IRONCORE LABS

DATA CONTROL WHITE PAPER

How to secure and track sensitive data in the cloud

OVERVIEW

Data control is the ability for data owners to know how their data is being used and by whom and to be able to independently revoke access, even from cloud service providers, at any time.

"Security and/or privacy concerns continue to be the top inhibitors to public cloud adoption."

- Gartner

Data control means no more wondering if a hacker or a curious administrator has peaked at the data. Even if they have permission to do so, they can't do it without leaving a trail.

Imagine you grant your doctor access to your medical records. You notice that your doctor is sharing your data with insurance firms, billing companies and outside research institutions. You decide that you are not comfortable with this sharing, so you click a button and instantly revoke access. You are the data owner in this scenario. Your doctor is your service provider. The insurance, billing and outside research institutions are third-party providers. Monitoring is your ability to always see who can access data and whether, when, and how they use it. Revocation is your ability to click a button and instantly erase your data from systems even if the data is held by partners.

Now instead of the individual level, imagine this power in the context of a business. Businesses own sensitive data with regulatory requirements and fines if that data is accessed inappropriately. Data control is a game changer. It brings privacy to businesses. It means businesses can think about the data rather than the systems where the data lives. It means making everything developer-proof and curious administrator-proof.

Data control is the solution to the age of data paranoia and the killer differentiator for cloud service providers.

IronCore brings privacy and security to any application

At the heart of data control is encryption coupled with unbypassable audit trails. We use these building blocks to build zero-trust systems that are data centric and storage independent. Developers add the IronCore libraries to their applications at the points where sensitive data needs to be entered or accessed. Optionally, this can be pushed out to client devices like the browser.

No longer do data owners need to literally hand over the keys to their most valuable resource and trust that all will go well. No longer do companies need to hesitate before moving to the cloud. No longer does the question, "what if an intruder gets past our perimeter and is in our network" mean that there's a breach that must be disclosed or any sensitive data that will be inappropriately accessed.

Data Control Principles

Data control is classically characterized by four key principles:

"Corporations do not have a right to 'personal privacy,' the Supreme Court ruled unanimously."

- L.A. Times, 3/2/2011

1. **Discover:** Control means knowing where data, particularly sensitive data, is stored. That includes any copies, such as backups, caches, storage on mobile devices, etc.

2. **Manage:** Control means deciding which actors (users and systems) have access to sensitive data and acknowledging that those decisions cannot be circumvented. Optionally these decisions specify not only the actors, but the devices or locations from which access is allowed as well.

3. **Protect:** The ability to guard against data loss and unauthorized access and to protect the data as it moves in and out of different storage systems is critical for control. This means ensuring that data is self-defending, with provable access guarantees.

4. **Monitor:** Supervision is the final key element of control. An initial promise of good behavior doesn't mean that a partner is able to fulfill it on an ongoing basis. Monitoring allows customers to see how data is being used, by whom, via which devices, and from where. Proper monitoring includes detecting anomalous behaviors such as unexpected devices or unusually large data transfers and being able to respond to those anomalies.

Data control must not be something that requires correct coding by developers. Instead, a separation of concerns that allows data administrators to set and enforce policies independent from developers must be in place.

Cross-cutting concerns

In modern cloud environements there are several cross-cutting concerns that become critically important for managing data. No longer is it true that the data we must protect is solely in our possession, on our servers, or behind our well-protected perimeters.

In the new normal, data is shared with partners, stored in cloud platforms, and distributed around the world under the jurisdiction of a variety of regulatory bodies and governments. Consequently, the management of that data must adhere to these additional principles:

1. **Platform Independence:** data control should work regardless of where the data is stored, who has possession of it, who owns the servers where it is stored, or what jurisdictions it lies within.

2. **Zero-trust Architecture:** Once upon a time we had internal networks that we trusted. Now we assume some of those computers are compromised. The perimeter-focused security model has completely collapsed and inter-server authentication is the new normal. Similarly, trust models between partners and vendors must be minimized to achieve zero-trust architectures with no unvalidated assumptions. Ultimately, no entity should be fully trusted with data access, but instead each piece of data should only be accessible by users and services with the right to see that specific data.

3. **Revocation Anywhere:** It can no longer be assumed that data that we control is housed on servers we own. True data control requires us to be able to revoke access no matter where the data is stored, even if it's in offline backups or with partners.