BASELINE CONFIGURATION MONITORING

ConsoleWorks

Protecting your network from threats and vulnerabilities is critical, but how can you do this effectively if you don't know the true status of your devices or if changes to them have occurred? Configuration monitoring reduces and eliminates the security gaps that leave you vulnerable to cyber attacks.

ConsoleWorks identifies and validates your devices by talking to them in their native protocol. Its agentless automation lets you check them against your baselines as often as you want to or need to, saving both time and money, and simplifying the process of auditing your environment.

Automate the collection, comparison, alerts and auditing of configuration baselines, eliminating the majority of human errors and minimizing the impact of intentional or unintentional erroneous activity that makes your assets vulnerable.

USE CASES

SET A GOLDEN IMAGE

Prevent configuration drift by setting a golden image to automatically compare your devices against.

Know where all your devices are. Know how they are configured. Know if they are out of compliance.

VALIDATE YOUR DEVICES

IDENTIFY THREATS

Catch serious threats like malicious configurations during an attack or catch other threats like silent installs.

Run compliance audits on your assets automatically, in the device's native protocol without the need for an agent.

COMPLIANCE AUDITING

tdi

STAY COMPLIANT

ConsoleWorks enables automatic auditability of your environment, ensuring that your configuration is compliant. As often as you want, ConsoleWorks retrieves all configuration details about your assets and devices to build reports for audits. All endpoint activity is logged in ConsoleWorks, so proof of compliance is as easy as running a report to show when verification checks were run, what differences were found on the devices and acknowledged, and how these changes took place.

CUT THROUGH THE NOISE. VALIDATE WHAT IS REAL.

Many challenges arise around knowing what is happening in the field. Even if you get a tool to run asset discovery, there can be so much noise around those associated IPs, that it is hard to know what is real. ConsoleWorks cuts through this noise and validates your assets. Know exactly how many devices you have in your network, know where they are and know how they are configured.

AGENTLESS EFFICIENCY

The larger your fleet, the longer it takes to verify your devices are configured as they should be. ConsoleWorks talks to your devices in their native protocol automatically, reporting back patch levels, configuration and if it's the right device at the correct IP address. This whole process is fast and agentless, saving you money and giving back time to your most important asset: your people. No more rolling a truck out to a location, manually verifying information, driving back and uploading everything.

HACKERS ARE NOT YOUR ONLY THREAT

ConsoleWorks protects you from external threats. Though malware or a bad actor may reconfigure a device to suit their malicious intent, there are many factors in your environment that could result in the configurations of your assets changing. While you may be focused on preventing an attack, ConsoleWorks is focused on everything. As devices in your environment are replaced, reconfigured based on user preferences or machines silently install new software, ConsoleWorks will alert you to changes of devices against your baselines.

AUTOMATED PATCH ANALYSIS

The "every 35-day analysis" required from the NERC CIP-007-6 / R2 patch management process is a task requiring many man hours. With ConsoleWorks, this whole process is made easy. ConsoleWorks can run this analysis for you every 35 days, producing dashboards and summary reports of the status of your environment, the patch gaps that exist, and the location to download the patch.

ConsoleWorks integrates with workflow management solutions to provide these automated processes and mitigation policies required by NERC.

ConsoleWorks

SECURE CYBERSECURITY OPERATIONS PLATFORM

To work on your devices and keep them updated and configured properly, you must connect to them. ConsoleWorks does more than monitor the configurations of your network's devices, it is a true cybersecurity operations platform.

Least-privileged, Secure Remote Access – ConsoleWorks keeps your IT and OT networks more secure by protecting unrestricted or unsecured access to your critical assets. User access stops at the front door of ConsoleWorks, which manages the privileged connections to endpoints in your network. Only show users devices in your network that you want them to see and only allow them to perform actions on those devices that you want them to.

Beyond Zero Trust – ConsoleWorks innately enforces a Zero Trust security architecture and then goes beyond it, giving you greater insights into what is happening on your network, automating important security functions like password management and compliance activities, reduces your footprint on endpoints and gives you greater insight into who is doing what on your network and devices by capturing activity down to the keystroke.

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.

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.