FinalCode Enhances File Collaboration Security for Pasona N A

Background

Pasona N A selected FinalCode to secure their file collaboration with employees, temporary employees and their customers. The project to enhance protection of files containing business sensitive and regulated data was to choose a tool that was easy to administer, scalable and utmost provided ease of use for their internal and external users. Pasona N A reported that the FinalCode deployment mitigated their major business risks around data security and also resulted in experienced benefits that range from ease of implementation and management and cost effectiveness, to a variety of applications and short time-to-value. The level of file security FinalCode provided allows Pasona NA to alleviate the real data protection concerns of their shareholders, customers and prospects.

"Data protection is essential for our company. Since our business relies on efficient sharing of information, we recognized the potential risk of exposure of sensitive data and shared files. With FinalCode, we now have confidence in our ability to better manage that risk in a cost-effective way. FinalCode delivered on our adoption and management expectations – we found it extremely easy to use, deploy and manage. The level of file security it provides allows us to alleviate the real data protection concerns of our shareholders, customers and prospects." Kenji Furushiro, President and COO of Pasona

Business Problem

Pasona N A, Inc. provides professional HR services such as temporary staffing and recruiting services, as well as accounting outsourcing services to medium and large enterprises. The Company's headquarters is located in New York and they have 10 offices throughout the U.S.; in New York, California, Georgia, Texas, Illinois, and Michigan. Part of a global organization, the Company has hundreds of customers, thousands of temporary employees and job applicants and more than 7900 employees worldwide. The Company's business, by nature, is data and collaboration intensive. Thousands of files containing sensitive and regulated data are managed through its operations, which is the motivation for enhancing security capabilities, in order to protect the files from unauthorized access.

The information that Pasona N A processes often contains financial records, business analytics and personal identifiable information (PII) which may include email, bank accounts and social security numbers. The organization wanted to make sure that they could secure files being accessed internally and shared with their customers and candidates.

Sayaka Doi states, “As Director of Professional Services, it is my responsibility to not only ensure our systems are appropriate and available, but also that they are secure. I wanted to see if I could enhance security capabilities for file collaboration which represents a good part of our business. I also wanted to achieve this in a way that would be cost-effective and have broad application. We not only exchange files via email, but also through file collaboration platforms such as Dropbox, so we were also considering the security of files shared in any way. After presenting the options and value to our business, our president gave the final approval to choose FinalCode.”

Selection Process

Key considerations for Pasona N A in the selection process were usability, low implementation and administration effort, and the means to have file security easily extended to users, such as customers and job candidates, outside of the Pasona N A organization.

From the business perspective, major consideration factors were that the security must be effective, but not cumbersome, for users or administrators. Pasona N A only considered systems that offered centralized policy management and would easily support customers and candidates. The product would need to offer a low cost of deployment which could work in their current environment, as well as accommodate external user PCs. It was imperative for Pasona N A staff to easily exchange files with external parties and for these parties to easily be included in the file information rights management system.

After assessing various alternatives, Pasona N A believed a SaaS would be faster to set up and manage versus on premise solutions. The vendor needed to support common applications such as Adobe Acrobat, Microsoft Office and also media files. About half of the Company’s use would relate to protecting file attachments in email and the other half concerned protecting files distributed through a cloud-based content manager. They needed support for Windows computers and Apple and Android tablets and smart phones; in the future they will consider Macintosh computers, but that was not an immediate requirement.

The company looked into cloud-based file sharing products and other approaches that applied encryption based on password protection. Pasona N A felt that the security controls outside the service were not strong enough. The cloud file sharing products did not offer data protection outside of the cloud application, so an authorized end user receiving a file would have the ability to share the file with others and that file could not be tracked. As a result, Pasona N A could still have an exposure of sensitive information.

Pasona N A also investigated a password-protected file encryption vendor that supported Adobe Acrobat but did not apply strong usage control or track files. This would require users to manage passwords for each file or each time they used the system. Pasona felt that this approach would not be easily managed as the company grew, especially since users often forget passwords, and also because the product only put controls on Adobe files. A third solution option worked with Microsoft applications but would make it difficult to support external customers, contractors and job candidates. After testing it, Pasona N A believed it had the potential to disrupt operations and would only apply to certain Microsoft applications. The Company determined that FinalCode would be the most appropriate solution, offering greater flexibility for implementation and use, with broader and more effective defenses.

