

eCloud Integration

Combine iSign Products for Secure
Data Storage and Communication



iSign International

Providing data security is a primary concern for cloud service providers as data is transmitted to remote servers over the Internet. Read on to learn how iSign's eCloud, coupled with its other platforms, provides a robust cybersecurity infrastructure for individuals.

Cloud computing is the new computing archetype that can provide services on demand at a minimal cost. It is an emerging and promising technology for the next generation of information technology (IT) applications. The hurdles toward the rapid growth of cloud computing are data security and privacy issues.

Wave Browser Featuring eCloud

iSign's proprietary AI Security Protocol has successfully made other companies' attempts at multi-factor authentication obsolete. iSign proactively identifies and blocks rogue hacking activity on the user's network, even on IoT devices, thereby protecting them and their data from all external and internal cyberattacks. iSign believes that its technology, which is covered by several patent-pending claims, constitutes a game-changing approach in data security as it renders hacking impossible.

eCloud provides a secure file storage system and, when coupled to iMail, is the perfect Secure File Sharing Platform. All the data security policies of iSign are inherent in the design of eCloud. It comes with a host of other benefits like data protection, encryption, and access control.



Differences Between Traditional Cloud and eCloud

Data security is a consistent and significant issue in IT. It becomes particularly severe in cloud computing environments because data is stored in different locations around the world. Privacy protection and data security are the two primary user's concerns about cloud technology. Here's a look at how iSign International's eCloud platform addresses these concerns:

- **Security:** Data protection and security are the primary factors for gaining user's trust and allowing for successful adoption of cloud technology. Security is the combination of several aspects:
 - Prevention of unauthorized access
 - Prevention of tampering or deletion
 - Prevention of lockouts

While traditional cloud may be lacking, for eCloud security is a top priority.

- **Privacy:** Privacy is a user's or group's ability to decide whom to share information with, keeping it inaccessible to anyone else. In cloud computing, privacy means that, when users work with sensitive data, the service provider prevents potential hackers from inferring the user's behavior by their visit model (not direct data leakage). In eCloud:
 - Users have control over their data. Thus, they can avoid theft, nefarious use, and unauthorized resale.
 - Users are guaranteed to avoid data loss, leakage, and unauthorized modification or fabrication.
- **Encryption:** While most privacy experts agree encryption is the cornerstone of security, they also stress that implementing it in the cloud can be a daunting task. eCloud allows the customer to encrypt the data before it is sent to the cloud for storage or processing. Users can independently verify the messaging correspondents' identities by utilizing the unique id and GPS tag attached to every document.



Integration for Data Security, Storage, and Scalability

Individual users and organizations are moving away from paperwork and upgrading to electronic document platforms. iSign International's solutions -Wave browser, iMail, and eCloud- provide a secure cloud-based platform where all the essential documents are available anytime, anywhere in an encrypted system. Storage is accessible by the user's biometric signature utilizing our proprietary technology, eliminating alphanumeric passwords that are frequently lost, stolen, or hacked. Users can collaborate within their organizations on encrypted documents using the eCloud platform and utilize iMail for end to end encrypted communication. Thus, they can increase workflow within the organization with unmatched security. iSign International offers solutions for large corporations and individual users with superior scalability.

Elements	Standard and Unsafe	Standard and Unsafe	Unified Front Triple Threat to Hackers
Web Browser	Internet Explorer / Edge	Chrome	Wave Browser
Email Client	Outlook	Gmail	iMail
Cloud Storage	OneDrive	Drive	eCloud
Unified Front Against Hacking	✗	✗	✓

All iSign platforms use end-to-end encryption to secure all communications to other iSign users. They can be used to send and receive encrypted instant messages, group messages, attachments, and digital content. iSign International's proprietary end-to-end encryption is a communication system where only the communicating users can read the messages. It prevents potential eavesdroppers – including Internet providers, telecom providers, and even the provider of the communication service – from accessing the encrypted message. The system can defeat any attempts at tampering or surveillance because no third parties can decipher the data being stored or communicated. For example, enterprises that use our end-to-end encryption cannot hand over the texts of their customers' messages to the authorities.



Conclusion

To ease the migration to a cloud computing platform security concerns of users and organizations must be addressed, creating a trustworthy environment. eCloud addresses data security and privacy concerns while providing a secure file storage system.

To learn more about iSign and its SmartGuard innovative solution, which helps monitor and detect malicious activities in real-time by leveraging hardware-assisted security assurance for home and business environments visit our website at <https://isigninternational.com/>.