# Table of Contents

1. **INTRODUCTION** ........................................................................................................................................... 3  
   1.1 **WHY IS SECURITY IMPORTANT?** ........................................................................................................ 3  
   1.2 **SECURITY IN A CONTACT CENTER** .................................................................................................. 3  

2. **PHYSICAL SECURITY** ..................................................................................................................................... 5  

3. **NETWORK SECURITY** ...................................................................................................................................... 5  

4. **COMMUNICATION INTEGRITY** ...................................................................................................................... 5  

5. **SOFTWARE AND APPLICATION SECURITY** ................................................................................................ 6  
   5.1 **SOFTWARE HIGH AVAILABILITY** ........................................................................................................ 6  
   5.2 **CONTAINING IMPACT OF ATTACKS BY DISTRIBUTION OF APPLICATION LOAD** ......................... 7  
   5.3 **ACHIEVING CLOUD COMPUTING SECURITY IN MULTI-TENANCY** .................................................... 8  

6. **DATA CONFIDENTIALITY AND INTEGRITY** .................................................................................................. 9  
   6.1 **USER AUTHENTICATION AND AUTHORIZATION** ............................................................................. 9  
   6.2 **NO DEFAULT ACCESS FOR NEW USER** ............................................................................................ 10  
   6.3 **PROTECT SENSITIVE DATA** ............................................................................................................. 10  
   6.4 **AUDITING** ........................................................................................................................................... 10  
   6.5 **OTHER PROTECTION** ...................................................................................................................... 10  

7. **SECURITY STANDARD COMPLIANCE AND LEADERSHIP IN SECURITY RESEARCH** ................ 11
1 Introduction

1.1 Why is Security Important?

Today companies conduct business 24/7 throughout the year and therefore rely on the continuous operation of information systems. Customer service organizations use electronic information extensively to support their daily processes. Threats to information and processes can prevent businesses from offering consistent and high-quality customer care. Furthermore, customer information could be disclosed, affecting the company’s credibility. If data on customers, products, etc. were to become available to competitors or become corrupted, false or disappear, it could result in major financial loss for the business, or even be a violation of the law. When deploying advanced software solutions into a contact center, enterprise or service provider environment, it is imperative that systems and networks are built in such a way that protects your investments and satisfies your customers.

1.2 Security in a Contact Center

An unsecured hosted or enterprise contact center network provides an avenue of attack against the traditional phone environment, internal data networks and other critical service provider or corporate infrastructure. Furthermore, as traditional voice environments are being migrated to Voice over Internet Protocol (VoIP or IP telephony), existing voice security threats are extended to include entirely new VoIP vulnerabilities.

The front-end of a contact center operation, such as telephone banking, order placement, balance inquiry, and airline ticket booking, expose security vulnerabilities that could be accessed and manipulated through PBXs, Interactive Voice Response (IVRs), Automatic Call Distribution (ACDs) and other voice systems. For example, a ‘spoof’ might use Dual Tone Multi-Frequency (DTMF) tones to guess passwords in order to commit theft of services and access private information. Many organizations have employed caller identification and authentication, but the potential problems with these are complicated by Caller ID spoofing. Security attacks can also come internally - from disgruntled employees, if their access to the system is not restricted appropriately. Several well-published security incidents show that internal attacks have caused as much, if not more, damage as an external one.

These threats translate into potentially expensive fraud scenarios in which a malicious entity can:

- Steal account credentials from a customer of the enterprise employing the contact center by masquerading as an agent.
- Steal enterprise services (or, directly, money) by masquerading as a customer.
- Gain access to both the enterprise and private customer information by eavesdropping. (Securing and protecting customer information is often mandated by government regulations.)
- Effectively derail the business by modifying the application code or data by illegally gaining access to the system. (This can be achieved in many ways, including the spread of malware.)
- Take the system out of service by executing all manner of denial-of-service attacks, of which flooding the system with calls is the best known example.
The advance of Cloud Computing and specifically multi-tenant support within Cloud based deployments complicates the situation in that an extra door is opened to these threats. For instance, if one tenant is infected with a virus, the infection can spread to all other tenants on the same server or same network.

