



# Whole-of-State Cybersecurity: From Edge to Edge

**MARKET TRENDS REPORT**



# Introduction

---

State, local and tribal governments are grappling with how to protect their data from ransomware and other forms of cyberattack. It's not always easy — state, municipal, county and other agencies may have different cybersecurity processes and tools, making it harder to exchange information safely or smoothly. Smaller entities often lack funding and talent to keep up with increasingly sophisticated risks. Local weaknesses can lead to statewide breaches, undermining constituent confidence that government can protect their information and costing millions.

Increasingly, states are turning to a **whole-of-state approach** — one that fosters collaboration among levels of government, educational institutions and the private sector to share cybersecurity tools, resources and information. It leverages state expertise to help localities up their security game and standardizes tools and workflows so agencies can share data using secure cloud technologies that can be deployed and monitored statewide.

**To improve public trust, states must protect the way they process, store and transmit data.**

That means moving away from paper-based processes to digital workflows. Tracking, verifying and securing paper documents as they move among offices and agencies is cumbersome, if not impossible. They need to reduce the fragmentation among agencies and localities, build consistent document security pathways, and help smaller entities choose and implement secure data-handling tools.

For this Market Trends report, GovLoop partnered with DocuSign, a leader in agreement management and the expert in secure electronic signatures. We'll discuss how digital document workflows can support a whole-of-state cybersecurity strategy.

# By The Numbers

# 82%

of all breaches involved data stored in the cloud — public, private or in multiple environments.

# \$2.6 million

is the average cost per breach for public sector organizations.

## Mean Ransom Payments for State & Local Government:

2022: \$213,801

2023: **\$1,078,913**

Customer and employee personally identifiable information (PII) was both the costliest and most common type of compromised record.

- Customer: **\$183 per record**
- Employee: **\$181 per record**

In 2022, Ransomware attacks affected **220** local governments, health care facilities and schools in the United States:

- **106** local governments
- **44** universities and colleges
- **45** school districts (*1,981 schools*)
- **25** health care providers (*290 hospitals*)

# \$720,000

The cost per breach for organizations with mature cloud security practices was \$720,000 less than for those with no such practices.

*“To build more resilient cyber safeguards, [state chief information security officers] need to collaborate and share information on cyberthreats with all levels and branches of government and the private sector within state borders. **A whole-of-state approach** — encompassing this full array of stakeholders — is key to fortifying protections wherever vulnerabilities may occur.”*

- 2022 Deloitte-NASCIO Cybersecurity Study: State Cybersecurity in a Heightened Risk Environment

# How Document Management Contributes To Whole-of-State Cybersecurity

---

## **The Challenge: Fragmented Processes and Reliance on Paper**

State, county and municipal agencies exchange documents constantly. “The state is typically the top administrative and oversight layer, and the counties and cities are involved in day-to-day execution,” said Todd Kyle, Area Vice President of Public Sector Sales for DocuSign. “There are always going to be those up and down actions.”

But agencies differ in the way they process and secure their data. That fragmentation can interfere with the flow of information and create limited visibility. With the inconsistency and fragmentation comes a patchwork of security measures with the potential for weak spots.

That’s exacerbated by the ongoing reliance on paper. Paper forms can be misplaced or misdirected. It can be difficult to track where a paper document is on its journey, whether it’s been changed and who’s handled it.

“We spend a lot of time, resources and money on security in the main system of record, and we don’t spend enough time thinking about the true edge of the transaction, which is often a piece of paper or a form that should be digitized securely,” Kyle said.

From permit applications to human resources documents, agencies handle PII and other sensitive data every day. Even documents from the procurement process may reveal an agency’s supply chain model or other elements that should be kept confidential.

“Not having control over those documents, not having proper document management, makes it easy [for unauthorized people] to collect data and use it to attack organizations,” said Rainer Villamercado, DocuSign’s Senior Director of Public Sector Security.

Scanning documents and sending them by email doesn’t solve the problem either; unencrypted email is notoriously insecure.

“Whether it’s paper *paper* or *digitized* paper, it represents a huge risk that’s unnecessary,” Kyle said.

## **The Solution: Consistent and Secure Document Management Statewide**

A whole-of-state approach can address these concerns. Leveraging state resources to help agencies and municipalities adopt cloud-based technologies strengthens security across linked systems, lowering the risk of attacks at the edge, and if they do occur, stopping them before they reach critical data. And cloud-based monitoring allows visibility into the whole network — not only for security, but to better track agreement data across its lifecycle.

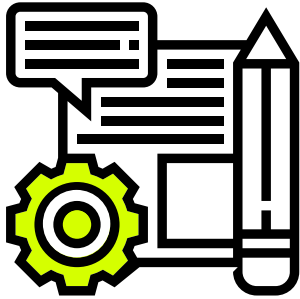
“If you don’t have a whole-of-state approach, from a [data] governance perspective, then you’re going to have those weaker spots that allow perpetrators to gain access,” said Villamercado. “Platform security, information security and compliance security — those things are what encompasses defense-in-depth. And digitizing your workflows allows for those things.”

Whole-of-state also facilitates the use of common processes. For example, digitizing documents and introducing electronic signatures can help bring that data into the cloud where it can be secured. State and local agencies can digitize and standardize the handling of applications, contracts and other documents in a secure environment.

Take the example of an elementary school that shares records with its surrounding county or state. School records frequently contain student PII and have become a target of ransomware attacks. “The digitization and transport of those documents in a secure workflow is everything,” said Kyle. “If you don’t have those documents encrypted, the workflow encrypted and a very, very secure pipe to put them through, you can open yourself up to risk.”

“Consistency across those levels is super important. That really has to be driving everything — not just cybersecurity, but everything that we do,” said Kyle. “State, county, city level — they all need to be consistent in their approach and in their standards. A whole-of-state approach is by far the best way to achieve that.”

