



CONSOLEWORKS JOINT-SOLUTION

Nozomi Networks

TDi Technologies Introduction

TDi Technologies has provided Remote Access solutions for mission critical applications in the Energy, Healthcare, Telecommunications, Finance and Government & Intelligence markets for over 20 years. We have many highly visible clients in all of these markets – some we can talk about and some we can't (Defense & Intelligence).

The ConsoleWorks solution is highly-regarded in the Energy market with a number of very large clients and highly visible partners including NCCOE, DOE, PNNL, ORNL, AFIT, University of IL, CREDC, SEEDS, and others on various US Department of Energy cybersecurity research teams.

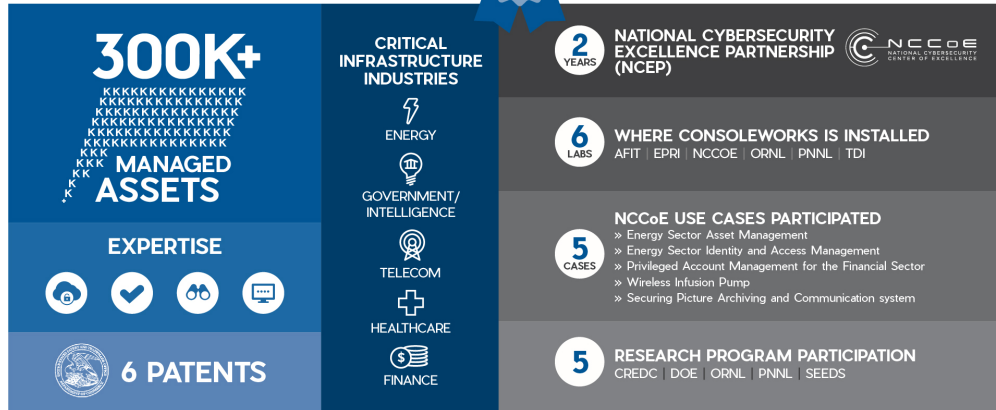
TDi Technologies has been involved in 2 US Department of Energy funded projects:

1. Program for patch management of ICS assets with FoxGuard Solutions – 3 years funding
2. Govern human activity when using cyber access to control grid operational characteristics - 3 years funding granted in October, 2018 (new).

Customers will benefit from the results of both programs and from the numerous patents that have been granted for the ConsoleWorks technology.

We are a very active member of NCCOE's NCEP program where we play a critical role in 5 of their use cases including: Energy Sector Asset Management, Privileged Account Management for the Financial Sector, Energy Sector Identity and Access Management, Wireless Infusion Pump for Healthcare (ICS) and securing Picture Archiving and Communications System in Hospitality.

Today, there are several hundreds of thousands of assets that are managed by the ConsoleWorks Cybersecurity / Operations platform.



TDi Technologies Company Overview

Our customers choose to use ConsoleWorks for their mission critical application because of the level of capability and insight provided by the technology. To that end, a quote from a former Deputy Director of the NSA, about ConsoleWorks...
 “ConsoleWorks provides visibility with a level of fidelity not available in other solutions.”
 This is one reason why our customers choose ConsoleWorks!

Finance	Utilities	Healthcare	Government	Telecom

TDi Technologies Markets and Sample Customers

As part of these various programs and industry involvement, TDi Technologies has made a significant investment (through the DOE and our clients) in our own lab, focused on the Energy industry, specifically. This lab continues to grow as more and more customers ask us to provide more automation around their assets. TDi has committed to

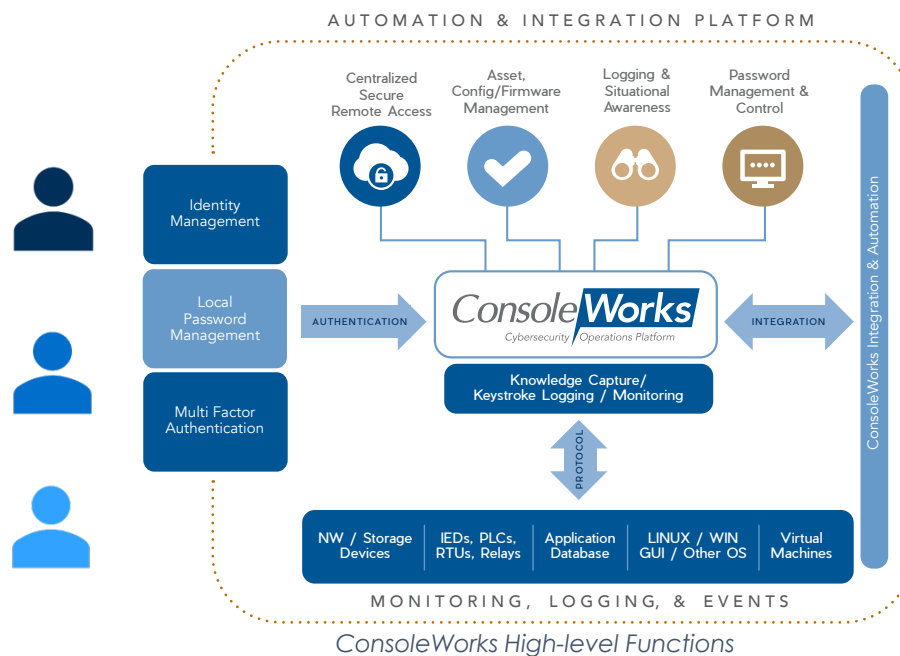
investing a percentage of all revenue from our Energy clients into our lab so that we can continue to provide the level of support they are demanding.

