

Boomi AtomSphere[®] Security Overview

For any SaaS application or Cloud service, security is a multi-dimensional business concern that must be carefully scrutinized. At Boomi, we are keenly aware that our AtomSphere platform manages the integration of your most critical business information and business processes. We have engineered Boomi AtomSphere to address security at three distinct points: the network and facilities infrastructure, the application and platform layer, and at 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 can access your data whenever and wherever you want.

Network & Facilities Infrastructure Security

The Boomi infrastructure has been deemed SAS 70 Type II compliant as per the audit requirements of the American Institute of Certified Public Accountants. The configuration of the data center includes SAS 70 Type II attestation and Level I PCI DSS compliance, best-of-breed security (routers, firewalls, IDS and DDoS protection), redundant IP connections to world class carriers terminated on our carrier grade network, 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 Boomi Atom has been carefully architected with your security in mind. Because the Atom can reside on your network or be hosted in our data center, it is important that there are extensive security measures in place in order to prevent any compromise in your data or the Atom. During installation, the Atom download and all of its contents are verified and authenticated by the Boomi data center before deployment.

The Atom communicates information to the Boomi AtomSphere in two modes, ongoing/automatic communications and user-initiated communications. During ongoing/automated communications the Atom transmits operational information to the Boomi AtomSphere data center, including online status to monitor uptime, tracking

Security At-a-Glance

- SAS 70 Type II
- Level I PCI DSS
- Dedicated firewall services
- IDS and DDoS safeguards
- Public/Private Key Encryption
- SSL 128 bit encryption
- Verisign/Thwate key support

information to catalog process executions, integration process configuration updates, and periodic checks for updates to the Atom code. User initiated communications occur only upon the request of an authorized Boomi AtomSphere user and include logging information about a specific integration process, capturing error messages and failures for diagnostic purposes, and retrieving connector schema to define mapping and rules for new integration processes.

On-Premise Data Communication Security – After the Atom is deployed behind the firewall, the Atom will be in contact with the data center for ‘tracking’ and ‘status’ information. No inbound firewall ports need to be opened in order for the Atom to communicate with the data center. The Atom always initiates the connection and there is **never** ‘pushing’ of data from the data center to the Atom. When the Atom initiates the connection to the data center, it authenticates the data center before sending data using an SSL handshake and a digital certificate.

Data Communication Security Standards – To ensure the security of data in transit, Boomi AtomSphere makes use of the latest and most stringent data communication security standards. All communication from Atom to data center uses SSL 128 bit encryption. All outbound communication from Atom to data center is HTTPS. Atoms use a standard SSL Handshake to authenticate with platform.boomi.com.

Password Encryption Security – When a user registers and activates an account, Boomi generates a private/public x509 key (PKI). We store both the public certificate and the private key in our secure data center. When creating a Connector, users will be prompted to create their 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. When atoms are deployed, the entire encrypted string is deployed to that Atom and the credentials supplied unlock the password at runtime.

Certificates – Certain AtomSphere Connectors use certificates in order to ensure security when transmitting data across a communication protocol. Connectors such as FTPS, SFTP, HTTPS, AS2, 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 Boomi.

Data Security

It is important to note that at no point during the integration process does Boomi store data. Boomi AtomSphere is engineered to optimize interoperability of applications and facilitate your integration processes without saving your data in our data center, unless specifically configured to do so.

On-Premise Data – Data that processes through an ‘On Premise’ Atom will never actually flow through the Boomi data center. The data is stored behind the firewall on a customer server where the Atom is deployed and is transported directly to either the SaaS or ‘On Premise’ application through a Connector configured to the specific security requirements of the user.

Hosted Data – For Atoms deployed in our data center, you will have all the security that our data center infrastructure provides in order to ensure that your data resides in a system that will keep it secure. These data centers provide the highest level of SaaS security available. This will ensure that all your data for your hosted Atoms is fully secure and only accessible by your account.

Boomi Corporate Headquarters

801 Cassatt Road
Suite 120
Berwyn, PA 19312

Toll-Free 1.800.732.3602
www.boomi.com