WHITE PAPER

StrideLinx Platform Security

Today's machines/systems are more connected than ever before with many utilizing cloud networks for remote access. Cloud networks come with inherent security risks and the StrideLinx platform goes above and beyond to ensure data security.

By Jonathan Griffith
Product Manager, Automation Controls & Connectivity, AutomationDirect

AUTOMATIONDIRECT.com
The #1 Value in Automation.™

WHITE PAPER

StrideLinx provides a fully integrated cloud-based Industrial IoT solution for machine builders, building automation integrators and system integrators. The StrideLinx Cloud platform together with a connectivity gateway, the StrideLinx router, offers an all-in-one solution for safely and easily setting up remote access to your machines, monitoring machine status and receiving alerts about important machine events — all within your own branded StrideLinx Cloud portal. While operating in the cloud does provide many benefits, it also comes with inherent security concerns. StrideLinx products and services are designed with this in mind and provide better security than many traditional on-premises solutions.

This whitepaper outlines StrideLinx's approach to security for the StrideLinx Cloud platform and the associated router. StrideLinx's security strategy is based on the CIA triad: a security management model for protecting the confidentiality, integrity and availability of information. Companies nationwide have already chosen the StrideLinx Cloud solution and with the rapid growth of platform users, it's imperative that all customer data is kept secure following industry best practices.

Information Security Management

A better world starts at home. We believe that you can only provide a secure cloud solution if all internal processes and procedures are secured as well. That is why StrideLinx is supported by a comprehensive information security management system (ISMS).

The ISMS of IXON B.V., the company powering the StrideLinx platform, is certified according to the ISO 27001 standard: the leading global standard for information security in organizations. It requires adherence to several disciplines, including access control, (cyber)security, compliance, risk management and business continuity. Compliance with ISO 27001 shows that organizations have implemented comprehensive security programs and controls that protect their information and those of their customers in accordance with internationally recognized standards.

The ISMS covers:

- Development of cloud connectivity solutions for machines and devices
- Gateway production for connecting machines and devices to the StrideLinx Cloud platform
- Management and maintenance of the StrideLinx Cloud platform
- Supporting StrideLinx products and services

WHITE PAPER

In order to achieve the ISO 27001 standard, a series of extensive audits by DigiTrust, an RvA-accredited certification body was conducted on the ISMS. The ISMS was found to be of excellent quality and protects all data according to the highest industry standards. Continuous improvement of the ISMS ensures compliance with the latest industry best practices and technological advancements. This will be verified on a regular basis through internal audits and external audits by DigiTrust. With the ISO 27001 certification, you can rest assured that all data is protected allowing you to focus on remote machine uptime and process improvements.

Cloud Services and Servers

The StrideLinx Cloud is a complex network of over 50 servers, distributed worldwide. It is structured to provide the best performance, availability and security. It consists of numerous server and database types, of which the key types are discussed below in more detail. All servers are located in data centers which uphold the highest security standards and have obtained ISO 27001 certification. And most importantly, we do not own any data stored by users in the StrideLinx Cloud; all data is owned by its users.

API Services

The application programming interface (API) services are the heart of the StrideLinx platform. They handle key processes in the StrideLinx Cloud, including authorization, configuring VPN connections and connecting to databases.

MQTT Broker Services

The StrideLinx Cloud uses the Message Queuing Telemetry Transport (MQTT) protocol for data transfer. The MQTT protocol over TLS is ideal for the Industrial Internet of Things because it is highly efficient, secure, has minimal overhead and greatly diminishes bandwidth use.

StrideLinx's MQTT broker services are used for pushing router configurations, firmware upgrades and for the transmission of Cloud Logging and Cloud Notify data.

WHITE PAPER

VPN Servers

VPN servers are located in data centers around the world to provide low-latency connections. The VPN server network is redundant, so if one VPN server goes down, the other servers will take over automatically. The API decides which VPN server is best for setting up a secure VPN tunnel, based on the physical location of the router and its nearest VPN server. All you need to do is install the VPN client to set up a secure connection from your browser to your remote machine.

