Security is our number One priority.

1. How Security is ensured at the Production Facility

At the production facility the SiteManager is installed. The SiteManager obtains an IP address via a DHCP server, just as a PC. The SiteManager typically uses the existing corporate infrastructure to reach the Internet in order to establish an AES encrypted connection to a central GateManager server via standard web ports (https/443), just as a web browser would do. At installation, the SiteManager is configured to connect to a specific GateManager (IP or DNS) and a specific customer domain on the GateManager.

The connection is based on TLS, and protected against man-in-the-middle attacks by letting every GateManager have a unique TLS certificate/key, to which the SiteManagers binds (aka ToFu “Trust-on-first-use). To remove the binding between a SiteManager and the GateManager, you will have to explicitly reconfigure the GateManager settings in the SiteManager. Since a man-in-the-middle cannot do that by just intercepting the connection, he cannot direct the SiteManager connection to another GateManager even if he had one.

In a normal setup, the SiteManager is connected permanently and makes keep-alive heartbeats to the GateManager every 10 minutes. But remote access to / from the SiteManager can additionally be controlled by the operator either by powering off the SiteManager when not used, or by connecting a on/off switch to an input signal of the SiteManager, which opens and closes the GateManager connection.

In the SiteManager, you configure so-called Device Agents that will allow LinkManager users, which have been granted access to the agents, to connect with their LinkManager client to the equipment represented by the Device Agent. The LinkManager user cannot redirect a configured agent to other equipment unless he has been specifically been granted access to reconfigure the SiteManager. If for instance an agent has been defined as "Siemens / Ethernet", this agent will open ports only relevant to Siemens equipment. Or if you configure a PC agent for a Microsoft server, remote users can only access the Remote Desktop of that server, but none of the other services run by that server.

Some of our customers evaluate "Security" and "Safety" in the same process. The SiteManager is prepared for the different safety regulations subject to industrial communication, such as the "EN415 Safety of packaging machines" directive that, among other things, requires that machine builders must make sure that remote service access to machines is properly signaled to the operators. All SiteManagers support an output signal that can be linked with e.g. a warning light. which will inform local operators that remote access/maintenance is in progress, and they should be extra careful when operating or servicing the equipment.

2. How Security is ensured in the Office Network

The SiteManager contains a stateful inspection firewall between the Uplink port that is used for GateManager access, and the Device port that connects to the network with the industrial equipment. This means that no communication can be made from the corporate network to the device network and vice versa. The firewall is simply configured to block all communication except authorized and encrypted data sent between the SiteManager and the GateManager. Furthermore the SiteManager is based on a hardened operating system, which prevents hostile persons or programs to exploit the connection. This neutralizes both internal and external threats.

The SiteManager can be configured to connect to the GateManager via a secure Web Proxy (including NTLM) which enables the IT department to further control and monitor its access. The IT department can also decide to limit Internet access based on the SiteManager's IP address or its MAC address, or alternatively limit its connection to another port (11444), which will enable the IT department to distinguish Internet traffic generated by the SiteManager from other users.

If IT corporate policies prevents any form of Internet access via the corporate network, you have the possibility of connecting the SiteManager via 2G/3G/4G. Even the SiteManager models without built-in broadband modems can access the Internet, simply by inserting a standard USB broadband modem into the SiteManager. This option is also ideal as a temporary solution in case remote service of machines must start before the IT approval process can be finalized.

3. How Security is ensured at the Remote Client side

The LinkManager is the client software installed on the technician's PC

The LinkManager connects to the GateManager the same way as the SiteManager. The LinkManager remembers the certificate/key of each GateManager it has received LinkManager certificates from. So if man-in-the-middle intercepts the connection, the LinkManager simply does not connect. Combined with the two-factor security of the LinkManager (using a local x509 certificate with password), the LinkManager represents maximum security. The LinkManager can even be operated with three-factor security by combining the password and certificate with a one-time pincode received by SMS.

When logging in, the LinkManager will establish an encrypted connection via the LinkManager virtual adapter on the PC. The adapter is closed for all other traffic than generated by its session with the GateManager. When logged in, the LinkManager user will see a list of sites and devices that his account is allowed to connect to. When connecting to a specific device, a route entry is created on the PC that will allow access to the IP address and the specific ports of the device agent representing the device. The LinkManager user has no possibility to reconfigure connections on the LinkManager.

All information about the GateManager to connect to and the account is encrypted into the x.509 certificate. The LinkManager user therefore does not configure anything, but only installs the LinkManager software, installs the x.509 certificate and logs in with the associated password. This also reduces support considerably as well as ensures that security risks due to mal-configuration is eliminated. In fact the biggest risk is, if the PC with the LinkManager got stolen, and the LinkManager certificate was created with a weak password that a person could easily guess. If this actually happens, the LinkManager account can be closed by one click by the GateManager administrator.

4. How Security is ensured on the central M2M Server

Central to the solution is the GateManager M2M server that functions as a secure proxy for the SiteManager and LinkManager data connections, based on the access definitions configured by the GateManager administrator.

GateManager is the only component in the solution that has ports exposed on the Internet, but only connections that can be validated by a proper x.509 certificate will be allowed. The only theoretic security risk would be if a man-in-the-middle could intercept the private key. Otherwise the TLS connection cannot be established. A known exploit of TLS is to start with certificate/key and after handshake ask the TLS connection to re-sync. (while man-in-the-middle listens in). We have eliminated that, simply by not letting our TLS implementation support re-sync, so man-in-the-middle cannot exploit this TLS risk.

Should someone be able to obtain access to the server where the GateManager is running, it would still not be possible to connect to any of the equipment managed by the central proxy, simply because connections are not statically open as known from VPN solution, but are only opened on request by a LinkManager user, and are only accessible from programs running on that LinkManager PC.

Also the GateManager administrator must login with a web-browser using two-factor authentication known from web-banking solutions. The most important features of the GateManager administrator portal GUI is to create LinkManager user accounts, organize SiteManagers and Device Agents into logical domains, and to grant access to specific LinkManager users to these domains. A key design goal has been to make this very intuitive in order to eliminate the risk of granting unintended access. It is all controlled by drag and drop, and with clear indication of who has access to what.

Generally the Secomea solution fulfils all the security standards stipulated by the National Institute of Standards and Technology (http://www.nist.gov) for encryption and key negotiation. It has complete end-to-end security, ensuring that no one - and nothing - can access equipment without permission.

Most importantly the GateManager ensures that all events are logged. When a LinkManager established connection to a given device, when a configuration change is made on a SiteManager, when a SiteManager is rebooted, when a firmware is upgraded, when an alert email or SMS was triggered etc. All these events are logged with time stamp, description and the user that caused the event.

NOTE: Secomea offers hosting of your account on our GateManager servers. Only authorized Secomea personal will have access to your account, and will only access your account in relation to support questions initiated by the authorized customer representative. All actions performed by Secomea will be logged in the event log of your account.

If your IT policies dictate not to allow third parties access to your equipment or if you have a policy of not being dependent on a third party, you can decide to host your own GateManager. A GateManager is provided either as a virtual image ready to install on a ESXi, VMWare or HyperV server, or as a stand-alone hardware server with a specially hardened OS that eliminates the need for keeping your OS up to date with security patches.