WHITE PAPER:

Managing CAD File Data Leakage Risks in Design-centric Businesses

www.FinalCode.com

FINALCODE®

Drawings, illustrations, designs, specifications, blueprints, prototypes, creatives and models held in CAD (Computer Aided Design) files are highly valued. Whether in manufacturing, architecture, defense, construction, high tech, entertainment, life science, infrastructure or aerospace, exchanging confidential information, including Intellectual Property (IP), is a business necessity and business risk.

Project collaboration during the design and production process is often crucial to meet business and client needs and deadlines. Projects typically involve multiple managers, partners, contractors and subcontractors that require access and use of CAD files, or derivative information shared in Adobe Acrobat files, that contain sensitive designs, build plans, schematics, blueprints, project details and production manuals. It is also common to have employee, contractor and client turnover with potential inappropriate acquisition of these files. And with an increasingly mobile workforce needing off-site file access, unprotected files are often shared across users, devices, networks and collaboration services. As a result, file sharing in design-centric environments runs the risk of compromising a company's and their client's data protection obligations.

How can companies share CAD files with their engineering and production teams, contributors, contractors, supply chain, customers and prospects knowing that the sensitive content is safe against unauthorized access and usage? This paper shares the risks, file protection mechanisms, and pragmatic steps to allow design-centric organizations to effectively reduce file data leakage risks. The paper also shares FinalCode's easy, flexible and persistent approach to file collaboration security.

50%

of respondents had experienced frequent file data leakage incidents according to an EMA research report, the State of File Collaboration Security.

File Sharing Data Leakage Risks

According to an EMA research report, the State of File Collaboration Security, more than 50% of respondents had experienced frequent file data leakage incidents. This survey of mid-tier to large enterprises in North America cited that over 84% of respondents indicated that their organization had only moderate to no confidence in their security controls and auditing capacity to secure files. The top 3 likely causes of file data leakage were files inappropriately shared internally, those inappropriately shared externally and files exfiltrated through hackers and malware. Key file sharing risks identified in the report with regards to the most impactful file security incidents include:

- **65%** FILES INAPPROPRIATELY SHARED EXTERNALLY
- **58%** FILES EXFILTRATED BY MALWARE, HACKERS
- **56%** FILES INAPPROPRIATELY OBTAINED BY A TRUSTED INSIDER
- **52%** FILES MISTAKENLY SEND TO WRONG RECIPIENTS
- **49%** FILES INAPPROPRIATELY SHARED INTERNALLY
- **90%** FILES LEAKAGE VIA FILE LEAVING CLOUD-BASED REPOSITORIES AND MOBILE CONTAINERS

Clearly, the threat of file data leakage and actual incidents not only adds reputation risk but introduces compliance liabilities ranging from fines and loss of business transactions to possible imprisonment. CAD files do often contain confidential information and IP which have legal data protection obligations. Furthermore, should a related design file contain regulated information, such as personal identifiable information or financial source and transaction details, various data protection compliance mandates may at risk. For these confidential and regulated data types, design firms and departments need to ensure that the CAD file was encrypted and only accessible by appropriate persons, else various data breach safe harbors will not be available to an organization.

CAD files do often contain confidential information and IP which have legal data protection obligations.

Top File Protection Mechanisms for Design-centric Environments

There are a variety of controls that design-centric organizations are applying to reduce file data leakage risks due to the diversity of users, networks, devices and applications that can be used to share sensitive CAD and Acrobat-format files.

Email file security. Most collaborators use email to share files. Popular email encryption programs, such as PGP, allow users to apply file encryption to files as attachments in email. This requires a common system and trust relationship between sender and recipient organizations, which will automate authentication and file decryption processes.

Network file share access control. The most common way to collaborate internally is to set up access controls against public directories on networks that can be shared by different users and group. This method ensures appropriate access to files by authorized internal users, but it depends on the network share management efficacy, which often relies on the efficacy of user, resource and group directory services.

Secure File Transfer Protocol (SFTP). This method relies on maintaining access control lists and often password-based authentication mechanisms to allow a secure means for internal and external users to remotely access files.

File application invoked encryption. Popular applications, such as those from Microsoft and Adobe, have built in file security services. This involves the end user invoking the file protection and supplying a passcode from within the application. The passcode is then shared with the recipient which will allow the recipient, using the like application, to open the file. Here the risk is the passcode type, sharing, management and recovery.

