# Security Suite

Mobility | Analytics | **Security** | Compliance

The modern enterprise's data estate consists of billions of files distributed across multiple geographic locations in a hybrid cloud infrastructure. The challenge enterprises face today is from both rogue agents and employees that may access and expose those files, resulting in a data breach. According to Gartner, an average data breach in the US costs an enterprise $7.91 million dollars, not including the reputational and credibility loss and the associated impact. Diligent monitoring and securing of files with the highest potential exposure is of the utmost importance.

The **Security Suite** of the **Data Dynamics Unified Unstructured Data Management Platform** and provides the ability to secure and protect data and generate immutable reports on that data. Its functionality includes:


## Immutable Audit Reporting

With ControlX, files can be classified and tracked utilizing block chain technology to create an immutable audit report that can be utilized for regulatory and internal data governance. The blockchain keeps a record of every time the file is accessed or modified, providing a digital chain of custody for files with critical business information. Immutable audit reporting is the foundation for enterprises to develop into secure file sharing across business units or even outside the enterprise.

The **Security Suite** and **ControlX** as part of the Data Dynamics platform empowers the enterprise to proactively mitigate risk, provide scalable security remediation, and generate immutable reports for validation.

## Intelligent File Re-permissioning

Generally, file permissions are assigned at time of creation or inherited based on the location where they are stored. Over the years, employees leave the firm and new employees join, creating a risk of inadvertently granting file access to unintended individuals. Using intelligent file re-permissioning, enterprises can provide access based on which employees need access on a regular basis or restructure access to meet the requirements of the business. Ongoing, policy-driven or user-led use of intelligent file re-permissioning ensures a consistent means to manage file permissions and, in turn, mitigate risk.

## Quarantine

When files have personal or business-sensitive information and are accessible by a multitude of users, this creates exposure and exponentially increases risk for rogue usage. **Quarantine** provides the ability to move files to a specified location and isolate them without anyone being allowed access. The air gap provided by Quarantine, with no means to access those files, helps you to prevent ransomware attacks on critical files whilst providing immediate protection.