InstruLogic Cloud
Integrated. Accessible. Secure

Is Cloud-Based SCADA Secure?

With the emergence of cloud-based SCADA services many operators are wondering, *"Is cloud-based SCADA Secure?"* The simple answer is *"no."* No SCADA system nor any other type of IT infrastructure is intrinsically secure from malicious intrusion. So this is the wrong question. A better question is whether Cloud-Based SCADA is less secure than on-premises SCADA system. The answer to this question is more like *"it depends."* It depends on how server resources are managed and how much resource you can invest in securing your on-premises hosted SCADA system.

Where are the vulnerabilities?

Physical Security Practices

The issue that impacts security more than anything else is user-access. If you can keep bad actors from accessing your systems and data, you will have have fewer problems. Some operators go so far as to "air-gap" their systems from internet-connected networks and epoxy shut USB ports. But even these extreme measures won't protect your systems from physical access by intruders and disgruntled employees who can enter the building and access a terminal. So physical access to terminals and servers is a must if a system is to be considered secure.

Identity and Access Management Practices

All systems are vulnerable to penetration if lacking adequate security measures. It cannot be overemphasized that organizations must implement more stringent and tightly controlled **Identity** and **Access Management (IAM)** polices. If users are allowed to login with passwords like "*PASSWORD*" and administrative resources can be accessed with a password like "*ADMIN"*, it doesn't matter where your servers are located. Furthermore, access privileges must be managed and enforced carefully to keep unqualified and unauthorized users from gaining entry to vulnerable system resources.

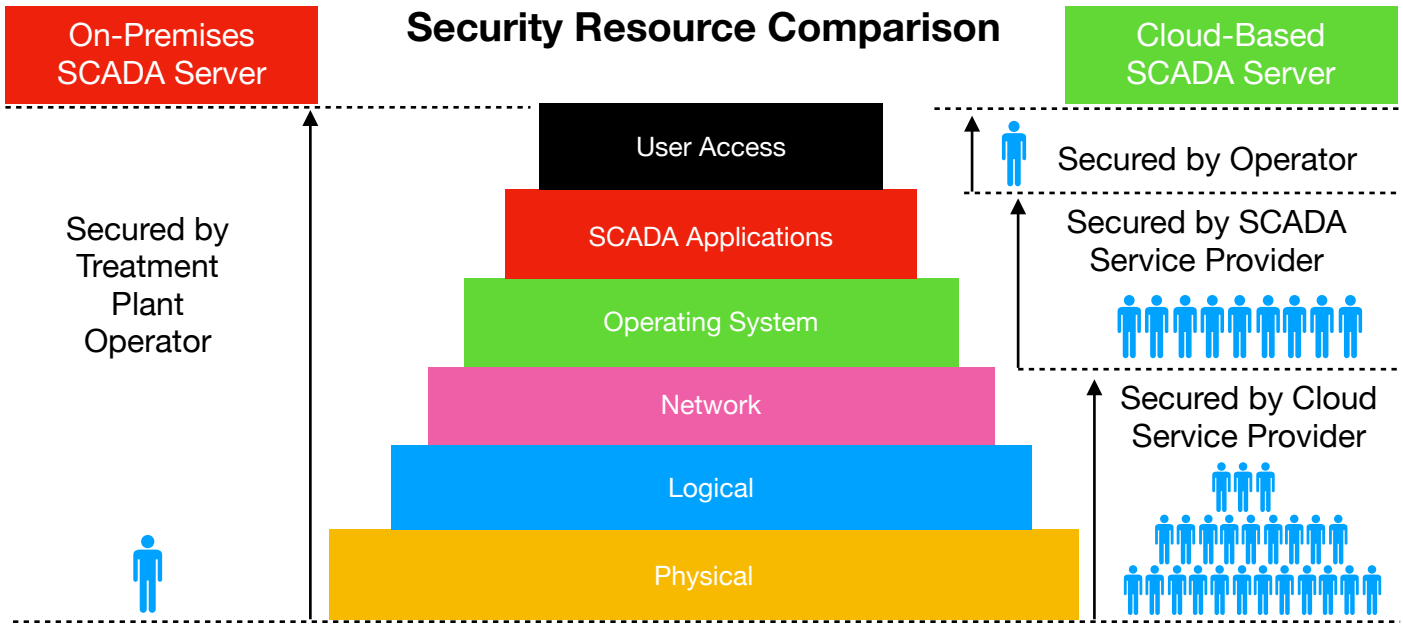
So the real key to system security isn't found in the location of the server assets but in establishing policies and procedures for limiting access to them. Systems built without implementing and maintaining rigorous security won't be secure, whether they are cloud-based or not.