Mobile Device Management (MDM). MDM systems rely on a client or profile services being activated on a mobile device (smartphone and even notebook) that is set up for corporate use to allow for mobile security standards and a container to be centrally managed. While files can be secured in a container, the control only pertains to files held in the MDM container and MDM systems have varying data wiping features.

Enterprise and Cloud-based Content Management. Enterprise Content Management (EMC) solutions facilitate access, search and governance services to be applied to files distributed within an enterprise's file storage infrastructure. While conventional ECM solutions are for internal use, File Sync and Share (EFSS) solutions extend these services through cloud-based storage and remote access means to files for both internal and external users.

Digital Rights Management (DRM). DRM systems provide companies the means to apply discovery, management, search, access, entitlement and other controls to files being access, shared and used. DRM services can be invoked as features within ECM applications or are separate systems that complement file services and ECMs. While the majority of these systems are designed for internal use, some provide means to facilitate DRM services outside an organization and as a complement to EFSS.

Certainly, the most widely adopted file security control is that of legal terms and conditions that set requirements for the protection and use of sensitive, confidential and regulated data often agreed between parties in a disclosure section of a business agreement. An organization would apply a set of controls based on sensitive file types and business transactions depending on business requisite, cost, business impact, practicality and risk appetite.

Of the file protection technical controls listed above, the majority lack necessary persistent access controls, usage controls or means for successful adoption by users outside an organization. Many of the controls above simply involve allowing secure network access to a file, or the encryption and decryption of files between authorized users. In this regard, once the recipient has local access to the file, other controls, such as restricting means to further prevent sharing of the file, limiting the use of the file, or tracking the subsequent access and use of a file are no longer active. Nor do these systems have a means to delete a file after it is local, having been removed from a repository or container. Next generation file-based digital rights management (F-DRM) solutions, such as FinalCode described later in this paper, address many of these file collaboration control limitations and more."

Next generation file-based digital rights management (F-DRM) solutions, such as FinalCode, address many of these file collaboration control limitations and more.

5 Steps to Reduce File Data Leakage

Given the necessity of file sharing, respective risks and obligations, and available file protection mechanisms, what is a pragmatic approach for organizations in design-centric environments to reduce IP and business loss due to file data leakage.

1. **File data classification and discovery.** The first step is to establish a working process to map different classes/types of files based on the information and the respective business or regulatory compliance obligations to protect the data in the file. Part of this step is to identify various sources and categorize different activities where sensitive files requiring protection exists, as well as the users, systems, tasks and business terms related to such activities.

2. **File sharing exposure risk and control gap analysis.** This step involves assessing how sensitive files in each data classification are currently secured and subsequently shared within and outside the organization across categories of business activity. The process further examines the potential probability and ramifications of exposure in each file data class and sharing activity group. The resulting risk assessment should reveal data protection priorities and gaps. The organization can then systematically assess what additional file data protection process and controls measures are needed.

3. **Policy definition enhancement and dissemination.** This step involves examining current data protection policies to determine which policies need to be improved to better manage risk that accommodate new categories of sensitive data and file collaboration activities. These policies should be vetted with, agreed upon and communicated to those managing data sources and data owners. This way the policies can be effectively adopted by IT management and business management.

4. **Technical control application.** This step takes the control gap analysis and policy definition processes into account by identifying where technical controls, such as the ones described earlier, should be applied. This step should assess each control's functional scope, and also consider management, implementation and cost factors. As in other IT projects, once a control is accepted, deployment, training, usage and administration should be coordinated.

5. **File security management tracking.** The last step is the management tracking of file security measures including some method of tracking and reporting policy adherence, control implementation, exceptions and additions, and control usage. In this way, managements can gain a management vantage point with regards to file data leakage risk reduction, and operations can establish a baseline for continuous improvement.

The FinalCode platform lets organizations, engineers, and design staff easily set file access and usage permissions, track file activity, and dynamically adjust policy for recipients as needed.

FinalCode File-Based DRM

FinalCode's persistent file security platform protects CAD files and respective derivative content in Adobe Acrobat files containing sensitive information no matter how these files are shared inside and outside of your company. The platform lets organizations, engineers, and design staff easily set file access and usage permissions, track file activity, and dynamically adjust policy for recipients as needed. Should a file be forwarded by mistake, copied or shared without authorization, or if the third party no longer should have access to the file, the file owner can change the policy and even delete the file remotely, ensuring any confidential or restricted information remains secure.

