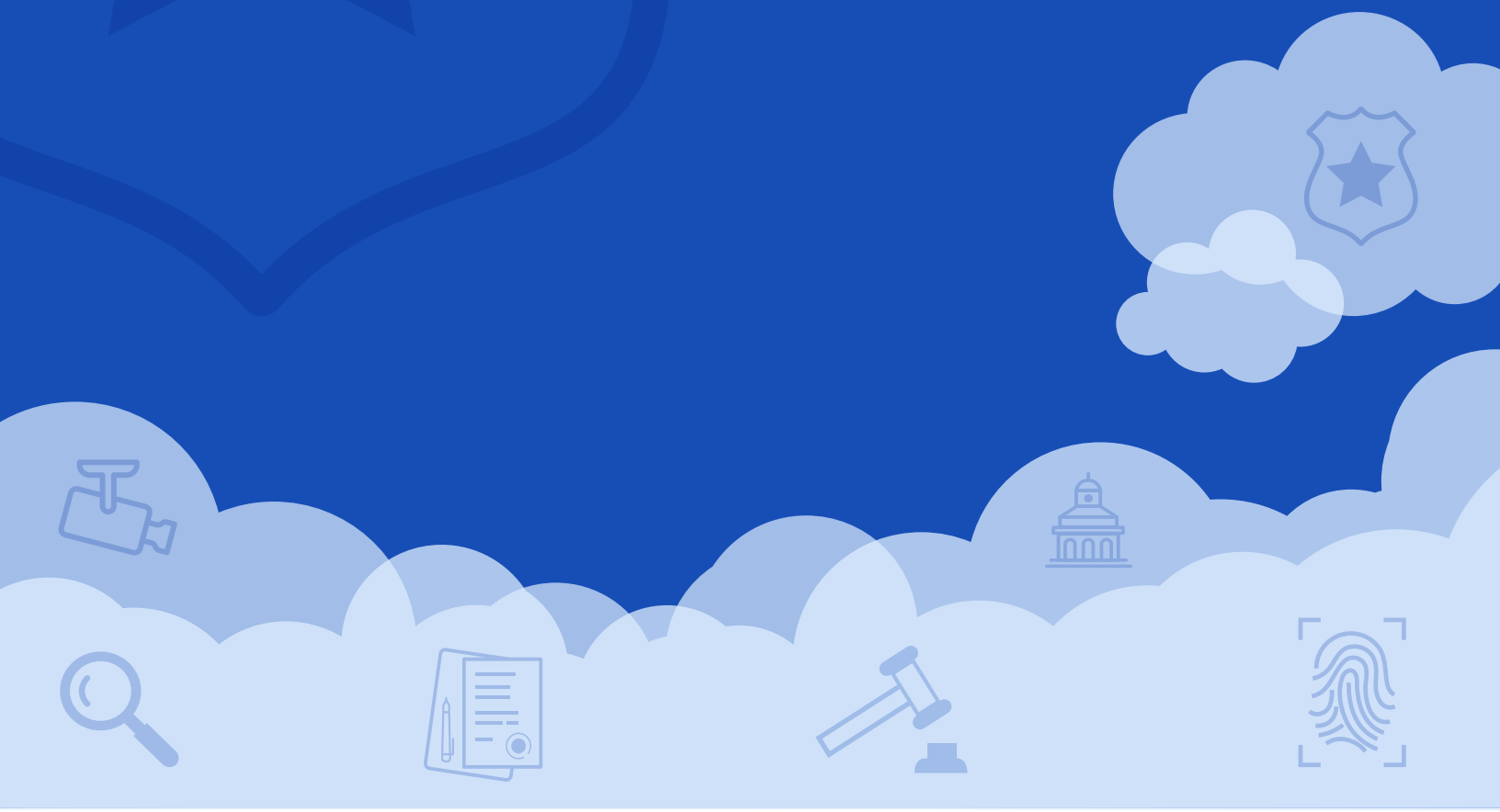
CJIS Compliance in the Cloud:

Uncovering a Solution for Securing CJI Stored & Shared via Cloud Email and Files



virtru

Protecting the Data that Protects Our People

One of the most tragic crimes in Connecticut history might have been prevented if law enforcement could have shared criminal justice information more effectively. In 2007, two parolees raped and murdered a mother and her two daughters during a home invasion in Cheshire, CT. Unfortunately, the board who approved their parole never saw a sentencing transcript where one of the parolees was described as a "calculated, cold-blooded predator."

