Silverfort

Solving key identity security challenges in state and local government with Silverfort

The state and local government sector continues to be a significant target for ransomware and data breaches. In 2024, 34% of U.S. state and local government organizations reported being hit by ransomware attacks. However, the financial impact of these attacks has intensified. The average recovery cost for affected entities more than doubled, reaching $2.83 million, up from $1.21 million in 2023.

Ransomware attacks often exploit compromised credentials, allowing threat actors to infiltrate and navigate government networks undetected. The continued reliance on outdated legacy systems and custom-built on-prem applications often lacks modern security controls. This creates critical blind spots that threat actors can exploit with ease.

Without proper security controls, state and local governments remain at risk of significant security challenges, especially against identity-based attacks that utilize compromised credentials.

What makes the government sector a key target for identity threats?

Authentication to legacy servers

Active Directory authenticates to legacy servers with NTLM and Kerberos which does not support MFA, leaving them open to malicious access with compromised credentials.

Securing Third-Party and Vendor Access

Governments often rely on external vendors and contractors, but lack of strict identity security controls and for these users creates additional exposure.

Limited Visibility into non-human-identities

Despite the critical role NHIs play in every environment, they suffer from extremely low visibility, exposing them to compromise and lateral movement.

How Silverfort solves identity security challenges in the government sector

Secure authentication to legacy servers

All user access requests are forwarded to Silverfort via its native integration with Active Directory. This includes authentications made via NTLM and Kerberos, so legacy servers can be protected with MFA.

Access Policies for Third-Party and Vendor Accounts

Silverfort enforces access policies and MFA for third-party and vendor accounts across all systems, blocking unauthorized access through real-time login verification.

Full NHI visibility and security

Silverfort automatically identities all NHI within the environment and offers the identity and security teams the tools to secure them based on each account's behavior.

Learn more about how Silverfort helps state & local government solve their key identity security challenges.