Achieving DevSecOps via Increased Data Security

Security is at the top of all IT professionals' minds when implementing new technologies. That's why ionir ensures security throughout all stages of the pipeline to achieve **DevSecOps**.

59% of DevOps professionals are worried about security and compliance needs and potential threats to containers.

Nearly 75% of organizations have a DevSecOps initiative in place with approximately 49% of organizations still in the very early stages of implementation.

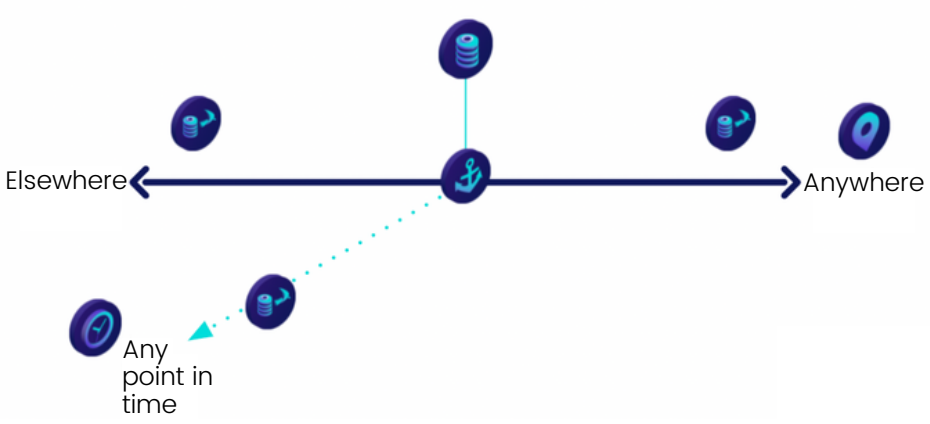
Data + Threats = Your Worst Nightmare

- Ransomware
- Corruption
- Theft
- Unauthorized access
- Other data loss

94% of organizations that endure severe data loss do not recover.

ionir enables DevSecOps Teams to Restore Data to Any Point in Time

With ionir, data can be presented at any point in time simply by adjusting the metadata name to include only blocks from that time. Persistent volumes created can be cloned and automatically protected with one-second granularity.



ionir enables DevSecOps teams to recover data that has been affected by corruption or loss to its most ideal state at a previous moment in time.

Data Addressing by Name Enables Data Mobility of Time

Data addressing by name allows the definition of data to move between systems without affecting the application's ability to access it.

ionir improves data security by providing an immutable and yet fluid dataset — impenetrable by attackers, resilient in the face of accidents, errors, deletion, and overwrite.

Kickstart your DevSecOps journey. Start your free trial of ionir.