BeyondTrust | FOR PUBLIC SECTOR

GOVERNMENT SOLUTIONS

State and Local Critical Infrastructure Security

Privileged Remote Access for mission essential IT and OT environments

State and local governments sit at the center of critical infrastructure outcomes. In many jurisdictions, they own and operate essential services like water and wastewater systems, emergency services, dams, and transportation operations. Even when they do not own the physical asset, they provide enabling services that determine resilience, including identity services, network services, third-party access governance, procurement, and incident response coordination.

Critical infrastructure is also increasingly cyber physical. The "critical" service is often delivered through operational technology, the systems that monitor and control physical processes across utilities, transportation, facilities, and life-safety environments. As OT adopts more connectivity and remote access, old assumptions about isolation keep fading.

This shift changes the threat equation. Many disruptive incidents begin with access. Threat actors look for exposed remote services, weak authentication, default credentials, shared accounts, reused passwords, and vendor pathways built for convenience instead of accountability. When access persists, attackers persist.

Solution Benefits

1) Govern privileged remote access end to end:
Access is time bound, scoped to the task, and tied to a real identity so teams can prove control across operators, admins, and vendors.

2) Support OT segmentation without widening exposure:
Enable point to point access into OT zones and constrained environments without making broad network connectivity the default operating model.

3) Reduce credential risk at the session level:
Use just in time access, RBAC, per session MFA, and credential injection to limit misuse and shrink the paths attacker use.

4) Standardize third party access across distributed sites:
Apply consistent policy and oversight for integrators, contractors, and vendor teams that support many facilities and maintenance windows.

5) Make investigations and oversight faster
Evidence is ready when leadership asks. Session proof stays consistent and complete, so teams are not stuck rebuilding events from scattered logs.

Key Outcomes

Faster restoration during outages and time-sensitive maintenance

Operators and specialists can reach the right systems quickly, even across segmented environments and remote locations. Fewer brittle workarounds show up when time is tight.

Fewer "temporary exceptions" that become permanent exposure

Access stops living as standing privileges and shared accounts that linger for months. Requests are time bound, scoped, and easier to review, which helps prevent lingering pathways that attackers can reuse.

Reduced blast radius when an identity is compromised

Privileged access stays constrained to approved systems and approved actions. That containment matters in OT-adjacent environments where lateral movement can quickly turn into service impact.

Clear accountability for contractors and third parties

Third-party access becomes easier to govern across sites and systems. You can answer the hard questions quickly: who accessed what, when they accessed it, and what they did.

Address security and compliance expectations

Rely on a secure remote access approach that supports common public sector requirements, including NIST guidance and state-level audit expectations. FERPA, FedRAMP, NIST CSF 2.0, CMMC, TX-RAMP and more.

BeyondTrust | FOR PUBLIC SECTOR

GOVERNMENT SOLUTIONS

Critical Infrastructure Security Mission Alignment

Keep essential services running under pressure

When water, transportation, emergency services, or facilities systems are disrupted, the community feels it immediately. Operational continuity is the mission.

Support distributed operations with limited staff

Many teams cover dozens or hundreds of sites. Remote access has to work reliably without creating a permanent new attack surface.

Treat vendor access as a reality, not an exception

Integrators and OEM specialists are part of day-to-day operations. Governance has to be built in, not bolted on after something goes wrong.

Align to Zero Trust goals without slowing response

Access decisions should be scoped, attributable, and consistent, even during urgent maintenance windows and incident response.

Be ready to explain what happened

Oversight follows disruption. State and Local teams need session-level proof that stands up to review without weeks of manual reconstruction.

Why State and Local Governments Choose BeyondTrust

State and local teams choose BeyondTrust when they need secure remote access that fits real critical infrastructure conditions. OT environments are specialized, distributed, and often constrained by segmentation and uptime requirements. Vendor access is constant. Outages are high consequence.

BeyondTrust helps agencies turn remote access into a governed, time bound, fully attributable capability that supports operations while reducing disruption risk and reduces risk from an attack. It also gives leaders the evidence they need for oversight, incident review, and accountability, without forcing teams into manual work during the moments that matter most.

Critical Infrastructure Identity Security Features

- Outbound only, session governed connectivity that limits exposure and avoids inbound access dependency
- Point to point access to sensitive systems, including segmented and non-routable OT environments
- Per session MFA and role based controls to enforce identity at the moment of privileged access
- Credential injection and controlled workflows to reduce shared accounts and password exposure
- Full session recording and detailed metadata to strengthen oversight, investigation readiness, and accountability.

Take the Next Step

Contact us: beyondtrust.com/public-sector

Learn More:

https:/https://www.beyondtrust.com/solutions/industry/critical-infrastructure-us-public-sector

FedRAMP | TX-RAMP CERTIFIED | GOVRAMP MEMBER