Securing a Contact Center infrastructure includes prevention, detection and accountability, recovery, prevention of outages, as well as management of security-related information. Customers want to know that their personal information is protected, but they are starting to demand procedures that are simpler and more convenient. Voice print technologies used in tandem with other verification processes such as Internet PIN, IVR queries serve as additional validation steps when necessary. Organizations must design a highly secure Contact Center infrastructure that includes security for physical access to data, administrative access to systems, as well as the network and communications.

One important aspect of securing Contact Center infrastructure, especially in the Cloud Computing or Hosted/SaaS environment, is Identity management. Identity Management is viewed as one of the keys to unlocking value inherent in the relationship that the Service Provider — as well as the applications it hosts — has with subscribers and end users of those applications. Since Service Providers often host contact centers, almost all interactions with the end-points can be enhanced by knowing and using the authenticated identity of the subscriber and additional profile information. Likewise, interactions between the Service Provider and an external party are increased in value if the authenticated identity and profile is communicated to the external party. The application of security mechanisms to identity management are discussed in Section 6.

Overall, Genesys Contact Center solutions have been specifically designed to handle security requirements. To deal with security threats, Genesys systematically applies a holistic best-practice system approach according to the following outline:

- Physical security
- Network security
- Communication Integrity
- Application security
- Data security

Genesys Contact Center solutions also comply with the industry standards and government regulations described in subsequent sections.

Genesys Security and Compliance Whitepaper
© 2011 Alcatel-Lucent - All rights reserved
2 Physical Security
Genesys Contact Center solutions can be deployed at network data centers for hosted/SaaS solutions, or at the customer premises for enterprise deployments. In either case, it can be physically secured by applying technology such as electronic access control systems, video surveillance system (VSS) cameras, or mantraps which often have two sets of interlocking doors where the first set of doors must close before the second opens. Biometric devices such as fingerprint readers or iris scanners can also be used. The security features described in this paper assumes that all of the hardware that is hosting Genesys software is physically secured if required. However, such physical security requirement is not mandatory for a Genesys solution to be deployed.

3 Network Security
Network security generally refers to providing protection at the boundaries of an organization by keeping out intruders. There are several technologies that can be leveraged to protect the system from network level attacks that include:

- Firewall, and Multilayer Firewalls
- Zones and Separation, including NAT and DMZ location
- Intrusion Detection System (IDS)
- Session Border Controller (SBC)
- Client blocking/permission list

The security features described in this paper assume that the proper network security devices or software are implemented at the boundary of the data center or enterprise premise, or within the data center or enterprise if necessary. Genesys Contact Center solutions can be deployed all together behind the same firewall, or distributed across several locations behind different firewalls.

4 Communication Integrity
Transport Layer Security (TLS) is an Internet Engineering Task Force (IETF) protocol for secure communications on the Internet, and it is the successor of Secure Sockets Layer (SSL) 3.0. TLS provides strong authentication, message privacy, and integrity capabilities. TLS secures data transmission by using a variety of encryption options. TLS authenticates servers to prove the identities of the parties engaged in secure communication. It also provides data integrity through an integrity check value. In addition to protecting against data disclosure, the TLS protocol is used to help protect against masquerade attacks, man-in-the-middle attacks, bucket brigade attacks, rollback attacks, and replay attacks.

Genesys applications support TLS as well as other application-layer secure protocols such as HTTPS, LDAPS, and SRTP. These protocols are supported whether they are the communication between a client and a server, or the communication between servers.
With that, Genesys supports the use of public key infrastructure (PKI) and provides a security deployment document that details out the procedures that are required to install certificates and configure TLS.

