

# Privileged Remote Access

## Close Your Biggest NERC CIP Gaps with Privileged Remote Access

NERC CIP standards are tightening ahead of the April 1, 2026 enforcement date (Source: <https://www.nerc.com/standards/reliability-standards/cip/cip-003-9>), and utilities must be able to prove exactly who accessed Bulk Electric System (BES) Cyber Systems, when, why, and under what approvals. However, most organizations still rely on legacy VPNs, shared credentials, and unmanaged vendor access, all of which create blind spots that auditors flag as high-risk. These gaps also increase exposure to ransomware, identity misuse, and unauthorized lateral movement across OT and IT environments.

BeyondTrust's Privileged Remote Access provides a secure, auditable, and least-privilege approach to all remote access into critical infrastructure. Eliminate standing credentials, route access through policy-based controls, and record every privileged session for full oversight. The product also supports segmented OT networks, air-gapped designs, and strict approval workflows.

With Privileged Remote Access, SMB utilities, electric cooperatives, transmission operators, and other Bulk Electric System (BES)-connected organizations can strengthen NERC CIP readiness—without slowing operations.

## Key Security Outcomes

### Control Remote Access to Critical BES Assets

Broker all privileged remote access through a secure, monitored gateway. This removes unmanaged VPNs, limits direct network exposure, and enforces consistent controls across staff and third parties. Access into BES environments stays segmented, authorized, and fully visible, reducing risk and demonstrating that remote connectivity is governed and controlled.

### Enforce Strong Authentication & Just-In-Time Permissions

Tie every privileged session to a verified identity and time-bound access. Multi-factor authentication, role-based permissions, and approval workflows ensure users receive only the access they need for the task. This reduces standing privileges, prevents credential misuse, and strengthens governance across all privileged accounts.

### Monitor, Record, and Retain All Privileged Activity

Capture full session activity like keystrokes, commands, and file transfers, with tamper-proof logs. Security teams gain a clear, re-constructable record of who did what and when, simplifying audits, supporting incident response, and ensuring privileged activity within BES environments is fully visible and accountable.

## Client Success Stories

"I'm proud to say that at this point, we don't have a single third party with VPN access to our network. That's important because we have people that rely on our services every single day and for them to be able to access those services while reducing our overall risk, we put ourselves in a long-term position for success."

— Chris Hardy, Chief Information Security and Technology Officer, Town of Truckee.

## Town of Truckee Benefits:

- **Efficient Provisioning:** Privileged Remote Access enables the team to avoid unnecessary provisioning, streamlining IT operations
- **Cost Savings:** The team saves ~\$10,000 in hardware costs and \$5,000 in licensing fees annually
- **Enhanced Security Measures:** Third-party VPN access has been eliminated, ensuring secure access for employees and external agencies

**Simplify NERC CIP compliance and secure every privileged session with BeyondTrust Privileged Remote Access**

**Start your free trial or request a demo at: [beyondtrust.com/products/privileged-remote-access](https://beyondtrust.com/products/privileged-remote-access)**