Security Considerations
For an IP PBX and Contact Center Application Server
CIC Version 2.4

WHITEPAPER

By Peggy Gritt
Senior Director, Product Marketing/Channels

September 27, 2005

Abstract

As voice and data communications increasingly migrate to Internet networks and voice over IP (VoIP), communications security has taken on added importance for customer privacy and regulatory compliance in contact center and other consumer-oriented industries. This paper discusses the OSI Model for network and communications system security and how it applies to the Customer Interaction Center® (CIC) application server, with specific emphasis on how version 2.4 of the CIC software conforms to an organization’s existing network operating system environment and security policies for compliance requirements.
# Table of Contents

**Introduction**

**The OSI Model for CIC Security Considerations**
- Layer 1 – Physical Layer
- Layer 2 – Data Link Layer
- Layer 3 – Network Layer
- Layer 4 – Transport Layer
- Layer 5 – Session Layer
- Layer 6 – Presentation Layer
- Layer 7 – Application Layer

**Considerations for Network Policies and Standards**

**Platform and Operating System Controls**
- Security Policies and the Windows Operating System
- Hardening the Operating System
- Security Patch Verification
- Virus Protection
- Connections to Other Applications on the Network

**Interactive Intelligence and Regulatory Compliance**
- ISO Registration
- Customer Regulatory Issues
- Globalization

**Conclusion**
Introduction

Interactive Intelligence has been taking a software approach to voice and data communications for more than 11 years. Because our multi-channel software architecture is designed to process voice interactions, phone calls, Web chats, e-mails and associated interactions alike, products such as the Customer Interaction Center® (CIC) give contact centers and business enterprises far more than just a PBX phone system or automatic call distributor (ACD). Also because the open standards CIC software comes equipped for voice over IP (VoIP) and the Session Initiation Protocol (SIP) communications standard that supports VoIP networks, Interactive Intelligence continues to focus on security issues well beyond voice traffic on an IP communications network — unlike many proprietary vendors currently in the VoIP market.

Multi-box Architecture Amplifies Security Concerns

Rather than proprietary systems that connect one hardware “box” after another for Internet-driven VoIP (as shown in top graphic), Interactive Intelligence designed the CIC software on a common communications processing architecture that acts similar to other business applications on an organization’s network. The net result is reduced complexity in a telecommunications infrastructure (bottom graphic) since CIC eliminates the need for separate PBX, ACD, voicemail, IVR and reporting systems. CIC also replaces fax servers, antiquated call recorders, Web chat and collaboration systems, and e-mail routing and queuing systems. With fewer “moving parts” and less complexity to concern IT security teams, CIC gives security-minded organizations a more secure environment for IP communications.

Single System across Media Types: One Vendor, One Set of Security Concerns

Interactive Intelligence designed CIC’s server-based applications to run on the Microsoft® Windows® operating system, to integrate to desktop applications for improved user productivity, and to handle SIP-compliant station devices such as SIP phones and communications on the network via SIP gateways.
The Open Systems Interconnection (OSI) Model

The Open Systems Interconnection Model provides some of the most stringent security capabilities possible for mission-critical communications systems, and is the only internationally accepted standards framework that supports communications between various systems from different vendors.

This paper presents the Customer Interaction Center’s security capabilities from the OSI Model standpoint, discussing each “layer” of the Model’s categorized communications security process:

**Layer 1** – Physical Layer

**Layer 2** – Data Link Layer

**Layer 3** – Network Layer

**Layer 4** – Transport Layer

**Layer 5** – Session Layer

**Layer 6** – Presentation Layer

**Layer 7** – Applications Layer
Introduction / OSI Model (continued)
Interactive Intelligence takes a unique standards-based software approach to business communications that leverages the Session Initiation Protocol (SIP) standard for VoIP network implementations. Security mechanisms for the CIC software can therefore be deployed between the CIC application server, the SIP gateway, and SIP telephone devices for enhanced network security in a VoIP configuration. Mechanisms can include a Virtual Private Network (VPN), Virtual Local Area Network (VLAN), Transparent LAN Service (TLS), Secure Real-time Transport Protocol (SRTP), Access Lists, and Authentication.