Overall, the ease of use, simple administration, and range of security features distinguished FinalCode from other solutions. Pasona N A especially appreciated the automated provisioning, document tracking and remote file deletion capabilities.

Rather than bring the platform in-house, Pasona N A preferred to use an application as a hosted service which follows their corporate-preferred license model. The Company determined that it would make the procurement and deployment more manageable while also generally reducing operating costs and capital expenditure. They were able to get FinalCode SaaS up and running with very little effort and without a full time dedicated administrator.

Solution

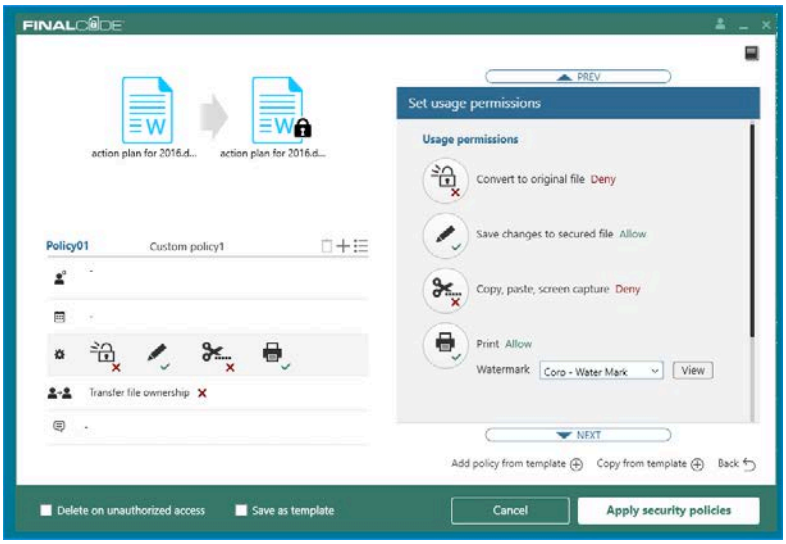
Pasona N A is extremely pleased with how simple the FinalCode platform was to deploy and expand to use. Since its IT operations is mainly outsourced to outside contractors, the Company wanted to make sure that the day-to-day administration would be minimal. They literally rolled out the system and communicated to internal and external users, in a matter of weeks, without any issues or roadblocks. Pasona N A only purchases licenses for employees that use FinalCode, with no charge for external customers and job candidates. They found it extremely easy to administer and has strong user acceptance. As a result, Pasona NA advanced their data security controls and can keep track of all business files being shared.

“User and customer satisfaction is highly important for any security application that can affect workflow and how we conduct business,” said Sayaka Doi, Director of Professional Services at Pasona N A. “I am pleased that our users find the product very simple to use either by setting recipients, encryption and permissions as needed, by invoking a pre-defined template or by merely dropping a file into a FinalCode-monitored folder.”

The first run deployment was to a handful of internal users and some customers to test different use cases. The production deployment was applied to more than 60 employees across California, New York and Illinois, including hundreds of clients and candidates. Pasona N A can purchase additional licenses as needed, rather than for everyone up front. The next phase will expand use to approximately 100 users within North America and a much broader external user install base. The roll out of FinalCode has been smooth and serves as an example of proactive management for other parts of the company.

"The FinalCode platform was really that simple to implement. After an internal process and communications review, and informing internal and external users of our data privacy policy and new file security tool, we have not experienced any unusual help desk call volume and have had no significant issues. It just works," added Sayaka.

FinalCode allows users to apply ad hoc file security controls, but the system also supports template use. Pasona N A has created a set of templates, based on different requirements, file information and recipient, to allow users to very quickly apply security to a file using a literal point and click process. This includes which users and companies can access files, how long access is granted, and if they may only read or have editing permission within a secured file, or merely encrypt and keep track of files that are being accessed. Pasona N A plans to use the folder monitoring capability to further protect internally shared files or those accessed by data processing partners.



