ISI ANALYTICS

Infortel Select
Cloud Data Security

When considering cloud-hosted vendor solutions such as ISI's Infortel Select Cloud and Cloud Pro, the integrity, privacy, 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. All customer data is classified as confidential.

Data collection, storage and transport must be conducted in a way that does not jeopardize data integrity, allows 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 maximizing data usability. This document addresses each of the various areas of concern and how ISI ensures integrity, security, and availability.

PURPOSE OF DATA PROCESSING

ISI processes data submitted by customers for the purpose of providing ISI's online services to our customers. To fulfil these purposes, ISI may access the data to provide the services, to correct and address technical or service problems, or to follow instructions of the ISI customer who submitted the data, or in response to contractual requirements.

DATA PROCESSED

ISI collects, processes, stores, and provides reporting on communications events occurring on corporate telecommunications platforms and/or corporate owned mobile devices. Event records typically represent one or more types of communication events based upon the platforms involved and the service configuration including voice calls, video calls, or meetings. Communications events may include internal (peer to peer) conversations, outbound or inbound calls with external parties and conference calls involving multiple parties. Event records only contain metadata and do not include the content of the conversation. The following types of Personal information may be collected, stored, and reported upon:

- Company Name
- Organizational Hierarchy
- Department Name
- Employee Name
- Employee Title
- Employee email address
- Employee UPN
- Employee Telephone Number, Extension Number, or SIP URI

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.

Processed call information is made available to customers via a secured web interface or delivered directly to authorized customer recipients based upon customer instruction. ISI does not own or control any of the information it processes on behalf of ISI's customers. All information is owned and controlled by ISI's customer. In this capacity ISI receives information transferred and acts as a processor on behalf of its customer. ISI's customer retains ownership and remains the data controller.[1]

COLLECTION OF CUSTOMER DATA

ISI employs several different methods of collecting call detail records (CDR), Quality of Service records (QoS), contact center statistics, and directory information from customer premise telephone equipment, VoIP appliance, Cloud UC system, or directory source – simply referred to as "customer systems" throughout the balance of this document. The method used in any given customer instance is determined by the make and model of the customer system as well as the deployment environment. The hallmark of ISI's

[1] For more information, see ISI's Privacy Policy at https://isianalytics.com/privacy-policy/

data acquisition strategy is to ensure that all customer data remains encrypted.

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) or ASCII text files written to a shared network drive (NEC and others), or sending via a local connection to a directory source such as Active Directory, or a proprietary IP transmission protocol (Avaya Reliable Session Protocol.). In such circumstances ISI provides either a hardware appliance (buffer box) or a software device (ISI Remote Collectionor) for local deployment to collect and temporarily store raw CDR and directory data 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 Unified Communications Manager). Typically, this employs a regularly scheduled direct SFTP push initiated by the customer 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. The data is collected locally and stored on the Remote Collection server and transferred to ISI via SFTP.

Cloud based systems (Cisco Webex and Microsoft Teams, Azure Active Directory) use an API to securely deliver data.

Finally, some systems such as Session Border Controllers deliver CDR via RADIUS. The ISI Remote Collection software has a built-in RADIUS server. Records are received and then securely sent to ISI via SFTP.

When there are multiple CDR delivery methods or protocols supported by a customer 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 supported customer 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 most common method of transporting CDR and directory information 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 customer 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 device behind the customer's firewall. ISI does not require direct access to the customer network.

During service implementation, ISI will provide information on hardware requirements and utilized port numbers to facilitate opening of appropriate ports in 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.

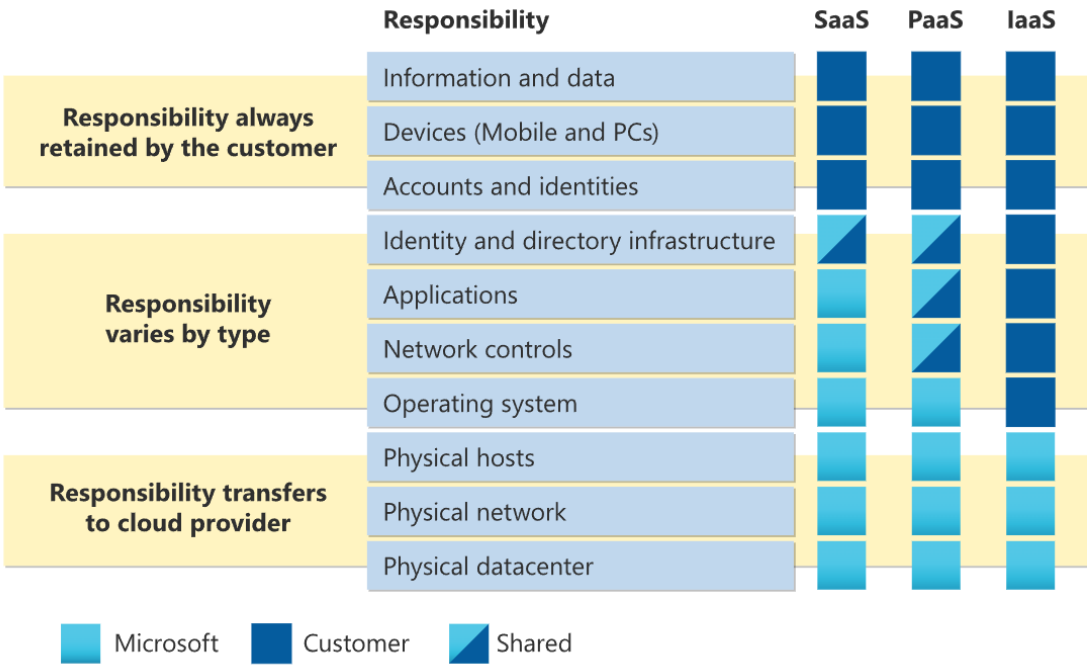
Within the ISI data center, each customer account is assigned a unique FTP server login and password to establish secured access and ensure that the transported data is deposited in the appropriate location. Once received in the data center, collected data is processed and reviewed to flag potential problems such as incorrect date, data corruption, interruption of call record flow from the customer 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.

