Data Protection Checklist

Maintain privacy, compliance, and control across multi-cloud environments.

As organizations embark on digital transformations—more than **90%** store data in the cloud, **84%** of whom have multi-cloud environments—data protection is a top concern. Protecting data from unauthorized access is key to preserving privacy, meeting compliance requirements, and maintaining control, yet multi-cloud environments and digital sharing workflows often leave sensitive data at risk of exposure.

Combined with a constantly evolving regulatory landscape and increased public sentiment toward data privacy, today's multi-cloud, digital workplace means organizations must examine their data management and privacy programs more closely. Data, in its many forms, can uncover insights to optimize your operations and power growth opportunities, but it is hard to manage. And without the right protection and controls in place, data can be a major vulnerability.

Based on security and privacy best practices, this checklist keeps essential evaluation criteria top-of-mind to ensure successful implementation of a data protection tool that enhances your organization's security posture.

End-to-End Encryption: Solutions that offer true end-to-end encryption ensure that only authorized users can access sensitive data to ensure privacy and regulatory compliance.

Key Considerations:

- [ ] Does encryption occur directly within the email client, as soon as the content is drafted?
- [ ] Is the encryption happening at the object-level, protecting individual messages and files with unique encryption keys, to prevent unauthorized access wherever sensitive data is shared?
- [ ] Does the solution support encrypted file sharing?
- [ ] Is encryption available on-demand for end users with an intuitive user experience?

Access Controls and Granular Audit: Access controls should allow administrators and end users to proactively adapt access privileges as data travels and context around it changes. For compliance reporting, administrators need granular visibility over where data has traveled throughout its lifecycle in order to create audit trails.

Key Considerations:

- [ ] Are controls available to both end users and admins in real-time?
- [ ] Does the solution offer rights management features, including expiration, instant access revocation, and disabled forwarding?
- [ ] Can controls be added to files to prevent download/printing, or watermark files to deter leaks?
- [ ] Can file owners maintain control and ownership of email attachments, even after the attachment has been downloaded and stored beyond the initial email?
- [ ] Can data loss prevention (DLP) rules automatically enforce access controls? Can they be set up and managed at the user, OU, group, or enterprise level?
- [ ] Do end users and admins have granular visibility into where sensitive data has traveled and who has access to it?
- [ ] Are comprehensive audit trails available for compliance reporting and full chain of custody?

Key Management: Encryption is only as effective as the methods that protect, manage, and exchange encryption keys. Flexible encryption key management options better support compliance and data privacy by granting customers full control over where and how encryption keys are hosted and managed.

Key Considerations:

- [ ] Does the solution support encryption and decryption without requiring senders and recipients to manually exchange encryption keys?
- [ ] Does the solution support customer-hosted key management infrastructure that lets you directly control and manage your encryption keys?
- [ ] Does the solution allow you to meet data residency requirements?
- [ ] Does the solution prevent blind subpoenas that can leave your data exposed to government surveillance?
- [ ] Does the vendor use a split-knowledge architecture that stores encryption keys separately from encrypted content?
- [ ] Does the solution prevent unauthorized parties—including cloud providers and the solution vendor itself—from accessing encrypted content?

Ease of Use: User awareness and adoption are core aspects of a successful security program, and when it comes to encryption, this is especially true. When introducing a new solution, employees still need to be productive and get their work done. If encryption doesn't integrate with everyday business tools and workflows, employees will find workarounds that inhibit widespread adoption and weaken security.

Key Considerations:

- [ ] Is the solution straightforward to set up and implement?
- [ ] Can users leverage existing credentials?
- [ ] Do users have to install new software?
- [ ] Does the solution provide a centralized administrative interface?
- [ ] Are there customization options available?
- [ ] Does the solution offer seamless end-user encryption workflows to enhance security awareness and minimize administrative support costs?

Learn how Virtru easily protects data wherever it's created or shared.
virtru.com/contact-us.

Virtru is a proven innovator in data-centric security and privacy. As data is both the most valuable business asset and greatest risk, Virtru empowers every organization to take full control of all human and system generated data to optimize its value, while maintaining privacy. Creators of TDF (Trusted Data Format), the open industry standard for persistent data protection, Virtru offers a portfolio of products and tools based on its data protection platform that together create a protective ecosystem for better and more controlled collaboration throughout the data lifecycle—from data capture, to transmission, storage/organization, analysis and sharing. More than 5,000 organizations of every size and industry trust Virtru for data security and privacy protection. For more information, visit virtru.com or follow us on Twitter at @virtruprivacy.