(Note: the Communité® unified communications software from Interactive Intelligence and the Enterprise Interaction Center® IP PBX software from Interactive Intelligence subsidiary, Vonexus, incorporate the same security mechanisms.)

Given CIC’s multi-channel event-processing software architecture — along with sub-systems that connect to voice/data (via SIP), Web applications, database applications, e-mail servers and other systems on an organization’s network — Interactive Intelligence understands that communications security must be addressed at all levels to be effective. The following sections discuss CIC’s application server connectivity on the network with regard to the OSI Model’s seven layers of security.

For more than a decade, Interactive Intelligence has provided innovative multi-channel software solutions for the contact center market and other consumer-oriented industries, making regulatory requirements and compliance one of our highest priorities for product development. Our experience with compliance issues, and with helping organizations avoid the potential legal ramifications of non-compliance, has thereby made our solutions popular among healthcare providers, government agencies, public companies, and financial institutions as well as contact centers.

The OSI Model for CIC Security Considerations

Layer 1 – Physical Layer Security

Overview
The OSI Model’s Physical Layer of security applies to all physical devices in a communications system and their availability in mission-critical situations. For the Customer Interaction Center (CIC), physical device availability encompasses system power, environmental control, inputs (physical access), device disconnections and other associated physical factors.

Because CIC’s server-based applications are developed to run on the Microsoft Windows operating system, all seven layers of security within the OSI Model actually apply to the CIC software. Regarding the Physical Layer, however, the majority of organizations using CIC install the CIC Server on their network alongside other existing Windows-based servers — essentially aligning the CIC system under the same physical security policies they employ for their building, data center (typically the CIC Server location), and desktop equipment for end-users. But the CIC system can also offer a few additional measures of system security when applied to the OSI Model’s Physical Layer.

Preventing a Loss of Power
To survive a power outage, organizations can co-locate the CIC Server with all other data servers for connection to a back-up generator, or can optionally connect the CIC Server to a UPS. A UPS configuration gives system administrators sufficient time to convert the CIC Server to a disaster recovery server at an alternate location. (Many organizations house the CIC Server in a locked environment along with other mission-critical servers.)
To overcome a loss of power to CIC end-user devices, SIP telephones such as those from Polycom® have the ability to use power from the Ethernet network cable rather than from the wall outlet. In this case, the phones must also be connected to a router that supports power over the Ethernet network. CIC additionally supports analog media gateways that can power an analog telephone during any outage, as long as the media gateway maintains power via a UPS.

Environmental Control
Organizations should maintain the CIC Server in an environment where the temperature control is set for a mission-critical server. Also as it is with any mission-critical server, it’s important to secure the CIC Server with key or keypad access.

Business Continuity via Remote Locations
CIC allows multi-site organizations to locate a primary CIC Server at their headquarters and extend IP PBX call processing and ACD routing to branch offices or contact centers via a SIP-based VoIP network. For outage security in such a configuration, Interactive Intelligence offers a SIP proxy called Business Continuity Manager that allows any branch site to maintain basic inbound and outbound call routing should the primary CIC Server connection be disrupted at HQ. Whether the main office experiences a WAN link crash, power outage or some other disaster, CIC simply routes calls to a remote office to uphold business continuity.

Disaster Recovery with CIC’s Centralized Architecture
The centralized software architecture CIC provides for all communications applications and makes it easier to support disaster recovery processes throughout an organization. By establishing a CIC-based disaster recovery server off-site, the disaster recovery server takes over should an outage occur where the primary CIC Server is housed. Users can then use any telephone to log in to the CIC system from home or an alternate location, and still receive ACD calls as well as their own extension calls. If users have a data connection, they can also remotely perform CIC functions such as unified messaging and Web chat as if in their normal office setting. Businesses can therefore leverage CIC to effectively manage disaster recovery plans, maintain business continuity and connectivity with customers, and prevent potential revenue loss from communications system disruptions.

