COHESITY

PUBLIC SECTOR:

When identity fails, mission-critical services stop

Half of public sector attacks begin with compromised credentials.

Identity is the attack vector

Public sector organizations face unique vulnerabilities that expand their identity attack surface:

- **Legacy infrastructure:** Decades-old Active Directory environments with accumulating misconfigurations and attack paths. Bad actors know this and target AD specifically. In fact, Cohesity's CERT team finds that 95% of security incidents involve AD.
- **Underfunded IT security:** Limited budgets restrict cyber defenses while threat actors grow more sophisticated
- **Public-facing services:** Expansive digital footprint with citizen portals, payment systems, and records access creates multiple entry points
- **Compliance constraints:** CISA guidelines and data retention requirements expand exposure to identity-based attacks

Public sector case study

St. Paul, Minnesota: State capital shut down by Active Directory attack (July 2025)

Target: St. Paul is the state capital of Minnesota that has a population of roughly 300,000.

Attack Vector: Interlock ransomware gang infiltrated St. Paul's network around July 20, 2025, deploying SystemBC remote access trojan. For 5 days, attackers moved laterally through the identity infrastructure—compromising credentials, escalating privileges, and mapping Active Directory before deploying ransomware on July 25.

Business Impact:

- Full network shutdown on July 28: All 3,500+ city employees locked out of systems
- State of emergency declared: Minnesota National Guard's 177th Cyber Protection Team deployed—first in-state deployment in unit's 8-year history
- 43GB of employee data stolen and published on dark web leak site
- Over 30 days to restore core services: Phone systems, water bill payments, library systems offline for weeks
- Enterprise-wide password reset: Manual security checks for 3,500+ devices and employee accounts

Cohesity Identity Resilience:
Detect, withstand, and recover from identity-based attacks

Detect	Continuously monitor and harden AD and Entra ID against identity threats and vulnerabilities with threat intelligence from leading identity security experts. Reduce attack likelihood by 25% while spending 40% less time monitoring.
Withstand	Automate rollback of malicious and suspicious identity changes to prevent compromise. Protect AD and Entra ID data with immutable, hardened backups. Simplify identity recovery testing to meet RTO objectives and enhance readiness.
Recover	Fast, automated, malware-free AD forest recovery and Entra ID with a few clicks for 90% faster recovery. Advanced post-breach forensics that speed remediation and prevent follow-on attacks and validate trust in your identity systems.

How identity compromise affects the public sector

Active Directory isn't just IT infrastructure—it's the foundation of public safety and civic operations. When identity systems fail, critical services immediately stop:

- 911 dispatch systems: Computer-aided dispatch (CAD) reverts to manual radio and phone—dispatchers write instructions by hand
- Court operations: All hearings, trials, jury duty canceled—no citation payments accepted
- Permit and licensing systems: Building permits, business licenses, inspections halt
- Public records access: FOIA requests, property records, marriage licenses unavailable
- Payroll processing: Employee payments delayed, manual workarounds required
- Utility billing: Water, sewer, waste management payments offline with citizens accumulating unpaid balances
- Internal operations: anything from email, file access, to business applications and more

Cost of downtime: $2.7M in lost labor and revenue. Without identity resilience, recovery can take weeks.

Is your identity infrastructure resilient?

- ✓ Have you tested and proven that you can meet your identity recovery RTOs after a cyber-incident in the last 90 days?
- ✓ Do you have immutable backups of AD and Entra ID?
- ✓ Can you detect identity-based attacks (Golden Ticket, DCSync) and automatically remediate them in real-time?
- ✓ Can you validate that your identity recovery is malware-free?
- ✓ Can you perform recoveries without internet access?

If you answered "no" to any of these, your business is at risk.

Get a free identity security assessment today.

Contact your Cohesity rep to schedule a no-obligation assessment of your identity security posture.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

9100106-002-EN 6-2026