



Security, Reliability & Privacy

i-Sight Blog: <http://i-sight.com>
Corporate Web Site: www.customerexpressions.com
i-Sight for Complaints: www.complaintsoftware.com
i-Sight for Investigations: www.investigationsystem.com

Table of Contents

What are the Advantages of Web-Based Software?....	3
The SaaS advantage	3
On-Premise Disadvantages.....	3
SaaS Advantage	3
Web-based software is safer	3
Everything is together in one place	4
Your data is automatically backed up daily.....	4
Your data is safe and secure	4
There’s nothing to install – ever	4
Everything is “compatible”	4
Work from home, or work on the road	4
What Makes i-Sight Secure & Reliable?	5
Standard Operating Procedures.....	5
Secure Data Centers.....	5
Access control and physical security	5
Environmental Controls.....	5
Power	6
Network	6
Fire detection and suppressions	6
Secure Transmission.....	6
Network Protections.....	6
Disaster Recovery.....	7
Backups.....	7
Does i-Sight Comply with Global Privacy Laws?	7
United States.....	7
Canada	7
European Union.....	7
Accountability for Personal Information.....	8
Identifying Purposes for the Collection of Personal Information.....	8
Consent for the Collection, Use, and Disclosure of Personal Information.....	8
Limiting Collection of Personal Information	8
Limiting Use, Disclosure and Retention of Personal Information	8
Ensuring Accuracy of Personal Information.....	8
Ensuring Safeguards for Personal Information.....	8
Openness about Personal Information Policies and Practices	9
Individual Access to their own Personal Information.....	9
Challenging Compliance with the Privacy Policies and Practices.....	9
Mitigation	9

What are the Advantages of Web-Based Software?

The SaaS advantage

On premise software is more expensive to deploy and maintain than SaaS solutions. SaaS solutions like i-Sight eliminate capital expenditures; reduce IT personnel costs associated with implementation and ongoing support and enable businesses to pay-as-you-go. Most traditional software involves a very large upfront license fee and annual maintenance costs that generally exceed 20 percent of the original license fee. i-Sight eliminates this upfront cost, enabling business to quickly realize a return on investment.

<u>On-Premise Disadvantages</u>	<u>SaaS Advantage</u>
<ul style="list-style-type: none">- Long & complex implementation cycle (typically 12-18 months)- Hardware & infrastructure costs + replacement costs- Scarce availability of technical resources- Ongoing cost of technical personnel- Large upfront license fees- High recurring costs of annual maintenance fees- Long testing cycles- Re-implementation cost in 3-5 years	<ul style="list-style-type: none">- Rapid Deployment (typically under 2 months)- Low upfront investment- No 3rd party tools, modules to purchase- Faster Time-to-Value

Web-based software is safer

With i-Sight your data is backed-up daily and stored on secure, always updated, enterprise level servers in a state-of-the-art, highly secure data centers.

With traditional software employees save data on their desktop, laptop or USB drives. Laptops are stolen, desktops aren't backed up properly and it's difficult to keep up with security patches and updates.

Everything is together in one place

You can't leave information in the wrong place or on the wrong machine. All of your data is stored in one place and accessible from any computer, any time. Safe, secure, password protected, and encrypted.

Your data is automatically backed up daily

All your data is backed up every day. Backups are stored in multiple locations to ensure data is never lost. We run regular restoration tests to ensure that in the event backups are needed we can quickly get you back up and running. Since our first day in business, over ten years ago, we have never lost any data.

Your data is safe and secure

Our world-class data centre has guards on duty 24 X 7, bio-metric locks, chaperon only access to servers and 24-hour video surveillance. Our software and hardware are regularly updated to ensure we are using the latest security patches. All network traffic is routed through enterprise-class firewalls to keep your information safe.

There's nothing to install – ever

You already have everything you need to start using i-Sight today! There is nothing you need to download or install on your computer or network. Just like your banking site, you simply log in to i-Sight using your web-browser.

Everything is “compatible”

Traditional software requires that you have the matching operating system or that your IT group support the software “platform” it's built upon. Because i-Sight is hosted, web based software it works on any platform with a web browser and an Internet connection.

Work from home, or work on the road

With i-Sight, your office is everywhere. You can access all you case information from work, home, the road or a hotel room.

What Makes i-Sight Secure & Reliable?

Standard Operating Procedures

CEC follows a very detailed set of operating procedures. The procedures govern every aspect of our business to ensure that everything from our hiring practices to our change control processes are executed to ensure security of customer information.

Secure Data Centers

Our world class data centers are located in secure, unmarked “class A” facilities with multiple connections to Telco fibre rings, advanced security systems, 24 hour Network Operation Centers, fire suppression systems, uninterrupted power supply and high capacity generators.

