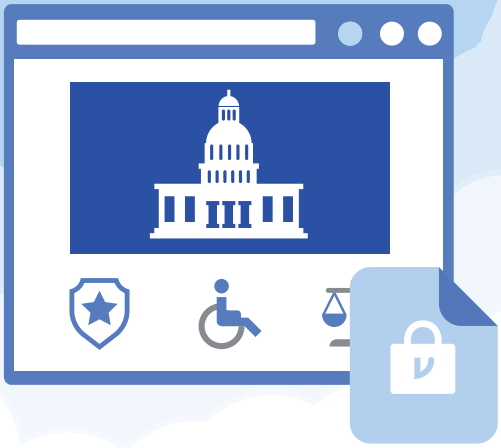
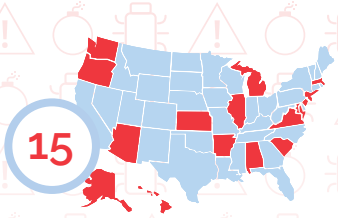
Securing Your Government Data in the Cloud

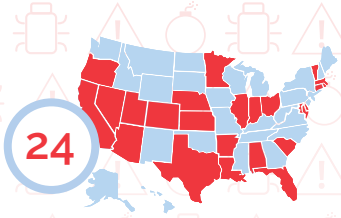
It's no surprise that you have concerns about the privacy and security of your sensitive Intellectual Property (IP) in the cloud. In 2018, more data was stolen than ever before, with a total of **4.5 billion records compromised** in the first half of the year alone.



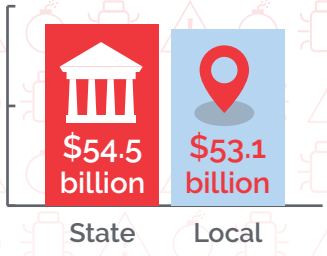
The right security controls, policies and technology are a must to prevent data breaches and ensure privacy.



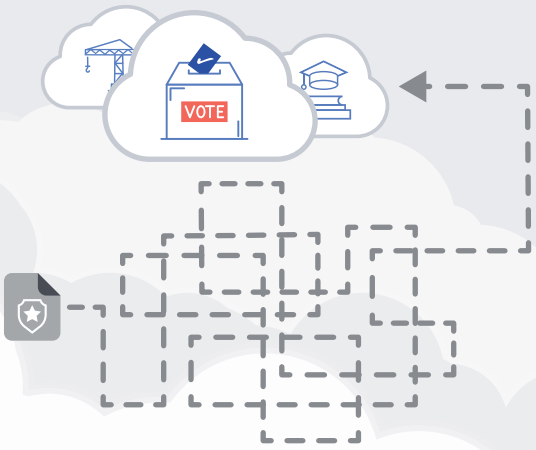
At least 15 states require government entities to destroy or dispose of personal information so it's unreadable or indecipherable.



Additionally, at least 24 states have data security laws that apply to private entities.



Modernizing IT infrastructure is costly. Governments allocate billions to IT security spend.



It Doesn't Have to Be So Complicated

Whether you've already migrated to the cloud or are thinking about it, your journey doesn't have to be risky. The cloud is loaded with benefits that are aimed to increase your business agility, flexibility and long-term growth and innovation. Why keep your IP on-prem or in tricky hybrid environments?

Are you ready to take the next step in your cloud journey?

Get in touch with Virtru to see how you can maintain protection and control of your data across all environments.

virtru.com/contact-us

virtru

Four Ways to Secure Government Data in the Cloud

The time to move from on-premises environments to the cloud is now.
Don't let concerns about storing and sharing sensitive data block your full-scale cloud adoption.

Look for a data protection solution that makes it easy to share securely across platforms and devices in any environment:

1

End-to-end Encryption to ensure cloud vendors and unauthorized parties will not be able to access your proprietary data, like regulated content, citizen PII and financial information.

2

Customer-hosted Keys that give you direct control of your data stored in the cloud, to support existing cryptographic workflows, and enforce policy on data that is shared externally to remain compliant.

3

Access Controls to ensure your proprietary data is only accessed by authorized collaborators and remains private, wherever it's shared, ensuring internal employees and third-parties are following mandatory privacy policies.

4

Granular Audit for visibility into who has accessed your proprietary data, when and where, making it easy to achieve PII data compliance and meet federal regulations like FERPA, HIPAA and CJIS.

Maryland

"By enabling full compliance for our law enforcement agency, Virtru gave us a path toward a complete cloud migration."

– Susan Lyon, Manager of Google Cloud Team, State of Maryland

virtru