Providing Secure Connected Products

The ThingWorx platform delivers the highest levels of security, performance, and availability, helping customers with best practices for an overall security design.

Executive Summary

Security is a primary concern of ThingWorx customers — especially device manufacturers and end-customers that deliver and use connected products. These customers demand a proven solution that protects them and their customers against hackers, malware and unsafe operations. In addition, they require a solution that supports interaction with their deployed intelligent devices in an IT friendly fashion, and extends their current network security model so that they can meet critical certification and compliance requirements. Since the manufacturer's devices are connected to their customer networks, the end-customers also need to be assured that the connected product supports their security model, provides granular control over user access, and offers easy-to-use audit and tracking capabilities.

Leading device manufacturers across many industries are delivering business-critical connected products with the ThingWorx Platform delivered either at their own premises, or via our SSAE 16/ SOC 2 audited on-demand centers with ISO27001:2013 certified systems and operations group with commitment to the security of our services for our customers. The ThingWorx Platform addresses the end-to-end security requirements of manufacturers and their end-customers, while enabling them to grow revenue, reduce costs, increase customer satisfaction, and manage risk without additional IT burden and investment.

Because customers' devices may track patient records, financial data, and other types of private and protected information, security and compliance capabilities are among the most important requirements evaluated in any connected product solution. IoT projects are particularly sensitive to security issues because an attacker can spy on unprotected machines and cause physical damage by executing malicious commands. This paper details how ThingWorx meets the requirements of security-concerned manufacturers and their end-customers.

ThingWorx incorporates an end-to-end security strategy covering all levels, including network, application, user, and data security, as well as security training for its employees, and having dedicated Certified Information Systems Security Professional (CISSP)

personnel on staff. The primary ThingWorx data centers are ISO 27001:2013 and SafeHarbor certified.

As more and more of your infrastructure is plugged into the LAN/WAN/Internet, security must be one of the foremost tenets of the design of your systems. An overall security design must be a combination of software and hardware infrastructure, plus pervasive security policies enforced by business practices. This white paper discusses the security measures built into the ThingWorx Platform and best practices for a secure implementation to help you fit ThingWorx solutions into your overall security design.

Overview

The ThingWorx Platform was built from the ground up with security in mind. While collaboration implies value creation through open interaction amongst members of a community, the business focus of the platform requires strict security and privacy. This is needed to comply not only with business requirements but regulatory constraints as well. By incorporating the latest in Internet standards and architecture, the ThingWorx Platform succeeds in creating a real-time, context-based collaboration environment while still maintaining a high level of data and user security.

ThingWorx strives to address all of the key security concerns which are discussed in this document. To understand the security provisions of the platform it is best to look at the individual components of the ThingWorx Platform and how they interact.

Two primary components of the ThingWorx Platform are the ThingWorx Server and ThingWorx Edge components, including the Edge MicroServer (EMS) and various software development kits (SDKs) referred to collectively as the EMS in the rest of this document. The Server handles user and device authentication, brokers communication between systems, people, and things in the solution landscape, and handles data transformation, data persistence, and business logic, as necessary, for the end user application. The EMS enables devices to securely communicate to the ThingWorx Server, and be full participants in the solution landscape. The EMS, as indicated by its name, is not a simple "connector," but allows intelligence and pre-processing of data to be moved to the edge.

Processes and Technology

ThingWorx has a strong commitment to continued development and support of security processes and technology to ensure that it stays ahead of security issues, and threats to data, intellectual property and operations. ThingWorx has robust internal application security testing capabilities with a large team of trained security staff in-house. Frequent security testing is executed at the network and application level, for both the platform and the edge components. Additionally, network and application vulnerability testing using both internal and external tools are conducted, along with periodic internal and external security audits.