These VPN servers are also used for setting up Cloud Access connections to your HMI or web-based controls. A secure VPN tunnel is created from the StrideLinx router to the server and its contents are then streamed to your browser using an HTTPS connection.

Figure 1: StrideLinx Cloud data center locations across the globe.

Kubernetes Cluster

The StrideLinx Cloud platform contains a Kubernetes cluster for enabling and managing microservices. This modern architectural style ensures optimal scalability and availability of the StrideLinx Cloud platform. Microservices allow large applications to be structured as a collection of loosely coupled, smaller applications (services) that can be managed and updated individually. Each microservice is built as a Docker container and Kubernetes is used for managing all these microservices.

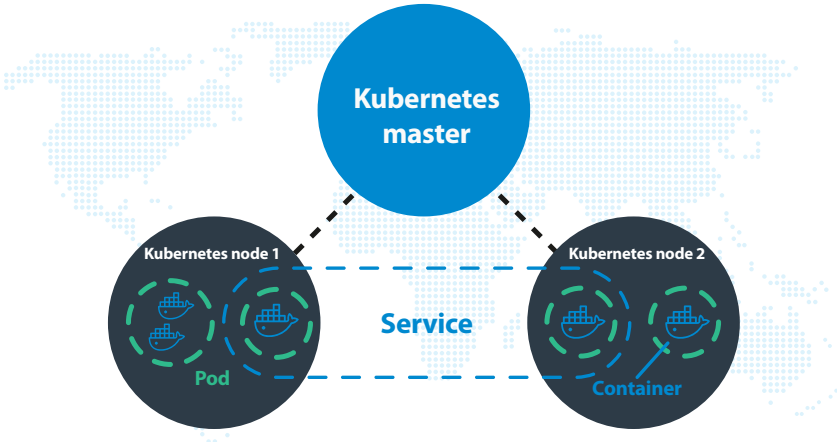

Figure 2: Kubernetes cluster. The Kubernetes master acts as a manager for Docker containers. It can manage and update these containers individually, in order to build a modern, fast and scalable application.

Save on STRIDE IIoT/Cloud Solutions:
www.AutomationDirect.com/stride/stridelinx

AUTOMATIONDIRECT.com
The #1 Value in Automation.™

WHITE PAPER

Relational Database Cluster

The relational database stores information about StrideLinx Cloud users, companies, devices, etc. It is set up redundantly using a master-slave structure across multiple data centers. The Master receives and processes all requests to view or edit the database.

The Slave replicates all write/update events on the Master and creates a backup every four hours. In case of any issues with the Master, the roles can be switched to ensure database availability. Only the StrideLinx API, Slave and Kubernetes cluster are able to communicate with the Master; all other connections are refused outright.

Non-Relational Database Cluster

The non-relational database stores data on StrideLinx Cloud platform events, generated alarms, logs, etc. This database is configured as a replica set, of which the primary server receives and processes all requests, and the secondary server replicates the primary server. This configuration ensures high availability and redundancy for the non-relational database. Only the StrideLinx API, other servers in the replica set, or Kubernetes cluster are able to communicate with the non-relational database; all other connections are refused outright. These database servers are also located across multiple data centers.

Time Series Database Cluster

As mentioned previously, machine data is sent to the StrideLinx Cloud using the lightweight and highly efficient MQTT protocol. This protocol uses the MQTT broker: a central station for receiving and sending data messages. After the StrideLinx router collects the data, it's first passed to the MQTT broker. There it is time stamped and stored in a buffer database. Next, a time correction is applied to account for any possible discrepancies between the router's internal clock and the NTP time (actual time).

Finally, the data is stored in a time series database cluster (InfluxDB). The main advantage of a time series database is that it's optimized for handling timestamped data. This allows users to request data over a large period of time in just a few milliseconds and perform operations, such as calculating the mean value, in a fast and highly efficient manner. Furthermore, time series databases allow for advanced data life-cycle management options, such as aggregation or down sampling of your machine data.

