ConsoleWorks

Cybersecurity | Operations Platform

YOUR CHALLENGES ARE **DIFFERENT...**

The power of one solution provides a unified security approach for consistent insight, reliability and responsiveness to IT/OT cybersecurity and operational challenges facing today's industries.

One Platform. One Path.

PRIVILEGED INTERACTIVE ACCESS

ConsoleWorks provides a secure, persistent connection to streamline access and control to any device for privileged users. The solution is always monitoring, auditing and logging activity down to the keystroke to support regulatory, cybersecurity best practices and IT/OT operations while providing a staunch defense against access by unauthorized users.

ConsoleWorks is unique because the platform sits between the privileged users and the assets they interact with, enabling the ability to automate activities like configuration monitoring, password management and other cybersecurity and operations functions using the assets' native language.

SECURITY & OPERATIONS KEY FEATURES

» Secured Role-Based Access Control for asset specific, task-based, user privileges

» Agentless, persistent monitoring ensuring no gaps in monitoring

» Capture recording and playback capabilities for user sessions, across RDP/VNC and web applications

» Scanning of incoming data streams for pre-defined text patterns such as failed login attempts

» All log-ons, log-offs, and failed log-on attempts are captured, logged, and alerted

» All privileged user activities and resulting system responses, down to the keystroke, are captured logged and alerted

» Multiple users can be granted simultaneous access for collaboration regarding remediation.

» Centralized command control through whitelisting and blacklisting

» Direct access to the 'leaf' device, automating the navigation through the hierarchy of assets to the endpoint

ASSET, PATCH & CONFIGURATION MONITORING

ConsoleWorks automates the collection, comparison, alert/notification and auditing of any changes to configuration baselines, eliminating most of the human errors.

ConsoleWorks can be configured to monitor functional settings that determine how the asset operates. The solution can monitor versions of installed software including BIOS, firmware, operating systems, applications and patches, including installed security patches. Active ports and listing services are also monitored within the platform.

SECURITY & OPERATIONS KEY FEATURES

Automate Asset Configuration Retrieval, Establish Baseline & Current Asset Comparison
ConsoleWorks can manually trigger or automate scheduling of baseline checks. It captures, documents and secures the configuration data programmatically.

Automate Event Detection and Alerting of Unauthorized Changes
When a difference is detected, ConsoleWorks logs that a configuration check has occurred, and differences were found. It alerts the appropriate personnel or can automate the generation of a trouble ticket.

Secure Logs for Compliance Reporting and Forensic History
All activity, down to the keystroke, is logged in ConsoleWorks for compliance reporting. The report includes the dates and times that the configuration checks were run and when differences were found and acknowledged.

Automated Patch Analysis
ConsoleWorks can be configured, via a schedule to perform patch analysis. After the current patch state data is gathered, integration with industry or custom solutions provides automated patch gap analysis.

LOGGING & SITUATIONAL AWARENESS

ConsoleWorks acts in a multi-dimensional fashion by monitoring, not only applications, but also servers, virtual machines, networks, and storage devices that support them. It provides managers and administrators an end-to-end management solution that controls system access, monitors and manages all log files and watches for specific events that may occur across the organization.

Monitoring is done in real-time and in all machine states—power on, single user, maintenance, production and failure modes. Its persistent connection also locks down the "back door" entrances that are overlooked by similar, agent-based solutions.

The end-to-end view helps administrators understand WHY something went wrong and quickly determine and implement the resolution. During the process, ConsoleWorks captures the exact steps used by an experienced administrator to remediate an issue and stores it in the knowledge base for future reference.

SECURITY & OPERATIONS KEY FEATURES

Log File Aggregation
The aggregation of all log files enables administrators to view multiple log files, in context, to help in root cause analysis.

Common Clock
A patented timestamp format to include year, month, day, hour, minute, second and sequence number within a second.

Keystroke Logging and Best Practices
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.

Proof of Compliance & Reporting
Aggregates and summarizes audit logs that record user activities, exceptions, and information security events. Log files are digitally signed for each device as they are written, allowing detection of line deletion, insertion or modification for operating system, applications etc. as they are written allowing detection of line deletion, insertion or modification.