Server Security

- Uses standard PKI infrastructure for certificate validation
- TLS 1.x support -Supports both client and server certificate validation
- 128 Bit AES encryption or higher (configurable set of ciphers supported)
- FIPS validated ciphers supported
- Fine grained visibility, access, and permissions model
- Integration into LDAP/Active Directory or other authentication back ends
- AES Encrypted data fields supported

Secure Design Principles

The ThingWorx development process follows secure software development best practices, which include:

- A risk assessment – Initially, a high-level assessment to identify major risks, followed by other iterations examining all other risks. The security risk assessment reviews begin during the design phase and the engagement lasts through launch to ongoing operations.
- Security requirements definition – Conducted during inception and elaboration phases of projects to ensure that the resulting product will be highly secure to meet all customers' security needs.
- Formal design reviews - Conducted during and at the end of the design phase to determine whether established security requirements, security design concepts, and security-related specifications have been satisfied.
- Security code reviews – Conducted throughout development to ensure that the code is implemented in conjunction with software development best practices and that implementation does not stray from design.

ThingWorx Platform Security Features

Authentication and Authorization

The ThingWorx Platform has an extremely granular security model to enable data isolation and service execution at any required level. The ThingWorx Platform supports HTTP authentication, which requires a user to establish a web session using a user name and password. If desired, The ThingWorx Platform can delegate the authentication of the credentials to an LDAP system, allowing the LDAP system to manage password policies such as password expiration, account lockout, password dictionary use, password history and password strength.

In addition, The ThingWorx Platform has a pluggable authentication model which allows customers and partners to implement their own business process specific authentication model. This extensibility also enables The ThingWorx Platform to release new authentication modules independently of major releases. The ThingWorx Platform can support standard industry mechanisms such as SAML, and SSO integration from other tools such as Salesforce.com, SAP and others.

The ThingWorx Platform has an Access Control List (ACL) model that allows administration of ThingWorx Platform authorization to a very granular level. The ThingWorx Platform has overlaying levels of security that can be applied. Access control can be granted or denied at the most granular level, such a specific read or write access to a single Thing Property. In case of a conflict, the most restrictive security setting is honored. There are separate permission settings for Design-Time and for Run-Time. Both Design-Time and Run-Time permissions can be set for any entity in the system. All entities follow essentially the same model.

Design-Time permission settings are as follows:

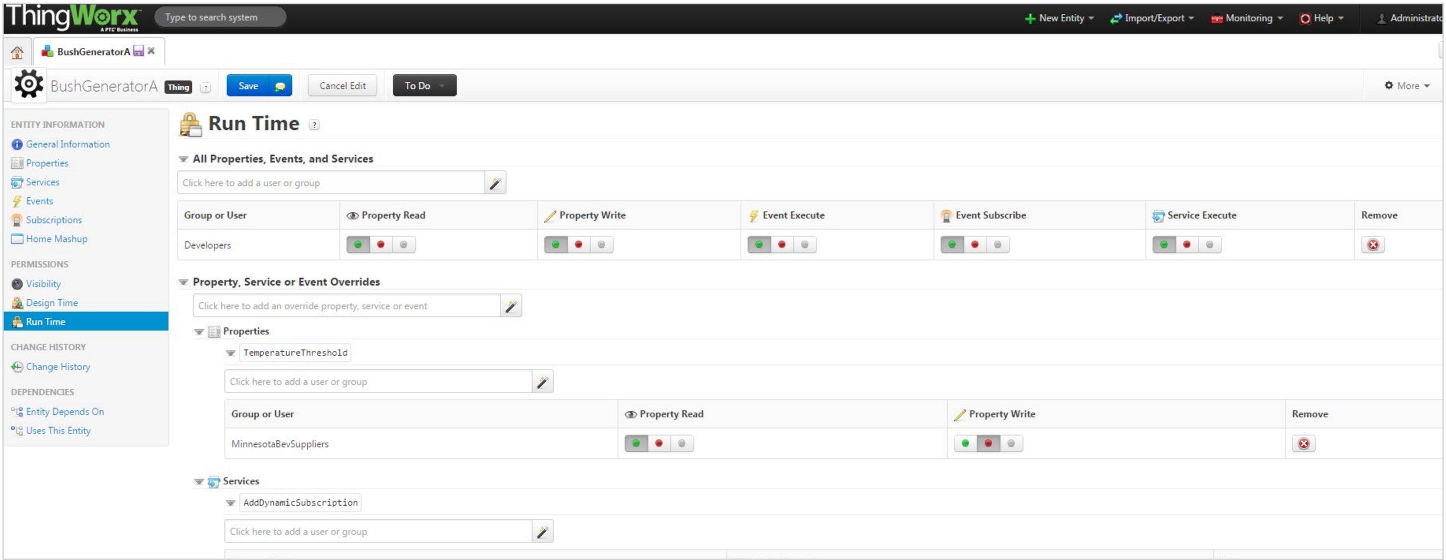
- Create entity
- Read entity
- Update entity
- Delete entity

