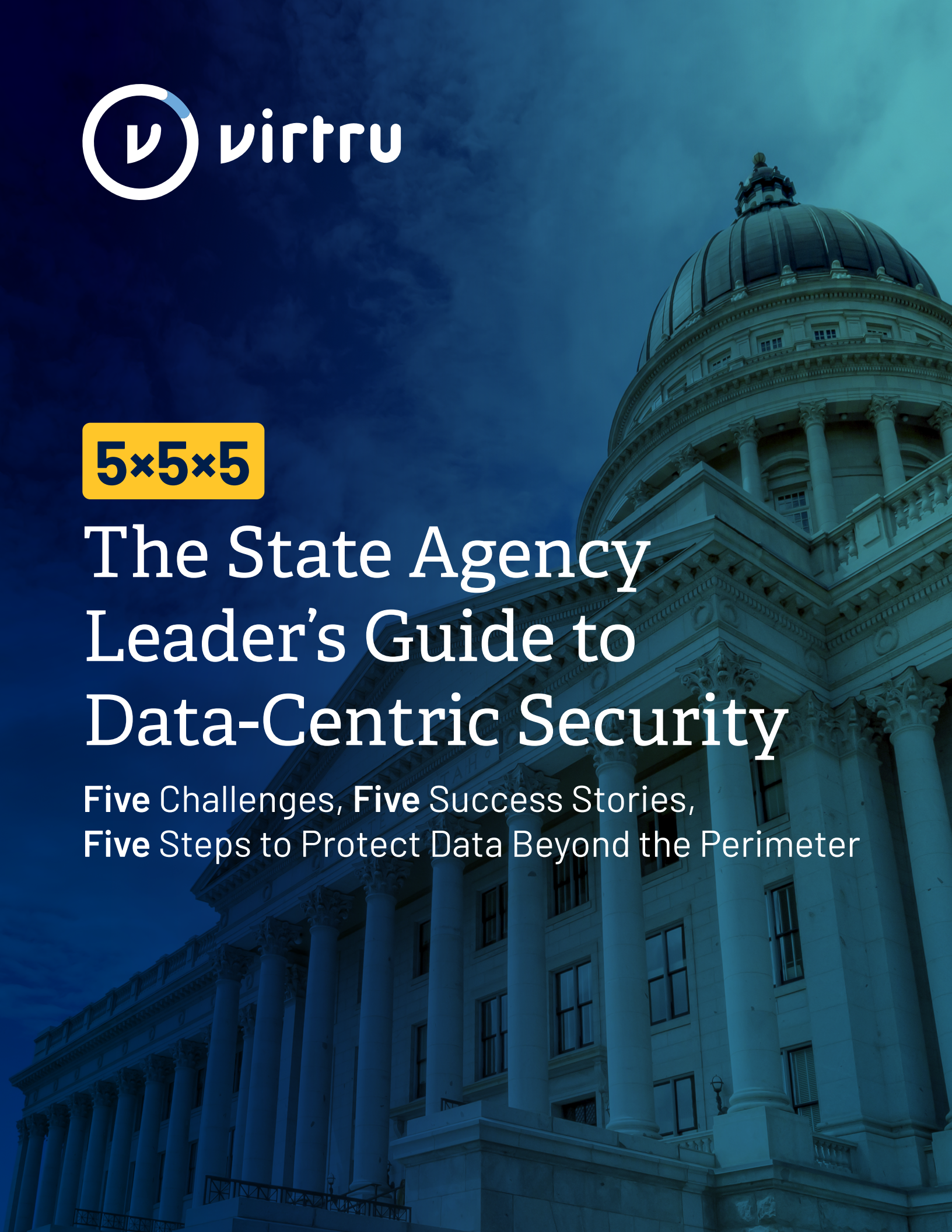


virtru

5×5×5

The State Agency Leader's Guide to Data-Centric Security

Five Challenges, **Five** Success Stories,
Five Steps to Protect Data Beyond the Perimeter

State government agencies — from the Department of Justice (DOJ) to the Department of Homeland Security (DHS) and the Department of Revenue (DOR) and beyond — operate in a highly complex and interconnected environment, with a patchwork of software, tools, and workflows that must coexist in order to deliver critical services. State agencies must routinely collaborate and share sensitive constituent information, including Criminal Justice Information (CJI), Protected Health Information (PHI), and tax records, both internally and externally.

