Security Standards

1 - General Security

DataZeo's CSST product transmits all data using AES 256 highgrade encryption over SSL (HTTPS) connections. Servers reside behind a network appliance and authorized traffic is limited to specific port assignments.

The in transit IP data travels in a private VLAN. This segregates the IP traffic in the secure VLAN. This is important in preventing other devices such as; iPhones, Android phones or Air cards from being able to breach or attempt to send traffic to secure M2M devices. All traffic is sent to DataZeo CSST over IPSEC using AES 256 encryption. GRE and BGP routing to is used to secure data payload, and the product supports MPLS fiber options for future growth.

All this combined provides security for data in transport, plus allows the devices to have limited preauthorized access to the Internet for necessary business traffic. The DataZeo CSST requires web and device passwords to ensure secure access. In addition, DataZeo partners with MDM device management providers, such as Fiberlink, to allow control of the device itself.

Stored customer usage data in databases is encrypted in part or whole and the databases are password protected.

DataZeo retains the ability to disable individual accounts or users based on any security threats. We also retain the ability, if ne be, to disable entire sections of code, if security threats are detected.

2 - Physical Security

The equipment (servers) used to host the CSST applications are housed at a third party hosting company in San Luis Obispo California called Digital West. Digital West has the following strict requirements for securing the facility:

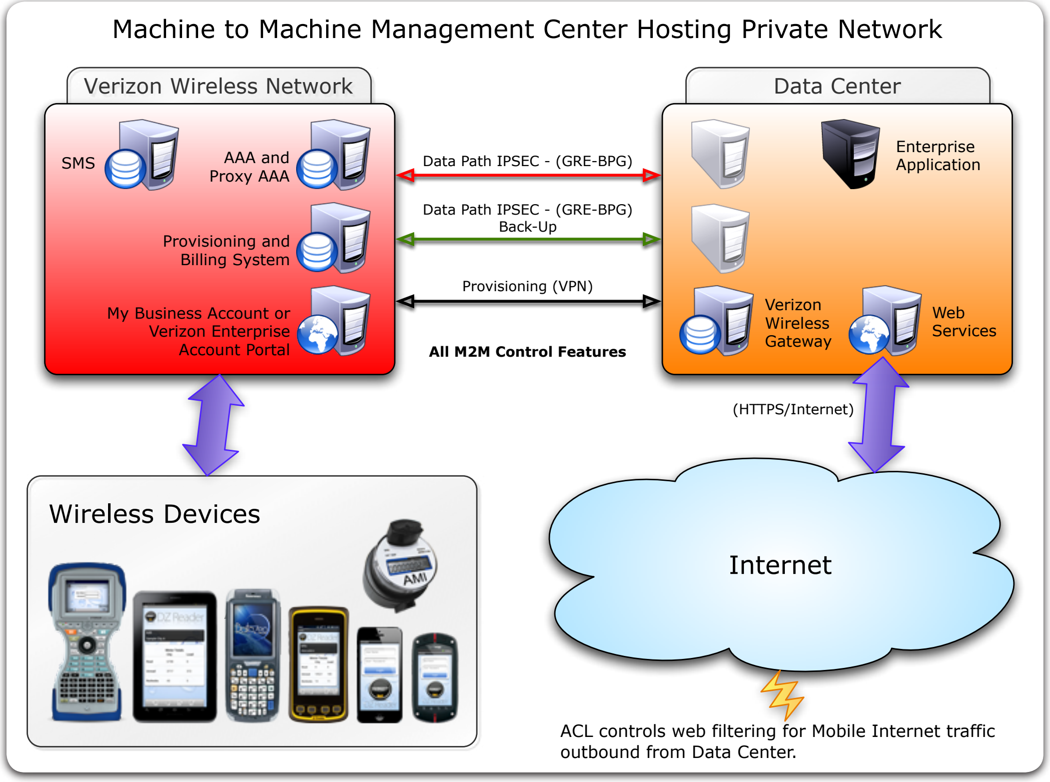
- Video ID and Surveillance Cameras
- Biometric Hand Scanners
- KeyLocked Cabinets
- Onsite personnel 24/7/365

DataZeo corporate policy has strict guidelines that all employees must pass a complete and thorough background check before employment. The background check is processed through a third party called "Talent Wise". Four criteria are completed; (1) SSN Trace, (2) Multi –State Instant Criminal Check, (3) Nationwide Sex Offender Registry Check, (4) Criminal Check by Jurisdiction.

3 - Network Security

The equipment (servers) used to host the CSST applications are housed at a third party hosting company in San Luis Obispo California called Digital West. Digital West has the following strict requirements for securing the facility:

- The DataZeo Smart Server Connection goes over the Internet.
- Data is transferred over HTTPS, providing bidirectional encryption.
- Data is transferred over HTTPS through an IPSEC VPN.


Machine to Machine Management Center Hosting Private Network
Verizon Wireless Network
SMS
AAA and Proxy AAA
Provisioning and Billing System
My Business Account or Verizon Enterprise Account Portal
Data Center
Enterprise Application
Verizon Wireless Gateway
Web Services
Data Path IPSEC - (GRE-BPG)
Data Path IPSEC - (GRE-BPG) Back-Up
Provisioning (VPN)
All M2M Control Features
(HTTPS/Internet)
Wireless Devices
DZ Reader
AMI
Internet
ACL controls web filtering for Mobile Internet traffic outbound from Data Center.