System Administration Practices

A third area of concern is system administration. Maintaining a successful defense against cyberthreats requires constant vigilance in assuring that system resources have adequate protections against malevolent attacks. This means keeping an eye on software revisions, installing security patches to your operating system and keeping antivirus and malware protections in place and up to date. SCADA packages often have unique operational and performance requirements that add complexity to managing system resources for maximum security. Nevertheless, vigilance is required.

Security and the Location of System Assets

The location of the servers probably has less to do with system security than you might imagine. The ability to maintain a robust and affordable defense against intruders is the real issue. In fact, large Cloud Services Providers (CSPs) like IBM, Microsoft and Amazon invest significant resources monitoring threats and ensuring that their infrastructure is available and secure. After years of evolution, they have become experts in securing the lower layers (physical, logical and network layers) of system architecture. Their facilities are located in geographic regions that are not prone to natural disasters or political/social unrest. Facilities access is restricted to appropriately authorized and carefully screened personnel under active supervision. At the application level, CSPs have dedicated System Administration resources to ensure that operating system security patches and updates are are quickly installed as they become available, minimizing the time that your application will be vulnerable to new security threats. Furthermore, the best CSPs segment each application to its own Virtual Private Cloud, (VPC) limiting the ability of a breach in one application from moving to other applications on the same physical server.



Rarely will a small municipal utility operator have the resources to match this kind of vigilance. In terms of manpower, CSPs have a large pool of highly talented professionals assigned to securing their infrastructure. So unless you have dedicated staff to secure your facilities and network, monitor for threats and update your systems, CSPs will usually provide a more secure environment to host your applications. Using a 1st tier CSP to host your SCADA and having a competent and experienced SCADA Service provider to customize and maintain it for your operations is like having a highly trained and effective army to defend your Treatment Operations from cyber threats.

Security based on best in class resources

Is Cloud-based SCADA secure? It depends on whom you depend to make it work. We can't speak for all Cloud-Based SCADA service vendors. Those who offer services on a shoe-string budget are likely to cut some corners to keep costs down. But InstruLogic Cloud cost-effectively provides **best in class security resources** at every subscription level.

Cloud Service Provider: Amazon Web Services GovCloud

Amazon Web Services GovCloud is our Cloud Service Provider. As a GovCloud customer, you will benefit from a data center and network architecture built to meet the requirements of security-sensitive industries like Financial Services, Public Sector and Healthcare. AWS customers include NASDAQ, Phillips and The United States Department of Defense. Amazon provides server resources for the first three levels of our Service SCADA system architecture.

AWS GovCloud

System Administration: InstruLogic/Sophos

Typically the performance demands and I/O intensive nature of SCADA systems require a more attention to system administration details than most business related applications. Operating system upgrades, software updates and security patches must be carefully evaluated before they are installed in production systems to make sure they don't negatively impact operation. As a result, many municipal operators are unable to keep their systems up to date and appropriately secured. Service SCADA from Instrulogic includes full system administration support provided by highly trained SCADA experts to ensure optimum system operation and security.

The performance demands and I/O intensive nature of of SCADA operations also require additional care in selecting utilities like **virus protection.** Some virus and malware protection utilities consume system resources that can slow a system down, limiting its effectiveness. Some virus protection is incomplete, leaving systems vulnerable. Some virus protection is limited only to the server but not connected user-devices (smart phones and tablets). Sophos provides up to date and **end-to-end protection** in a low overhead utility. Service SCADA by Instrulogic includes Sophos protection configured, installed and monitored by our SCADA and Security experts.