FinalCode enables design teams to readily define who and how sensitive files can be used by contractors, clients, partners and auditors. Our platform simplifies file encryption and permission management processes because it does require sharing passwords, managing certificate infrastructure or requiring complex trust models with those outside your organization. File owners have an intuitive interface to define security settings or use predefined personal or corporate templates. Once secured,

the protected files can be flexibly stored and sent using your current infrastructure and preserving existing workflows. Collaborators merely install a lightweight FinalCode client which allows authorized recipients to open and work with the CAD, Adobe Acrobat and other popular file type in the application they are accustomed to and according to policy. Key features include:

- Supports 2-D, 3-D and business specific modeling platforms from AutoDesk AutoCAD and DWG TrueView and Dassault Solidworks.
- Set up external users quickly and easily to allow for practically immediate secure collaboration.
- Reduce the risk of data theft with strong 256-bit AES file encryption, comprehensive file-based IRM controls and rich activity logging.
- Restrict access and usage by recipient, time and other attributes for files shared with customers, prospects, partners, contractors and supply chain.
- Delete files on demand, by policy or automatically if shared with an unauthorized user.
- Securely share, review, edit, print, and forward business critical and privacy-sensitive CAD and files across public or private networks, collaboration platforms and popular devices.
- Low total cost of ownership as the solution can be selectively implemented by department, division, project or application – with free use for recipients external to the organization.

FinalCode's file-based DRM solution, in conjunction with other available technical controls, offers an flexible and effective means to reduce CAD-file data leakage risks across different infrastructure, collaboration methods and business requirements.

An innovator in file-based information rights management (IRM), FinalCode's platform is easy, interoperable and scalable to provide fast and reliable file collaboration security that complements existing file storage, enterprise content manager systems and cloud-based file collaboration. Delivered as a SaaS or on premise solution, FinalCode can be rapidly deployed and scaled as needed; by project, department or enterprise-wide. Apply it to specific internal and external users, or projects, to gain immediate persistent file protection; deploy at a greater scale later as your collaboration security requirements grow. There's simply no easier way to keep your engineering project files secure as they are shared within and outside your organization.

CAD File Collaboration Protection Begins Now

Alongside the task of maintaining fluid but authorized access to network file storage resources, organizations need to apply file protection that offer appropriate levels of control for the internal users and the variety of external users requiring access to sensitive content. Satisfying these challenges is necessary to protect the intellectual property of the business and its clients, and to manage the reputation and liability risks associated with confidential information obligations. An organization does not have to take an "all or nothing" approach to implement file data protection capabilities. While the steps presented in this paper to reduce file data leakage can be an enterprise-wide initiative, the process can be successfully applied to specific business activities and design projects. FinalCode's file-based DRM solution, in conjunction with other available technical controls, offers an flexible and effective means to reduce CAD-file data leakage risks across different infrastructure, collaboration methods and business requirements.

About the Author

Scott Gordon (CISSP) is the Chief Operating Officer at FinalCode. Scott has over 20 years' experience contributing to security management, network, endpoint and data security, and risk assessment technologies at innovative startups and large organizations. Prior to FinalCode, Scott held several senior management positions at ForeScout Technologies, Protego Networks (acq. Cisco), Axent and McAfee. An infosec authority, speaker and writer, he is the author of "Operationalizing Information Security" and the contributing author of the "Definitive Guide to Next-Gen NAC." Scott holds a CISSP-ISSMP certification, an MBA, and earned his BA in MIS and marketing from Hofstra University.

Take the Next Step

With FinalCode, your employees can share sensitive files internally and externally with confidence, knowing that unauthorized recipients will not have access. Better yet, your company can rapidly implement strong file protection, entitlement and auditing capability that preserves user expe¬rience and your investment. FinalCode's persistent file security platform provides an easy and flexible approach allowing you to use your existing file share, enterprise content management, cloud storage and collaboration platforms.

www.FinalCode.com inquiries@finalcode.com
3031 Tisch Way, Suite 115, San Jose, CA 95128 P: 855-201-8822 (Toll Free)

FINALCODE®