ISI Empowering Communication

Infortel Select Cloud and Cloud Pro Data Security

August 14, 2019

When considering cloud-hosted vendor solutions such as ISI's Infortel Select Cloud and Cloud Pro, the integrity, security, and availability of the application, the adherence to appropriate security standards and the commitment of the hosting organization to periodic audit and certification are all paramount to choosing a vendor. ISI recognizes that call detail records, subscriber database and account profile information used to process call records is sensitive and must be treated as confidential.

Similarly, data collection, storage and transport must be conducted in a way that does not jeopardize data integrity, allow unauthorized access to call records or breach customer voice and data network security. Confidentiality and data integrity are the foundation of ISI's standards of doing business. Our applications and infrastructure are designed and managed to minimize risk while and maximizing data usability. This document addresses each of the various areas of concern and how ISI ensures integrity, security and availability.

COLLECTION OF DATA FROM CUSTOMER PREMISE EQUIPMENT

ISI employs several different methods of collecting call detail records (CDR), Quality of Service records (QoS) and contact center statistics from customer premise telephone equipment, VoIP appliance or UC application – simply referred to as "telephone system" throughout the balance of this document. The method used in any given customer instance is determined by the make and model of the telephone system as each manufacturer employs one of several methodologies to publish raw data for use in reporting and analysis, with some variations imposed due the customer's deployment method, network environment and network security guidelines.

Some of these methods only support delivery of data to a local destination. Examples of this include; ASCII data transmitted via a serial data port connection (legacy Nortel, legacy Avaya and others), ASCII text file written to a shared network drive (NEC and others), population of an ODBC database (Skype for Business) or transmission to a designated local

IP destination using a proprietary IP transmission protocol (Avaya RSP). In such circumstances ISI provides either a hardware device (buffer box) or a software device (ISI Remote Data Collect) for local deployment to collect and temporarily store raw CDR on site prior to scheduled transport to the ISI data center as described in the section below.

Other methods support direct IP delivery to the ISI data center without the need for a local hardware or software device (Cisco). Typically, this employs a regularly scheduled direct SFTP push initiated by the telephone system as described in the section below.

In the case of the Cisco Unified Contact Center Express, data is obtained in two ways; via CTI link and via queries of the UCCX Informix Database. This data is typically transferred over a VPN link between the premise telephone equipment and the ISI data center.

Various additional secure collection methods such as RADIUS over VPN or API calls over HTTPS may be used, depending on the phone system.

When there are multiple CDR delivery methods or protocols supported by a telephone system, customer preference and best security practice will be used to determine the methodology for data collection. ISI maintains separate documentation to address the specifics of many popular telephone system interfaces in greater detail. Please consult with your ISI sales representative or an ISI solution consultant to determine the collection methodology(s) appropriate for your telecom environment and available ISI documentation.

ENCRYPTED TRANSPORT OF CDR TO ISI'S DATA CENTER

The preferred method of transporting CDR from the customer premise to the ISI data center is via public Internet connectivity using Secure FTP (SFTP) protocol. This ensures that call detail information is encrypted while passing through the public IP network. Some telephone systems (such as Cisco Unified Communications Manager) can natively push data via SFTP to ISI. In other cases, ISI provides software or hardware that can push data to ISI using SFTP.

This SFTP Push approach is typically the most desirable data transfer method because the session is initiated by a de-vice behind the customer's firewall. This "inside" initiated session is preferred over the alternative "outside" initiated session since ISI does not require access to any customer equipment or network.

During service implementation, ISI will provide information on utilized port numbers to facilitate opening of appropriate pinhole(s) through the customer's firewall to accommodate these transport sessions to occur.

If desired, a customer-provided and maintained proxy server may be employed to consolidate and redirect one or more SFTP sessions to the ISI SFTP server, thereby providing additional security.

Within the ISI data center, each customer account is assigned a unique FTP server login and password to establish se-cured access and ensure that the transported CDR is deposited in the appropriate location. Once received in the data center, collected data is processed and reviewed to flag potential problems such as incorrect date, data corruption, interruption of call record flow from the telephone system and failed transmission attempts. Daily review and corrective response to any resulting alarms or error logs ensure that data collection problems are diagnosed and escalated for timely resolution.

ENCRYPTION OF DATA IN MOTION AND AT REST IN THE DATA CENTER

All data traversing the ISI network remains encrypted at all times and data at rest is also encrypted using an AES 256-bit methodology.

DATA CENTER SECURITY

ISI has chosen Microsoft Azure to house its data center. Azure is a state of the art, SSAE16 SOC 2 audited, highly redundant service which provides ISI with a highly available and secure environment for compute, storage, and net-work infrastructure. Microsoft's facilities

feature the highest levels of physical and network security, 24x7 professional monitoring, redundant power, telephone and Internet connectivity situated in a facility built to withstand most natural disasters.

