

03 · ENFORCE — SECURE REMOTE ACCESS

Controlled Access to Every Critical Device — for Everyone Who Connects

Engineers, contractors, vendors, and remote workers all need access to critical devices. Each connection is a risk. ConsoleWorks Secure Remote Access (SRA) gives operations teams direct, monitored, session-recorded access to specific devices — enforcing Zero Trust principles at the connection level, with full control over who connects, when, and to what.

0 Agents

Nothing installed on managed devices

100% Capture

Every privileged access session recorded

Every Protocol

SSH, Telnet, serial, PowerShell, RDP, VNC

THE CHALLENGE

Every Connection Is a Risk That Must Be Managed

Remote and third-party access to critical devices is unavoidable — but often ungoverned.

- Engineers, contractors, and vendors each require access to critical devices — with no consistent enforcement of who gets in or what they can do.
- Traditional VPN approaches grant broad network access — the opposite of Zero Trust, and far exceeding what any individual connection requires, leaving lateral movement paths open.
- Session activity is rarely captured in a way that supports compliance review or incident investigation.
- Credential sharing among field teams is common — making activity attribution after an incident difficult or impossible.
- Access provisioning and deprovisioning is a manual, error-prone process that frequently leaves stale access in place.

**Most organizations know a vendor was on the device.
Few know what they did while they were there.**

THE SOLUTION

Know Who Connected. Know What They Did.

At the core of SRA is a protocol break architecture. Two separate sessions are established — one from the user to ConsoleWorks, and one from ConsoleWorks to the target device. The user never has a direct network path to the device. ConsoleWorks sits in the middle, enforcing policy, recording every interaction, and maintaining the complete audit trail. This architecture applies Zero Trust at the session layer — eliminating shared credentials, preventing lateral movement, and ensuring every access event is attributed to a specific identity.

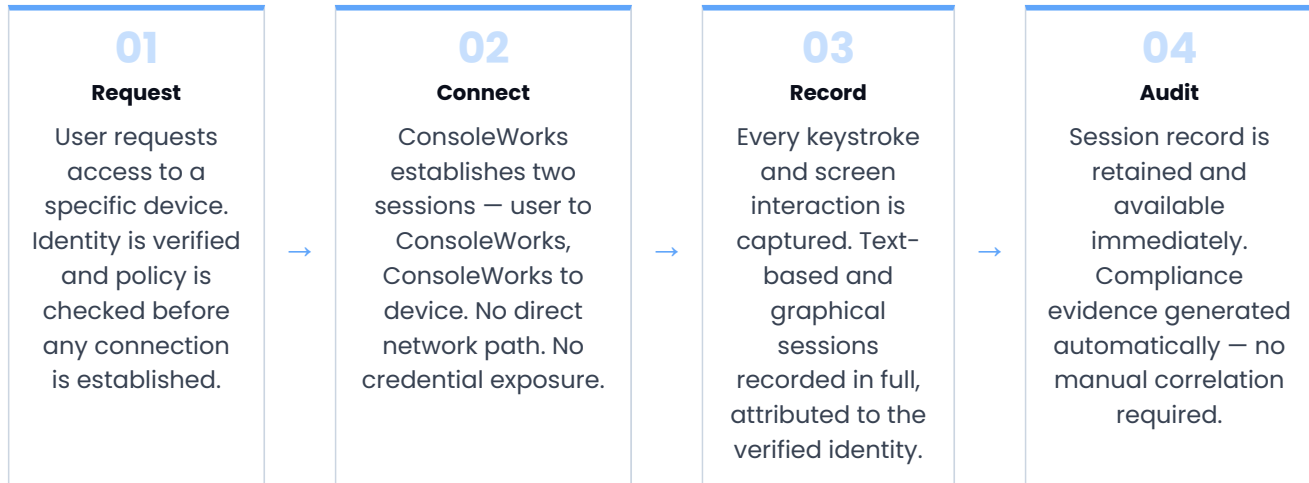
SRA works across text-based protocols — SSH, Telnet, serial, PowerShell — and graphical protocols including RDP, VNC, and web. Every session is captured in full, tied to a verified identity, and retained as audit-ready evidence. Operations teams have a complete record of every privileged access event across every device in the environment.

ConsoleWorks SRA directly connects authorized users to the specific device they need — and only that device. This is least privilege in practice: access scoped to exactly what the user requires, nothing more. Access is controlled, monitored, and fully recorded for every connection, regardless of protocol. No broad network exposure. No shared credentials. No blind spots.

ConsoleWorks SRA is the only access solution built specifically for the protocol and operational requirements of critical infrastructure — covering every device, every user, every session.