This lab is also utilized by our partners for building use cases as well and includes manufacturers like GE, SEL, HP, Cisco, NovaTech, ABB, Allen Bradley, Rockwell Automation, Honeywell, Emerson, Coopers, and numerous others.

Consoleworks Overview

TDi Technologies has been a leader in providing secure remote access solutions to the energy market for many years. The ConsoleWorks platform has been built, from the ground up, to support the subtle (but extremely important) requirements of mission critical application for industrial control systems.

ConsoleWorks is a single platform for IT and OT security, operations and compliance of diverse, privileged resources – people and critical assets.



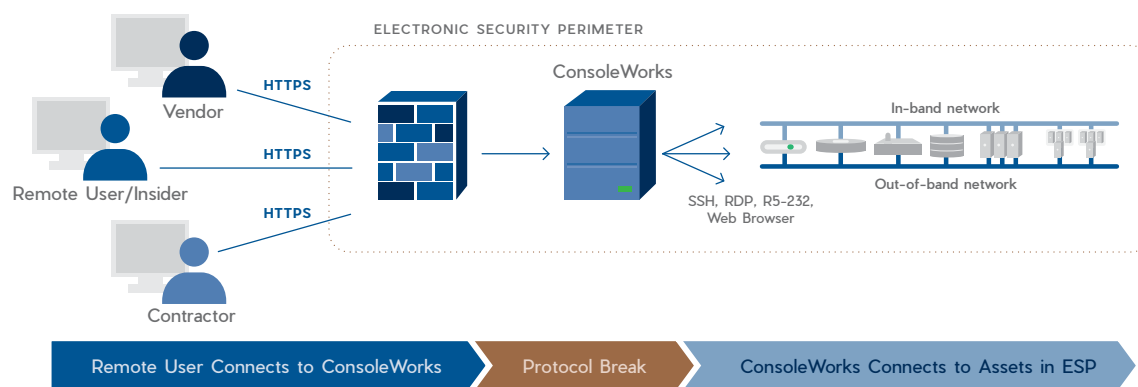
Centralized, Secure Remote Access – Secure Remote Access is the defense against unauthorized access to the Electronic Security Perimeter (ESP). Many authorized users within corporate offices, the control room, at plants or substations, on the move, and 24/7 support from home (or wherever a person may be), depend on the ability to securely and remotely access these assets, to address security, operational and

compliance needs. ConsoleWorks facilitates these authorized users, while providing a defense against access by unauthorized users.

ConsoleWorks provides true separation of networks (remote user, ESP), by default, providing a protocol break between the user and the devices to which the user is interacting (no viruses or malware).

The fine-grained privilege model in ConsoleWorks enables a level of control over assets to which each user may interact. Detailed activity logs (down to the keystroke) and video recordings (RDP, VNC) provide comprehensive forensic reporting, compliance data, and situational awareness of all user activity and resulting system responses from the assets managed by ConsoleWorks.

ConsoleWorks controls access by allocating specific permissions/ privileges to a user based on the ConsoleWorks role-based permission model. The permission model specifies which assets/devices a user may access and at what level of privilege they may access those assets. ConsoleWorks can also support command-by-command privilege grants for absolute control.



ConsoleWorks Protocol Break

A user logs into ConsoleWorks using industry-standard web interfaces using HTTPS. ConsoleWorks is able to communicate to assets using their native protocols (SSH, Serial, etc.) – just as a user would interact – providing the protocol break that prevents malware and viruses from penetrating the ESP. ConsoleWorks does all of this without adding “agents” (software) to the endpoints, which is critical in industrial environments.