Genesys applications also support protection of the system from rogue client software gaining access to the system. These protections are achieved by:

- Rejecting calls from an unknown Gateway. Genesys SIP solution will reject the calls if the calls are coming through an unknown gateway.
- Client side port definition (permission list). The client-side port definition feature enables a customer to better control the data connections through their firewalls, by enabling them to precisely define the connections that can tunnel through the firewalls. This reduces the susceptibility to Denial-of-Service (DoS) attacks from a rogue client, where an excessive number of malicious application-level requests arrive at the same server-side port from that client.

5 Software and Application Security
Genesys solution software is designed with security attack impact in mind. Security consideration is one of the driving forces for software high availability, software load distribution, and multiple tenancy support.

5.1 Software High Availability
A complete application failure can be the result of either a DoS (Denial of Service) attack, for example, a flood of requests sent by a malicious application, or an external event (i.e. a power failure). It can manifest itself either as no response from a process, or as termination. Typically, if a solution component stops working, the solution is no longer available to process customer interactions.

Redundant applications (typically server applications), provide backup capability in the event that an application fails. That is, if one server (the primary server) goes out of service for some reason, such as failure due to security attack, the other server (the backup server) can act as the primary server, with little or no loss of service.

In case of application failure, an external mechanism for both detection and correction of faults of this type is automatically triggered in a Genesys Contact Center solution. The Management Layer components of the solution serve as such a mechanism. To detect an application failure, the Management Layer employs a simple monitoring component called Local Control Agent (LCA), which continuously maintains a connection with the Contact Center applications, confirming both their existence and their ability to communicate. To ensure that an application failure is never confused with a connection failure, the LCA that monitors a specific application always resides on the computer where the application itself is running.
The Genesys solution supports the following redundancy types:

- **Warm Standby.** Genesys uses the term *warm standby* to describe the redundancy type in which a backup server application remains initialized and ready to take over the operations of the primary server. *Warm standby* redundancy minimizes the inability to process interactions that might have originated during the time it took to detect the failure. It also eliminates the need to bring a backup server online, thereby increasing solution availability. The backup server does not process client requests until its role is changed to primary by the Management Layer. When a connection is broken between the primary server and the LCA running on the same host, a failure of the primary process is reported. As a result, the Management Layer instructs the backup process to switch its role from backup to primary, and the former backup starts processing all new requests for service.

- **Hot Standby.** Genesys uses the term *hot standby* to describe the type of redundancy in which a backup server application remains initialized, clients connect to both the primary and the backup servers at startup, and the backup server data is synchronized with the primary server. Data synchronization and existing client connections to the backup guarantee higher availability of a component. For a complete description of hot standby redundancy, refer to the appropriate product documentation.

### 5.2 Containing Impact of Attacks by Distribution of Application Load

Proxy and parallel servers add efficiency to large configurations, and can limit the damage caused by an outage or security attack.

Both configurations are distributed configurations, however they differ in how the workload is distributed between the servers.

- In a proxy environment, each proxy server takes a portion of the workload and works on that portion exclusively.
- In a parallel environment, the workload is distributed among all of the servers, with one server attempting to keep the distribution as balanced as possible.

The use of proxy and parallel servers greatly reduces the loss of functionality and data if a server goes out of service.

- If a proxy server fails, you lose only the clients associated with that proxy server. In a non-proxy environment with only one server instance, if that single server goes down, all the clients are lost.
- If a server in a parallel configuration fails, new requests are distributed to the remaining servers.
5.3 Achieving Cloud Computing Security in Multi-Tenancy

Multi-tenancy is about enabling a single instance (or single deployment) of a particular software product to serve multiple “tenants”, where each tenant is an organization, department, or some other distinct user. For service providers who provide hosted contact center services, multi-tenancy support is an important feature.

The security aspects of multi-tenancy become one of the key considerations when multiple customers are using a hosted service. In fact, in a Frost & Sullivan survey of more than 300 business decision makers, 33% of executives cited security concerns as being their main barrier to adopting a hosted or SaaS solution. The Genesys software suite can be securely deployed on-premise or in a hosted/SaaS environment via a network of experienced service provider partners to directly address these concerns.

