White Paper

alpineaccess®

Security Best Practices for Cloud Contact Centers
How to Minimize Risk When Outsourcing Essential Services

Overview:
This white paper, intended for both business decision-makers and IT professionals, outlines a set of best practices for consideration for securing cloud-based contact centers with work-at-home agents. Security for the cloud infrastructure must prevent unauthorized access, and ensure the confidentiality and integrity of all communications end-to-end from the enterprise to the agents. Best practices also require that all employee agents be fully vetted and trained, and that their home offices be properly configured with robust security provisions. Anything short of these measures increases the risk for organizations seeking to take advantage of the cost-saving and other advantages of outsourcing some or all of their contact center workload to a work at-home provider.

Introduction

Two trends are converging in a way that raises new security considerations. The first is the increased use of outsourcing as a means for organizations to gain access to new or expanded services, and/or to save money based on the greater efficiencies involved. The second trend is the emerging virtual workplace where employees are able to work effectively from their homes.

Both trends have had a profound effect on today's contact centers. The concept of the "cloud" embodies how any organization is able to outsource its contact center, as well as how the many employee agents are integrated into the virtual workplace. Security in a cloud-based contact center must, therefore, be both solid and seamless end-to-end, from the organization's customer relationship management or other application to the virtual work @home office.

This white paper outlines a set of best practices for consideration for end-to-end and top-to-bottom security for the cloud-based contact center. The material is organized into two main sections addressing both the network infrastructure and the virtual, home-based employee agents, including their home office work environment.

Network Security

Potential threats to the network infrastructure, including the application servers, come in two basic forms: unauthorized access; and the snooping or hijacking of sessions. End-to-end security provisions capable of preventing both threats are necessary because any chain is only as strong as its weakest link.

The security provisions covered here consist of proven practices for protecting enterprise networks from both threats, and thereby avoiding the dreaded headline news report of the theft of customer account information. Securing the cloud-based contact center from the same threats requires a similar set of provisions and best practices.

Unauthorized Access

Hackers are constantly attempting to gain access to networked resources through a variety of means. With most of these means now well-known and with solid defenses against each currently incorporated into basic system software and various network security provisions, the real threat is the so-called "zero-day" attack. A best practice for preventing these new forms of attacks (at least for organizations that are not its first victim!) is to keep all systems fully up-to-date with the latest software releases and patches. This applies to all internetworking equipment and all application servers, as well as to all of the separate security provisions covered here.

The first line of defense in any network is the ***firewall***. Firewalls are pervasive today, but any coverage of best practices would be remiss in not mentioning their use and importance. Most configurations now employ the "firewall sandwich" for protecting both the Web application servers (the "meat" in the sandwich with firewall "bread") and the back-end systems (normally in the client organization's data center). This configuration is particularly important in the cloud, where back-to-back firewalls often exist at the boundaries of the service provider and enterprise network infrastructures. Note that this security provision is so fundamental that it is now being integrated into other systems, such as the VPN Gateway (covered later).

Authentication is the process (embodied in a protocol) for determining users are who they claim to be. The simplest form of authentication is the user ID and password, and with the use of strong passwords, this method is adequate for many applications. For agents in a work @home contact center cloud, however, something more rigorous is warranted.

The strongest forms of authentication are those that use multiple factors. Normally the factors involve something the user knows (usually a password, preferably a strong one) and something the user has. With this approach is the One Time Passwords (OTP), which is delivered to a user during log-on via a separate device or hard token. Another common and proven approach is to implement certificate-based authentication that utilizes a pair of public and private encryption keys unique to a device possessed by the agent.

An additional layer of protection is afforded by context-based authentication, which uses contextual information to help confirm a user's identity, such as if s/he is scheduled to work during the period of the log-on attempt. A combination of multi-factor and context-based authentication should be considered the best practice for virtual work @home contact centers.

After being authenticated, users are then authorized to access certain (and only certain) resources. Authorization is formally associated with authentication in a "Triple-A" — Authentication, Authorization and Accounting (AAA) — server that provides policy-based management for these three important network access functions. Common AAA servers include RADIUS (the Remote Access Dial-In User Service) and LDAP (the Lightweight Directory Access Protocol), and these servers are also used to manage the next layer of network security: the Virtual Private Network protecting private session traffic traversing public networks.