ConsoleWorks has the ability to access endpoints through a number of different means:

- Using a number of different protocols (RDP, HTTPS, TELNET, Serial, MODBUS, SSH, and others)
- Through modems
- Through the device hierarchy
- Using vendor software

The ConsoleWorks solution supports integration with an IdAM solution and supports RBAC from an Active Directory server. The product was designed with the open ability



to integrate its authorization / authentication services with many other authentication technologies.

Integration with Nozomi Networks

The integration with Nozomi Networks automatically presents to ConsoleWorks a list of newly Nozomi-discovered assets. The ConsoleWorks administrator, then, has the ability to further define the asset for secure remote access by adding credentials and other meta data required by ConsoleWorks. This process ensures that administrators are always aware of assets as they are added to the network. ConsoleWorks provides the oversight to assist in determining whether it needs to be put under secure remote management for security and compliance purposes.

The amount of information that ConsoleWorks requires is dependent on the ConsoleWorks features used.

Asset, Patch Analysis & Configuration Management – Active Configuration management is a way to reduce or eliminate security, compliance and operational issues resulting from assets that are not properly configured. These gaps occur when changes are not documented, when required changes (such as security patches) are not implemented, when configuration changes are made without approval, and when configuration or firmware change mandates are not implemented on cyber assets. ConsoleWorks addresses key security regulations pertaining to notification of device configuration changes, such as:

- Functional settings that determine how the asset operates
- Versions of software currently installed including BIOS, firmware, operating system, applications, etc.
- Patches, including security patches that are installed
- Ports that are active and how they are configured
- Services that are enabled
- Accounts that exist

ConsoleWorks automates the collection, comparison, alert/notification and auditing of any changes to configurations, eliminating the majority of human errors and minimizing the impact of intentional or unintentional, erroneous activity. The automation built into ConsoleWorks includes the following:

- Collection of the device configuration – ConsoleWorks captures and documents the configuration data from each asset.
- Establishing a specific configuration as the master – Once the configuration is captured, it can be defined as the master (or baseline) and used as the standard for which all other like devices are compared.
- Comparison of the current asset configuration to the master configuration – ConsoleWorks automates the comparison and determines where differences exist.
- Device Patch or Firmware Analysis – ConsoleWorks can be configured, via a schedule to perform patch analysis. Once the current patch state is gathered, ConsoleWorks can integrate with industry or custom solutions to assist in automating the patch gap analysis.

- Event Detection and Alerting of authorized or unauthorized changes – When a difference is detected, ConsoleWorks logs that a configuration check has occurred, and differences were found. ConsoleWorks subsequently Alerts the appropriate personnel of the difference that is found.
- Manual triggering or scheduling of configuration checks – At any time a configuration or firmware check can be manually executed within ConsoleWorks.

Endpoint Password Management & Control – ConsoleWorks automates the ability to change access credentials on endpoints on a schedule or based on the defined security policy / password rules, eliminating the need for a user to know endpoint access credentials. From one centralized location, a user can schedule automatic password changes and set reset date warnings to meet compliance requirements. ConsoleWorks can recover or change a password or export all passwords, securely.


A list of features includes:

- Ability to maintain adequate equipment and system password complexity
- Address password frequency of change
- Ability to detect if vendor passwords exist – notify and change
- The ability for each device to have a unique password
- The ability for groups of devices to have the same password (by substation, type, or any user-defined group)
- Detailed audit information
- Ability to request a device password, securely, in the case of an emergency and then reset after the emergency is over
- Ability to generate reports

ConsoleWorks can be configured to conceal all end point passwords for full automation of this function. In this case, when employees leave or are terminated, simply removing their ConsoleWorks access, prevents them from accessing all endpoints. For further automation, if integrated with Active Directory, once removed from AD, ConsoleWorks automatically reflects that change in ConsoleWorks, providing full automation of that process. As such, it eliminates issues regarding employee termination, role change, etc.

Logging & Situational Awareness – The end-to-end, situational awareness view, provided by ConsoleWorks, helps users understand WHY something went wrong and quickly determine and implement the resolution. During that process, ConsoleWorks captures the exact steps used by an experienced user to remediate an issue and stores it in the knowledge base for future reference and for audit purposes.

- Event Monitoring – ConsoleWorks can monitor and manage almost any application or infrastructure interface – including routers, switches, servers, firewalls, virtual machines, HMI's, PLCs, RTUs, appliances, applications and networks – to provide the most comprehensive record possible. ConsoleWorks watches for messages, or Events, in the data streams of all the assets and applications it manages. When ConsoleWorks detects an Event, it alerts the appropriate personnel in real time, records the circumstances, and automatically performs the default or customer-



configured response(s). Users are able to respond to the asset or application error condition and immediately view the vendor-supplied explanation along with steps required to resolve the issue.