This communication lapse reveals the very problem that the Criminal Justice Information Services (CJIS) Division was developed to solve: how can government entities protect their most valuable data while keeping it easily accessible? While this problem remains as relevant as ever, many law enforcement and criminal justice organizations still struggle to find cost-effective, compliant ways to share their most critical information.

CJIS Overview

CJIS is the largest division of the Federal Bureau of Investigation (FBI). Established in 1992, CJIS enables the monitoring of criminal activities in local and international communities using analytics and statistics collected as part of standard law enforcement processes. CJIS provides centralized sources of criminal justice information (CJI), such as the National Criminal Information Center (NCIC) and National Instant Criminal Background Check System (NICS).

Any organization with access to these databases must ensure that its employees comply with CJIS regulations for keeping CJI secure. Examples of groups governed by CJIS compliance include US Federal Agencies, Police Departments, Departments of Public Safety, Departments of Corrections, Offices of Attorney General, Offices of the Public Defender, Offices of the US Courts, government contractors, and many more.

Common Examples of CJI

While CJI can take many forms, some of the most common types include:

- Arrest reports
- Fingerprint data
- Criminal background checks
- Stolen property records
- Protective orders
- Sentencing and parole reports
- Body worn camera footage

The CJIS Security Policy

The CJIS Security Policy defines standards for protecting the sources, transmission, storage, and generation of CJI, setting forth best practices that ensure timely, secure, and reliable access to services that help stop and reduce crime. The policy's executive summary states its purpose as such: "The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit."

In order to fulfill that purpose, CJIS contains 13 policy areas in all, and they share a common objective of preventing unauthorized access to CJI while maintaining its integrity. In order for law enforcement authorities to be effective, CJI must be protected from unauthorized disclosure, alteration, or misuse.

The standard approach to preventing unauthorized access to CJI is confining it to a physically secure location with stringent physical access authorization and controls. Personnel authorized to access a physically secure location under CJIS must undergo background screening and routine CJIS security awareness training. Historically, these guidelines meant that organizations often established on-premise IT infrastructure to maintain the security of CJI in digital formats.

The rise of cloud computing and rapid digital collaboration workflows, combined with the sheer cost and complexity required to keep digitized CJI confined to a physically secure location throughout its lifecycle, required agencies to rethink their approach to CJIS compliance. And as more and more organizations relied on third-party vendors to store and share data in the cloud, it also led to several revisions to the CJIS Security Policy itself to incorporate new standards and guidelines for protecting CJI.

CJIS Compliance Requirements in the Cloud

The latest CJIS Security Policy acknowledges the cloud's opportunities of cost savings and efficiency versus the challenges of less control and visibility of CJI. Prevalent cloud-based email and file solutions—such as Microsoft Office 365 and G Suite—operate in multi-tenant public cloud environments, powered by infrastructure that hosts and serves data belonging to hundreds (or even thousands) of organizations simultaneously. The personnel maintaining this cloud infrastructure are not agency officials but third-party cloud service provider employees, so while the agency gains efficiencies by delegating infrastructure administration, security, and maintenance to the cloud provider, it also loses direct control of the CJI.

Without added encryption, CJI in cloud-based email and file systems is stored in plaintext, such that cloud service provider personnel could obtain unauthorized access. Meanwhile, the notion of a "physically secure location" changes significantly in cloud environments. While Microsoft, Google, and other cloud vendors use security best practices, they don't meet all of the CJIS Security Policy requirements by default. As a result, cloud vendor personnel with access to the servers and databases hosting CJI on an agency's behalf would need to complete the same background screening and CJIS-specific security awareness training as the agency

employees who handle CJI day in and day out. Specialized SLAs and/or contractual clauses are also typically required in these scenarios. Fulfilling these prerequisites is a tall order for both the cloud vendor and CJIS-bound agencies, as they add to project costs and complexity and delay deployment timelines.