SOPHOS

SCADA Software : Ignition by Inductive Automation

Our Cloud-based Service SCADA is built on Ignition by Inductive Automation. Inductive offers a variety of configuration options to assure system security based on the application requirement. Instrulogic takes advantage of the following security features.

inductive automation
SCADA CERTIFIED PREMIER INTEGRATOR

Instrulogic has enabled **SSL encryption.** SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link

ensures that all data passed between the web server and browsers remain private and integral. This protects your installation from anyone "snooping" the data as it passes over the network. This also helps to thwart a security vulnerability known as "session hijacking."

Ignition security limits privileges and access to individuals based on their roles and responsibilities. This information can be pulled directly from other IT systems including **Microsoft Active Directory**. Any change in role or employment status will automatically be enforced on the SCADA system, limiting access to only current employees with appropriate privileges. Operators with robust identity and access management practices can easily extend these to treatment operations.

Automation Hardware PLC

Programmable Logic Controllers have direct connections to critical plant monitoring and control assets such as sensors, valves and pumps. Instrulogic utilizes **OPC UA Communications** supported by Ignition and embedded in selected PLC devices to secure communications. **OPC** Unified Architecture (**OPC UA**) is a machine to machine communication protocol for industrial automation. Direct connection from Ignition to OPC UA devices takes advantage of security features built into PLC devices.

User Access

Instrulogic security experts can even help you develop **Identity** and **Access Management Policies** to close the biggest security vulnerability most operators have. If the bad guys find your system too difficult to penetrate, they will probably move on to easier targets whose systems have less rigorous security.

Budgetary Advantages of InstruLogic Cloud

Even though the cybersecurity risks to your operations are reduced by cloud-based SCADA, embracing a new technology can be intimidating So what are the advantages of moving to the Cloud? We can't speak for all cloud-based SCADA offerings, but InstruLogic Cloud has several advantages over traditional SCADA offerings.

Low cost entry point

Typical SCADA projects require a large upfront investment and capital outlay. InstruLogic Cloud is offered as a service with minimal capital expenditure. Customized design, installation and support services are included with your subscription.

Only pay for what you need

Another advantage is that you pay for only what you use. Many computer purchases are sized for the performance and capacity projected as a worst case later in the project life-cycle. This strategy is widely employed in our industry to avoid costly computer upgrades down the road. But with InstruLogic Cloud, you don't buy any hardware and you only purchase the service level you need on day one. If your needs increase with time, the service can be resized to meet your future needs and only *if* you need it.

No obsolescence

Another advantage is that your system never becomes obsolete. Whenever you purchase hardware you run the risk that it can become obsolete and non-supportable. With InstruLogic Cloud, upgrades and obsolete component replacement is included with your subscription for the term of your agreement.

IT Costs are outsourced

With InstruLogic Cloud we provide all system administration and maintenance services. You don't have to budget for in-house IT staff.

Remote access

Measurement and Control resources and data are easily and securely accessible via web-based applications on internet connected computers, smart phones and tablets. It has never been easier or less costly to add user seats to your treatment plant SCADA.

Can your Cloud-based SCADA be secure?

By leveraging our resources and those of our best in class partners, your InstruLogic Cloud based SCADA provides reliable, secure and cost-effective automation and control to any treatment operation.

Call us for an @NoCharge consultation today.

- *IBM is a registered Trademark of the IBM Corporation*
- *Microsoft and Microsoft Active Directory are registered trademarks of the Microsoft Corporation*
- *Amazon and Amazon Web Services GovCloud are registered Trademarks of the Amazon Corporation.*
- *Sophos is a registered trademark of Sophos Ltd.*
- *Ignition is a registered trademark of Inductive Automation*

212 Fort Collier Road, STE.1
Winchester, VA
P. 540.338.2222
F. 540.338.1133
info@instrulogic.com

2600 Garner Station Blvd
Raleigh, NC
P. 919.557.7248

www.instrulogic.com

InstruLogic
An INFRAMARK Company