ShoreTel does everything we can to spot irregularities before they become a problem—from securing our borders and monitoring call patterns, to having a detailed end user password policy in place.

The first step in fraud prevention is access control. Every ShoreTel Sky customer designates a “Decision Maker,” who is responsible for maintaining a current list of authorized contacts for the account. The platform can also be configured to restrict international and directory assistance or require an authorization code before making calls.

ShoreTel and carrier partners monitor for toll fraud 24x7x365. In addition, the system is programmed to terminate access after the third invalid attempt to log into a voicemail account. Of course, the best prevention against fraud is policing a strong password policy.

- Update passwords every 90 days.
- Do not use the same password for all profiles.
- Use longer passwords.
- Include a minimum of four non-repeating digits.
- Do not use last digits of your phone number.
- Do not use sequenced numbers such as “1234” or “1111.”
In the event a breach is suspected, the Security Incident Response Team (SIRT) is notified. This team consists of designated members of the systems and networks team, a security officer, and department managers. SIRT then investigates the extent of the breach and ways to mitigate any damage and eliminate or minimize the vulnerability.

**Loss of control**

Deploying cloud services means letting go of some of the daily management activities of your systems. This decision can have distinct benefits in cost reduction, departmental efficiencies, and in overall system reliability and availability.

ShoreTel architecture is built, managed and maintained by some of the most talented and qualified experts in voice over IP. Our customers have succeeded because they are focused on the result rather than the investment and process to obtain that result.

**Malicious insiders**

The disgruntled employee has always been a potential source of trouble for an organization. Corporate espionage is not a new concept. The key is to maintain an easy-to-use checks and balance management system that prevents unauthorized users access to data above their clearance level.

ShoreTel recognizes that both the technical and human components are necessary to maintain a truly secure system and therefore holds a zero tolerance policy for putting customers at risk, imparting strict guidelines for employee and vendor behavior alongside comprehensive checks and balances within engineering and development to detect and deter potential intrusion.

Only approved network operation center staff have logical access to data, calls, or call recordings. Any staff member connecting remotely must use a two-factor method of authentication before being allowed to connect; this provision applies equally to the ShoreTel Sky network connection as well as any information resources residing within the network. Additionally, shared privilege passwords (i.e. “root” or “administrator”) are changed whenever an individual with administrator-level access leaves the firm. ShoreTel also conducts background checks to ensure that the employees we hire possess the highest possible level of integrity and business ethics.
Conclusion

It is important to determine your acceptable risk, weighing the pros and cons of threat versus quality of service. In many cases, in the rush to get a communications system up and running, security isn’t at the forefront of mind. However, asking questions in advance can assist in preventing security issues that become heavy liabilities after vulnerabilities are compromised.

When deploying a system it is always wise to employ a healthy dose of common sense. Most companies are already well entrenched in the world of cloud, using external servers and data centers for services such as email, document storage and databases.

Survey respondents that use cloud services for other business purposes

<table>
<thead>
<tr>
<th>Service</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>56.8%</td>
</tr>
<tr>
<td>Document Storage</td>
<td>51.7%</td>
</tr>
<tr>
<td>Databases</td>
<td>30.4%</td>
</tr>
<tr>
<td>CRM</td>
<td>28.1%</td>
</tr>
<tr>
<td>Virtual Desktop</td>
<td>16.2%</td>
</tr>
<tr>
<td>Open source API applications</td>
<td>10.9%</td>
</tr>
</tbody>
</table>

Many vulnerabilities are already familiar within the industry and methods/best-practices are readily available—both in the case of proactive protection and reactive problem solving. Others are still being studiously investigated.

Communications systems are not an all-out either/or proposition. Many systems already reside in a private cloud, and hybrid cloud solutions are a burgeoning option as well.
The beauty of constantly evolving technology is that we are able to keep pace both with simplifying tasks as well as making sure business continues as usual despite potential security threats.

**Checklist of questions to ask your UCaaS provider**

- How does your service make it easy to provide access to qualified users while blocking non-authorized users from gaining access?
- Does the system comply with corporate access policies?
- How are firewalls configured?
- How is data encrypted? Can critical data be encrypted in transmission and for storage?
- What policies are established to mitigate any data disclosure?
- What are the backup and restoration policies and procedures?
- If data is stored externally, are all systems compliant with government regulations?
- Is an Intrusion Prevention System (IPS) installed on the cloud network? What kinds of penetration or compliance testing are run regularly?
- How does the cloud service interface with my on-premises security environment?
Summary

The ShoreTel Sky system comprises four components:
1. Gateway network, where IP Gateways, using P2P and MPLS infrastructure, route voice and data traffic from client sites to our VOIP network.
2. Internet Service Network, which controls the calls from SIP carriers and forwards them to the cluster Session Border Controller (SBC).
3. Clusters, which is responsible for call flow applications such as SIP, SCCP, user database, and the gatekeeper.
4. Management, which contains APIs, which process all service and web portal requests.

To protect customer data, security for the system includes:
- A range of Tier 1 voice and data providers that afford significant redundancy and enhanced call completion and data connectivity capabilities.
- Daily off-site backup of customer configuration data.
- Connectivity with individual telephone and data carriers that spans multiple locations so that if connectivity to one location is lost, calls will be rerouted to another location.
- System and server virtualization that quickly restore to new hardware in the event of a failure.
- Multiprotocol Label Switching (MPLS) utilized for customer connectivity and delivering an efficient and scalable network.
- A multidisciplinary team of ShoreTel engineers and operations professionals who constantly review threat assessments and disaster recovery protocols.

About ShoreTel

ShoreTel is a provider of business communication solutions whose brilliantly simple unified communications platforms, applications and mobile UC solutions promise a new rhythm of workforce engagement and collaboration. With costly complexity eliminated by design from its award winning, all-in-one IP phone system, UC and contact center solution, and its industry leading hosted business phone system, workers enjoy a freedom and self-reliance that other providers can’t match. Users have full control to engage and collaborate, no matter the time, place or device, for the lowest cost and demand on IT resources in the industry. ShoreTel is headquartered in Sunnyvale, California, and has regional offices and partners worldwide. For more information, visit shoretel.com or shoretelsky.com