Password Keystroke and Input Logging
A system administrator must first access the CIC Server via Windows security but can also establish an adjoining CIC password. If the CIC Server is locked, no person other than the system administrator can access the server’s keypad to log on to the CIC system. Each desktop machine should also be password protected on an organization’s network, with network policies in place to lock each PC or workstation when an employee leaves their desk for a predetermined number of seconds or minutes.
Disconnection of Physical Links
If multiple gateways are established on the network (LAN or WAN) in a CIC system configuration, an organization can use back-up lines in the event that a particular line to a gateway is unavailable. Organizations should also consider other physical links that can potentially be disconnected as part of their overall network security plan for routers, phones and other devices. To monitor the CIC system in real-time, the CIC Server offers the pre-integrated Interaction Supervisor module (shown here) to quickly determine when segments on your network are down, which can prevent the CIC Server from physically connecting to a database server for report logging, to an e-mail server for unified messaging or e-mail queuing, etc. Alerts in Interaction Supervisor immediately notify a system administrator if CIC loses connectivity to other servers on the network.

Physical Telephones in Open Areas
Organizations can secure telephones in open areas such as office lobbies, employee lunch rooms, etc. by disallowing long distance or toll calls without an 800 number or calling card. Telephones with no users logged into them can be further secured by requiring an authorization code to dial long distance numbers.

Phone Configuration on the Network
CIC’s Phone Configuration Utility includes a Trivial File Transfer Protocol (TFTP) server that specifies all extensions an organization can upload with the CIC system. Even though the TFTP server is in read/write mode, it does not allow phone configuration (.cfg) files to be overwritten or modified, which addresses any security concerns for phone devices and their individual configurations.

Layer 2 – Data Link Layer Security

Introduction
The OSI Model’s Data Link Layer provides the security level data packets are prepared for network transmission by the Physical Layer.

Access List Support
From the Layer 2 perspective, an organization can configure its network to support MAC-based access lists that prevent “man in the middle” attacks as well as rogue device connections. Defined, a Media Access Control Layer is that layer of a distributed communications system concerned with access control to a medium shared between two or more entities. Organizations should therefore create an access list for specific MAC addresses to heighten access security for all switches on a network.
Layer 3 – Network Layer Security

Introduction
The OSI Model’s Network Layer of security covers the topology of a network and typically considers the IP addresses of network nodes. The Customer Interaction Center (CIC) application server provides security at this layer by supporting standard firewalls and lists of invalid IP addresses, and by handling Denial of Service Attacks on the network itself.

List IP Addresses to Deny Communications
The CIC Server supports the ability to list forbidden IP addresses, which enables an organization to configure the CIC Server to understand IP addresses that aren’t allowed to communicate directly with the CIC Server. Under the OSI Model for CIC, the firewall provides universal control for the Network Layer.

Firewall Support
The CIC product and its add-on modules (Interaction Dialer®, Interaction Recorder®, Interaction Tracker and other add-on applications) run behind the firewall just as any other business application server on the network would. It also is possible to separate/control each type of communication via a firewall. Since CIC uses different TCP/IP ports for Web, application (Notifier), and data (SQL Server), access can easily be controlled via the firewall. Also for SIP session routing, organizations can make the firewall “SIP-aware” to handle SIP-based calls; for instance on the WAN they use for their SIP network.

Denial of Service Attacks on the Network
A Denial of Service Attack is a malicious network attack that keeps users or devices from accessing a normally available network service. DoS Attacks are considered extremely difficult to defend against due to their changing nature, and typically occur through open ports on a communications network.

