Selling UCaaS in Regulated Industries

By Michael Cobb

APRIL 2017 | US$25 | S110417

Channel Partners™

Selling UCaaS in Regulated Industries

By Michael Cobb

APRIL 2017 | US$25 | S110417

Channel Partners™

Table of Contents

Channel Partners™

About the Author

@thehairyitdog

MICHAEL COBB, CISSP-ISSAP, is 20-year veteran of IT security with a passion for making industry best practices easier to understand and implement. As an adviser on security controls and information handling practices to companies and government agencies large and small, Cobb has helped numerous organizations achieve ISO 27001 certification and successfully migrate data and services to the cloud. Cobb has also worked with CESG, the Information Security arm of GCHQ, to promote security best practices in government. A renowned author and presenter, Cobb has written numerous technical articles and webcasts for leading IT publications as well as the book "IIS Security." He has also been a Microsoft Certified Database Manager and registered consultant with the CESG Listed Advisor Scheme (CLAS).

Selling UCaaS in Regulated Industries

THE MOVE TO SOFTWARE-AS-A-SERVICE TRANSFORMED HOW BUSINESSES OPERATE. CUSTOMERS

get scalability, continuity, better security, increased employee productivity and cost control along with a move to opex, all without having to hire internal IT staff. In many cases, SaaS is the only viable option for small shops looking to adopt the latest enterprise-class technologies and maintain a competitive edge. Partners, meanwhile, can resell SaaS and develop a healthy monthly recurring revenue stream.

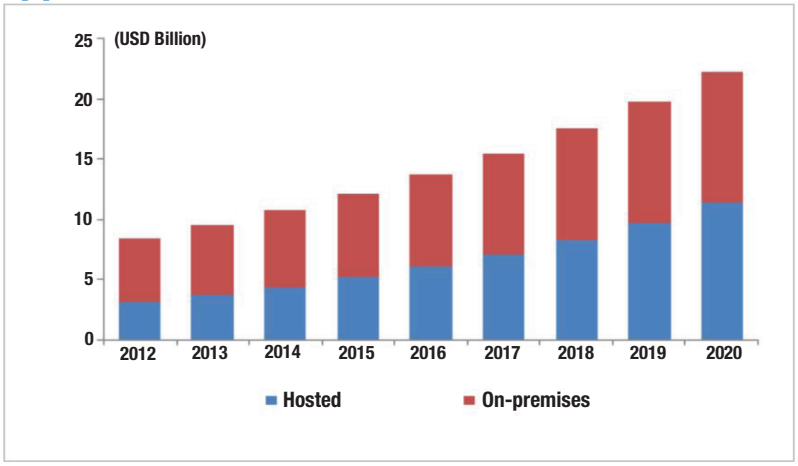
All this can go off the rails, however, when dealing with regulated industries such as health care or financial services. While the SaaS provider owns and maintains software, hardware and infrastructure, the customer is still responsible for protecting sensitive data and communications.

As a trusted adviser, you need to be able to assure customers that a SaaS vendor is following the regulatory rules. That means verifying that data is stored in U.S. facilities, when required, that all the provider's employees undergo proper background checks and that the proper physical security measures are in place, to start. Hightail provides a comprehensive SaaS security assessment guide that includes questions to ask as well as explanations of why various points are important.

Not All SaaS Is the Same

Some types of SaaS bring additional challenges. One of the more popular options for channel partners to sell is unified communications-as-a-service (UCaaS). IDG Enterprise's 2015 Building the Mobile Enterprise Survey reported that 68 percent of companies said improving internal communication is critical. As a result, Grand View Research's

North America Unified Communications Market by Application, 2012-2034



Source: Grand View Research

prediction that the global unified communications market will reach $143.49 billion by 2024 is no surprise. The consultancy says that growth is driven by increasing numbers of remote employees and the need for communication systems that further the easy exchange of information. According to a BroadSoft study, UCaaS is expected to reach 41 percent market penetration by 2020.

However, again, compliance concerns are holding back use in regulated industries.