Yet, agency cybersecurity leaders face a persistent reality: They must execute this mission across a deeply fragmented, decentralized IT ecosystem, without compromising sensitive data. Different state departments, local municipalities, and third-party contractors often run entirely disconnected security systems, leaving agency data vulnerable the moment it crosses the perimeter.

Statewide IT consolidation to "whole of state" security remains a worthy long-term goal, but agency leaders cannot afford to wait years for unified architecture. They need practical, deployable solutions now. This white paper examines the five data-sharing challenges that agency leaders most commonly encounter: Decentralization, Mismatched Toolsets, Lack of Visibility, Lack of Compliance, and Lack of Security. It will explore how a shift to data-centric security, rather than perimeter-centric security alone, can empower individual agencies to protect their data, meet compliance obligations, and serve constituents securely — regardless of the systems their partners use.

5 Data-Sharing Challenges Facing State Agencies in 2026

Agency CISOs and IT directors must simultaneously defend against targeted cyberattacks and facilitate seamless inter-agency cooperation — objectives that often feel at odds with one another. Their efforts are routinely undermined by systemic challenges inherent to fragmented government ecosystems.

1. Decentralization

A typical state government comprises roughly 50 distinct agencies within the executive branch alone, alongside independent judicial and legislative bodies, local municipalities, and tribal governments. For any single agency, this decentralization creates significant operational bottlenecks.

When your agency needs to share sensitive data, whether during a crisis or for routine coordination, such as the Department of Corrections transmitting case files to the Attorney General's office, you are navigating siloed infrastructure over which you have little to no control. You cannot dictate the receiving entity's security posture, which means relying solely on perimeter defenses to protect your data is no longer a viable strategy.

2. Mismatched Toolsets

In a federated ecosystem, agencies typically have wide latitude to select their own IT platforms. The result is rampant toolset fragmentation. Your agency might be fully cloud-adopted on Microsoft 365,

while a frequent collaborator relies on Google Workspace, and a local law enforcement partner still operates on-premises with legacy Exchange servers.

This mismatch creates immediate friction. When systems cannot easily communicate, employees resort to workarounds (personal cloud storage, unencrypted email, even physical media) that bypass approved IT infrastructure, and compliance requirements, entirely. It also strains budgets, as IT leaders must manage overlapping licenses and shadow IT simply to bridge communication gaps between agencies.

3. Lack of Visibility

When toolsets are disconnected, data visibility erodes. Consider a common scenario: An agency employee receives a physical document, scans it to a desktop, and uploads it to a cloud drive. Security teams have a line of sight into only that final step—roughly 20% of the document's lifecycle.

The problem deepens when your agency shares files externally with contractors, partner departments, or constituents. Once a PDF containing a Social Security number leaves your network, it may persist indefinitely on a contractor's server, a constituent's smartphone, or a third-party backup archive. Your agency remains fully liable for that data, yet you have no ability to track it, audit access, or revoke it. In an environment where nation-state cyber attacks are on the rise, there's a considerable risk of this sensitive data being exposed — if not today, then sometime in the future.

4. Lack of Compliance

State agencies are bound by stringent regulatory frameworks like CJIS, IRS Publication 1075, PCI, HIPAA, and others. Maintaining compliance across a fragmented ecosystem becomes even more complicated when staff must rely on legacy media or unencrypted channels to communicate with external partners running incompatible systems.

To work around file-size limits or platform barriers, employees and constituents frequently default to mailing physical documents, sending unencrypted faxes, burning CDs, or uploading files to personal cloud storage. These methods often violate federal and state compliance mandates, fail to meet eDiscovery requirements for public records requests, and leave no auditable trail. Without automated, cross-platform guardrails, compliance depends on individual judgment — an unacceptable risk for any agency handling regulated data.

5. Lack of Security

State and local governments are among the most heavily targeted entities by nation-state actors and cybercriminals, who actively seek the weakest links in an interconnected environment. Even if your agency's perimeter is well-defended, the data you share with an underfunded local municipality or a vulnerable third-party vendor remains at risk once it leaves your control.