Miercom testing for DoS Attacks
To enhance security against DoS Attacks, the CIC software was thoroughly tested by Miercom, an independent network consultancy and test lab, as part of their voice over IP security assessment for communications products in the contact center segment. Using a simulated DoS Attack on the CIC’s event processing software architecture, Miercom testing personnel determined a medium to low degradation. Contact centers implementing CIC are advised to structure all communications between network services in a proprietary encrypted protocol; any network messages received on CIC’s open ports are then simply ignored or disregarded to provide additional protection for the CIC Server if a DoS Attack occurs. In short, the CIC Server will not fail to perform in the event of a DoS Attack on the network. As proof, Miercom simulated a random ACK character “flood” for CIC’s data communications and found no noticeable degradation to the CIC system’s CPU performance (Low rating). Also of note, the CIC Server that Miercom tested wasn’t “hardened.” Subsequently, considering the operating system wasn’t prepared for this sort of test, the CIC software itself performed very well. Moreover, CIC is designed to prevent DoS Attacks for SIP systems via a configurable access control list whereby the CIC administrator can grant or deny access by specific IP addresses, or range of IP addresses, when establishing a SIP connection.
Layer 4 – Transport Layer Security

Introduction

The Transport Layer focuses on ports in a communications system and is the OSI Model’s first logical layer for security. Transport Layers are normally built for speed and utility, and present vulnerabilities related to the source of a data packet communication — primarily when open ports are used for too many purposes and make security more difficult for the firewall. Again for the OSI Model, firewalls are the Customer Interaction Center (CIC) software’s common control at the Transport Layer of security (discussed in the previous section).

Digest Authentication

With Digest Authentication in CIC, passwords are never sent across the network without being encrypted. The CIC system encrypts all passwords and data passed between the CIC Server and the desktop client.

Open Ports

Enabled transport protocols, services and ports can pose a high level of vulnerability to outside attacks on a communications network/system. To decrease such vulnerability, the CIC system incorporates a proprietary Internet Protocol for communications, making it difficult for hackers to access information data packets being passed over a network. (Using this approach, CIC requires only two ports to be opened.) The CIC Server also includes a TCP/IP port that enables proprietary CIC messages to be handled between the CIC Server and desktop clients. If using Microsoft’s NT authentication, organizations may also need to enable Distributed Component Object Model (DCOM, Microsoft’s distributed version of its COM). CIC-based firewalls require nothing to be enabled.

Layer 5 – Session Layer Security

Introduction

The OSI Model’s Session Layer is concerned with the communication session protocol a communications system utilizes, such as the Session Initiation Protocol, or SIP. The Customer Interaction Center (CIC) software uses SIP as the Session Layer protocol for voice over IP and/or, on the data side, the authentication and password control of the session initiation. This section discusses CIC’s encryption capabilities for protecting the Session Layer and how data packets are transmitted using the SIP session for information such as numbers, passwords, etc.

Encryption Standards

CIC offers encryption both for voice and data communications on the network, since organizations sometimes pass sensitive customer and user information (related to customer accounts, names, etc.) between the CIC Server and the user interface. For example, a contact center will often use an IVR system to request a customer’s account information prior to routing that customer’s call to an agent. The customer’s entered information is then used to “screen pop” an application at the agent’s desktop as the call arrives. For data security, contact centers and other organizations can encrypt all data traffic between the CIC Server and the end-user’s desktop CRM application using the symmetric Advanced Encryption Standard (AES) in CIC. All data destined for a host is encrypted directly on the CIC Server. And while a full message is encrypted, a notifier header is not. Data also is not decrypted in CIC, except by the host receiving the message. For more secure applications, the CIC software supports IPsec IP Security measures that in turn support an “authentication header” to verify the validity of an originating address in the header of every packet within an IP network packet stream.
Secured Voice Messaging Traffic

Note: The following encryption options will be released in the CIC 2.4 SIP Feature Pack available in early 2006.