Run-Time permission settings are as follows:

- Property Read
- Property Write
- Event Execute
- Event Subscribe
- Service Execute

Both Design-Time and Run-Time permissions can be set at the following levels:

- At the collection level. For example, it is possible to grant the ability to read all properties for all Things in the system. This can then be overridden at lower levels.
- At the ThingTemplate level. ThingTemplates are a way to combine shapes (multiple sources of data) that allows you to add additional property services, subscriptions and events to create a unique template that allows for the rapid creation of any new thing. ThingTemplates are unique in that there are also ThingTemplate Instance permission settings that may be set and inherited by all Things that are implemented using that Template. These also can be overridden at the Thing level.
- At the Thing Level. For example, Property Read access can be given for all Properties of a Thing.



Run Time

All Properties, Events, and Services

Click here to add a user or group

Group or User	Property Read	Property Write	Event Execute	Event Subscribe	Service Execute	Remove
Developers	[✓ ●] ● ●	[✓ ●] ● ●	[✓ ●] ● ●	[✓ ●] ● ●	[✓ ●] ● ●	☒

Property, Service or Event Overrides

Click here to add an override property, service or event

Properties

TemperatureThreshold

Click here to add a user or group

Group or User	Property Read	Property Write	Remove
MinnesotaBevSuppliers	[✓ ●] ● ●	● [✓ ●] ●	☒