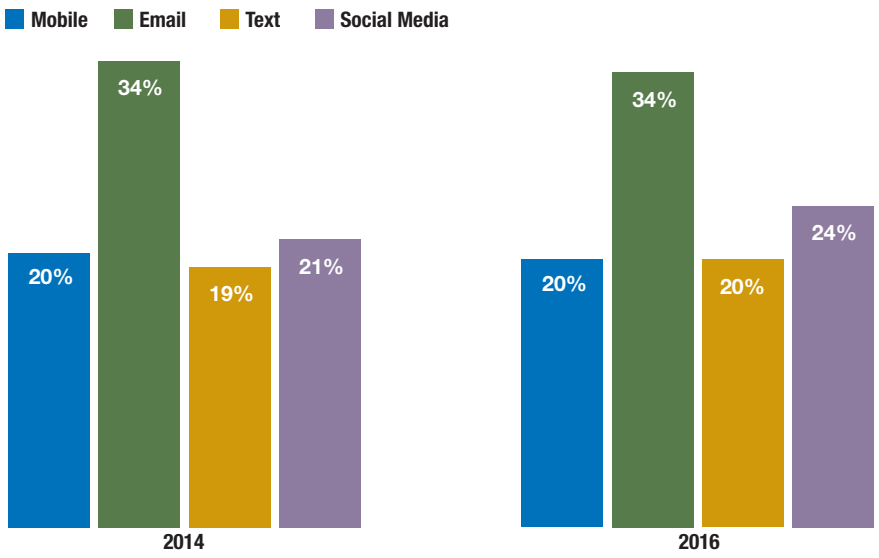
As UCaaS is a subset of SaaS, the same cloud security and compliance principles apply — along with additional considerations. Many industries require all customer communications to be recorded, for example, so the ability to record and archive any mode of UC is essential: not just voice calls but IM, video- and audio-conference sessions, and mobile and VoIP-based calls.

The security controls and procedures protecting this data need to meet regulatory rules, so choosing a UCaaS provider that meets or exceeds relevant standards is also essential. Compliance with SSAE 16, CSA STAR and ISO 27001 should be a prerequisite.

For a small customer, keeping in-house systems compliant with these standards is often an expensive pipe dream. SaaS providers, including UCaaS environments, can be more reliable and secure than on-premises systems, but there are important questions to ask any potential UCaaS provider.

Health Workers & Mobile Security

How confident are you that the following devices used for business are HIPAA compliant?



Source: NueMD survey of more than 900 doctors, administrators, staff and billers

Ken Shulman, Broadview Networks' CTO and CIO suggests getting detailed answers to the following questions:

- What security measures does the provider take to secure data in its cloud?
- Does the provider meet my customer's industry compliance requirements?
- Are calls, meetings and messages secured through encryption or other means in transport and when stored on provider servers?
- What measures does the provider have in place to lessen the risks of downtime or data loss?
- For UCaaS specifically, what employee or company data will be stored locally on smartphones, tablets and other devices?
- Can you provide copies of your SOC 3, and, if needed, SOC 2, reports to ensure the proper measures are in place to protect critical data?

If you serve customers in multiple verticals, you need to be mindful of specialized requirements.

"For example, organizations in the health care field should ask if providers will sign BAA agreements to meet HIPPA requirements," says Shulman, referring to the required **business associate agreement.** These contracts describe actions, such as using appropriate safeguards to ensure personal health information is used appropriately, that must be taken by a variety of partners.

Hosting Models and Security

Another key consideration when security is paramount is whether to opt for multitenant or a hosted service delivery hosting model.

A traditional single-tenant model requires a separate physical or virtual machine to be individually provisioned for each customer and independently secured. "Multitenant" has become a very generic term, so partners need to understand how customer and session information is kept separate and secure. Mike Sapien, vice president of U.S. research, enterprise, at Ovum, recommends asking how customer data is partitioned in a multitenant environment and what security is integrated into the UCaaS platform to make sure data cannot be lost or accessed by unauthorized users.

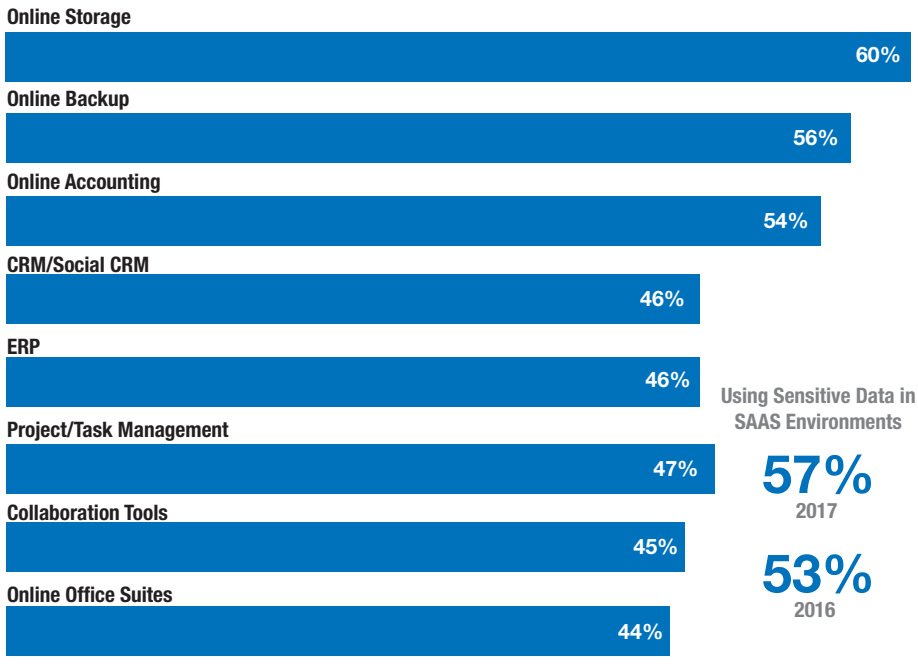
"UCaaS providers need to offer and articulate the multiple layers of security, from end-user access to complete session auditing, included in their basic UCaaS offer and premium options," says Sapien.