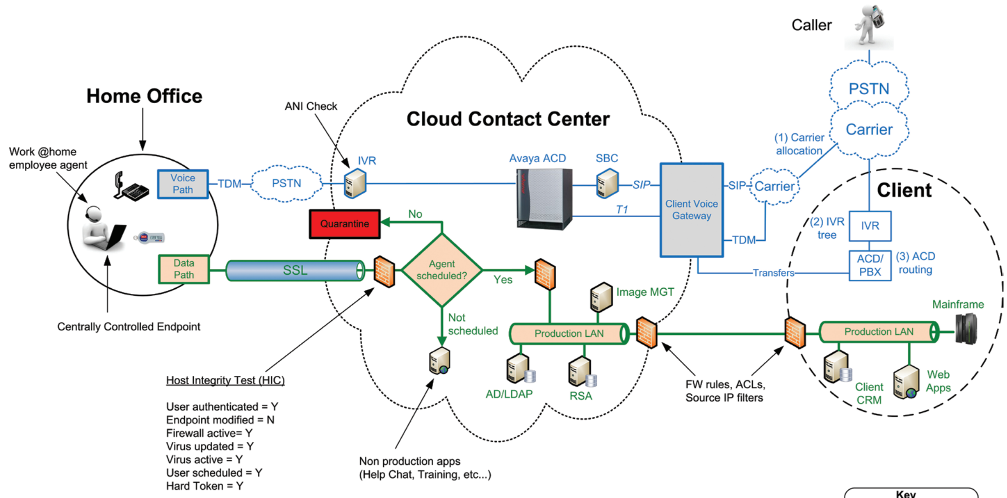
Session Snooping or Hijacking

The cloud's public network infrastructure presents some additional vulnerabilities that must also be addressed. Hackers attempt to "tap" into sessions to snoop or capture traffic, or worse yet, to actually take over or hijack the session by pretending to be the legitimate user. The first offense undermines the confidentiality of the session; the second offense undermines its integrity.

To address these potential security risks, the industry created the ***Virtual Private Network*** (VPN). VPNs establish encrypted (and, therefore, private) "tunnels" through the public network by encapsulating traffic in special packets. The use of strong encryption, such as that afforded by the 256-bit Advanced Encryption Standard (AES), makes it virtually impossible for hackers to snoop or hijack virtual private network traffic. Setting up the VPN essentially involves a process similar to authentication where the users or systems at either end authenticate one another and exchange a set of cryptographic keys.

The typical virtual contact center utilizes two different types of VPNs. Between the service provider and the client organization is the IP Security or IPSec VPN. IPSec is a general-purpose protocol that operates at the Network Layer (Layer 3 of the ISO Reference Model) where the popular Internet Protocol (IP) resides. As such, IPSec is ideal for securing communications between servers, or even between servers and storage area networks.

The second type of VPN operates at the Transport Layer (Layer 4) where the ubiquitous Web browser resides. These Secure Sockets Layer (SSL) VPNs are easier to use, but with rigorous authentication and strong encryption (via the Transport Layer Security protocol), they are just as secure as IPSec VPNs. It is important to note that SSL VPNs also work with other Transport Layer applications, including desktop virtualization solutions such as those from Citrix Systems or VMware, that are capable of adding another layer of security to the network.



Host Integrity Test (HIC)

User authenticated = Y
Endpoint modified = N
Firewall active= Y
Virus updated = Y
Virus active = Y
User scheduled = Y
Hard Token = Y

To be fully effective, cloud contact center security must be both continuous and comprehensive—from the client's data center through the virtual network infrastructure to the work at-home environment.

VPNs are often implemented in dedicated VPN Gateways. The gateway terminates the inbound VPN tunnels, producing cleartext packets for the private enterprise or service provider data center network; for outbound traffic, the VPN Gateway initiates the encrypted tunnels. It is also common for VPN Gateway to integrate other layers of security, particularly a firewall, to minimize the number of devices that must be managed.

Virtual @Home Security

Security for the work @home cloud contact center environment involves both the employee agents and their equipment, particularly the PC and telephone. The people must be effectively screened and the systems must be properly protected. Outlined here are some best practices for making the work @home arrangement as secure as possible.

Virtual Home-based Agents

With working spouses, active children and the housing crisis making it more difficult for people to dig up roots and relocate these days, finding qualified and dependable home-based employee agents can actually be easier than finding regular employees. There are some important differences, though, especially in the ongoing management of the employer-employee relationship.

Outsourcing sometimes means offshoring to utilize cheaper labor in distant lands. For some contact center functions, such as simple scripted calls or back office data services, an offshoring arrangement may be acceptable. But when financial or healthcare matters are involved, some customers may feel uncomfortable due to cultural differences and the sensitive nature of the information shared during the call. For these personal needs, the exclusive use of “homeshore” employee agents that are 100% dedicated to one client account is a far better practice, particularly because the higher wages can usually be offset by lower training and turnover costs, and faster first call resolution.

All employee agents should undergo an intensive vetting process, and a best practice for cloud contact centers is to conduct a particularly rigorous set of background checks. At a minimum, the background check should include verification of citizenship, validation of the Social Security Number, a credit check, and a search of criminal data bases. For certain programs, additional vetting may be warranted, including for education and employment experience, and drug testing may be justified in some situations.

It is also important to have formal employment agreements with all employee agents, which is not possible with contract workers. The agreement should outline the agent’s (versus a contractor’s LLC) responsibilities and obligations, especially with respect to client and customer confidentiality. Initial and ongoing training requirements should also be specified, which cannot be accomplished as easily with contractor agents. The agreements should include provisions for ensuring conformance with its terms and conditions.

