ConsoleWorks

SECURE REMOTE ACCESS

Secure Remote Access (SRA) makes your IT and OT network more secure. With increases in remote workers and multiple high-profile breaches happening from compromised remote access, SRA reduces the risk to your network and keeps bad actors out.

The ConsoleWorks platform protects unrestricted or unsecured access to your critical assets. Users log into ConsoleWorks, which then makes or brokers the privileged connections to endpoints in your network.

Enforce a Zero Trust security model with ConsoleWorks by giving employees, third-party vendors and contractors just the right amount of access needed, and only when they need it, to do their job based on their assigned role. User access is monitored, logged (keystroke and video capture) and reported to know what is happening when, where it occurred, by whom and their actions taken.

USE CASES

IMPLEMENT ZERO TRUST

Enforce the "least privileged user" approach from Zero Trust and secure access to your most valuable assets with ConsoleWorks.

ALWAYS BE AUDITING

Always be audit ready. ConsoleWorks gives a built-in approach to compliance and audit reporting with consistent, completeness of information.

PROTECT OT OPERATIONS

Protect your OT operations by knowing who is accessing your devices and when, and verify their intent before, during and after they access it.

REMOTE WORKFORCE

ConsoleWorks creates a protocol break between the user and your network. No viruses, malware or ransomware gets through your security perimeter.

tdi

ConsoleWorks

PROTECT YOUR DEVICES

All activity from users, 3rd-party vendors, contractors is logged. Forensic record of activity is generated on assets.	*ConsoleWorks maintains a consistent connection to ensure nothing is missed. No buffers, no polling. Always on.*	*Provides comprehensive security model with granular permissions to give least-privileged access.*

MONITOR YOUR NETWORK DEVICES

SRA is more than just controlling who can access your network. You also want to know what a user did while they accessed it.

ConsoleWorks keeps detailed logs of everything every user does while accessing your endpoints.

- *It uses a "common time stamp" so forensic investigation and root cause analyses has context of what came first.*
- *User inputs are logged down to the keystroke and video of their session is recorded.*

If a user does something he isn't supposed to do, ConsoleWorks acts accordingly and alerts you to what is happening or terminates the connection. This prevents activity of bad actors, but also protects you from more innocuous mistakes.

ONLY SHOW WHAT YOU WANT THEM TO SEE

You control who accesses what, when and for what purpose. A user only has access to your devices when and why you want them to. A contractor servicing a ticket is only allowed into the network during the timeframe given and all access is related to their ticket. A technician only sees his industrial device on the network and can only make changes related to the scope of his work. Your partner only sees parts of the network you want them to see. You control everyone.

REALIZE ZERO TRUST SECURITY

Today's security model is moving away from the "castle and moat" and over to Zero Trust.

ConsoleWorks supports your security models by giving users the least-privileged access needed, only when it's needed.

REALTIME AWARNESS OF YOUR EVENTS

ConsoleWorks gives you complete lifecycle awareness of events in your network. Recognition, notification and remediation. You set event priority and ConsoleWorks keeps you updated as it happens.

PROTECTION
AGAINST YOUR BIGGEST THREATS

ConsoleWorks

PROTECT AGAINST VIRUSES, MALWARE AND RANSOMWARE

ConsoleWorks sits between the user and your IT or OT assets that you are protecting. The privileged user connects to ConsoleWorks through a standard web browser using HTTPS.

This creates a protocol break giving the security needed to proactively protect against viruses, malware or ransomware.

Then ConsoleWorks makes the connection of the user to the endpoint using its native protocol. No user ever directly connects to your endpoints in your environment.

PROTECT YOUR PASSWORDS

Compromised credentials are one of the easiest and most common methods used to gain access to a network. Often, passwords are shared between contractors, vendors and within departments. This compounds the vulnerability for easy entry by a bad actor into your network's most critical endpoints.

ConsoleWorks' SRA means users only log into ConsoleWorks using their specific credentials. Users will never know the passwords to your network's devices. Access to endpoints is always managed and authenticated by ConsoleWorks.

The overhead of password and user management is now simplified. User access is easily managed by admins in ConsoleWorks and the headaches of password rotations across devices and individuals are gone.

WHAT SECURE REMOTE ACCESS LOOKS LIKE

PROTOCOL BREAK

Privileged users connect to ConsoleWorks. ConsoleWorks brokers the connections to your devices in your IT/OT network, protecting you from viruses, malware or ransomware.

ZERO TRUST SECURITY

Enforcing the least-privileged access model is easy. ConsoleWorks empowers you to give your users only the level of access they need, only when they need it.

MONITORING

Configure your own alerts. If a connected user performs an action against their purpose for connecting, you are notified or the user session is terminated immediately.

SITUATIONAL AWARENESS

Know which users are connected to what devices and what they are doing. Sessions are recorded and keystrokes are logged with a universal time stamp. You are never in the dark.

WHAT SECURE REMOTE ACCESS LOOKS LIKE

MINIMIZE OPERATIONAL DISRUPTIONS & MEAN-TIME-TO-REPAIR

- *Agentless Monitoring*
- *Scalability*
- *Heterogenous deployment*
- *Security*
- *Log File Security*
- *Audit & Compliance Reporting*
- *Session Management*
- *Command Control*
- *Intelligent Event Modules*
- *Event Management*
- *Automated Actions*
- *Event Rememdiation*
- *Log Forwarder*
- *Multiple User Engagement*
- *Logical & Hierarchical Grouping*
- *Multi-connect*
- *Multifactor Authentication*

- *Secure Role-Based Access for asset-specific, task-based, user privileges*
- *Agentless, persistent monitoring ensuring no gaps to your monitoring occur*
- *Capture complete recordings, with full playback capabilities for user sessions across RDP/VNC and web applications.*
- *Scanning of incoming data stream for pre-defined text patterns, such as failed login attempts*
- *All logins, logoffs and failed login attempts are captured, logged and alerted*
- *All changes – down to the keystroke – are captured, logged and alerted*
- *Complete intelligence gathering, including source and account IDs, incident context and commands executed and their results.*
- *Centralized command and control for physical, logical and virtual console connections, Syslog messages, SNMP traps and other streams of information*

- *Connected secured using SSL and SSH encryption*
- *All asset activity logs digitally secured for easy detection of modifications*
- *Color-coded logs from different information sources facilitating drill-down analyses in aggregated log views*
- *Event consolidated from all data sources using a common time stamp, independent of asset vendor or type*
- *Sub-second timeframe for insightful granularity*
- *Multiple users granted simultaneous remote access to a single asset*
- *Integrated incident recognition and response*
- *Complete event lifecycle management: Recognition, notification, remediation*
- *Prioritize events by severity, 100 percent customizable by users*
- *Realtime, customizable graphs and charts for NERC CIP audit reporting and business intelligence*

PEOPLE · DEVICES · ACCESS

One Platform. One Path.

TDi Technologies is the first solution provider to offer a unified system for cybersecurity/operations. Our patented technology provides flexibility, automation, optimization, control and management capabilities that dramatically improve the ability to meet operational and security demands.

We have a diverse, global customer base serving key verticals such as Financial Services, Healthcare, Telecom, Utilities, and Government in both the Tier 1 and Tier 2 markets in North America and Europe. Our solution helps customers reduce operating costs, meet compliance requirements, and improve service delivery.

TDi Technologies' headquarters are in Plano, Texas. We have been recognized as a high-growth technology company numerous times, receiving the Deloitte Technology Fast 50 award, the Texas Crescent Fast 50, Dallas Business Journal Fast Tech 50, and Tech Titans DFW Technology Fast 50.