The following is a partial list of security credentials which Microsoft Azure maintains through periodic audit and certification of compliance:

- ISO 27001 (general data security standard)
- Cloud Security Alliance STAR certification (data security standard for cloud providers)
- ISO/IEC 27018 (Standard for processing personal information for cloud providers)
- SOC 1, SOC 2, and SOC 3 (controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.)
- NIST CSF Framework (standards for US federal computing)
- SSAE (Corporate auditing standards)
- PCI (credit card processing)
- HIPAA (healthcare privacy)
- HITRUST (combined security certification)
- FERPA (education privacy standard)

For additional information on the security of the Azure environment please consult the Microsoft Trust Center at https://www.microsoft.com/en-us/trust-center.

DATA CENTER NETWORK INFRASTRUCTURE

In addition to the core network infrastructure provided in Microsoft Azure, ISI employs a FortiGate Virtual Appliance to deliver complete, end-to-end security for the software defined data center. The FortiGate appliance provides:

- Firewall Protection
- Intrusion Prevention
- Intrusion Detection
- VPN connectivity to customer infrastructure

ISI has also deployed the FortiAnalyzer Security-Driven Analytics and Log Management solution. FortiAnalyzer provides deep insights into advanced threats through Single-Pane Orchestration and Automation & Response for our entire attack surface to reduce risks and improve our overall security. Integrated with Fortinet's Security Fabric, FortiAnalyzer simplifies the complexity of analyzing and monitoring new and emerging technologies that have expanded the attack surface, and delivers end-to-end visibility, helping ISI identify and eliminate threats.

BACK-UPS, GEO-REDUNDANCY AND DISASTER RECOVERY PROVISIONS

Backups are performed daily and sent to a regionally disparate data center. Backups are retained for sixty days and can be used to recover information when needed. Additionally, ISI uses Azure Site Recovery to provide continual replication of data to a data center hundreds of miles away. With Azure Site Recovery, we can quickly switch the entire application so that it runs in a different region. Once the disaster ends, we can quickly switch back to the primary data center.

SYSTEM MONITORING

An enterprise-wide management system monitors all servers and network components, for availability and failures. Additionally, our monitoring solution provides alerts for several other functions such as CPU utilization, disk utilization and critical services. Alerts are monitored 24x7 by ISI's highly trained personnel.

APPLICATION ACCESS SECURITY

Access to the Infortel Select application in a cloud deployment is limited to authorized web user sessions through a supported web browser. User authorization is controlled using SQL database and its inherent security capabilities. Identification of users is accomplished

through a User ID and password pair. A user entering a valid User ID and Password is considered authenticated and granted access to the application subject to what they are authorized to do and see.

If desired, single sign-on provisions may be implemented to synchronize with and leverage the customer's network security authentication. ISI supports use of either SAML or OAUTH standards to achieve single sign-on.

When Infortel Select user access accounts are created, the system administrator assigns access rights specific to each user based upon up to 5 dimensions of security attributes. What the user can see and do within the application is dependent upon a combination of the following attributes:

- Data Source access rights
- Organizational access rights
- Module access rights
- Report Menu access rights
- Queue access rights

Data Source access rights determine which telephone system(s) or other sources of call detail records a user is authorized to see in any reports the user runs or summary gates they add to their dashboard views. If a customer has a unique data source dedicated to each location, Data Source access rights may be useful in effecting data security by location. Otherwise location-based security may be defined through Organizational access rights.

Organizational access rights determine which organizational entities' call detail records a user is authorized to see in any reports the user runs or summary gates they add to their dashboard views. Access may be granted to one or more specific organizational unit(s) with implied access to any and all child entities. For example; a VP may be given organizational access rights to his/her division and will be allowed to view call activity from that division, all

child departments within that division and all employees assigned to those departments. Activity from employees and departments within other divisions will not be visible to this VP.

Module access rights determine which of the thirty plus application modules a user is authorized to utilize and were applicable, their level of rights within that application as a User or an Administrator. A list of the available modules follows:

- Account Codes
- Alarms (Admin or User)
- Call Editing
- Call Exploration (Admin or User)
- Contact Center (Manager, Reports or User)
- Dashboard (Admin or User)
- Directory (Admin or User)
- DNIS Codes
- Export Processed Data
- Export Summarized Data
- Extension Locations
- Facilities (Admin or User)
- Hunt Group Database
- Import Directory
- Manage Auto-Reports
- Manage Pricing
- Phone Number IDs
- Phone Number Search
- Phone Number Translation
- Price-a-Call (Admin or User)
- PSP Admin
- Reports (Admin or User)
- Statistics

- System Config
- Traffic Analysis

Report Menu access rights allow custom report menus to be created and users selectively allowed or denied access to those report menus so that list of available reports an individual has ability to see and run may be restricted to selected reports.