Access control and physical security

- Biometric security enforced through an iris scanner
- Guarded entrances have security cameras to scan and digitally record the interior and exterior of the facility 24 hours a day
- Video surveillance incorporates low-light technology to allow clear visibility at night
- Unified security breach alarm with access monitoring
- Client security escort
- Electronic motion detectors
- Reinforced exterior and interior walls
- Raised floors for secure routing of cables
- Secure staging rooms for setup and maintenance of equipment

In order to access hardware within the datacenter CEC personnel must provide suitable ID or must pass (retina scan) biometric authentication. Information on any software or hardware to be added or removed from the CEC equipment must also be listed prior to the visit. The datacenter itself is protected with a live security guard 24/7. Surveillance cameras are operated both externally and internally and all authorized visitors are accompanied by a data center escort at all times of their visit. Within the datacenter access is also controlled using electronic locks.

Only CEC network and application server personnel have access to the hosting environment. Logs are maintained of all visits and the purpose of those visits.

Environmental Controls

- Redundant Liebert air conditioners and compressors

- Humidity controlled
- Raised floor designed for efficient cooling

Power

- Fully redundant UPS
- Static transfer switches
- Redundant 650 Kilowatt generators
- Generators housed in underground bunker
- All power from redundant NuWave modular UPS

Network

- High bandwidth capacity
- Network neutral, multi-homed network

i-Sight runs on a "multi-homed" network, consisting of redundant backbone connections to four major backbone providers. With high-speed DS3 and OC3 connectivity to four major networks, traffic bypasses busy Network Access Points (NAPs) and is sent quickly to end-users.

In addition to the multi-homed backbone connections, powerful Cisco routers and switches are at the core of the network to provide redundant internal connectivity. This network infrastructure provides an additional level of protection against hardware failures.

Network connections into the Data Center are provisioned over diverse fiber and multiple Telco providers, eliminating the risk of a single fiber cut anywhere in the public network taking down our high-speed links to the Internet. The combination of these four backbone connections provides an aggregate bandwidth of over 100 MBPS.

Fire detection and suppressions

- Early smoke detection system
- FM-200 gas fire suppressions
- Back-up sprinkler system – pre-action dry pipe water-based

Secure Transmission

- All connections via 128-bit SSL ensuring secure connection from browser

Network Protections

- Firewalls in place
- Network based intrusion detection systems report events for logging and reporting

- Third-party service provider scans network externally

Disaster Recovery

- CEC maintains a secondary data center infrastructure for disaster recovery
- DR site data is updated daily via encrypted links
- DR tests conducted to ensure rapid recovery time

Backups

- All data is backed up to tape each day
- Tapes are maintained on a rotating schedule of incremental and full backups

Does i-Sight Comply with Global Privacy Laws?

Most jurisdictions around the world have implemented legislation to govern the handling and use of personal information. We understand that many organizations operate across multiple jurisdictions and we follow a set of procedures to ensure compliance with all of the legislation listed below.

United States

- (HIPPA) Healthcare Insurance Portability and Accountability Act
- (GLB) Financial Modernization Act of 1999 or Gramm-Leach-Bliley

Canada

- (PIPEDA) Personal Information Protection and Electronic Documents Act of 2000

European Union

- EU Data Protection Directive
- EU E-Privacy Directive

The following is a list of principles that are built into CEC operations and the i-Sight software to ensure compliance with privacy laws.

Accountability for Personal Information

CEC is responsible for protecting all personal information under its custody or control and has designated a Privacy Officer who is responsible for CEC compliance to Privacy Principles.

Identifying Purposes for the Collection of Personal Information

At or before the time personal information is collected by CEC personnel, CEC will identify the purposes for which personal information is collected.

Consent for the Collection, Use, and Disclosure of Personal Information

The knowledge and consent of the individuals are required for the collection, use or disclosure of personal information, except where inappropriate.

Limiting Collection of Personal Information

The collection of personal information will be limited to that which is necessary for the purposes identified by CEC. Information will be collected by fair and lawful means.

Limiting Use, Disclosure and Retention of Personal Information

Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by contract or law. Personal information will be retained only as long as necessary for the fulfillment of those purposes.

Ensuring Accuracy of Personal Information

Personal information will be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

Ensuring Safeguards for Personal Information

Security safeguards appropriate to the sensitivity of the information will protect personal information.

Administrative, physical, and technical safeguards are provided to ensure that all personal information is readily available at all times to those that have access rights to the information. CEC Information Technology Policy (ITP) Manual outlines those safeguards.

Openness about Personal Information Policies and Practices

CEC will make readily available to individuals upon request specific information about its policies and practices relating to the management of personal information as outlined in this manual.

Individual Access to their own Personal Information

Upon request, an individual will be informed of the existence, use and disclosure of his or her personal information and will be given access to that information. An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Challenging Compliance with the Privacy Policies and Practices

An individual will be able to address a challenge concerning compliance with the above principles to the Privacy Officer, whose contact information is available on the CEC website.

Mitigation

In the event that personal information is incorrectly disclosed (violation) by CEC 'personnel, the Privacy Officer will advise CEC' client of all details of the disclosure for purposes of mitigating any harm to the client's customer. The Privacy Officer will also keep a listing of all such disclosures and subsequent corrective action (if required).