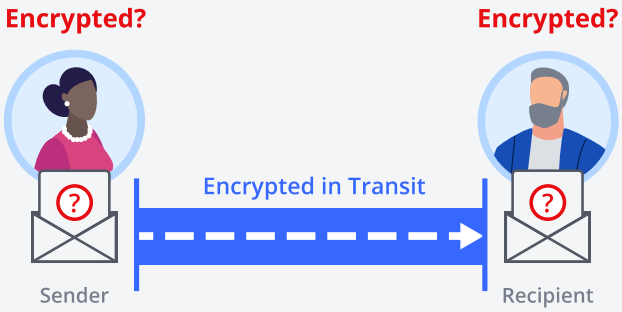
Encryption and CJIS Compliance

CJIS outlines encryption requirements to preserve the integrity of CJI when it is transmitted or stored outside of the boundary of the physically secure location. For encryption in-transit and at-rest, FIPS 140-2 certified cryptographic modules and a symmetric cipher key strength of at least 128 bits are the minimum requirements for protecting CJI as it's stored and shared in cloud environments.

Natively, cloud environments provide Transport Layer Security (TLS) to encrypt the network layer, but this only protects the perimeter and the communication channels through which CJI is shared, not the actual CJI itself. Added encryption is needed to meet CJIS requirements for preventing unauthorized access to CJI shared outside of physically secure locations.

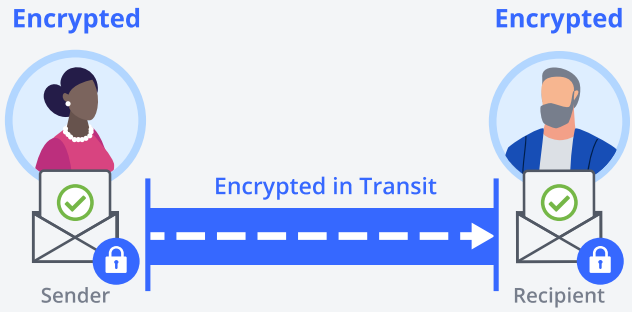
TLS Encryption vs. End-to-End Encryption

TLS Based Encryption



- Doesn't ensure CJIS compliance
- Only encrypted in transit
- Content may/not be encrypted when stored
- No visibility or control
- Cloud vendor personnel may be able to access CJI

End-to-End Encryption



- Ensures CJIS compliance
- Keeps CJI encrypted at all times, from originator to authorized recipients
- Plaintext CJI is never accessible to third-party cloud vendor personnel or other unauthorized recipients

End-to-End Encryption and Challenges with Traditional Approaches

Due to the limitations of native TLS encryption combined with complexities associated with adapting cloud vendor processes to meet CJIS requirements for physically secure locations, the CJIS Security Policy suggests using client-side end-to-end encryption:

> "Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data."

With end-to-end encryption, only the originator or owner and authorized recipients and collaborators can access the plaintext CJI, fulfilling CJIS compliance requirements for preventing exposure of CJI while maintaining its integrity. Therefore, client-side, end-to-end encryption can make widespread cloud adoption a reality for CJIS-covered entities, allowing organizations to forgo the previously mentioned administrative and contractual burdens, yet still keep CJI protected from exposure.

Traditional approaches to end-to-end encryption, such as PGP and S/MIME, typically require manual key exchanges that make it difficult to deploy. In general, this means that for officers to send an email or file encrypted client-side to employees in another department, they would first have to retrieve a unique encryption key from that employee. The employee would also need to have the same encryption technology implemented on his device. If the officer were to lose the employee's key for any reason, he would have to repeat the process again.

These traditional approaches to client-side encryption may alleviate law enforcement's most immediate security concerns, but they introduce technical complexity that frustrates end users and ultimately prevents adoption of the very tools intended to protect CJI. Law enforcement agencies need a user-first, data-centric approach to protect CJI and maintain compliance.

