OIL&GAS JOURNAL

FAQ

How Centralized Cybersecurity Protects Pipelines and Other Remote Assets

Ransomware cyberattacks are on the rise and pipeline owners have become prime targets. From disrupting fuel supplies to operational failures and safety risks, any incident highlights the vulnerability of critical infrastructure and brings unwanted attention to the pipeline owner.

Increased investment has led to greater awareness, increased vigilance, and better detection and prevention, but cybercriminals, hacktivists, and state-sponsored actors are an ongoing menace. The recent state-sponsored Salt Typhoon attack on U.S. infrastructure and government agencies and the Volt Typhoon attack on U.S. energy, telecommunications, and transportation networks are evidence that the threat has not gone away.

Centralizing cybersecurity is a proven way to safeguard vulnerable assets, but implementing a reliable solution requires perception, planning, and persistence.

What are the difficulties in providing cybersecurity for operational technology (OT) infrastructure?

The biggest challenge is for companies to understand what might not be secure and challenge conventional thinking with respect to OT. Field equipment was designed for a service life of 10-20 years, and designers did not prioritize cybersecurity. This equipment uses legacy communication protocols and technology, which make it vulnerable to cyberattacks.

Many owners think because equipment is not connected to the internet or is behind a firewall, it is secure. This outdated thinking presumes that the firewall is the only pathway to the network. In fact, people regularly interact with the system. Field technicians connect to devices, people nearby can connect to the SCADA network, and even people using USB keys have introduced issues.

On the IT side, people rely on corporate IT to manage security, but until recently, this centralized approach to cybersecurity was not possible for geographically distributed hardware. Today, that same centralized security is available for hardware in the field, even for devices that are only intermittently connected.

What is different about a centralized approach to cybersecurity?

A centralized solution is comprehensive and includes remote terminal units (RTUs), flow computers, and software that works with components from multiple vendors and manufacturers. Effective systems follow guidance from the Joint Cyber Defense Collaborative (JCDC), which was formed by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to unify cyber defense capabilities from government, industry, and international organizations.

Security can be designed such that the Active Directory domain service used by IT can control access to RTUs, flow computers, and SCADA systems and also monitor activity. This simplifies the process of meeting exacting requirements from agencies like the Transportation Security Administration (TSA), which is working to enhance U.S. pipeline cybersecurity. TSA requires that credentials change at regular intervals and when an employee leaves the company. Without a centralized system, it is nearly impossible for pipeline owners with a large workforce and thousands of devices in the field to meet this requirement. With a centralized system, when an employee resigns, their login credentials are immediately disabled.

How do the concepts of "Defense in Depth" and "Zero Trust" fit into the picture?

The idea of Defense in Depth is that no single vulnerability in any level of control should compromise the system; so there are multiple levels of defense. For example, a system might have a firewall that protects from the internet, internal zones that separate critical areas, and a system that monitors network traffic. This approach also protects modern hardware, ensuring firmware is valid, is introduced by appropriate personnel, and is monitored after it is installed.

Zero Trust is a security architecture that questions the safety of every piece of software and each individual component. In the past, owners assumed that legacy devices connected on the network could be trusted, but this is not the case. For example, a field technician could update equipment with a compromised laptop. Zero Trust requires everything to be authenticated before any action is taken because a system is only as secure as its weakest feature.

Defense in Depth and Zero Trust prevent incidents like the recent Russian attack on the Viasat communications network in Ukraine, in which a lack of multifactor authentication between IT and OT networks allowed the introduction of rogue firmware that compromised critical infrastructure and affected tens of thousands of customers.

How do companies implement IT cybersecurity solutions for OT infrastructure when these teams traditionally have been kept separate?

The key is to educate both sides so IT and OT workers are looking at the big picture. OT engineers need to understand that IT professionals know a lot about cybersecurity because they have been dealing with it for a long time and have experience with the tools and infrastructure. And IT professionals need to understand OT equipment isn't standard. There is a wide range of equipment from different vendors, and that needs to be taken into account when a cybersecurity plan is being developed.

What makes this approach particularly appropriate for pipelines?

Distributed assets are challenging to protect because they are spread over a large area, some of which are not easily accessible.

A centralized system configured with industry standard tools simplifies implementation and makes it easier to maintain cyber safety. A technician can use a secure laptop to log into the network from a hotel or corporate domain service to update field assets and have the same level of security achieved using that same laptop in the field.

Planning is important, and implementation requires buy-in from every level of the organization from the C-suite to the field. When a centralized, standardized solution is in place, monitoring cybersecurity across a complex set of assets is simplified.

A standardized approach also leads to a much more fortified infrastructure, ensuring data always flows securely from the field to the edge and into the cloud.

Sponsored by

EMERSON