For CIC-based SIP configurations, Interactive Intelligence provides standards-based encryption using the Transparent LAN Service (TLS, described in the SIP RFC 2246) and Secure Real-time Transport Protocol (SRTP, described in the SIP RFC 3711). Interactive Intelligence uses the open SIP standard at all times and therefore utilizes the standard encryption method. All components must also support the RFCs referenced here in order for the encryption to work, which requires a CIC configuration for SIP to include the Intel® NetStructure™ Host Media Processing (HMP) Software, media gateways, and SIP-compliant telephones. Intel’s HMP software enables CIC to stream RTP audio on the network; Intel is expected to support these required SIP standards in early 2006. Interactive Intelligence is actively working with Microsoft, Intel, AudioCodes, Polycom, and net.com to deploy TLS and SRTP for the CIC 2.4 SIP Feature Pack.

Encrypted Voice Payload

A common concern with network-driven voice communications is an unwanted person’s ability to “sniff” a network and eavesdrop on a call from their PC. Interactive Intelligence understands such concerns and, to our knowledge, can say this has never occurred with the CIC system. To further ensure network and call security, however, CIC and other products from Interactive Intelligence will continue to support SRTP across all voice interaction types in conjunction with Intel and other VoIP vendors.

Once again due to the nature of our software, this measure secures all voice traffic whether directed to an ACD, individual PBX users, or a caller in an IVR or voicemail process.

Layer 6 – Presentation Layer Security

Introduction

The OSI Model’s Presentation Layer provides transparent communications services by masking the differences of varying data formats (such as character codes) between dissimilar systems. The Customer Interaction Center (CIC) optimizes this layer of security through CIC’s single comprehensive framework for system and user administration, as discussed in the following subsections.

Administrative Rights

The CIC system’s single administrative environment makes it much easier to track the administration of CIC’s inherent PBX, ACD, IVR, voicemail and fax server capabilities plus any integrated business communications applications. Because the CIC software “acts” as all of these components, it is important that the system’s administrative environment be secured on a granular basis. That is, administration access to individual CIC components can be granted to an administrator on as-needed basis. As an example, a workgroup administrator isn’t authorized to administer trunk or SIP “lines” in the CIC system. As another example, an IT administrator (or group of administrators) can be authorized solely to administering the CIC dial plan. This granular assignment of administrative rights ensures that departments and IT groups can control their own business application server.

Administrative Audit Trails

To audit changes to the CIC system, CIC’s administrative change log lets administrators know who made a specific change in the administrative environment, and track changes via CIC’s out-of-the-box administrative change log reporting tools.
User Rights
Just as granular rights are available within the CIC system’s administrative environment, the system also is set up for individually-assigned access rights to CIC’s various features and functions. Most user functionality licensed to a CIC user requires a license key that can be assigned to the user or station. This allows an organization, for example, to designate that a user is a “business” or PBX user who should not be equipped with CIC’s call center features, such as Web chat. Conversely, access to features such as call recording, the supervisory ability to listen to a call center agent, or the ability to make more than X number of calls at a time can be assigned by workgroup, role (class of service) or by individual. CIC user rights also offer a global setting to set an access level for all users, such as CIC system access for 900 calls.

Layer 7 – Application Layer Security

Introduction
The OSI Model’s Application Layer includes functions for specific applications services, such as file transfer, remote file access and virtual terminals. The Customer Interaction Center (CIC) software extends several user and applications security measures at this level, with a specific focus on remote users and CIC’s “virtual office” capability.

Password Encryption
All user/administrator passwords in CIC are encrypted when entered on application command lines and when passed to the CIC Server. Passwords also are concealed on the CIC system’s dialog box. It is important to note that the CIC system supports required password changes to the CIC user name/password. CIC additionally offers features that let an organization establish parameters for the character length and type of user passwords, including available password security settings determined by user role.