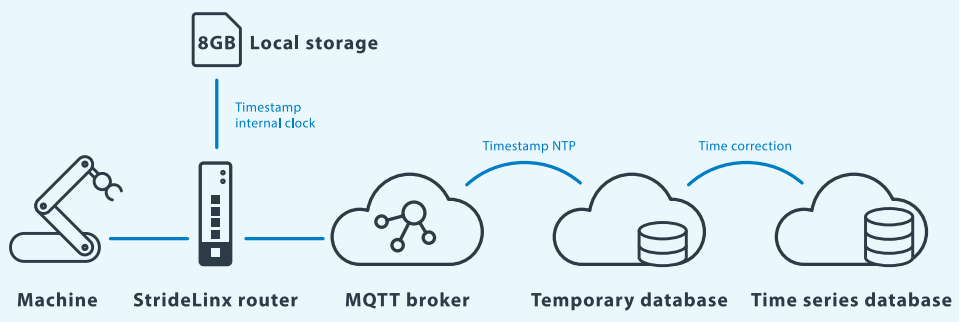

Figure 3. Machine data: the road from machine to the StrideLinx Cloud.

WHITE PAPER

Cloud Security Controls

Encrypted Connections

Encrypted connections are necessary to prevent unauthorized access to accounts and sensitive information. All connections to and from the StrideLinx Cloud and between Cloud services are therefore encrypted using HTTPS with TLS 1.2 or higher. MQTT connections are also TLS encrypted to ensure the confidentiality of your machine data. VPN connections use single-use VPN certificates and are encrypted using AES-256-CBC with SHA512. Cloud user passwords are stored as hashes using PBKDF2 with 12 bytes salt, 12000 iterations and SHA512 + HMAC.

Figure 4: The StrideLinx platform connections are made using secure encryption to protect sensitive data

Centralized Monitoring, Logging and Analysis

The StrideLinx Cloud is monitored 24/7 and logs are stored and analyzed on a centralized logging platform. The centralized logging platform is mainly focused on collecting information about server performance and database requests. It uses artificial intelligence to detect critical events and anomalies in real time before they affect users. All monitoring and logging reports are analyzed quickly to identify and react to any performance issues, unusual server activity or unauthorized actions.

Vulnerability Management

A third-party vulnerability solution scans the StrideLinx Cloud regularly for any external vulnerabilities. Scan results are reported in a centralized overview and assessed by the security officer. In addition, StrideLinx's servers are audited daily by another third party specialized in server security and system hardening. Server auditing is aimed at determining system health by detecting any internal vulnerabilities or configuration management weaknesses.

A centralized overview of the audit results shows the status of each server and provides guidance for improvement. This enables a quick response to any vulnerabilities and confirmation that each server matches the highest security standards.

Access Control

Strict internal control policies for accessing servers has been implemented. Only a few senior developers are able to access the StrideLinx platform servers. Other developers may be given access to a server temporarily, if this is necessary for their task, under the direct supervision of a senior developer. Developers log into servers using their own unique SSH key. All server logins and changes are monitored 24/7 and logged to the centralized logging platform for analysis.

Software Development Life Cycle

The software development life cycle is focused on delivering secure, high quality software. All software is tracked through an advanced software versioning management system. New code is developed following language-specific coding conventions and secure coding techniques.

All software changes are reviewed by at least one other developer and are thoroughly tested through manual and fully automated tests. The software versioning management system has been designed for continuous integration, delivery and deployment. This means that for most software updates, all code is:

1. Automatically tested with 100% code coverage
2. After all tests have passed, software changes are automatically scheduled for release
3. Software is then automatically released, without human intervention

This method of automated testing and releasing software changes greatly reduces risks for each release and enables developers to get valuable features and improvements out fast and in a sustainable way.

WHITE PAPER

Router Security

Built-In Firewall Separates Your Machine From the Internet

Machine controllers were never designed for security. Their operating systems are not updated and do not contain the latest security mechanisms. It is imperative that these machine controllers are never connected to a company network while linked to other devices. The StrideLinx router can isolate these controllers from the company network with its built-in firewall.