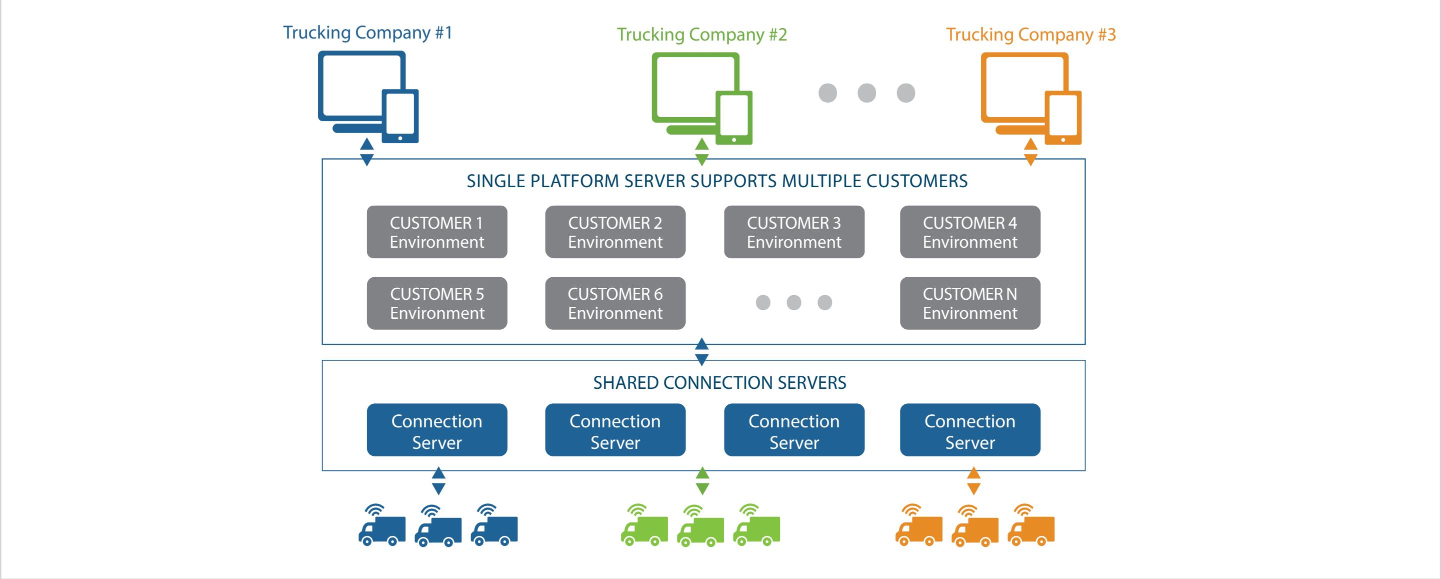
Services

AddDynamicSubscription

Click here to add a user or group

Run-Time permissions settings

THINGWORX MATRIX MULTI-TENANCY – SUPPORT FOR CUSTOMER TENANTS



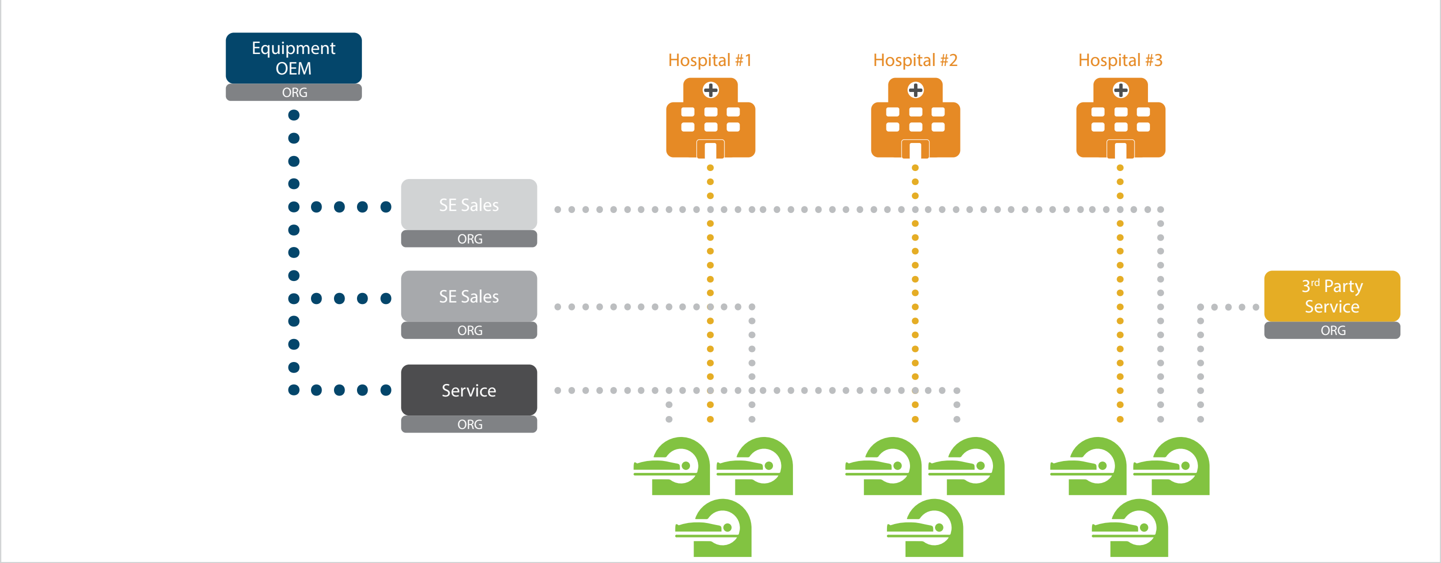
Traditional Multi-Tenancy

- At the specific Thing Property, Service or Event level. For example, a specific grant or deny can be assigned for a specific Thing Property Read or for a specific Thing Service Execution.

