white paper

serenova®

Contact Center Security in the Cloud: Questions to Ask & Answers to Expect

Table of Contents

7300 RR 2222, Bldg III, Ste 200
Austin, TX 78730 USA
toll free 1-800-411-4700
www.serenova.com
sales@serenova.com

Executive Overview

During the past decade, organizations have been increasingly moving away from environments where data is centrally accessed and stored, and into distributed, more efficient virtualized environments. Moving to the cloud provides significantly more business benefits than a traditional infrastructure; however, confidence in cloud security is a justifiable and top-of-mind concern. Adequately securing a cloud-based contact center is more than possible today with the right partner.

The goal of this paper is to provide contact center decision makers and influencers with the information they need to have an intelligent discussion with a cloud contact center provider's security experts. With security being among the top two concerns about moving mission-critical enterprise contact centers to the cloud, it is imperative that decision makers understand that just being able to have an intelligent discussion with cloud providers is not enough. Identifying the right contact center provider that can be a trusted partner also requires adjusting security-related questions in the RFI. With that in mind, at the end of this paper is a list of recommended questions for an RFI.

Armed with this information, locating a cloud contact center provider to partner with for the long term and feel confident they are providing the right security for success in the cloud is possible.

Multi-layer Security

Contact center security requires providers to continuously invest in their platform and applications in order to develop new functionality that simplifies the job of managing agents, driving performance, and enhancing security, which taken on an even greater importance in the cloud.

When evaluating an enterprise cloud platform cloud provider, contact center decision makers and influencers should look for a solution that addresses security in multiple layers:

- » Physical Security
- » Network Security
- » Systems and Applications Security
- » Information Security & Audit
- » Agent Security

Each layer plays a vital role in protecting a mission-critical enterprise. Below is a description of each layer and what the decision-maker should expect when evaluating cloud providers:

Physical Security: In the cloud, data resides in one or more data centers.

INQUIRE ABOUT: the data center itself should be protected by several layers of security perimeters, including mantraps, surveillance cameras, and well-credentialed security staff. Ideally the provider will have the following:

- Security perimeters including mantraps with layers of biometrics
- 300 or more surveillance cameras supported by infrared, ultrasonic and photoelectric motion sensors
- 24X7 security staff compromised of ex-military and law enforcement

Network Security: Weak network security is one of the biggest threats to corporate data.

INQUIRE ABOUT: The provider's network should have multi-layer protection that includes multiple network and application firewalls and intrusion detection systems. The bottom line is that the network architecture must be secure—ask about it.

Systems and Applications Security: Security must be an integral part of how a provider designs and builds its cloud contact center platform and applications. Security must be considered through every stage of the development lifecycle. The platform and applications should be thoroughly tested to prove adherence to industry-standard security requirements. Ensuring the security of applications is critical, as such all code releases should undergo automated and manual secure code reviews, as well as an in-depth penetration testing prior to release. In addition, Developers and QA should complete ongoing Application Security Training.

INQUIRE ABOUT: The systems and application level security should exceed industry-leading standards. In addition call recording encryption should be used, preferably using NIST FIPS 140-2 3 Hardware Encryption devices.

Information Security and Audit: The company should either be ISO 27001 certified, or should be in compliance with the requirements of ISO 27002.

If applicable, the provider should be compliant with the 12 security domains of PCI-DSS Level-1 Service Provider. Ask the provider if the systems and application level security exceeds industry leading standards, including scan and code review. Plus call recording encryption should be NIST FIPS 140-23. For healthcare-focused companies, the provider must also be HIPAA compliant.

INQUIRE ABOUT: If the provider has a well-credentialed cloud-provider security staff. It's not uncommon for established on-premise, brick-and-mortar contact center providers to have a Chief Information Security Officer (CISO) on staff. However, among cloud providers, this position is not as prevalent since there is a difference between security for brick-and-mortar centers and security in the cloud. There are fewer cloud-experienced CISOs. Pay attention to how long a cloud provider has had a CISO on staff and specifically the CISO's credentials.

While cloud-based contact centers have been in existence for at least a decade, technical security has been around for many decades. But the move to the cloud has created a whole new look at security from a regulatory and compliance perspective. CISOs who are dedicated to ensuring their employers and their employer's customers have optimum cloud security are actively involved with the security industry at-large. It's not enough to hold the title of CISO. This is one position where experience and credentials matter just as much as security industry involvement. Knowing the CISO's background can tell you how committed the provider is to cloud security. The longer they have been committed to security, the more likely they are a partner you can trust.