Introducing Virtru's Easy End-to-End Encryption for CJIS Compliance

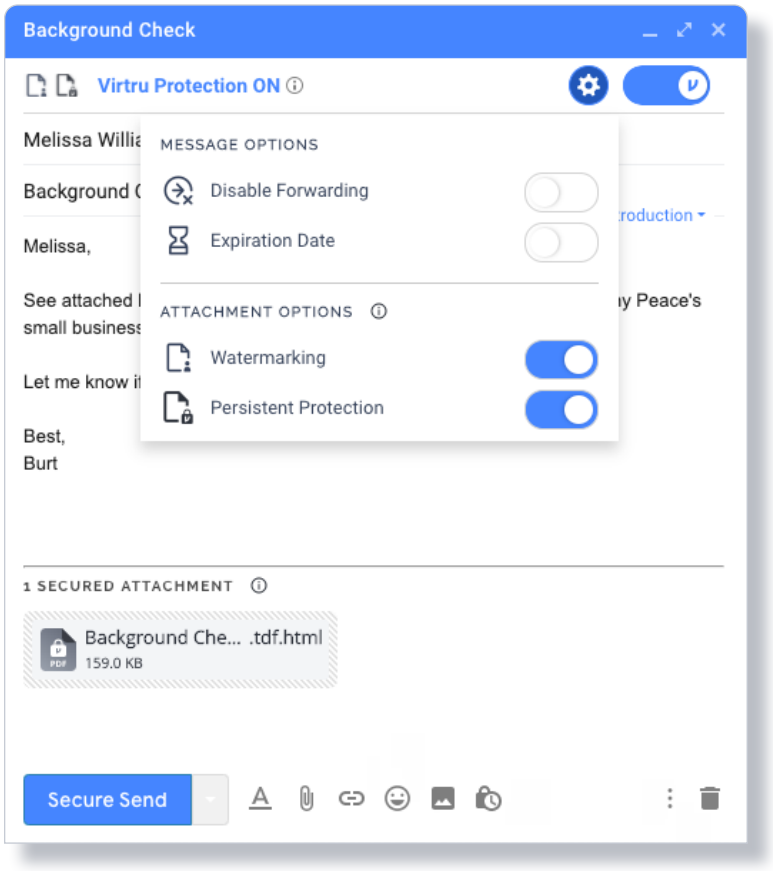
Virtru's email and file protections offer data-centric security via end-to-end encryption that prevents unauthorized access and enables persistent control and visibility as sensitive CJI is shared. With data-centric security in place, protection, control, and visibility persist throughout the full data lifecycle, enabling full adoption of cloud systems without risking compliance violations. And seamless user experiences ensure end-to-end encryption is used to the fullest extent.

Easy End-to-End Encryption and Key Management

Virtru's data protection solutions employ 256-bit AES encryption, which exceeds the CJIS policy requirements for a minimum 128-bit encryption strength, to encrypt CJI both at rest and in-transit. Virtru also supports FIPS 140-2 cryptographic modules to align with CJIS guidelines.

Third-party vendor personnel cannot access sensitive CJI, even when it's stored in multi-tenant public cloud environments. As CJI is shared throughout digital collaboration workflows, Virtru's encryption persists with the data, keeping CJI protected as it is transmitted between servers, devices, and unknown cloud environments.

Virtru hosts and manages the encryption keys and access control policies in protected environments that employ security best practices, while allowing customers to host the encryption keys directly using on-premise infrastructure for true "hold your own key" security.



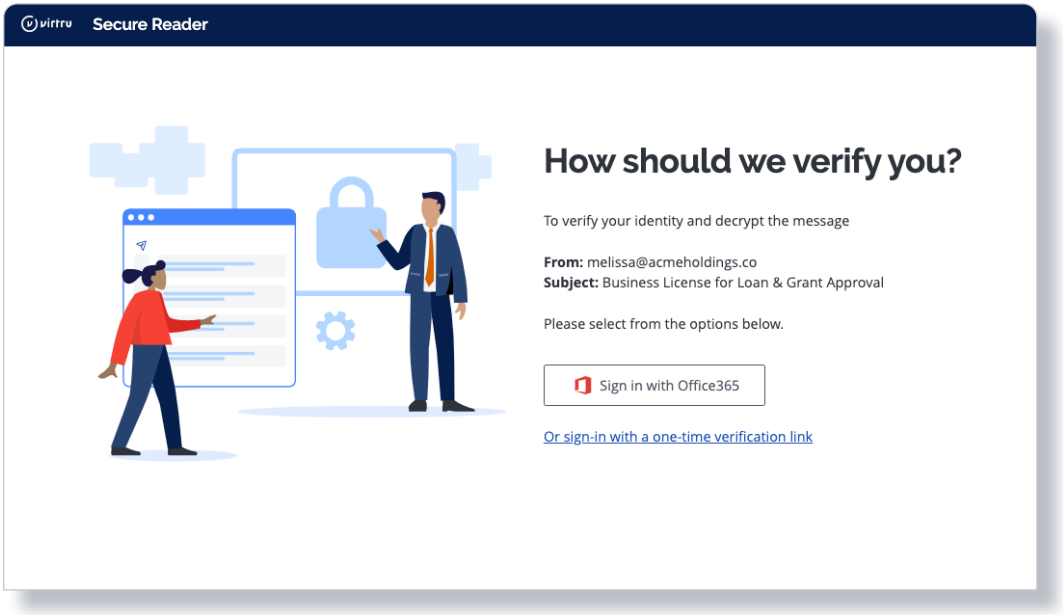
End-to-end encryption and granular access controls are embedded directly within email clients like Gmail for client-side protection of CJI.