Matrix Multi-Tenancy

Matrix Multi-tenancy is a patent pending innovation that allows entity visibility to be defined in a series of overlapping "Organizations". Organizations are structures that allow isolation of parts of the ThingWorx Model. An organization is made up of a hierarchical set of organization units. The hierarchy looks like an organization chart. You can then assign a special type of permission, named Visibility, to entities in the Model. Visibility is a key form of access control. If an entity is visible to members of an organizational unit, then only those members have access to the entity, and the underlying, granular security model determines what specific interaction any users that are members of that organization unit may have with a specific asset. If a user in the system is not granted Visibility, then that asset essentially does not exist within that user's domain. That user cannot see the asset, cannot list it, or

THINGWORX MATRIXED MULTI-TENANCY



Matrixed Multi-Tenancy

interrogate that asset's namespace or know that it exists at all.

It is possible to define the Visibility rules in a way so that you can make specific Things (such as specific physical assets) only visible to a single organization, or you can allow two or more organizations to be able to see an asset.

Security Logging Sub-System

The ThingWorx Platform has a full set of logging services for the application layer, the script engine, for configuration changes, and for security. All logins, successful or not, are logged and can be monitored.

In addition to the standard security logging, there are a number of security related events that may be used to capture additional information on system usage. These are in addition to other types of events that can be triggered within The ThingWorx Platform that are more application oriented, such as data change events or threshold violation events.

Users can log related event data for monitoring purposes. There are separate events for file transfers between edge devices and the server, and for remote desktop sessions to edge devices. For each event, you can create a subscription to log data. Each event data package has the initiator (from), receiver (to), time, data size, bytes transferred, event type, error message if any, plus additional transport information.

Each file transfer has the following different types of event messages that may be subscribed to and logged:

- Start of file transfer
- Receiving of file
- File sent
- File transfer completed

Each remote desktop, or tunnel session, has the following types of event messages that may be subscribed to and logged:

- Start of remote desktop session
- End (Complete) of remote desktop session

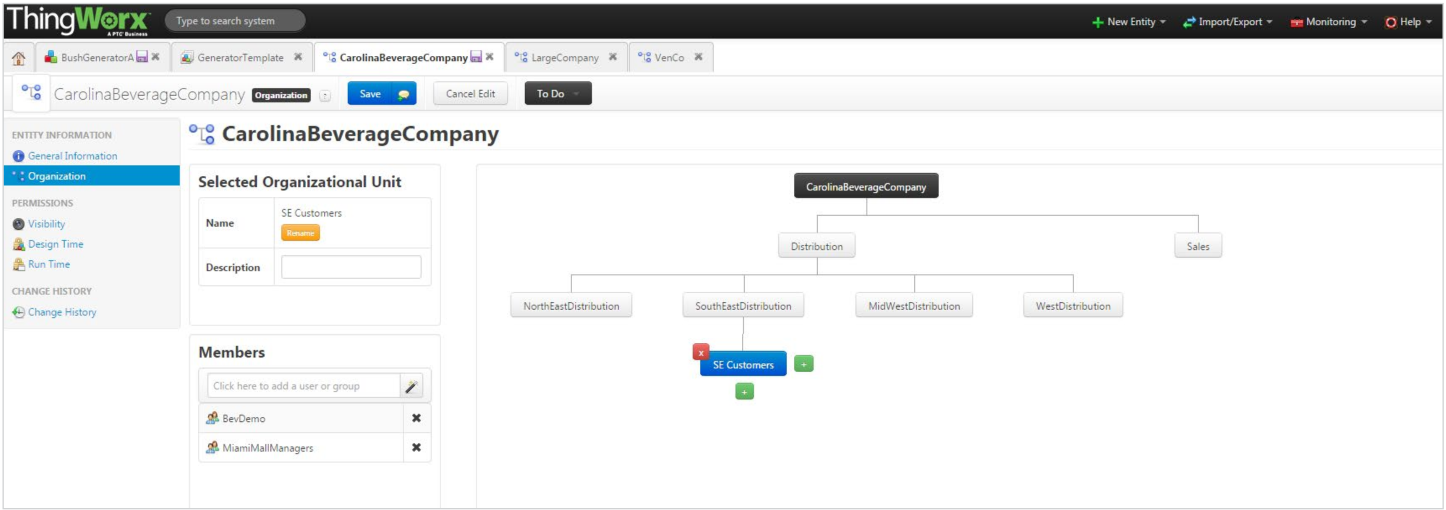
Encrypted Storage of All Sensitive Data

The ThingWorx Platform uses encrypted storage for sensitive data. Passwords are stored encrypted at all components within the ThingWorx solution. This includes passwords stored at the platform for user accounts, and passwords at the edge components for use in connecting back to the server.