- Log File Aggregation – ConsoleWorks monitors the asset logs in the context of all other managed applications or hardware. Its ability to aggregate error conditions across all log files enables users to view multiple log files, in context, to help in root cause analysis. In many cases, issues have been resolved before other solutions have been notified that an Event has occurred.
- Keystroke Logging and Best Practices – ConsoleWorks captures the steps taken for Event remediation down to the keystroke, enabling any ConsoleWorks user to leverage in-house past experience and acquire proven solutions faster. In this way,
- ConsoleWorks builds the business's data warehouse of intellectual property related to the problem resolution.
- Proof of Compliance – ConsoleWorks produces, aggregates and summarizes audit logs that record user activities, exceptions, and information security events. Log files are digitally secured for each asset, operating system, application, etc. as they are written allowing detection of line deletion, insertion or modification.

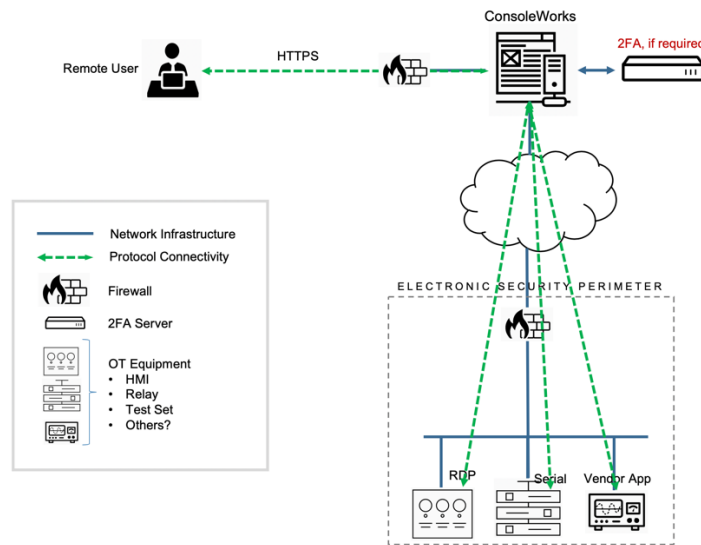
ConsoleWorks Architecture Considerations

Having ConsoleWorks installed in the plants or substations is for environments where the customer does not wish to have a single central instance of ConsoleWorks due to network infrastructure reliability or in cases that the customer has a weather or other event and they wish to have local instances for managing the remote site in an autonomous way, should it be required.

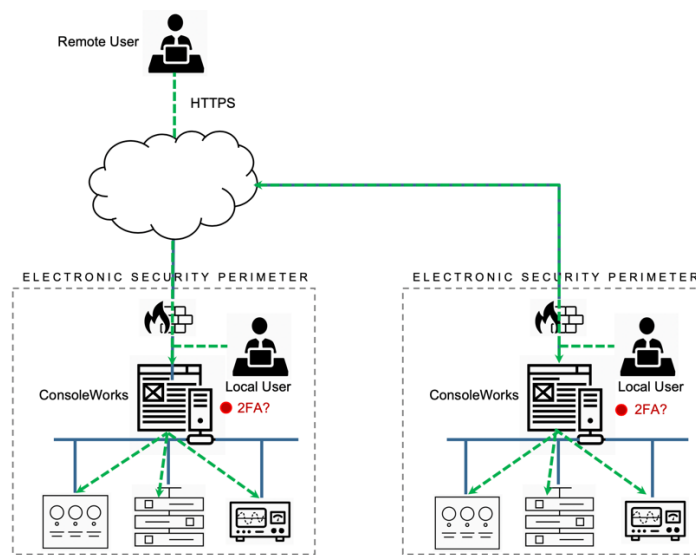
Where ConsoleWorks at the "Central" site is the chosen configuration, it would be used for situational awareness and potentially command and control for assets managed by ConsoleWorks in the remote site. The remote instance of ConsoleWorks is always used to control what the central site or other "Stacked" instances can do. It also controls what information is sent to the central site as well as whether or not the information is anonymized.

Having ConsoleWorks at each site comes at an additional cost but can provide better control in an environment where network reliability is not the best or where bandwidth is an issue. Having a single central site is easier to manage, costs less, but is vulnerable to network outages etc.

Having one or the other is simply a customer business decision and risk tolerance requirement.



Centralized Approach



Distributed Approach