4 - Host Security

DataZeo host servers utilize Ubuntu 10.x operating systems. DataZeo has applied all security patches for Ubuntu 10.04 to our servers. A complete list of applied patches is available at the following web address: http://www.ubuntu.com/usn/lucid. Our servers keep uptodate with new patches on a daily basis.

DataZeo also utilizes an SNMP Monitoring service, “Nagios” which conforms to the Industry Standard for IT Infrastructure Monitoring.

In the DataZeo CSST product there are back up processes occurring regularly to ensure that at all times, during the course of gathering data from the meters in the field and syncing to the server, there is a mirror image of the data kept in at least two locations. Key fields such as meter ID, date and time stamp are ensure that the data backed up is posted into the database in the correct location to ensure current data accuracy. In the proper location and is current in both the Cloud and handheld databases.

CSST backs up the entire database three times per 24 hour period. Full copies of this backed up data are then securely transferred offsite onto servers at two separate locations. In addition to the database backup, the most recent code base is transmitted securely to the offsite servers daily, as well as any new data that has imported into the database such as; client uploaded data files and photos. The primary host backup occurs at Digital West.

DataZeo provides robust password/login security for both the CSST and handheld login using the following criteria:

- Stored Passwords: Passwords are stored in oneway SHA1 encryption with a System Salt and a User Salt.
- Inactivity Lock: Accounts are locked from access after specified number of days of inactivity.
- Password Expiration: Accounts are locked after a specified number of days and a new password is required.
- This heightens security importance in the system.
- Password History: New passwords cannot be set to one that was used a specified number of changes back in history creating ongoing uniqueness to password login entry to the system.
- Login Attempts: Accounts are locked after a specified number of failed login attempts.
- Password Length: Passwords are required to be at least a specified length.
- Password Complexity: Passwords are required to contain a number of types of characters (lowercase, uppercase, numerical and special characters).
- Password Similarity: Passwords cannot be too similar to their username or first/last name.
- All account creation, authorization and termination are handled by only authorized administrative personnel and names / position of those will be supplied in the contract.
- DataZeo IT administration will work closely with you for account setup criteria and is handled in the pre-install document (see attached form).
- You will designate users and levels of permission to DataZeo and IT administration will set those users up on CSST.
- An email with temporary password is sent to the specific individual with login instructions.
- Training of this is provided to all departments of your organization upon installation.
- Terminated user accounts are handled by a "Removal of User" document that is sent to DataZeo from authorized personnel at your organization..
- Confirmation of removal is sent via email from DataZeo server.

All above features are tracked by date/time and user for accurate transaction recording.

5 - Web Security

Uses of Java, JavaScript, ActiveX, PHP or ASP (active server page) technology is secure because the web portal application uses PHP, and JavaScript. No ActiveX or ASP technology is utilized.

The process for doing security Quality Assurance testing for our applications is as follows. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.

The following procedures are in effect:

- DataZeo has numerous field employees testing the reading software, handheld application and functionality on a daily basis. We have designated key personnel to give feedback and enhancements for the product to the IT and development team.
- Accounting functions are monitored by DataZeo corporate office and monthly invoicing is compared to system reporting and database information.
- CSST database reports any exception, security abnormality or function that occurs in the program directly to the IT Manager and support.

6 - Cryptography

- DataZeo uses only industry accepted standard encryption algorithms.
- Encryption is performed using 256 bit AES.
- Hashing is done with SHA1
- The DataZeo Cloud is available using the SSL protocol over the Internet and IPSec from the handhelds.
- The DataZeo Cloud does not require PKI.

To provide the highest level of security, DataZeo employs encryption on certain pieces of information provided by the client. The goal being to protect the end customer from association with the data collected and referenced. The minimum set of data we work with includes once piece of information that is sensitive in this scenario such as the end customer's address. Without this key piece of information, the remaining set of data is a meaningless set of numbers and

values. In the encryption, DataZeo first must receive the information uploaded from the client. Upon receipt, DataZeo parses the information and updates the information in the database. At this stage, DataZeo encrypts the Address field. From this point on, the data representing the end customer's data is stored encrypted. The information is only decrypted to display to an authorized user or to export back to the client if their export requires it. As with all technology, there is a tradeoff. The encrypted Address is not searchable, except by complete and exact matching. Also there is a slight performance hit when dealing with encryption. DataZeo uses AES256 in cipherblock chaining mode to perform this encryption.

7 - Backup Security

- Database Backup is transferred using SCP over SSH.
- Code is transferred using GIT over HTTPS.
- The Database data is stored in Bzip2 compressed SQL text files.
- The Program files are a mixture of php, css, javascript and image files.
- The Database Backup is pulled from production by your organization's Backup Server.
- The Program Backup is pulled from our production release channel by your organization's Backup Server.
- The Database Backup uses SSH Keys to authenticate.
- The Program Backup uses a Username and Password to authenticate.
- DataZeo builds and maintains the backup software.