DATA RESIDENCY

ISI securely hosts all systems in USA-based Microsoft Azure regions. ISI will not host data outside the USA without prior approval. Our primary infrastructure is in the North Central Azure Region (Illinois) while our recovery region is the South-Central Azure Region (Texas). Some services are cross-region; however, all data will reside within the USA. We use Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) technologies to provide services to our customers.

CLOUD SECURITY

Microsoft Azure operates on a shared security model:



In this model Microsoft takes responsibility for the physical environment. ISI remains responsible for our applications. We have a combined responsibility for many functions such as the network. Together, we offer a multi-layered comprehensive approach to security and privacy.

DATA STORAGE

Received and processed data is stored locally within the ISI data center. All data is encrypted. ISI uses an Azure Platform Key to encrypt data. The keys are rotated annually or on-demand in case of a suspected breach. All data is replicated three times within the data center. This method provides 99.999999999% (11 nines) durability of objects over a given year. A write request to a storage account happens synchronously. The write operation returns successfully only after the data is written to all three replicas.

DATA RETENTION

All data retention periods are defined by the statement of work signed between ISI and the customer. Our standard retention policy includes thirteen months of storage. Additional storage may be purchased at an additional cost. Each night, older data is deleted.

The ISI customer owns all data provided. At the end of any contract or agreement, the customer is given the choice of having ISI return the data in

machine readable format prior to destruction. All data will be deleted using NIST 800-88 standards.

DATA SEGMENTATION

Systems hosting client accounts 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.

ISI provides each customer with their own unique database to store information. ISI provides physical and logical controls to ensure cross-customer access is not possible.

NETWORK SECURITY

Microsoft is responsible for providing secure, highly redundant network connectivity. ISI maintains responsibility for network security within our infrastructure. ISI deploys firewalls, intrusion detection, intrusion prevention, web application gateways, and web application firewalls to ensure the security and integrity of data. All data within the ISI network is encrypted using TLS 1.2. All ISI administrative access to our systems takes place over a VPN. We conduct internal monthly vulnerability assessments and annual third-party penetration tests to validate security. All findings are remediated based on published remediation commitments.

BACK-UPS, GEO-REDUNDANCY AND DISASTER RECOVERY PROVISIONS

All data is backed up daily to a geographically distinct data center. In addition to regular backups, ISI uses Azure Site Recovery to replicate all data continuously to the backup region. All backups remain encrypted in transit and at rest. ISI tests restoration of backups quarterly. ISI offers a stated twenty-four-hour Recovery Time Objective (RTO) and a twenty-four-hour Recovery Point Objective (RTO).

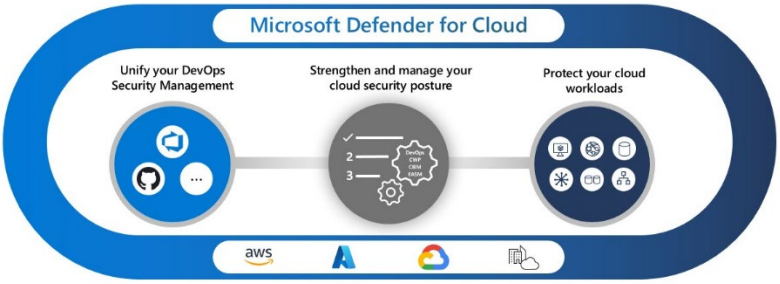
SYSTEM MONITORING

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.

LOGGING

ISI logs all network activity, diagnostic and performance information, and application logs using Azure Monitor. We have deployed an extensive system of alert rules to inform us of any security or operational issues. We capture traffic for forensic evaluation in case of breach. All logs are stored in read-only storage and cannot be modified.