User Authentication
CIC offers three options for user authentication. For companies that rely on the Microsoft platform, CIC user authentication can be based their NT authentication to validate each user (logged in to a system) against a domain that’s also valid for the CIC system. In this case, the CIC password is not required. The second option is available to companies that elect not to use NT authentication, and that instead have deployed their own method/standard for user authentication. In this case, companies can incorporate a Dynamic Link Library (DLL) to support customized user authentication methods. The third option is simply to use CIC’s user name/password authentication, which is always required to retrieve voice messages, but is an option for a CIC user’s desktop login.

User Remote Access
The CIC system offers remote user capability that allows work-at-home call center agents and mobile business users to log in to the CIC system from any TCP/IP connection. (An organization must authorize remote user rights and grant CIC system access, of course). Remote CIC users require a VPN connection to log in to CIC’s Interaction Client® desktop communications interface, and can use the Interaction Client’s soft phone by indicating their remote telephone number. Organizations can grant a telephone number for remote access based on a local or long distance number, but can also deny remote access if using an international number. Organizations also deploy Citrix or Terminal Services for remote CIC user access to their business applications, since CIC supports the Interaction Client interface to run in such environments. Interactive Intelligence does recommend that the VPN be used with IPsec to ensure the best security for remote connections.
Remote Access for System Maintenance Procedures

System administrators can access the CIC Server remotely via the Internet, a dedicated leased network line, or any method that allows them to connect to a standard Microsoft Windows 200X server. Organizations that perform remote CIC system maintenance on a regular basis can determine the best process based on their security requirements.

As with any kind of remote communications system access, organizations are concerned about the transmission protocols being used on the network and associated vulnerability. The CIC system supports common transmission protocols including FTP, SFTP, TFTP, SSH, SCP, HTTP, HTTPS, MQ, MQ w/SSL, Connect:direct/IP|SNA, SMTP, POP3, Citrix, SNA|IP|GRE, VPN, etc. The CIC system also uses a proprietary TCP/IP notifier protocol to enhance network security for remote access purposes.

The database protocol for CIC depends on which database an organization is using.

Database Controls

CIC uses the NT registry for the administration of user and system information, along with database resources for logging report data and user/workgroup contact directories. Moreover, the CIC system leverages database connections in its IVR component to support automated self-service applications that allow callers to access their account data, a company’s information, etc. Because the database itself is not encrypted, however, CIC employs the Advanced Encryption Standard (AES) encryption method to secure all connections between a database and the CIC Server. The CIC Server also requires an administrative user ID and password to connect to Open Database Connectivity (ODBC) drivers for ODBC-compliant databases, adding yet another level of database security. Finally to enhance database controls with regard to Web-based data transmissions, CIC supports Soap Tools to communicate to Web services on a Secure Sockets Layer (SSL), which in a CIC configuration provides the transport layer technology for authentication and data encryption between a Web server and Web browser when sending documents/data via the Internet.

For any organization using the CIC software and associated Interactive Intelligence products, system administrators benefit handsomely in that CIC utilizes a standard SQL or Oracle database for all event-logging and tracking for reporting purposes. Administrators can therefore implement their standard security procedures for maintaining the database, since the CIC architecture introduces no requirements for third-party or proprietary data systems.

Toll Fraud

Due to CIC’s PBX and ACD capability, another critical security concern is toll fraud protection (as it is with virtually any PBX or ACD product). By design, organizations can disable several areas of the CIC system to prevent toll fraud. One example is the CIC system’s “Available, Forward” feature, in which users can forward their corporate extension to a cell phone or home office phone when not at their desk working. Other CIC system features allow external access to CIC users via a company directory, allowing an organization to establish access points on a per-user basis to disable long distance or international numbers, or to disable access points completely. Interactive Intelligence provides an extensive list of areas within the CIC product that provide remote number access, as well as instructions to CIC system administrators on how to secure these features against toll fraud.
Considerations for Network Policies and Standards

Most organizations already have standards in place to manage network security for data driven applications. Beyond data applications, however, security concerns for voice over IP (VoIP) can come down to a new IP solution’s adherence to existing organizational standards for security components such as firewalls, intrusion detection systems, virtual private networks, and demilitarized zone (DMZ) sub-networks that sit between a trusted internal network (such as a private corporate LAN) and an untrusted external network like the Internet.