A Genesys hosted solution supports multi-tenancy from end to end and the tenant configuration is an integral part of frameworks. The run time applications support multiple tenants by design, while reporting and performance tools monitor applications to support the reporting data view and categorization based on tenant.

One very important security feature that is critical in multi-tenant environments is the ability to provide tenant isolation and separation, so users in one tenant environment cannot access information in another tenant environment. Genesys hosted solutions support the following forms of tenant separation:

- **Tenant separation at the network level** - The Service provider can choose to build a VPN for each tenant, and have a unique and isolated IP environment for each tenant. These tenants can still be managed by a single management system.
- **Tenant separation at the application level** - All Genesys applications can be deployed for a single tenant to ensure there is no application sharing within an application. This can be expensive for service providers, as the application needs as many instances as there are tenants; however, this approach ensures that no tenant can access data across the tenant boundary at the software application level.
- **Tenant separation at the data level** - Most Genesys applications support multiple tenants with a single running instance. The application is designed in such a way that access across tenants is administrated and governed by following the principle of data and object access. The proper resource usage cap is also implemented in the application to prevent one tenant from using up most of the resources (CPU, Memory) and effectively starving other tenants.

Depending on the security needs, the above approaches can be mixed and matched to satisfy most security requirements of a Genesys hosted Contact Center solution. In one example, the service provider chose to put some applications in separate tenant blocks, dedicated to each tenant, while the remaining applications were put in the common blocks, shared among all tenants. This mixed approach balances the hardware needs and security separation for large hosted contact center offerings.
6 Data Confidentiality and Integrity
Secure access to the resources of an interaction-management system plays an important role in ensuring trouble-free operation of all system parts and functions. Changes made by unqualified users can adversely affect system availability and the quality of service.

6.1 User Authentication and Authorization
Secure access to a system requires that each user pass the following tests:

- User authentication checks to see that the user is actually who he or she claims to be. This is usually carried out using a system of passwords or other unique and confidential (or unalterable) identifiers.
- User authorization. After the user is authenticated, this test determines that the user is entitled to access the system, either all or parts thereof, and defines what the user can do to or with the data that they can access. This is usually carried out using a system of permissions or similar access rules.

Authentication

The configuration parameters in a Genesys solution which define the agents and self service, as well as the configuration of applications and the solutions are described in the form of Configuration Database objects. To be authenticated, any person who needs access to this data or these applications must have an account in this database.

Authorization

User authorization is provided by the security mechanism implemented in the Configuration Application, which allows the system administrator to separately define a level of access for any account with respect to any object. User authorization is often accomplished with a permissions system, in which only authorized users can see (in some cases) only specific data and can perform only certain tasks on that data.

Genesys customers may use either an LDAP-based or Radius-based system to manage their accounts and take advantage of features there, while only authorizations would be managed by Genesys.

Genesys solutions use two levels of permissions to implement user authorization:

- Object-Based Access Control—what the user can see and do to an object is controlled by a set of permissions.
- Role-Based Access Control (RBAC) —provides an additional layer of data protection from unauthorized users by defining what is displayed in the interface and therefore limiting what actions the user may perform related to the objects to which they are permitted.

With these two levels of authorization controls, customers can configure the Genesys solution to achieve their specific business needs without compromising security requirements.
6.2 No Default Access for New User

New users created in a Genesys solution are, by default, not automatically assigned any privileges—either access permissions or role privileges. In effect, the new users cannot log in to any interface or use a daemon application. A daemon application is a program that runs in the background not under direct user control, but rather is typically initiated as a background process. Systems often start or “launch” daemons when booting up and can serve the function of responding to network requests, hardware activity or other programs by performing some task.

Each new user must have the appropriate access privileges and roles assigned by either a system administrator or another existing user with appropriate access rights. This feature guarantees that there may be no hidden security problem for any new user. The security right of the new user needs to be granted explicitly by an authorized person. (This feature can be disabled if desired.