Agent Security: There is also another important aspect of contact center security — the human factor. When contact centers move to the cloud, one of the biggest 'a-ha moments' is realizing the options they gain access to just because of the cloud: on-demand technology, on-demand applications, on-demand talent, etc.

On-demand talent typically means home-based or remote agents. This cost-effective agent staff is typically only paid while they are working; they are not paid to sit around and wait for the phone to ring. While Forrester, Frost & Sullivan and a host of industry insiders are reporting that home-based agents are the fastest growing segment because of the well-documented, higher quality of customer interaction and cost effectiveness, there remains a heightened concern about security.

Something to keep in mind when investigating cloud providers is if they do not have access to a community of agents and they are purely a technology provider, then how well does the provider truly understand the importance of agent security?

INQUIRE ABOUT: If the cloud platform and applications provider can provide agents, the provider should have the following security measures in place:

- Calls should be recorded for security compliance.
- Agents should be regularly subject to call monitoring and audits.
- Provider should have more visibility into data collected by each agent than they would in a traditional brick-and-mortar environment.
- Agents should be held 4 to the highest standards in the contact center business.

- Provider should have on staff service representatives who are Security Manager Certified.
- Agent-customer interactions should be audited by multiple auditors who listen to thousands of calls per day for compliance with fraud and security requirements. The higher the number of auditors the better.
- The provider should have in place a Secure Exchange application that restricts agents' access to sensitive data with seamless technology, and assures that captured data is encrypted whenever it is stored or transferred, and sensitive customer information cannot be accessed by agents.
- Agents should have a secure desktop that restricts their desktop, ensuring compliance and data encryption, as well as prevents data leakage and sanitizes data via deletion of browser history.

Importance of Security Industry Involvement

Independent Certification

The average enterprise contact center handles thousands to millions of customer interactions. Often this central location is the transaction hub for company business-in other words money is exchanged. It is in the best interest of any contact center decision maker to look for a cloud provider that is regularly audited by independent third parties to ensure the provider is fully compliant and certified with security domains.

INQUIRE ABOUT: When talking to a provider about their independent certification, ask if they are compliant and certified with 12 security domains of PCI-DSS Level 1 Service Providers. This credit card processing compliance requires secure data storage and strong policy and compliance measures.

Customers within financial services, health care, insurance, and a host of other industries might also require regular testing and auditing of the security of the provider's platform to ensure that it meets and exceeds the security requirements of specific industries. It's important to inquire about all third-party auditing requirements the provider undergoes.

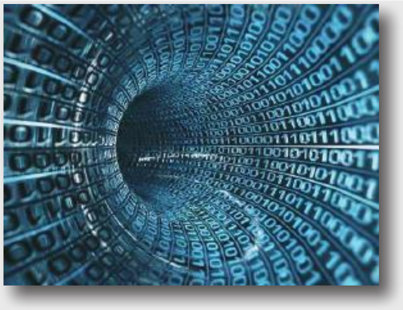
Industry Security Certifications and Memberships

Any cloud contact center provider committed to providing the best security for its customers should be actively participating in industry security programs and initiatives. Ideally the security staff and its leaders are doing more than just paying membership dues, but they should be actively engaged and making sure their voices are heard throughout the security industry. This includes authoring a number of industry security and risk white papers, chairing committees, speaking at conferences, and authoring articles for publication in security press.

INQUIRE ABOUT: When talking to a cloud provider, ask to see articles penned by members of the security team. Accreditations that you should ask about include:

- CISA – Certified Information Systems, ISACA
- CCSP - Cisco Certified Security Profession, Cisco
- CISSP - Certified Information and Systems Security Professional, ISC2
- CFE – Certified Fraud Examiner, Association of Certified Fraud Examiners

In addition, ask about having membership and taking an active role in industry bodies including the Cloud Security Alliance (CSA) which is essential for cloud security leaders, as well as membership in: the Association of Certified Fraud Examiners (ACFE), BITS Financial Services Roundtable, and



International Information Systems Security Certification Consortium (ISC2).

For financial services companies exploring cloud, inquire if the provider is active in programs such as the BITS Shared Assessments Program. This assessment program was created by financial institutions to evaluate the security controls of their service providers both in the US and internationally. It was created by the CEO-driven financial services industry consortium BITS, the leading financial institutions, financial services providers and assessment firms in the US, as well as the Big 4 Accounting firms acting as technical advisors.

