RED LION®

EXCELLENCE. REDEFINED.

Use Case

REMOTE ACCESS REAL-LIFE SECURITY LESSONS

When thinking about remote access, security is, and should be, top of mind.

Control engineers are fundamentally changing how they do their job, from being onsite to 1,000 miles away and simultaneously managing multiple sites without a single truck roll. However, there are several challenges associated with implementing a remote access solution that is easy to use and provides robust security measures, preventing unauthorized access. The biggest hurdles once deployed, are ensuring the solution will block all unauthorized access and any infrastructure changes made during installation don't leave open security loopholes in the architecture.

There has been a long-standing belief that ease of use and security are on a sliding scale. Solutions can be very secure, or they can be easy to use but not both. This is not true. Unfortunately, implementing a complex solution can leave employees feeling overwhelmed, resulting in shortcuts and creative workarounds. These workarounds may include leveraging non-sanctioned software tools or merely skipping steps to save time, which ultimately opens the door to security vulnerabilities.

Security Best Practices

Not conforming to security best practices is also a common challenge. For example, when IT mandates password policies where users must change their password every 30 days, many users increment their password by a digit or write the password down and keep it near the computer. Neither workaround conforms to security best practice, but it's easy and fast for the user.

Recently there was a cyber-attack against a water treatment facility in Florida. In the attack, a perpetrator remotely accessed and gained complete control of the automation system using shared employee credentials of a software-based remote access solution. The attack targeted a chemical dispensing system within the water treatment facility to increase the sodium hydroxide levels, which would have been disastrous to the water supply. Thankfully, this real-world attack was stopped by an observant Controls Engineer, who noticed the abnormal change in the chemical dispensing system and immediately took action.

How could this have been prevented, and how can companies protect their assets when they have remotely deployed systems?

The first option is to airgap or physically silo control systems by physically disconnecting them from the Internet. While this may be secure, the reality of managing these sites becomes nearly impossible. With no real-time data feeds, monitoring and managing assets in real-time is impossible.

Layered Security

A better option is a layered security approach that adheres to user security protocol "best practices" together with security-enabled software and hardware. This layered approach makes it significantly more difficult for a malicious actor to attack the system. An example of a "best practice" for a user security protocol is requiring two-factor authentication (2FA) for user email access. Email and any remote access should require multiple "keys" to authenticate a user to prevent the sharing of keys and compromised security. Additionally, selecting the right remote access hardware and software solution can provide real-time data monitoring without compromising system efficiency and access.

Red Lion's Secure Remote Access Platform

Red Lion Controls offers a next-generation Remote Access Platform that meets the most demanding security requirements of modern industrial applications. Red Lion's Secure Remote Access Platform centralizes the management of routers, allowing customers to quickly implement a policy-based approach, manage users, and ensure devices are operational. The ability to remotely access, monitor and manage diverse equipment helps to lower operational costs and downtime by reducing site visits and dramatically improving response times.