Because the employee agent is inevitably a total stranger to the customer, another best practice is to provide some means for protecting personally identifiable information. The preferred method is to enable customers to enter any such sensitive information directly via the telephone keypad: “At the tone, please enter your credit card number.” The identifying information (which may also be a Social Security or account number or a security code) is then associated with the caller’s entire session, but is masked on every screen so as not to be visible to the agent. Having the customer enter the digits directly also helps improve operational efficiency by minimizing keying errors.

Home Offices

An often overlooked consideration in the work @home environment is the workspace itself. The best home offices are characterized by four S’s: Safe, Secure, Secluded and Scheduled. Workplace safety is always important, and high productivity often demands some seclusion to minimize interruptions and distractions (unlike the cubicles at typical centers) throughout the scheduled work day. The focus here, however, is on making the home office at the edge of the cloud fully secure.

The best home offices utilize the Public Switched Telephone Network (PSTN) for production voice communications. Not only does the PSTN deliver superior voice quality, it is also inherently secure and reliable. In situations where Voice over IP (VoIP) communications is suitable, such as while the agent is being trained, the IP ACD/PBX (Automatic Call Distributor/Private Branch Exchange), potentially supplemented by a media gateway and/or Session Border Controller, is responsible for providing the secure voice communications.

Just as servers are vulnerable to hacking, so too are laptop and desktop PCs. This is why the best practices for securing home office PCs, whether issued by the contact center service provider or owned by the employee agents, is similar to those for servers. This requires implementing the very same layers of security found in the data center, in the home office, however, these are implemented instead in software directly on the PC. The

alpineaccess®

most common such security provisions are the firewall, and anti-virus and anti-spyware software.

A related best practice is to "lock-down" agent PCs to prevent any information from being copied, logged, transmitted or otherwise retained. This normally requires a special security application that disables some of the PC's system resources during the session. Depending on the situation and applicable regulations, the lock-down may involve disabling the ability to write or save files to disk (hard, floppy or CD/DVD) or any I/O port (LAN, WLAN, serial, parallel, USB or IR), and to disable the "copy and paste" function. Locking down the PC in this way prevents personally identifiable information from being exposed outside the strictly-controlled confines of the contact center application.

Another best practice for securing the work-at-home PC is the patch management system. For security software to be completely effective, it must be fully up-to-date with the latest version. A best practice here, therefore, is to have a patch cycle that regularly installs system and security software patches and updates, and also includes a prioritization plan to address critical security issues, especially for a new zero-day attack. Naturally, all patches should be tested following an established change management process, and periodic audits should be conducted to assess the effectiveness of the patch management system.

A common saying in national security issues is "Trust but verify." This approach is also applicable to the cloud, where the verification for work @home security is the endpoint HIC (Host Integrity Check). The endpoint HIC should also validate the registry settings, confirm that no unauthorized application is currently installed, and verify that the agent is attempting access at a scheduled time and via an authorized network.

If for any reason the employee agent (after being authenticated) does not pass the endpoint integrity check, the session should be placed immediately in a "quarantine" state. Normally, the only authorized activities during quarantine are those to remedy any shortcomings. For example, the remedy might be to reactivate the firewall or anti-virus software, or to install a critical update or patch. Only upon successfully passing the endpoint integrity check is the user permitted to exit quarantine and, thereby, return to normal, authorized operation.

Conclusion

Security is necessary in any contact center, whether physical or cloud-based. And with a full suite of security provisions implemented by adhering to a rigorous set of best practices, a cloud-based contact center can be made just as secure as one housed within the enterprise.

With a better understanding of the provisions and practices required, how compliant do you believe your (or your service provider's) contact center is currently? Is the network infrastructure secure end-to-end? Is every agent fully vetted, rigorously authenticated and always operating from a secure work environment? Do all transactions and communications afford complete confidentiality and unassailable integrity?

There is a way to know. Both HIPAA and the Payment Card Industry provide for various levels of compliance, and being certified is a testament to the effectiveness of an organization's security provisions. Alpine Access® has been able to achieve both HIPAA compliance and PCI DSS Level 1 certification—the highest rating available.

To learn more about how your organization can benefit from the many cost-saving and other advantages of contact centers operating securely in the cloud, **please visit Alpine Access on the Web at www.alpineaccess.com or call 866.279.0585.**

About Alpine Access

Alpine Access is redefining the contact center industry through its virtual outsourcing services and solutions. Founded in 1998, Alpine Access powers the customer service and technical support operations of many leading international brands through approximately 5,000 work-at-home professionals across the U.S. and Canada. The company offers a robust suite of distributed workforce solutions and capabilities, including SaaS-based talent management platforms, security solutions in the cloud, and consulting services. Rated the #1 contact center and CRM outsourcer for client satisfaction by the Black Book of Outsourcing, Alpine Access' clients include respected Fortune 1000 companies in the financial services, communications, technology, healthcare, retail, travel and hospitality sectors. For more information, visit the Alpine Access website at www.alpineaccess.com or call 866.279.0585.