Best Practices for Preventing Unauthorized Document Capture and Access

The Reality

Unfortunately, there's no foolproof technical solution to prevent screenshots. If someone can view a document on their screen, they can potentially capture it through:

- Screenshots
- Phone cameras
- Screen recording software

Practical Limitations

Prevention Through Access Control Rather than trying to block screenshots, focus on:

1. **Minimize Exposure**: Don't share sensitive documents digitally unless absolutely necessary
2. **Control Who Has Access**: Use role-based permissions (Managers, Editors, Viewers)
3. **Create Audit Trails**: Enable access logs so you know who viewed what and when
4. **Use Secure Platforms**: Store highly sensitive documents in end-to-end encrypted services like Tresorit rather than general cloud drives
5. **Implement Data Classification**: Classify documents by sensitivity level and apply appropriate security measures

Detection Over Prevention Since you can't fully prevent screenshots, focus on detection:

- Watermark documents with recipient-specific identifiers
- Maintain detailed access logs
- Use platforms that track viewer IP addresses and email verification
- Create clear policies about acceptable use

Technical Controls

Document Watermarking

- Add watermarks to sensitive documents for leak detection
- Tresorit offers watermarking features for shared videos and documents to prevent unauthorized re-sharing

Access Controls & Monitoring

- Use platforms like Tresorit that provide access logs to track who viewed documents
- Enable download tracking to monitor document access
- Implement time-limited access with expiration dates on shared links
- Use download limits (e.g., 5-10 opens) for highly sensitive documents

---

Revision #2
Created 6 November 2025 16:33:17 by Josh
Updated 6 November 2025 16:34:16 by Josh