Legacy file-sharing architectures compound this exposure. Centralized file-transfer platforms—such as those exploited in the MOVEit breach—serve as large, concentrated repositories of an agency's most sensitive data. Relying on these systems to bridge fragmented ecosystems inadvertently creates high-value targets for attackers.

A Practical Shift Toward Agency-Driven, Data-Centric Security

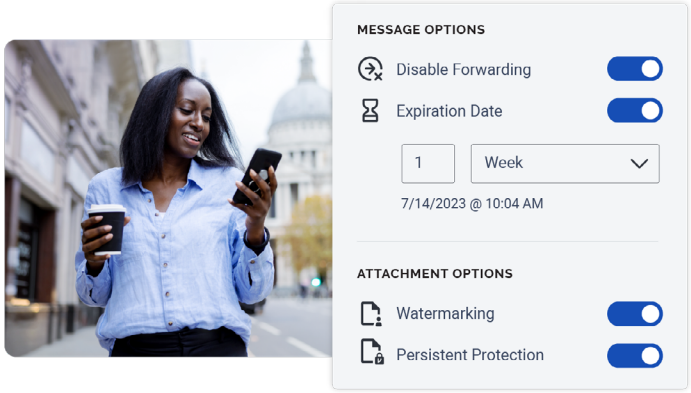
Rather than waiting for a top-down, statewide IT overhaul, agency leaders can take direct control of their data's lifecycle today. This requires a fundamental shift in thinking: Rather than relying on a secure perimeter to protect the data you possess, instead think about shifting the control from the perimeter to each data object itself, applying cryptographic protection and access controls directly to the data.

This doesn't mean encrypting everything, and it doesn't have to be complicated. It simply places the focus on the asset you are ultimately trying to protect: The sensitive data that you possess and must still share with authorized people and systems.

The central, load-bearing pillar of Zero Trust is data. By implementing ZT principles at the agency level, you operate on the assumption that external networks, devices, and recipients cannot be inherently trusted. Your agency's sensitive data remains encrypted, access-controlled, and auditable regardless of where it travels across the state's fragmented ecosystem. If a partner agency or contractor experiences a breach, then their access can be revoked instantly, and your data remains unreadable and under your control.

This is not a theoretical model. Agencies across the country are already deploying this approach—and seeing measurable results.

Data-Centric Security Made Simple: Virtru for State, Local, and Municipal Governments



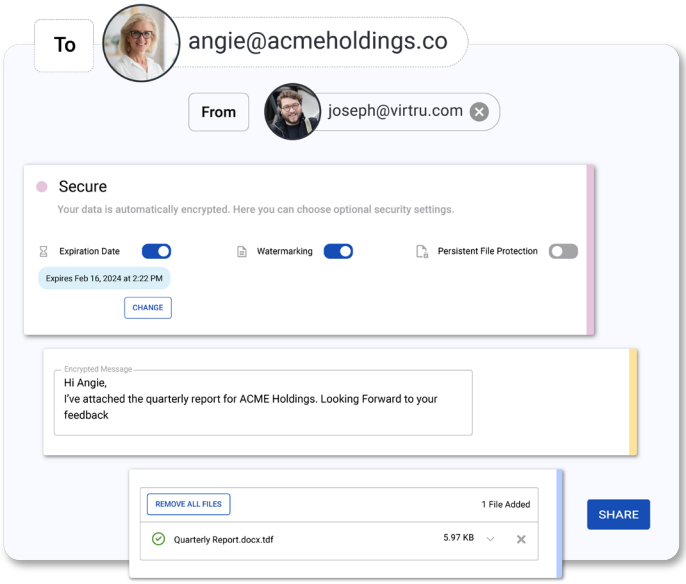
To achieve persistent data protection without slowing down mission-critical government operations, agencies across the country are deploying Virtru. Fully GovRAMP certified and trusted by government organizations in 19 states, Virtru provides a comprehensive suite of data-centric security solutions designed to integrate with the tools your agency already uses. This helps to bridge the gaps between disconnected ecosystems, rather than requiring you to navigate around them or replace them.

