Data Sheet

InterWeave Smart Solutions

Integration Solutions made Easy

InterWeave Smart Solutions
SECURITY AND PRIVACY OVERVIEW

At **Inter**Weave, our customers security and privacy is taken very seriously. Our **Smart** Solutions platform manages the integration of your most critical business information and business processes. **Inter**Weave **Smart** Solutions address security at three distinct levels: network and facilities infrastructure, application and platform and the data level. This three-tiered security approach ensures that your data is never exposed to unauthorized parties, remains safe in transit between applications, and that you are able to access your data whenever and wherever you want.

Rackspace Managed Hosting - The **Inter**Weave infrastructure is resident at Rackspace Managed Hosting, the Managed Services Provider (MSP) that is Sarbanes/Oxley, SAS70 (Type II compliant as per the audit requirements of the American Institute of Certified Public Accountants), Salesforce.com and Symantec certified. Rackspace configuration of the data center includes SAS 70 Type II attestation and Level l PCI DSS compliance, best-of-breed security (routers, firewalls, IDS and DDoS protection), redundant IP connections to world class carriers terminated at Rackspace, redundant UPS power, diesel generator backup, and HVAC facilities, and multipoint monitoring of key metrics alerts for both mission critical and ongoing maintenance issues.

Application & Platform Security - The **Inter**Weave platform has been carefully architected with your security in mind. Because **Inter**Weave connects to your network and is hosted at Rackspace, it is important that there are extensive security measures in place in order to prevent any compromise of your data. **Inter**Weave **Smart** Solutions communicate in two modes, user-initiated (manual) or scheduled (automatic). During scheduled communications, **Inter**Weave captures information regarding data and communication status of your solution in real-time, monitors and reacts. If you have a data or communication issue, **Inter**Weave captures the exception in your log files and notifies you via email or IM. If you are using manual mode, the same information is presented to you in your application window if the integration transaction does not complete.

Connector Security - To allow **Inter**Weave to communicate with your application, you open Port 2020 and download the connector behind your firewall. **Inter**Weave typically communicates with your database connector, which communicates with your database. All **Inter**Weave servers have signed digital certificates and use SSL to communicate with the connector.

Data Communication Security Standards - To ensure the security of data in transit, **Inter**Weave **Smart** Solutions makes use of the latest and most stringent data communication security standards. All communication from/to **Inter**Weave uses SSL 128 bit encryption. **Inter**Weave use's a standard SSL Handshake to authenticate communications.

Password Encryption Security - When a user registers and activates an account, **Inter**Weave generates a private/public x509 key (PKI). We store both the public certificate and the private key at Rackspace. When creating a solution, users are prompted to create their user ID and password. The password is encrypted and stored for the account. Only the account owner can decrypt with the password needed to unlock the encrypted private key.

Certificates - Inter Weave **Smart** Solutions use certificates in order to ensure security when transmitting data across a communication protocol. Connectors such as FTPS, SFTP, HTTPS, and many others require the use of certificates in order to encrypt data and channels and to verify the digital signature of the person sending the data. The Certificate Component can use an existing key obtained from a certificate authority such as Verisign/Thawte or a key generated by **Inter**Weave **Smart** Solutions.

Data Security - It is important to note that at no point during the integration process does **Inter**Weave store your data. **Inter**Weave Smart Solutions are engineered to optimize interoperability of applications and facilitate your integration processes. Only your userid and password is stored with **Inter**Weave.

On-Premise Customer Data - Data that processes through an **Inter**Weave **Smart** Solutions is sourced for your data repository (application A) and processed for only a millisecond on our servers invoking the configuration settings you selected and sending this data to your target repository (application B.)

Hosted Customer Data - Data that processes through an **Inter**Weave **Smart** Solutions is sourced for your hosted data repository (application A residing at MSP) and processed for only a millisecond on our servers invoking the configuration settings you selected and sending this data to your target repository (application B residing at MSP).

For more information, email Bruce Magown, CEO, at bmagown@interweave.biz or call 203-274-5226.