Summary

Moving contact center infrastructure to the cloud can meet an organization's most formidable security requirements. This innovative deployment model is being adopted rapidly by some of the largest and most trusted companies in the world: Salesforce.com, Symantec, and AAA to name a few. These companies have learned that operating a contact center in the cloud radically simplifies the deployment, maintenance, and access to platforms, applications, infrastructure, and talent.

There's no singular approach to security. By partnering with the right provider, contact center decision makers can be confident about moving to the cloud without compromising their contact center security.

Recommended Cloud Security Questions for Inclusion in an RFI

Following is a list of recommended security-related questions for inclusion in a cloud contact center RFI and the answers to expect (ATE).

1. How long has the provider been providing a cloud-based contact center platform?

   ATE: Minimum of 8-10 years focused on the cloud

2. How many security perimeters including mantraps and surveillance cameras does the data center currently have in place?

   ATE: Minimum of three security perimeters including mantraps and 300 surveillance cameras

3. How are surveillance cameras supported?

   ATE: Surveillance cameras are supported by infrared, ultrasonic, and photoelectric motion sensors

4. Do you have 24X7 security staffing for each data center?

   ATE: Yes

5. What are the credentials of each data center's security staff?

   ATE: Former military and law enforcement

6. Describe your network security.

   ATE: Our network security has multi-layer protection that includes multiple firewalls and intrusion detection systems.

7. Is security considered through every stage of the development lifecycle of the platform features and applications?

   ATE: Yes

8. Are you compliant with the 12 security domains of PCI-DSS Level 1 Service Provider? Provide the documentation.

   ATE: Yes, documentation provided

9. Does your systems and application level security exceed industry-leading standards, including scan and code review? Provide the documentation.

   ATE: Yes, documentation provided

10. Is your call recording encryption NIST FIPS 140-2 3? Provide the documentation.

    ATE: Yes, documentation provided

11. Are you HIPAA compliant? Provide the documentation

    ATE: Yes, documentation provided

12. Do you have a full time, on staff, CISO? What is his/her name?

    ATE: Yes, (first and last name)

13. How long have you had a CISO on staff?

    ATE: Greater than three years

14. What are your CISO's credentials?

    ATE: Our CISO's credentials include

15. Do you have access to cloud-based agents who work remotely/at-home?

    ATE: Yes

16. How many cloud-based remote agents do you have access to?

    ATE: 12,000 minimum

17. Are agents regularly monitored? How are the agents monitored?

    ATE: Agents are regularly subject to interaction monitoring including cloud-based real-time call and screen recording which provides more visibility into data collected by each agent than available in a brick-and-mortar environment

18. Do you have agent service representatives who are also Security Manager Trained and Certified?

    ATE: Yes

19. How many auditors audit your agent-customer interactions?

    ATE: Agent-customer interactions are audited by multiple auditors who listen to thousands of calls per day for compliance with fraud and security requirements

20. How do you restrict agents' access to sensitive data?

    ATE: We have in place tools and processes that restricts agents' access to sensitive data with seamless technology, and assures that captured data is encrypted whenever it is stored or transferred, and sensitive customer information cannot be accessed by agents

21. Describe the security of your agents' desktop.

    ATE: Agents have a secure desktop that restricts their desktop, ensuring compliance and data encryption, as well as prevents data leakage and sanitizes data via deletion of browser history

Additional Information

Guidance and review of the content of this paper were provided by Niall Browne, CISO and VP of Security for LiveOps. Niall is currently Chair of the BITS Shared Assessments Cloud committee, and vice-Chair of the steering committee. Under his leadership in July 2010 the BITS Shared Assessments Cloud committee published a 53-page document titled Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide.

As stated in the Guide's Forward: This guide was published to help businesses and individuals understand and evaluate the use of cloud computing in large enterprises. The authors' overarching goal is to raise awareness of cloud computing risks in order to better enable enterprise business to successfully deploy cloud computing technologies. This guide approaches various aspects of cloud computing environments from a risk perspective. While many aspects of cloud computing (such as contact center) resemble traditional hosting environments, new technologies often present unique unknown risks that must be considered before and during migration to the cloud. Below is the link to the guide: http://www.sharedassessments.org/media/pdf-EnterpriseCloud-SA.pdf.

Part II of this guide will be published later this month. When available, this whitepaper will be updated with the link to Part II. If you are interested in being notified when Part II is available, please forward your information to the following email address: tvictory@serenova.com.

Serenova®

For more information about Serenova™, please visit www.serenova.com.

Serenova, LLC.
7300 RR 2222, Bldg
III, Ste 200
Austin, TX 78730

toll free 1-800-411-4700

www.serenova.com
sales@serenova.com