Ease of Use

Virtru is embedded directly into existing user applications for email and files. In G Suite, Virtru integrates with Gmail and Google Drive native user experiences using an easy-to-install Google Chrome browser extension, giving users intuitive, on-demand protections. In Microsoft Office 365 and Exchange environments, Virtru works within the desktop Outlook application as an add-in that supports CJIS protections where your users already work.

Encryption is applied directly within email and file clients used in existing workflows, ensuring only authorized agency personnel and collaborators can access CJI. End users never have to manage or exchange encryption keys manually like they do with traditional end-to-end approaches; Virtru performs key exchanges transparently on behalf of users.

Recipient user experiences are seamless: collaborators from external departments or agency partners simply authenticate using their existing accounts to access protected CJI via the Virtru Secure Reader.



Virtru Secure Reader is a seamless web application that makes access to protected CJI easy. External recipients never have to create and manage new accounts or passwords.

Data Loss Prevention

In addition to on-demand encryption and access controls configured by end users, administrators can configure Data Loss Prevention (DLP) rules for email and attachments. With these DLP rules configured, Virtru scans content before it is shared, and if sensitive CJI is detected, Virtru automatically enforces encryption and access controls that keep the data protected and compliant throughout its lifecycle.

Persistent Access Controls

Virtru also provides powerful controls to reinforce protections against unauthorized access. As users share email and files, they can set expiration dates, disable forwarding or resharing, and apply watermarks that help prevent leaks throughout the CJI lifecycle. After encrypted data is shared, users can revoke access at any

time. Persistent protection can be applied to email attachments, allowing them to be stored beyond the initial email to desktops, shared network folders, and cloud platforms like Google Drive or OneDrive, while the file owner always maintains control.