Additional data can be encrypted for persistence if desired through available encryption functions.

Recommended and Supported Application Backup Strategy

ThingWorx has specific services to support complete application backup. In addition, there are content services to export configuration, model, and data objects, promote them through the landscape, and import those objects onto other servers. Customers running in the ThingWorx data center will have backups run periodically without the need to manage them.



Name: SE Customers
Description:

Members:
BevDemo
MiamiMallManagers

Organization View

Protection Against Common Vulnerabilities

ThingWorx software products are designed based upon industry secure coding practices (such as Microsoft's Software Development Life-cycle, Cigital Software Security Touchpoints, OWASP standards or SANS Top 10 where relevant). ThingWorx proactively protects against the exhaustive list of items that includes injection attacks and cross-site scripting (XSS). Statements passed into the ThingWorx backend are parameterized. Internal commands cannot be submitted through a URI call protecting your IoT infrastructure. SQL Injection and other similar attacks are mitigated in the ThingWorx architecture due to the use of prepated statements and parameter validation. As demonstrated in other sections of this paper, ThingWorx follows best practices to ensure that other common vulnerabilities such as broken authentication, missing access control and sensitive data exposure do not occur.

ThingWorx has procedures in place to identify security vulnerabilities in then-current releases of a commercial product, and provided a customer maintains a current maintenance/support plan, ThingWorx will provide updates for security flaws that require remediation in standard product releases or maintenance updates. Customers then need to implement the latest release or update following documented guidelines in order to apply security updates.

Backdoor Protection

All ThingWorx API calls are public utilizing well-established security processes. There are no secret "backdoor" APIs utilized for administrative use. All APIs require authentication and there is no ability to turn off encryption converting encrypted data to plaintext. ThingWorx applications utilize the same APIs as ThingWorx customers do, following security best practices to not have secret ways to access data.

Support for Transport Layer Security

The standard communication protocol recommended for clients to the web server is HTTPS (Secure Sockets Layer), so that all data transmission over the wire is encrypted. The standard communication protocol from the Edge MicroServer component to the server is the industry standard WebSockets protocol (RFC 6455), which runs on top of the secure and encrypted TLS protocol. The Edge MicroServer components also support HTTPS if that communication is required for specific scenarios. Note: ThingWorx follows industry best practices and utilizes TLS exclusively over the insecure SSL protocol.

Additional Security Features

In addition to the transport layer encryption, all files that are transferred between the edge and the platform (bi-directional) are encrypted before transfer and then decrypted after receipt. File MD5 hashes are calculated to ensure complete and successful file transfers as well as that the file has was not tampered with.

ThingWorx Edge MicroServer

The Edge MicroServer (EMS) and associated SDK components act as an interface between intelligent devices and the ThingWorx server. The EMS shares information and data with the server using the Internet Engineering Task Force (IETF) standard WebSockets protocol. The key security highlights of the ThingWorx edge connectivity are as follows:

- Based on well known, industry standards including Transport Layer Security (TLS) 1.2 with Advanced Encryption Standard (AES) 128 or 256 bit encryption, which are the same standards used in online banking applications. FIPS compliant encryption algorithms are supported for certain regulated environments.
- Multilevel authentication is built in to the underlying ThingWorx AlwaysOn™ binary protocol – Once a WebSocket is established the connecting device must provide credentials in order to be allowed to communicate with any other entities in the system.
- Firewall Transparency – the only connection required is a single established connection from the EMS to port 443 on the ThingWorx server. That connection can be direct to on site HTTP proxies and authenticating proxies for an additional layer of end customer monitoring and control. No listening ports need to be opened to the outside world from the edge device.
- Auditing – all file transfers and application tunneling (such as Remote Desktop) sessions are audited both at the server and on the edge device.