Virtru for Email: Frictionless Client-Side Encryption

Virtru delivers easy-to-use, end-to-end encryption that lives natively inside Gmail and Microsoft Outlook. Agency staff can securely share CJI, PII, and PHI with a single click. Because Virtru is platform-agnostic on the recipient's end, your Microsoft-based agency can send encrypted emails to a Google-based partner or a citizen's personal inbox without requiring them to create accounts or manage additional passwords. Recipients don't have to create any new accounts or install any software: They use the credentials they already have.

Virtru Secure Share: Compliant, Platform-Agnostic File Transfer

Legacy SFTP tools and physical media are inadequate for bridging agency silos. Virtru Secure Share enables employees to securely exchange large files — up to 15 GB, including bodycam footage, criminal justice records, and procurement contracts — through any standard web browser. It replaces vulnerable legacy file-transfer platforms with a right-sized, highly secure and controlled solution that ensures your agency's data never rests unencrypted on a third-party server.



Virtru Secure Share Enclave is the latest addition to the Virtru product suite, supporting highly regulated fields such as criminal justice, federal government contracting, defense, and intelligence. Virtru Secure Share Enclave is FedRAMP Authorized and FIPS 140-2 validated.

Virtru Private Keystore: True Data Sovereignty

For agencies subject to strict compliance mandates (CJIS, FedRAMP, IRS Pub 1075), who holds the encryption keys is as consequential as the encryption itself. Virtru Private Keystore allows your agency to host its own encryption keys on its own infrastructure, or in the public or private cloud of its choice. This ensures Microsoft, Google, and even Virtru itself have zero access to your unencrypted data. That's because the keys to unlock the content are in your hands, with a degree of separation from the data itself. This architecture provides true data sovereignty—shielding sensitive information from cloud providers and ensuring that even a legal subpoena directed at a third party cannot expose your agency's records.

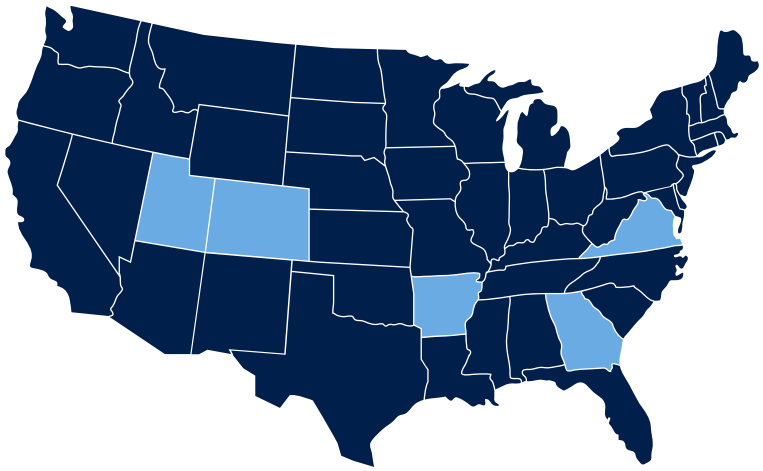
Virtru Data Protection Gateway: A Safety Net to Prevent Data Loss and Misdirected Emails

Human error is inevitable in any busy organization. The Virtru Data Protection Gateway serves as a server-level safety net, running in the background to scan outbound communications across all mail clients. It detects sensitive information however you choose to define it — Social Security numbers, tax IDs, CJI, CUI — and automatically encrypts it before it leaves your agency's network. Your security policies are enforced consistently, without requiring any action from the end user.

5 Success Stories

How State Agencies Are Deploying Data-Centric Security with Real-World Results

Leading state agencies have already demonstrated the effectiveness of this approach:



1. **Colorado Secretary of State**: After Proofpoint Secure Share reached end-of-life, the department needed to secure elections data, business filings, and financial reports within its Microsoft 365 environment. After evaluating alternatives, the team selected Virtru for its right-sized approach—powerful security without unnecessary complexity or cost. With Virtru Secure Share and Virtru for Outlook, Colorado gained granular access controls, including automatic 3-month expiration dates on externally shared data, ensuring access is governed and revoked without manual intervention.