Because the Customer Interaction Center (CIC) system acts as a business application server on the network, the CIC Server can fit securely into a current IT infrastructure for IP communications and easily adhere to the security policies and procedures a contact center or business enterprise already has in place. More so, CIC adds wide-ranging security enhancements specifically geared to VoIP — among them the Protection Monitoring Systems discussed here.

Protection Monitoring Systems
Interactive Intelligence products including CIC support the Signaling Network Management Protocol (SNMP) for SNMP monitoring, and also are certified with the Primary Response® application from Sana Security™. Primary Response is industry leading intrusion prevention software (IPS) that automatically detects, classifies and responds to complex threats — accelerating time to protection and enabling IT teams to deliver business continuity without compromising visibility and control. For CIC, Primary Response uses (1) an out-of-the-box knowledge-based system to protect end users, applications and systems; (2) Active Malware Defense Technology (Active MDT) that can
detect and prevent suspicious Malware activity such as Trojans, key loggers, silent backdoors and root kits based on a behavioral heuristic approach; and (3) Sana’s Adaptive Profiling Technology (SanAPT), which provides instant protection for memory-based attacks, learns normal application file path behaviors, and responds to anomaly-based threats.

Platform and Operating System Controls

Security Policies and the Windows Operating System

Two major issues relate to Microsoft operating systems security with regard to CIC. The first is “hardening the operating system” itself to ensure that it’s as secure as possible. The second issue relates to the handling of Microsoft security patches, and to Interactive Intelligence validation that a security patch is compatible with the CIC software.

Hardening the Operating System
Hardening the operating system refers to establishing all appropriate settings within the Microsoft operating system to ensure maximum security settings when running the CIC software. Security features in Windows 2003, for example, include an Authorization Manager for role-based access to applications, stored user names and passwords — which in turn allows an organization to secure stored CIC user names and passwords that are used to access external network and Internet resources on the CIC Server (and on other servers on the network). Interactive Intelligence offers a Security Precautions Guide that leads Interactive Intelligence implementation Partners as well as customers through security issues on the Microsoft Windows 2000 and 2003 operating system.

Security Patch Verification
Interactive Intelligence also has instituted a new procedure to quickly verify Microsoft operating system security patches, and to notify Partners and customers that a particular security patch is available and validated for use with the CIC software. This process is automated for regression testing against the CIC system, as is a notification system for when the validation process is complete. We understand that many of our customers use their own validation as well for security patches and operating system releases for Microsoft software, and continue to validate security patches for such customers as quickly as possible using our automated verification processes.

Validation simulation
Simulating the validation process encompasses four machines in our test facilities:
- Software Update Services (SUS) and Domain Controller
- Interaction Center 2.3.1 SR-A with Dialogic
- Windows XP Professional Client
- Windows 2000 Professional Client

The SUS Server downloads current updates for all languages from Microsoft and applies new operating system patches (a process performed on a daily basis). The SUS simulation processes CIC-based station-to-station calls, voicemail send and retrieval, fax,
and ACD e-mail queuing. Should a Microsoft patch cause one of these critical CIC functions to stop working, an event report is submitted to the Interactive Intelligence validation environment administrator for corrective action. Event report results are posted in the Support Area of the www.inin.com Web site and can be accessed at any time by a CIC-licensed network administrator or Interactive Intelligence Partner.

We also use Windows Software Update Services (the newer version of SUS) in our testing facilities, and route all critical Interactive Intelligence product updates, security updates, drivers, Feature Packs, Service Packs, tools, and update rollups via Group Policy to all test lab machines throughout the QA cycle.