The Edge MicroServer also includes a set of SDKs for device software component development. The support languages/platforms includes Java, C, .NET, and native SDKs for iOS and Android, with additional language SDKs will be provided over time. These SDKs allow customers and partners to leverage the security, efficiency and communication management available in the ThingWorx WebSocket based EMS while providing their own device or business process specific functionality.

File Transfer and Application Tunneling with the ThingWorx EMS

The ThingWorx Platform supports file transfer and application tunneling in a similar fashion. By using the encrypted WebSocket channel to establish a one-time use, dedicated channel between two users it ensures a secure, audited connection. Unlike other remote desktop or application tunneling solutions, the ThingWorx Platform uses end-to-end 128 bit encryption of the application or file data being transferred between the server and the edge device. In addition, the one-time use encryption keys are independently calculated at each end of the connection ensuring that the keys are never transferred over the Internet.

Because it uses the same WebSockets communications model, all communications are firewall transparent. The connections are initiated from the edge device inside the firewall out to the ThingWorx server, thereby removing the need for any open listening ports on either end of the connection. Finally, all tunnel connections are audited with the initiator, target, and start and end times and can be logged is desired.

Remote desktop applications offer additional security. The remote access server can be set up such that inbound remote desktop requests must be acknowledged and approved by an operator at the device in question, and the entire session can be recorded for later playback.

Secure and Scalable On-Demand Centers

ThingWorx on-demand center operations team's process is certified to meet the ISO Standard 27001 Information Security Management System (ISMS) framework. These well- documented operational standards include the typical components of:

- Incident management
- Security monitoring
- External audits validating our security methodology and processes
- Security awareness and training programs
- Risk management and business continuity planning
- Change and configuration management
- Capacity planning
- Proactive threshold monitoring of core resources

Given each of these processes is governed by the ISO Standard 27001 ISMS and is aligned with Information Technology Service Management (ITSM) best practices, ThingWorx customers can be assured their products and data are secure. The ITSM process has been thoughtfully designed as a component of the Information Technology Infrastructure Library (ITIL) standard.

ThingWorx's secure hosting partner – CenturyLink delivering the following advantages:

- Auditable Security SSAE 16 Certified. Your valuable IT assets are safeguarded against man-made and natural disasters. Our data center locations are designed to withstand extreme weather events and prevent unauthorized contacts from accessing your data center space. CenturyLink offers a wide range of Managed Security Services that help your organization to prevent potential data compromises, network breaches and unauthorized system access.
- Robust Protection from Physical Harm. CenturyLink prides itself on building advanced, cutting-edge, multi-level physical security into every data center to ensure that your infrastructure isn't compromised. CenturyLink also provides an extensive array of sophisticated managed security services that supplement our standard security measures.
- Standard Data Center Physical Security Measures.
- On-premise security guards
- Security systems on the building exterior: cameras, false entrances, vehicle blockades, customized parking lot designs, bulletproof glass/walls and unmarked buildings
- Biometric systems, including palm scanners
- Numerous security cameras with digital recorders
- Portals and person-traps that authenticate only one person at a time
- Power. To protect your technology investment and deliver the infrastructure availability you require, we utilize power management, power monitoring, advanced fire suppression, and HVAC (Heating, Ventilation & Air Conditioning) systems.

CenturyLink data centers are designed to prevent "single points of failure" that can reduce availability of your infrastructure and impact the quality of end-users' experiences. CenturyLink's most critical responsibility to customers is to keep their infrastructure functioning, despite potential disruptions such as lengthy

Connectivity Security:

- Standard PKI infrastructure for certificate validation
- TLS 1.x support
- Supports both client and server certificate validation
- Password protected PEM key file storage
- 128 Bit AES encryption or higher
- FIPS validated ciphers supported
- Encrypted configuration file entries

power outages.