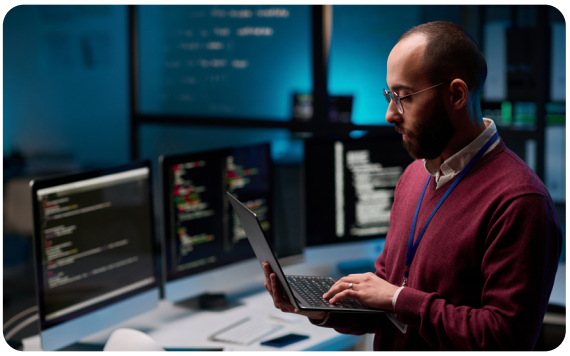
2. **Arkansas Game & Fish Commission (AGFC)**: Operating in Google Cloud, AGFC needed to share CJIS data securely with multiple disparate law enforcement agencies. The commission deployed Virtru for Gmail, Virtru Secure Share, and the Virtru Data Protection Gateway. Officers and park rangers can now collaborate with external agencies without friction, while the Gateway automates encryption to minimize the risk of human error.

3. **State of Utah**: Following the MOVEit breach, Utah recognized the architectural risk of centralized file-transfer servers—platforms where a single compromise exposes an agency's most sensitive data. They migrated to Virtru specifically because Virtru never has access to the files being shared. This removed the vulnerability at the architectural level while giving the state persistent control over files long after they leave the network.

4. **Commonwealth of Virginia**: Virginia adopted a pragmatic, parallel approach to data security. Rather than spending years cataloging its entire data environment before applying protection—a common "phase one, phase two" trap—the state integrated Virtru with Microsoft sensitivity labels. When an employee tags a document containing tax data or a Social Security number, Virtru automatically triggers encryption and sets an expiration date. Data is protected today, even as the broader classification strategy continues to mature.

5. **Georgia Technology Authority (GTA)**: As the central IT organization for Georgia state government, GTA handles criminal justice information, tax records, legal contracts, and PII for millions of residents. The authority deployed Virtru with Private Keystore to establish automated encryption guardrails across its Microsoft 365 environment—replacing an honor system with verifiable, policy-driven data governance. GTA's deployment now serves as a replicable blueprint for other Georgia agencies.

5 Actionable Next Steps for Agency IT Leaders



To build a resilient data security posture within a fragmented ecosystem, consider the following steps:

1. **Map Your Agency's Data Footprint.** Identify where your sensitive data (PII, PHI, CJI, CUI) resides, which external entities you share it with most frequently, and where gaps in visibility exist.
2. **Deploy Platform-Agnostic Tools to Bridge Inter-Agency Gaps.** Do not wait for partners or other agencies to adopt tools that play nicely with yours. Choose solutions built for flexibility, allowing Microsoft, Google, or even Linux users to share encrypted information with anyone, on any platform, without requiring recipients to change their workflows.
3. **Implement Granular, Persistent Access Controls.** Move beyond "fire and forget" data sharing. Adopt tools that enable you to revoke access, track opens, disable forwarding, watermark files, and set automated expiration dates—ensuring your data does not persist unmonitored on external systems.
4. **Automate Compliance Guardrails.** Reduce reliance on individual judgment. Deploy server-level data protection gateways that automatically detect and encrypt outbound data subject to CJIS, HIPAA, or IRS 1075 requirements before it leaves your network.
5. **Secure Dedicated Funding.** Leverage state and federal compliance mandates and grant programs to fund data-centric security investments. Frame the initiative to executive leadership not as an IT upgrade, but as essential risk mitigation for the agency's regulatory obligations.

What Comes Next?

In a decentralized state government environment, no agency can rely on the security posture of its partners — nor can it afford to wait for statewide unification. The responsibility to protect sensitive constituent data belongs to the agency itself.

By adopting data-centric security principles and deploying solutions like the Virtru suite, agency leaders can regain visibility and control over their most sensitive information. Data remains encrypted, access-controlled, and auditable throughout its lifecycle—across platforms, across agencies, and across state lines.

The result: your agency can share the information it needs to serve constituents effectively, with confidence that security, compliance, and data sovereignty travel with the data itself.

To see how Virtru can support your agency's data protection strategy, contact our state and local government team to schedule a demo.