Queue access rights determine which Contact Center Queues a user may view metrics from. This is helpful when an organization has multiple Contact Center Queues and different supervisors responsible for each Queue – ensuring that Contact Center Supervisors may only view Dashboard metrics and run reports on Queue activity and the Agents working the Queue(s) that they are responsible for. This feature is only active when the UCCX Reporting option has been purchased to provide visibility into Cisco UCCX Contact Center metrics.

When these attributes are combined, they provide a virtually unlimited flexibility in creation of user profiles with ac-cess authorization matched to their area of responsibility, technical capability and job function. SQL security prohibits users from being able to access data they are not specifically authorized to see through a combination of the above security attributes.

WEB SESSION SECURITY

When an authorized end-user initiates a web browser session to Infortel Select, all access is performed via HTTPS. This is the same level of web session protection typically imposed when you do on-line banking or conduct a financial transaction on the web. Requests for HTTP are automatically re-directed to HTTPS to ensure that all data remains encrypted. It should be noted that Infortel Select also allows reports to be distributed as PDF, ASCII, Excel or HTML files attached to an email message. Although this is a handy method to automatically distribute reports to recipients, this report distribution methodology does not utilize encryption and should therefore not be used to transmit sensitive information. Alternatively, report availability may be communicated to report recipients through Infortel

Select's Reports Portal utility. Reports Portal sends notification of report readiness via an email to each report recipient and provides a secure token through which the recipient may click to log onto the Infortel Select system securely where they can view their reports. Authorization and authentication is enforced to ensure that only the proper user can retrieve information.

PERSONAL DATA TRACKED

In determining the level of security that applies to a particular application, it is helpful to understand the nature of the data being transmitted and stored. The following is a list of potential data fields used and maintained within the Infortel Select application. Typically, the Call Detail Records will be automatically transmitted from the customer's telephony platform(s) to the Infortel Select application, while other fields may, if desired and as required, be supplied by the customer through various methods and ultimately associated with the Call Detail Records to enhance the usability of reportable data:

- Call Detail Records include; call date, call time call duration, internal party name and telephone number, extension or SIP URI, telephone number dialed, calling party number, city state and country of call destination or origin
- IM/chat records include date, time and internal party names or SIP URI (platform specific)
- Company Name
- Organizational Hierarchy
- Department Name
- Employee Name
- Employee Title, location, badge number etc.
- Employee Telephone Number, Extension Number, or SIP URI
- Other fields of information which the customer has specifically authorized ISI to collect, process, store and report upon in connection with provisioned services.

DATA SOVEREIGNTY

All data is retained in the United States of America. No data leaves the country at any time. In the future, ISI may offer alternative geographies. In this case, ISI will provide contractual commitments as to the location of data.

EMPLOYEE SCREENING & SECURITY POLICIES

All customer data is treated as confidential and safeguarded to meet demanding HIPAA standards established to protect patient health information in the Healthcare environment. ISI maintains certification of HIPAA compliance through annual 3rd party audits, is Privacy Shield and GDPR compliant for the benefit of EU organizations. These credentials, combined with the previously mentioned Azure data center provisions, allow all customers to operate with the assurance that their ISI-processed data is safe and secure, regardless of the nature of their business.

Employee Hiring

- All ISI employees go through a stringent interview process prior to hiring.
- All ISI employees go through a criminal background check prior to hiring.
- Many ISI employees have received government security clearance as part of their duties.

Employee Training

- All ISI employees undergo a fully documented and carefully defined training program. As part of this program, employees are instructed on issues of security and data confidentiality – including HIPAA and GDPR awareness. Training takes place at initial hiring and refresher training is performed annually

Client Data Network Segregation

• Systems hosting client accounts all client data storage are physically and logically segregated from the ISI corporate environment on a separate firewalled network segment. This separation provides an added level of security and protection of customer information.

RELEVANT ISI CERTIFICATIONS

HIPAA Certified

ISI Telemanagement Solutions offers the only HIPAA certified call accounting application avail-able on the market. We fully understand the needs of Healthcare Covered Entities and have created a product that meets all HIPAA requirements for protection of Electronic Health Information. Additionally, our entire business runs under a set of HIPAA compliant security policies.

Privacy Shield Certified

The United States Department of Commerce and the European Commission have agreed on a set of data protection principles (Privacy Shield Principles) to enable US companies to satisfy the requirement under European Union law that adequate protection be given to Personal information transferred from the EU to the United States. ISI is a certified and active Privacy Shield participant.

Additional Information

If any security questions remain unanswered or require additional clarification, please contact ISI for additional details.