# Best Practices for Implementing Whole-of-State



## Don't Reinvent the Wheel

According to Villamercado, states embarking on whole-of-state initiatives can benefit from working with organizations that have adopted standardized security requirements, such as StateRAMP and FedRAMP. By providing standards for data encryption, end-to-end encryption for PII, multifactor authentication and other elements of security, “they create the framework for us in the digitized workflow,” he said.

StateRAMP gives agencies at every level a common set of standards, making it easier to implement the consistency across agencies needed for whole-of-state security. Its ongoing monitoring and verification of products keeps its recommendations up to date.

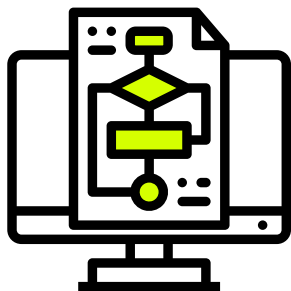
“Everybody’s late to the game when it comes to security controls, based on the number of attacks that are out there and how susceptible everyone is, particularly local governments that are under-budgeted and under-supported in that space,” said Villamercado. “So my main recommendation is to trust other organizations that are adhering to a common framework.”



## Make Sure You're Secure from Edge to Edge and Across the Lifecycle

A chain is only as strong as its weakest link. Often the weakest links in government security are at the edges — for example, where data on paper is manually entered into systems, by field agencies or staff working from home. That’s why document workflows should be secure from end to end, not just at city hall.

“Defense-in-depth might seem like a platitude,” said Villamercado, “but it’s essential to be able to provide multiple layers of security across your workflows. Ultimately, we need to make sure that your data is always protected, in every way, shape and form, in transit or at rest.”



## Don't Forget Internal Workflows

Individuals in the community are not a government’s only constituency, of course. Contractors, employees and other agencies need to trust that their data and documents are being handled safely. Onboarding new employees and tracking the procurement process also benefit from a consistent, secure document workflow.

“When we have consistency, when we adhere to consistent standards, [that] also increases the trust amongst agencies. That can improve data sharing,” said Kyle. “A lot of the challenges we see in government are because of siloed data — and sometimes that’s the unfortunate byproduct of mistrust. When we see standardization and an adherence to a common framework, that can encourage cross-pollination and sharing of data.”



## How Digitized Documents Protect Critical Data

When several agencies must respond to a situation, having a secure document flow is essential. In child welfare, teachers and school administrators are often mandated reporters — when they suspect a child is being abused or neglected, they're required to submit a report. "It goes up the chain to the state," Kyle explained, "and the state starts a process that calls for a wellness check. So they'll deploy a social worker to do that check."

"Think about where that data traveled. It went from a K-12 school to the state, to a caseworker, to a doorstep. And it's very sensitive information, probably both PII and medical information covered by HIPAA," he said, referring to the Health Information Portability and Accountability Act. "Think of all the points of potential risk. Having an end-to-end, [fully] encrypted transaction underscores the commitment to trust."

Another example is Medicaid, a joint federal and state program that counties manage. Recipients' sensitive health and income data flow up and down the information chain all the way from the individual to the federal Department of Health and Human Services. "That whole chain needs to be encrypted from end to end," said Kyle. "Those channels of communication involve forms and workflow and encryption, so when you apply those consistencies and those standards, you can help folks feel better in a time of crisis, in a time of need. Ensuring that trust is paramount to the success of that relationship."

### HOW DOCUSIGN HELPS

DocuSign is probably best known for its electronic signature solution, DocuSign eSignature, which millions of users trust. "When people see that little yellow sticky where it says, 'sign here,' they feel pretty good about it," Kyle said.

DocuSign solutions, including eSignature, adhere to stringent security standards and public-sector regulations. "Several of our solutions have achieved FedRAMP Moderate and StateRAMP Moderate authorization," said Villamercado. DocuSign allows documents to be tracked as they progress through the system and provides a record of changes.

Even courts have accepted eSignature, Kyle added.

DocuSign also offers the capacity to identify and respond to threats quickly and prevent unauthorized access. Using advanced analytics to track DocuSign web, mobile and API account activity across an organization, DocuSign Monitor provides near-real-time visibility into operations as they relate to existing DocuSign agreements and workflows.

And DocuSign CLM can analyze agreements for compliance gaps, flag potential data protection issues and get recommendations for mitigating risks.

"When you look at where we are with the DocuSign ecosystem, we have become synonymous with trust," Kyle said.

# Conclusion

---

To maintain public trust in the current heightened cyber threat environment, state and local governments must work together. A whole-of-state approach enables a consistent security posture, minimizing the gaps inherent in more fragmented systems.

Moving to cloud-based platforms allows better visibility and monitoring for threats and a faster, more coordinated response for agencies at all levels.

Cloud also provides the opportunity for more efficient and secure data sharing among organizations, through digital document workflows.

By handling data securely from end to end, whole-of-state helps government agencies, from the smallest to the largest, meet the challenges of today.



## ABOUT DOCUSIGN

---

DocuSign redefines how the world comes together and agrees, making agreements smarter, easier and more trusted. As part of its industry leading product lineup, DocuSign offers eSignature, the world's #1 way to sign electronically on practically any device, from almost anywhere, at any time. Today, over 1 million customers and more than a billion users in over 180 countries use DocuSign products and solutions to accelerate the process of doing business and simplify people's lives.

To learn more visit [www.docusign.com/government](http://www.docusign.com/government).



## ABOUT GOVLOOP

---

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to [info@govloop.com](mailto:info@govloop.com).



1152 15th St. NW Suite 800  
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

[www.govloop.com](http://www.govloop.com)  
@GovLoop