Virus Protection
Due to the mission-critical nature of the CIC system acting as a PBX and ACD in a VoIP environment, Interactive Intelligence pre-validates popular virus protection software to run on the CIC Server. Several anti-virus software solutions have been validated. Check with your Interactive Intelligence Partner or account manager as to whether your corporate anti-virus software is compatible with the CIC software.

Connections to Other Applications on the Network
The CIC system connects to other applications via TCP/IP communications on the network and takes several measures to ensure connection security. To connect to ODBC-compliant databases, CIC configurations typically use an ODBC connector that provides its own user ID and passwords to prevent unwarranted access to data. CIC also connects to an organization’s e-mail server via TCP/IP connection, and incorporates an administrative ID and password to safely send and receive e-mail from the e-mail server. CIC’s Web services subsystem additionally offers an optional encrypted path between the CIC Server and the Web server for even more peace of mind.

Interactive Intelligence and Regulatory Compliance

ISO Registration
It is important to note that Interactive Intelligence is ISO 9001-2000 and TL9000 registered. As part of a potential customer’s vendor research and product purchase process, we invite prospects to learn about our formal quality, testing, and development processes at any time. Many times, prospective customers will visit our headquarters to personally tour these departments and hear directly from departmental directors who govern our ISO policies and procedures.

Customer Regulatory Issues
Increasingly, contact centers and customer-focused businesses must comply with regulatory requirements for HIPAA standards, the Sarbanes-Oxley Act, consumer privacy policies and outbound telemarketing laws. More than ever, this new environment of regulation requires the business community to record and track transactions between employees and customers.

The CIC software is unique in its ability to not only track customer telephone calls, but also to track entire customer interaction histories for phone calls as well as faxes, e-mails, and Web chats using the Interaction Tracker add-on application from Interactive Intelligence. Just as critically for compliance issues, CIC’s Interaction Recorder® add-on product enables an organization to record customer interactions in full and store recording files in the Interaction Recorder database.
Security-wise, Interaction Recorder includes built-in administrative security controls to ensure that recordings aren’t tampered with, while Interaction Tracker tracks customer interactions on an event-by-event basis to compile the complete interaction history of any customer. Combine this functionality with Interaction Recorder’s Interaction Screen Recorder option, and CIC offers the most comprehensive compliance-tracking processes of any business communications system now on the market. In fact, many contact centers and businesses using CIC have realized concrete ROI statements due to their ability to respond quickly and accurately to regulators when a customer’s interaction activity is questioned.

Globalization

In the global deployment of nearly any communications system, encryption methods can be affected by technology or, more often, a country’s political issues. CIC is deployed in nearly 60 countries, and the encryption standards Interactive Intelligence uses for CIC can be disabled in countries where these standards are not accepted. Also to help offset encryption concerns, Interactive Intelligence offers the CIC product in 12 languages.

Based on our global experience, the Interactive Intelligence Global Services Organization, and a technology Partner network that spans the Americas, Asia-Pacific, Europe, the Middle East and Africa, CIC is backed worldwide by years of experience to ensure that regulatory and security issues are adequately handled for a particular global region.

Conclusion

With version 2.4 of the Customer Interaction Center (CIC) software, Interactive Intelligence provides a standards-based IP communications system for contact centers and enterprises that offers security at every level. As security standards evolve for network-based voice over IP and other communications technologies, Interactive Intelligence and CIC supply an open standards architecture that fits securely into an organization’s network and behaves just as any other mission-critical business application server on the network. Also while the CIC system connects to many other systems on a communications network, such as e-mail servers, databases, etc., each connection is secured individually to enhance CIC system security overall. The fact that CIC offers a single point of administration further eases the ability of IT staff to manage security issues, and reduces the number of vendors and complexities that can arise with a “multi-box,” multi-vendor hardware solution.