

Safeguard your sensitive data the right way using data-level protections

Every enterprise has a gap between a written data classification policy and technical data protections. A written policy provides helpful legal boundaries but does little itself to safeguard data outside a user-trust model.



Cyclotron provides a complete approach to identifying, classifying, protecting, and monitoring sensitive data in a corporate environment, resulting in real-time views into where your highest-value data lives and flows within and outside your environment. Cyclotron's approach starts at protecting sensitive information at the data-level; any remaining gaps are then plugged at the app-level, device-level, and identity-level. Cyclotron's data protection approach is agnostic to the on-premises environment, making enablement possible for both on-premises and cloud-first organizations.

Microsoft Information Protection helps organizations shift from a written data protection approach to a technical implementation available to both end-users and administrators. End-users can apply file-level classifications to their data and protect it sending internally or externally so only the appropriate audience can open, read, edit, and share that data. Administrators receive operational and management-level reporting to demonstrate how classified, unclassified, and protected data flows across and outside the corporate environment.

Cyclotron's MIP implementation includes:

- Classifying data in your environment based on content, location, or properties
- Protecting sensitive data automatically and enabling end-users to apply protection
- Making your data classification policy available for users to select across all devices
- Notifying your SecOps team whenever sensitive data is mishandled or shared inappropriately
- Protecting against data leakage on unmanaged devices
- Increasing adoption and usage of data classification with end-user communications and training

Key outputs



Layered, appropriate security protections automatically applied across your environment



Real-time monitoring of sensitive data usage on devices, apps and corporate storage



Increased security boundary for sensitive data, whether on-premises or mobile



Technical implementations of compliance guidelines

Contact our team of experts to know more!