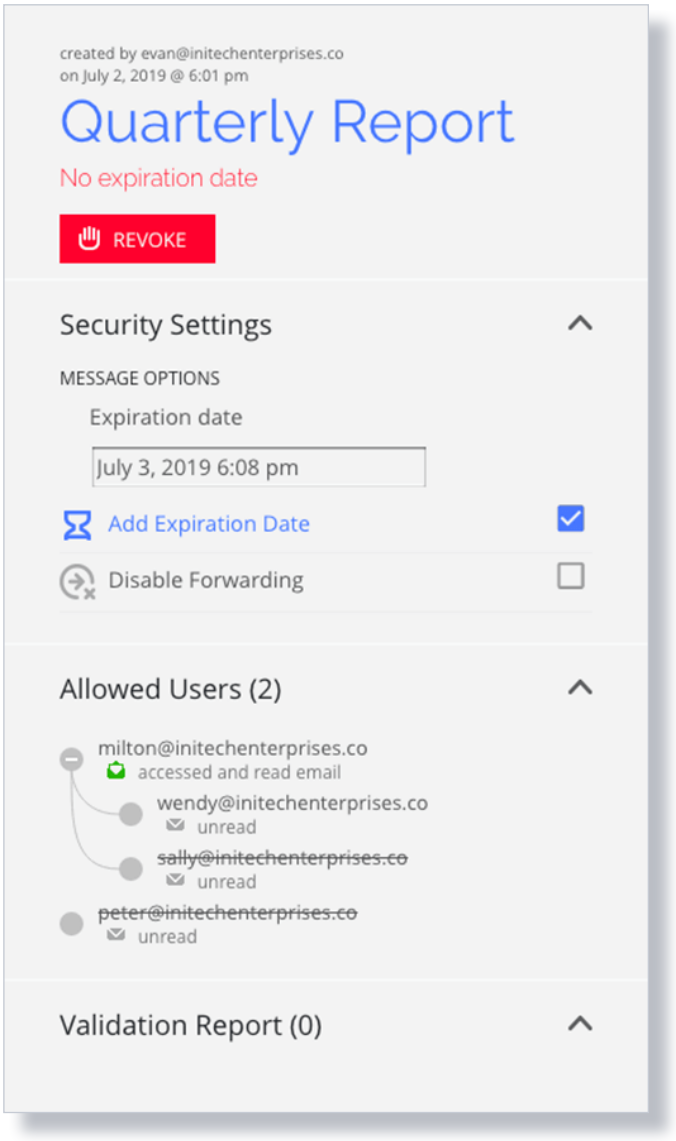
Visibility and Audit

Administrators and end users maintain visibility into all access and resharing activity. Forwarding trees allow owners of CJI to view who has accessed and forwarded sensitive CJI and offer the ability to selectively revoke access to specific collaborators, helping adapt controls as the context in which the CJI was shared evolves throughout its lifecycle.

All behavior on the Virtru platform, including end user protections and controls, access and sharing actions, administrative activity, and more, is logged continuously. Virtru customer organizations can export log data to conduct analysis and review, complete CJIS audit reports, or integrate with SIEM platforms for advanced threat management.

Painless Administration

Virtru can be deployed at scale in a matter of minutes using Managed Chrome and Group Policies in G Suite or Microsoft Installer in Exchange and Office 365 environments. Seamless user experiences reduce administrative burdens on helpdesk teams, freeing up resources to handle more strategic priorities. Administration is painless within the Virtru Dashboard, a centralized administrative console for user management and data monitoring. Virtru aligns with existing security infrastructure and key management process, with support for integration with hardware security modules (HSMs).



End users can easily see who has accessed, read, and forwarded email and attachments containing CJI and adapt access controls at any time.

Maryland

Maryland Enables Distributed Teams with Virtru's End-to-End Encryption for CJIS Compliance in the Cloud

Maryland's state government decided to migrate its IT infrastructure to G Suite to allow employees to use cloud-based systems for more rapid collaboration and service delivery across distributed agencies and departments. Before Virtru, roughly 10,000 Maryland employees were unable to fully migrate: the state's Department of Public Safety and Correctional Services (DPSCS) had to continue using on-premise email platforms, because they had no way to meet the client-side email encryption requirements for keeping CJI protected from unauthorized access in cloud environments.

All of that changed when Maryland's DPSCS decided to deploy Virtru, enabling Gmail users to send CJIS compliant email directly from their inboxes. Two months later, DPSCS deployed Virtru to another 2,000 employees and over the next few years, a full transition to Virtru for Gmail helped save Maryland significant costs by centralizing its IT needs under one platform.

Virtru for CJIS Compliant Digital Law Enforcement Workflows

Digital workflows and cloud-based systems bring plentiful opportunities to law enforcement agencies and other CJIS-bound entities, but they can also carry significant risks and complexities regarding CJIS compliance. Traditional methods of end-to-end encryption don't support the usability needs of modern organizations, especially when quick, secure access to CJI is critical to maintaining public safety and preventing crime.

Combining data-centric protections with a user-first approach to data protection gives agencies a leg up in serving their local communities. Easy end-to-end encryption embedded within native G Suite and Office365 workflows empowers users with secure digital collaboration workflows that enable effective law enforcement while protecting CJI and other private data to prevent the risk of noncompliance fines.

If your organization is interested in learning how Virtru can help modernize your service delivery models and internal collaboration workflows, contact us to see how easy it is to keep your digital workflows private and compliant.

virtru.com/contact-us

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 20,000 organizations trust Virtru for data security and privacy protection.

Visit virtru.com or follow us on Twitter at @virtruprivacy.