The StrideLinx router's built-in firewall completely separates the WAN port (company network) from the LAN ports (machine network). By default, the internal firewall blocks all traffic from the WAN to the LAN ports and vice versa. However, firewall settings can be adjusted according to individual needs via the StrideLinx Cloud. You may allow access from the machine network to the corporate network or internet and you can set up port forwarding. New settings and updates can be pushed to the router directly from the StrideLinx Cloud with just the push of a button.

Figure 5: StrideLinx routers provide an internal firewall to keep WAN and LAN ports isolated

WHITE PAPER

Outgoing Ports

The StrideLinx router only uses outgoing ports to establish a secure connection to the StrideLinx Cloud, so there is no need to open any incoming ports on the local firewall in the company network. This makes StrideLinx extremely IT friendly and will allow for approved installations in most sites.

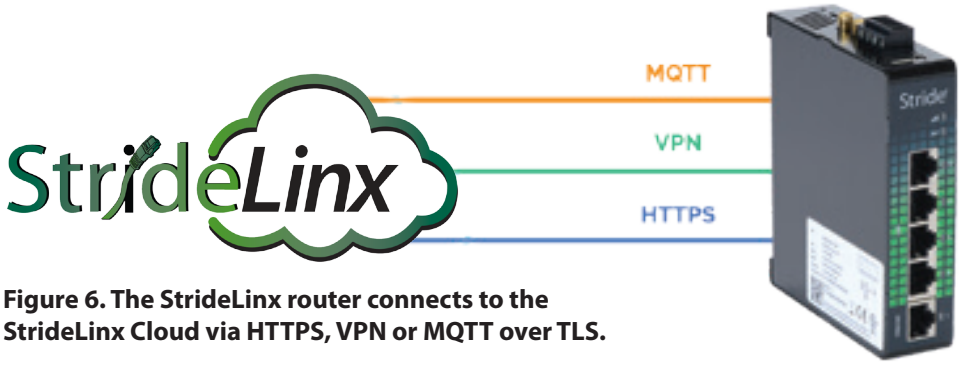

Figure 6. The StrideLinx router connects to the StrideLinx Cloud via HTTPS, VPN or MQTT over TLS.

Below is an overview of the outgoing ports and protocols that the StrideLinx router utilizes.

PORT	TRANSPORT	APPLICATION
443, 8443[1]	TCP	HTTPS, MQTT (TLS) OpenVPN
53[2]	TCP & UDP	DNS

(1) Port 8443 is only used when stealth mode is activated for connectivity via a censored internet connection (i.e. when located in China).
(2) DNS requests are often handled by local DNS servers. In those cases, the listed DNS port can be ignored.

Access Restrictions that Meet Customers' Security Standards

The local IT department may choose to only grant specific devices internet access, based on the MAC address or IP address of the device. The MAC address can be obtained from the label on the side of the StrideLinx router or from the info panel in the StrideLinx Cloud. The IP address can be set to a static IP address. However, by default, the IP address is set to be obtained automatically via DHCP.

Access to the StrideLinx router can be disabled locally using a digital input on the router. Wire this input to a switch and use it to "lockout" remote access to the router during system maintenance.

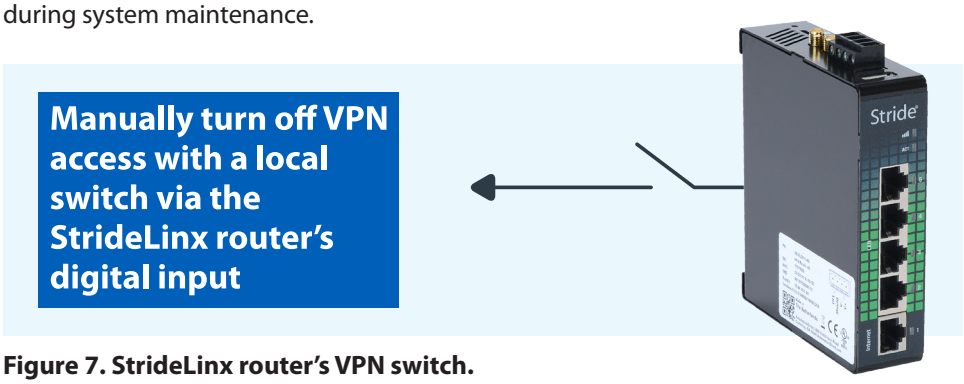

Figure 7. StrideLinx router's VPN switch.