VULNERABILITY AND SECURITY MANAGEMENT

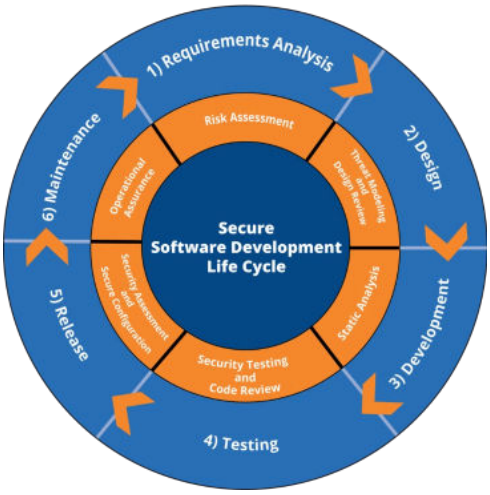


ISI uses Microsoft Defender for Cloud to manage security in our infrastructure. Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities. Defender for Cloud combines the capabilities of:

- A development security operations (DevSecOps) solution that unifies security management at the code level across cloud and pipeline environments.
- A cloud security posture management (CSPM) solution that surfaces actions that you can take to prevent breaches.
- A cloud workload protection platform (CWPP) with specific protections for servers, containers, storage, databases, and other workloads

ISI is automatically alerted to any issues so that we can quickly address vulnerabilities.

DEVELOPMENT SECURITY



ISI has developed a Secure Development Lifecycle (SDLC) process to ensure the security of all software developed. The SDLC document establishes guidelines for the development of software and systems that must be applied to all developments to ensure their maintainability, security and protection against cyber-attacks and accessibility. Key elements are:

1. Design Process – The ISI DevOps team will consider the security implications of any software development to ensure the security and stability of our application.
2. Development Process – All new software requires a detailed Product Requirements Document (PRD) provided by ISI Telemanagement Solutions product staff. In most cases, a technical specification will be created by the development staff. This technical specification should provide the implementation details and assumptions, data flows,

database schema changes, endpoints, and scope definition. The specification includes enough detail to understand what categories of personal information will be impacted by the feature, its purpose and how it will use, store, process, and transmit the personal information.

3. Secure Code Review – All software undergoes a secure code review to find any vulnerabilities.
4. Service Vulnerability Reviews – Products and services released by ISI require regular reviews for vulnerabilities and attacks.
5. Testing – All software undergoes functional and security testing. Functional testing consists of unit tests, systems tests, and integration tests. Security testing consists of Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST).

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 authentication is controlled using a either an ISI provided identity provider or via SAML 2.0 Single Sign on to a customer's identity provider. When the ISI Identity Provider is used, we provide the option for multi-factor authentication via email, SMS, or an authenticator app.

ISI provides a web-based administration portal that lets customer administrators manage users and user authorizations. The system

administrator assigns access rights specific to each user based upon up to five 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 customer 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 can 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 can be granted to one or more specific organizational unit(s) with implied access to 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 allows administrators to create custom report menus and provide user access to the menus. This lets administrators determine which reports may be run by which users.

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 unlimited flexibility in the creation of user profiles with access authorization matched to their area of responsibility, technical capability, and job function.

WEB SESSION SECURITY

When an authorized end-user initiates a web browser session to Infortel Select, all access is performed over HTTPS. Requests for HTTP are 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 may not utilize encryption and should not be used to transmit sensitive information. Instead, users can be notified of new reports via email. They would then click on a link, sign into to the Infortel reports portal and securely view or download the report.

ISI'S SECURITY MANAGEMENT PROGRAM

ISI's security policies and procedures are aligned with SOC 2, HIPAA, and GDPR. ISI has created a comprehensive security program that addresses:

Infrastructure: The physical and hardware components (networks, facilities, and equipment) that support our IT environment and help us deliver services.

Software: The operating software and programs (utilities, applications, and systems) we use to facilitate data and system processing.

People: The personnel (managers, developers, users, and operators) involved in the management, security, governance, and operations to deliver services to customers.

Data: The information (files, databases, transaction stream, and tables) we use or process within the service organization.

Procedures: The manual or automated procedures that bind processes and keep service delivery operating.

HIPAA Compliance

All ISI security polices, and procedures conform to the HIPAA standards. On an annual basis, we undergo a third-party risk assessment to ensure compliance.

Privacy Shield

ISI Telemanagement Solutions complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, Switzerland, and the United Kingdom to the United States. ISI has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/[2]

[2] On July 16, 2020, the Court of Justice of the European Union issued a judgment declaring as "invalid" the European Commission's Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield. As a result of that decision, the EU-U.S. Privacy Shield Framework is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States. That decision does not relieve participants in the EU-U.S. Privacy Shield of their obligations under the EU-U.S. Privacy Shield Framework.