HOW SRA WORKS
The Protocol Break Architecture

Every connection request passes through ConsoleWorks before it reaches the device. Two separate sessions are established – one from the user to ConsoleWorks, and one from ConsoleWorks to the target device. The user never has a direct network path to the asset. ConsoleWorks sits in the middle, enforcing access policy, capturing every interaction, and maintaining the complete audit trail from the moment a session begins to the moment it ends.



Traditional PAM tools manage credentials. ConsoleWorks SRA enforces Zero Trust at the session layer – controlling, recording, and auditing every connection with device context, asset records, and compliance mapping already built in.

WHAT THIS DELIVERS
Control, Visibility, and Accountability – for Every Connection

The result is a single, consistent access layer that applies equally to an engineer on the corporate network, a contractor connecting remotely, or a vendor accessing a device in the field. Zero Trust is enforced at the connection level – not assumed at the perimeter. Security teams get a complete, attributable record of every privileged connection. Operations teams get enforcement without disruption. Compliance teams get audit evidence that is generated automatically – not assembled after the fact. Each capability below is a function of that unified layer, not a separate tool bolted onto an existing access model.

Direct Device Connection

SRA connects users directly to their authorized device – not to a network segment. Least privilege is enforced at the connection level: access to one device, for one session, for one verified identity.

Full Session Recording

Every privileged session is recorded – text-based and graphical protocols. Complete session capture provides the audit trail required for compliance and incident response.

All Connecting Parties

Engineers, contractors, vendors, and remote workers all connect through the same controlled access layer – consistent policy enforcement regardless of who is connecting.

Credential Governance

Individual, attributed access replaces shared credentials. Every session is tied to an identity – supporting operational accountability and compliance requirements.

WHY CONSOLEWORKS SRA
Built for the Complexity of Critical Infrastructure

Standard privileged access management tools were designed around familiar IT assumptions — managed credentials, known users, and standard protocols. Critical infrastructure environments introduce greater complexity: legacy devices, mixed protocols, third-party vendor access, and compliance frameworks that demand a complete, attributable record of every session. ConsoleWorks SRA was built to meet those requirements across IT and OT environments alike.

Standard PAM / VPN	ConsoleWorks SRA
<p>Network or system-level access — broad exposure. Limited protocol coverage. Partial or no session recording. No link to asset inventory. Audit evidence requires manual assembly. High lateral movement risk from broad network grants.</p>	<ul style="list-style-type: none"> ✓ Device-level access — specific, enforced. ✓ Full protocol coverage — SSH, Telnet, serial, PowerShell, RDP, VNC. ✓ Complete session capture on every connection. ✓ Every connection tied to a known, classified asset. ✓ Compliance-ready records mapped to your frameworks. ✓ Lateral movement eliminated. ✓ Zero trust enforced at the session layer — not assumed at the perimeter.

Integrated with Asset Intelligence

SRA is connected to the ConsoleWorks asset inventory. Every connection is granted to a known, classified device — not an anonymous IP address. Access governance and asset governance are unified.

Compliance Evidence Without Extra Work

Session recordings and access logs are automatically mapped to NERC CIP, NIST, IEC 62443, SOC 2, and other framework requirements — audit evidence is a byproduct, not a separate effort.

SRA AND THE PLATFORM
Access That Connects to Everything Else

ConsoleWorks SRA does not operate in isolation. Because ConsoleWorks holds the asset record, the configuration baseline, the measurement state, and the event history for every managed device, every SRA session is enriched with the full context of the device being accessed — whether it's a server, a network device, or a field controller. When a vendor connects, ConsoleWorks already knows the device's classification, its current measurement status, and its configuration baseline — before the session begins.

When the session ends, ConsoleWorks captures not just the session record but the before-and-after configuration state via CCM — producing a complete picture of what was accessed, what changed, and who was responsible.

SRA CONNECTS TO THE FULL CONSOLEWORKS PLATFORM

<p>Asset Record</p> <p>Every session tied to a known, classified device — vendor, firmware, criticality, and compliance obligations visible before connection.</p>	<p>Config Baseline</p> <p>Before-and-after configuration capture via CCM — every session shows exactly what changed and who made the change.</p>	<p>Event Detection</p> <p>IEM monitors for anomalous session behavior — unauthorized commands, policy violations, and out-of-window access flagged automatically.</p>	<p>Compliance Evidence</p> <p>Session records auto-mapped to NERC CIP, NIST, IEC 62443, SOC 2, and other frameworks — audit-ready without additional effort.</p>
---	---	--	---