Have a provider:

- Describe the security services that are integrated and free, and list additional security options and the related charges
- List the security provisions for connections to third-party services and remote users
- Disclose any security breaches the provider may have had in the last three years

SAAS Security Data Security Concerns Remain High

Thales Group surveyed more than 1,100 senior security experts worldwide and found that despite concerns over the security of cloud services, use of sensitive data in SaaS environments is up.



Source: Thales e-Security

Partitioned correctly, hosted multitenant delivery models offer efficiencies, not only in hardware and administration, but also in the scale and scope of the security implementation. That scale allows the service provider to apply security across the entire service infrastructure, from hardware to software to physical security, backup and redundancy in a manner that isn't practical for individual environments. Providers may also deploy patches and security improvements more quickly in multitenant models, as only a few instances of the code need to be updated instead of thousands. Creating the same level of redundancy and security is possible with single-tenant environments, but it is far more challenging and expensive.

For optimal security, avoid having data stored on devices, especially mobile devices that are prone to loss. Calls carried over the internet must be encrypted, as should data secured in the cloud so that no sensitive information is ever left vulnerable.

5 Points to Consider

1. M&A, UC&C may equal risk: There is likely to be consolidation within the UCaaS industry; a lot of providers are chasing that market, and scale is a major cost factor both on the operations and customer acquisition fronts. There will also be more integration of popular office applications, like CRM. These sorts of expansive changes, while often welcome, can introduce new risk, so it's important to do a security checkup for regulated customers regularly, as well as after any M&A or integration activity.

2. Hybrid doesn't always equal safe: Some organizations with on-premises UC systems will want to move to a hybrid delivery model and transition over time to fully SaaS. Ensure that encryption is applied end-to-end and that patches are kept up to date across on-premises UC and PBX gear. End of life systems still need security updates.

3. Watch the weak links: Also consider end users — error is the biggest risk to data for most companies. And, as workforces become more dispersed and contract-based, demand for access to data over mobile devices is likely to increase. Telemedicine alone is adding entirely new challenges to HIPAA compliance.

"The days of humans conforming to how services are delivered are over," says Shulman. "Now technologies and services must adapt to the new ways and devices we use to get work done."

How well the user experience is delivered will have a big impact on security, as we discuss in this report. End users will quickly abandon a UC system in favor of their personal devices if they get frustrated, and these devices are not typically governed as carefully with respect to both quality and security. BYOD and bring your own technology (BYOT) already mean device management in the enterprise is a big issue, and this is compounded in regulated firms.

4. Cloud doesn't mean bulletproof: Be crystal clear on what a SaaS provider's disaster recovery practices are — UC demands a rethinking of BC/DR in any case — and what availability and performance guarantees it offers in the event of an emergency, whether local or regionwide.

Speaking of cloud, one thing it can deliver: centralized management. "UCaaS providers can enhance an IT department's overall mobile device security strategy, ensuring the installed UCaaS applications are properly protected by cloud-based registration authentication and security, and enabling access control," says Shulman.

5. Tailor the offering to size, not just vertical: Besides looking for UCaaS systems customized for the needs of regulated customers, Ovum's Sapien suggests that partners resell or build UC service bundles for different customer segments and modified to accommodate large enterprise, middle market and SMB customers, with each service portfolio having proper security baked in. SLAs should certainly make it clear whose responsibility it is to ensure relevant legal and regulatory data compliance and privacy laws are addressed.

Related Reports

Showing Savings With Unified Communications

Unified communications enable any size company to improve the way employees, customers and partners communicate and collaborate — from anywhere, over any accessible network, using any device, at any time. But when customers that still run voice, conferencing, mobile and other communications services in separate silos ask if they should (finally) adopt UC, the answer they will relate to most is, "Yes, because it will save you money."

UCaaS & Millennials: 8 Reasons Cloud Answers Gen Y Needs

Keeping millennials engaged and productive requires adopting next-generation tools. This Report provides key guidance on engaging in conversations with customers about unified communications-as-a-service (UCaaS) solutions to delight millennials and achieve business goals.

Channel Sales Handbook: Unified Communications

The goal with UC is to delight the customer, boost productivity and win repeat business. But agents and MSP sales professionals may be confused about how offerings differ, what those differences mean in terms of how systems perform and how to go about assessing prospects. This Report examines how to build a customer profile and then align the best solution.