To maintain power availability, all of CenturyLink's data centers utilize high-capacity, redundant generators that guarantee power availability even during metro-wide power outages. And, due to short-notice diesel generator refueling contracts with multiple vendors at each data center location, the electricity backup capabilities are extensive. This permits CenturyLink to supply necessary power to organizations that require around-the-clock infrastructure availability, such as online retailers, global financial services companies and healthcare providers.

- HVAC. The CenturyLink data centers allow for proper heat dissipation, permitting their sites to operate within an acceptable temperature range. To maintain the flow of air conditioning to the data center infrastructure, CenturyLink employ's redundant (N+1) HVAC units within each of their locations. The HVAC units are powered by normal and emergency electrical systems, in order to maintain their availability. Additionally, cold water tanks are installed that keep air conditioning units functioning when there is a requirement to transition from direct power to generator power during emergencies.

- Fire suppression. CenturyLink employs the latest fire suppression methods. To detect smoke from the earliest stage of combustion, fire suppression systems are installed at each of Savvis' data center locations. The systems utilize state-of-the-art "sniffer" systems, augmented by heat detection and dry-pipe sprinkler systems.

- Seismic engineering. CenturyLink has performed extensive seismic engineering to keep potential disasters from interrupting business operations. In regions that are prone to seismic activity, they provide the necessary level of bracing. Seismic isolation equipment is installed to cushion facilities against movement, in addition to installing earthquake bracing on all equipment racks. And, racks at all of CenturyLink's data centers — not just those in traditional earthquake zones — are anchored to the concrete slab below the site's raised floor.

- Network Connectivity. CenturyLink high-availability network and carrier connections provide strong global reach, allowing customers quick and convenient access. Colocation Services are offered in North America, Europe, and Asia, permitting the addressing of specialized business continuity and disaster recovery objectives. CenturyLink leverages geographical diversity to provide customers with failover and redundancy capabilities with many of their services.

- Industry Leadership. CenturyLink been offering secure hosting services to companies for more than a dozen years and continue to build on this expertise in areas of cloud computing and beyond. This includes membership in:

  - International Standards Organization (ISO)
  - PCI Standards Council, the Information Security Audit and Control Association (ISACA)
  - Information Systems Security Association (ISSA)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Computer Security Institute (CSI)

Application Security Perspective – Above the Infrastructure

Manufacturer's Requirements for Connected Product Security

The ThingWorx Platform meets stringent security requirements of manufacturers and end-customers so that they can achieve broad adoption and maximum use of connected products — instilling confidence that their connections are secure and private. Some of the most common manufacturer requirements include:

- Enterprise proven design – Connecting any computer to the Internet raises security concerns, and connecting intelligent devices is no different. Whether hackers are trying to harm a device with corrupt data or viruses, steal data traveling between the device and manufacturer, or gain unauthorized access to critical information, a connected product solution must guard against these and other threats.

- Support for multiple devices – Manufacturers need to securely support a nearly infinite number of device types and complex customer configurations without requiring major end-user changes.

End-Customer Requirements for Connected Products

Intelligent devices are connected to your customers' networks. Each customer has their own security policy and network protection in the form of firewalls, proxy servers, and addressing schemes. A device connected to their network will be protected behind these layers of security. If a connected product offering requires changes to your customer's network protection, it will likely fail to gain acceptance. Because of this, it is important to consider the requirements of the end-customer, including:

- Maintain current security model – The manufacturer's device must support the way that the organization manages security operations, policies, or procedures, and should adhere to accepted industry standards.
- Control user access – In line with the customer's security model, the manufacturer's device must provide the customer — not the manufacturer — with granular control and set policies on what actions can be performed on the device such as data collection and software updates, and when those actions can be performed. These policies need to be centrally defined for all devices at a customer location.
- Audit and track activity – Policy and regulatory compliance requirements dictate that the system must make auditing and tracking all user and administration activity easy.

The ThingWorx Platform delivers the performance, flexibility, and scalability required to meet the needs of the broadest range of device manufacturers by providing the widest range of data protection safeguards and security features.

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER INCLUDING ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE. NO LICENSE, EXPRESS OR IMPLIED, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED OR INTENDED HEREBY.

J5194-Providing-Secure-Connected-Products-0415