PASSWORD MANAGEMENT

ConsoleWorks automates the ability to change access credentials on endpoints on a schedule, based on the defined security policy/password rules, eliminating the need for a privileged 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 standards. ConsoleWorks can recover or change a password or export all passwords, securely.
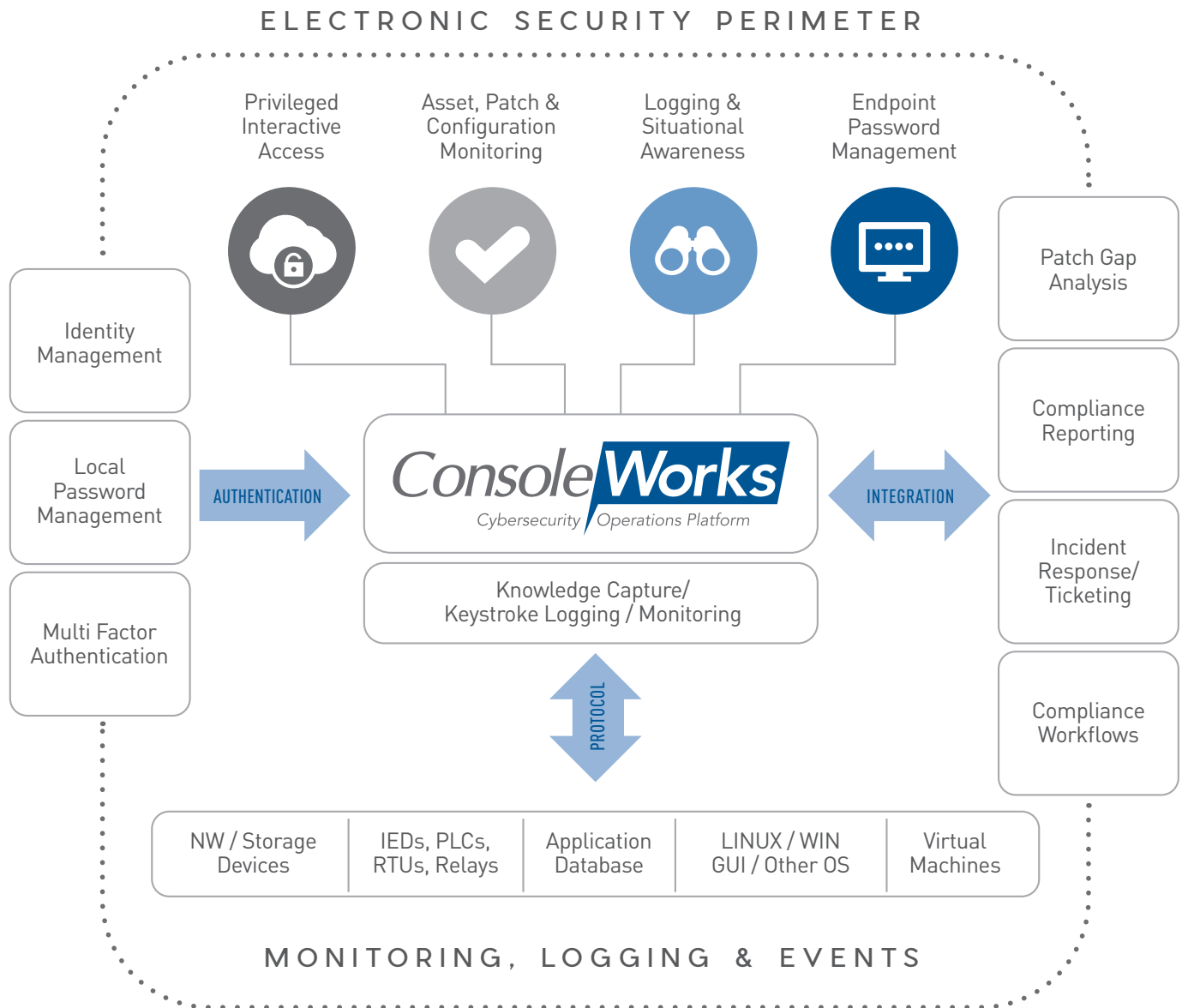
SECURITY & OPERATIONS KEY FEATURES

» The ability for each device to have a unique (or same) password

» Access Control Rules controls which roles (Profiles) can access features

» Flexible password complexity

» Detailed audit information

» Control of the password update frequency

» Ability to securely recover a device password

» Ability to generate reports

ConsoleWorks can be configured to conceal all endpoint passwords for full automation of this function. Where full automation is not a requirement, ConsoleWorks can support that as well. As such, it eliminates issues regarding employee termination, role change, or ease of building access termination.

ConsoleWorks
Cybersecurity Operations Platform

PEOPLE • DEVICES • ACCESS

QUICK ANSWERS TO COMMON QUESTIONS
TDITECHNOLOGIES.COM/FAQS

ELECTRONIC SECURITY PERIMETER

Privileged Interactive Access

Asset, Patch & Configuration Monitoring

Logging & Situational Awareness

Endpoint Password Management

Identity Management

Local Password Management

Multi Factor Authentication

AUTHENTICATION

ConsoleWorks
Cybersecurity / Operations Platform

Knowledge Capture/ Keystroke Logging / Monitoring

INTEGRATION

PROTOCOL

Patch Gap Analysis

Compliance Reporting

Incident Response/ Ticketing

Compliance Workflows

| NW / Storage Devices | IEDs, PLCs, RTUs, Relays | Application Database | LINUX / WIN GUI / Other OS | Virtual Machines |

MONITORING, LOGGING & EVENTS

TDi Technologies
1600 10th Street, Suite B | Plano, TX 75074

TDi Technologies, the TDi Technologies logo and the ConsoleWorks logo are registered trademarks of TDi Technologies, LLC.