WHITE PAPER

Always Keep Your Machine Online With the StrideLinx Router Failover

Should your preferred connection drop, the StrideLinx router will automatically connect to another network. This is fully configurable for Wi-Fi, 4G, and Ethernet. Each connection is constantly checked by sending keep-alive messages to a public IP address every few seconds.

If the connection fails multiple consecutive times, the connection is considered down and the router will automatically connect to the first (or second) fallback. If the preferred network is up again, the router will automatically switch back to the preferred network. The IP address for keep-alive messages and time interval can be changed according to individual needs.

Data Logging Even When Your Machine is Offline

Internet connections are not always stable and may go down from time to time. In some situations, such as on a ship at sea, there might not even be an internet connection available at all. This is problematic for users who wish to log their machine data in such conditions.

To solve this, the StrideLinx router has an 8GB flash memory which allows machine data to be stored offline for weeks at a time. As soon as the router comes back online again, all machine data is automatically sent to the StrideLinx Cloud over an encrypted connection.

Additionally, users are able to receive notifications when the router has been offline for a specified number of hours with the Cloud Notify functionality. This allows users to quickly react to any connectivity problems and fix these issues as soon as possible.

Hardware Certifications

The StrideLinx routers' certifications ensure that they match the highest safety, health and environmental protection standards. In addition, the StrideLinx router 4G (SE-SL3011-4G) has been certified to be fully interoperable with mobile networks and to achieve maximum connectivity performance with the AT&T network.

The StrideLinx router has been certified for:

- CE certification
- FCC verification
- cULus listing (E495151)
- PTCRB certification
- AT&T Network Ready Certification For USA and Canada

Save on STRIDE IIoT/Cloud Solutions:
www.AutomationDirect.com/stride/stridelinx

AUTOMATIONDIRECT.com
The #1 Value in Automation.™

WHITE PAPER

Browser and App Security

Login Security

The StrideLinx Cloud platform can be accessed via any web browser or via the StrideLinx app on your mobile device. Users log in with their username and password. If two-factor authentication is enabled, users are also prompted to enter a one-time password. One-time passwords add an extra layer of security to your account. They are generated by an app (e.g. Google Authenticator) on your mobile device and remain valid for 30 seconds.

Unsuccessful login attempts return the user to the login screen. After five incorrect attempts, the user is locked out of his/her account for a number of seconds. This time increases exponentially (up to 1 hour) with subsequent incorrect attempts.

Secure Online Purchase for Additional Cloud Services

Additional services, such as Cloud Logging, Cloud Notify and premium branding, can be purchased directly from the StrideLinx platform. All payments are handled by PCI-DSS level 1 compliant third parties. PCI-DSS level 1 is the most stringent level of certification available in the payments industry. This certification ensures that payment providers maintain the highest security standards and that your billing information is secured.

User Management

From the StrideLinx platform, administrative roles and user privileges can be configured and controlled by company administrators. This means that individual users in a company can access or manage certain services or make payments without gaining access to all settings and data.

A Safe, Reliable and Trustworthy IIoT Solution

With the StrideLinx Cloud, machine builders gain a highly secure and advanced Industrial Internet of Things platform. Comprehensive security controls and redundant servers worldwide are key in achieving a safe, reliable and trustworthy IIoT solution. Numerous companies trust StrideLinx with their most valuable asset: information. Protecting your information is our top priority and we will continue to pursue new innovations to allow StrideLinx Cloud users to benefit from its full potential in a secure manner.