6.3 Protect Sensitive Data

Genesys solutions enable customers to hide all or part of selected key-value (KV) pairs in the output of log messages generated by a Genesys application. This prevents unauthorized users from seeing particular data in the output of log messages. This feature is also useful for preserving the confidentiality of data that is provided by third parties, which might flow through the system as KV pairs and otherwise be logged.

6.4 Auditing

The Genesys solution tracks individual interactions, audit activities in the contact center, and stores alarm history in the centralized log. These audit logs can be later viewed by the security audit process to verify if the system has been accessed by un-authorized person, or whether the changes were made by un-authorized person.

6.5 Other Protection

In addition to the user authentication and authorization and concealment of sensitive data, Genesys solutions also support other features to protect data. Industry standard password encryption is utilized both in transit using AES256 and in storage where passwords are recorded as their hash value after applying a Salt. In password protection, salt is a random string of data used to modify a password hash. Salt makes it more difficult for an attacker to break into a system by using password hash-matching strategies, since adding salt to a password hash prevents an attacker from testing known dictionary words across the entire system which is a common tactic among hackers.

Transparent database encryption can be enabled through configuration. Session and inactivity timeouts can be used to close unused openings. Applications may present a custom message at startup such as a term of use message. Finally, applications may present a timestamp of the last time a user logged on to assist in detection of credential hijacking.
7  Security Standard Compliance and Leadership in Security Research

A Genesys solution is designed to be the core component of a fully functioning contact center, which may include certain non-Genesys components and customer systems. Genesys products provide customers with flexibility in designing their own contact center Solutions in term of security. It is possible for a customer to use the Genesys suite of products in a manner that complies with security-related business standards including European Data Protection Directive (EDPD), ISO 2700x, HIPAA, PCI DSS etc.

Genesys, an Alcatel-Lucent company, also actively participates in developing security-related standards organizations. In particular, Alcatel-Lucent has been actively participating, leading, and contributing to major security efforts in ISO/IEC, IETF, and ITU-T. Among the major most relevant projects lead by Alcatel-Lucent, based on Bell Labs technologies, are 1) ITU-T Recommendation X.805 (jointly standardized by ISO/IEC as International Standard 18028) and 2) The ITU-T Y.2700 series of Identity Management Recommendations.

The standardization work of ITU (International Telecommunication Union) dates back to 1865 and ensures the development of efficient and timely standards that encompass all fields of telecommunications on a worldwide basis.

Alcatel-Lucent has founded and drove standardization in the IETF of the Radius protocol, as well as its successor, Diameter.

Presently Alcatel-Lucent is also an active contributor to the IETF OAuth project. The Genesys eService solution, which provides customer service through E-mail, Chat, SMS, and Social media, also relies on OAuth standard. OAuth, or Open Authorization is an open standard that allows users to share their private resources (i.e. photos, videos, contact lists) stored on one site with another site without having to share credentials such as username and password. Users can grant third party site access to information that is stored with another service provider, without sharing their access permissions or data details.

In addition, various governments and government agencies (such as the National Institute of Standards and Technology [NIST], a U.S. government agency), professional organizations (such as the Institute of Electrical and Electronics Engineers [IEEE]), and industry develop essential standards or standards requirements for the relevant pieces of the industry. Nonetheless, these agencies, organizations, and partnerships still often rely on (or effectively drive) the results produced in one or more of the three standards bodies discussed here.

As part of Alcatel-Lucent, Genesys is also working closely with Bell Labs, the research and innovation arm of Alcatel-Lucent. The research results are being integrated within Genesys solutions to provide better protection for Contact Center operations. One example is the heuristic algorithm of Intrusion detection by anomaly detection, developed by Bell Labs. This algorithm provides better intrusion detection than commercially available products, and can be integrated into the Genesys solution for extra security protection.