Pasona N A was able to justify the purchase by representing the industry best practice of securing sensitive and regulated data to executive management, and by demonstrating how easy FinalCode is to manage, and how quickly it could be rolled out to internal and external users. They did not have any immediate need to address specific compliance requirements, but file encryption and access control supports a multitude of data protection specifications.

"Except for anti-malware, it is not often that you can implement a product and get immediate identification and prevention of an issue," said Kenji Furushiro. "FinalCode not only makes it easy for our users to protect files, but the file controls and automated response are so extensive within the system that the avoidance of the potential security incident validated our purchase and planned expansion."

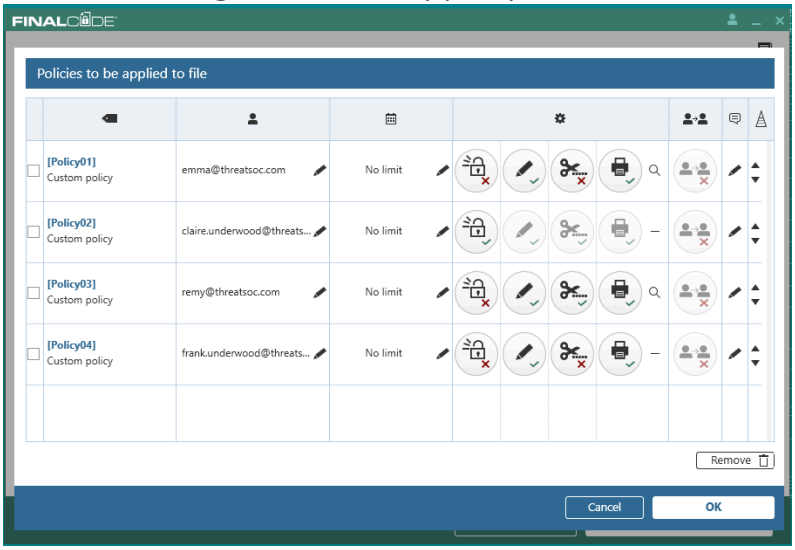
FinalCode Details

FinalCode offers a file encryption and file-based enterprise digital rights management (eDRM) platform that is agnostic to file storage, distribution and content management. As such, FinalCode can work with popular applications, devices, cloud storage, content management systems, and collaboration tools. Offered as either a software as a service (SAAS) or on premise virtual appliance software , the solution can be flexibly deployed as needed for an individual, department, business project, or enterprise-wide.

FinalCode delivers persistent file protection with strong encryption and an extensive array of granular controls including file traceability and means to remotely delete files even after they have

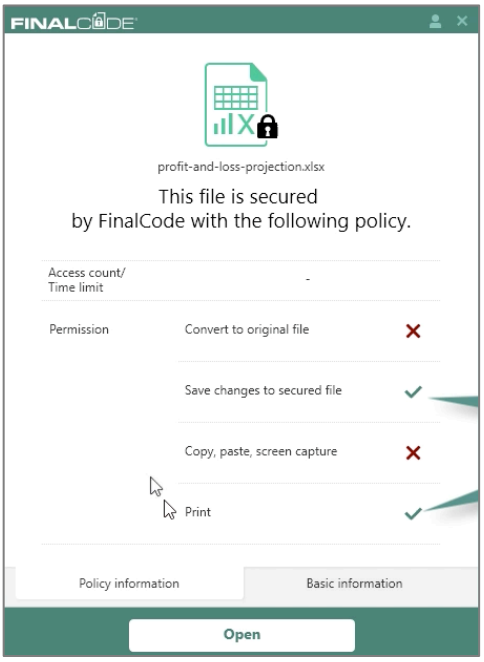
been distributed. Recipients of FinalCode-secured files have no learning curve. Once installed, FinalCode client presents recipients with a simple splash screen depicting the usage permission. As such, the approach preserves user experience by integrating within existing file sharing workflow and allowing the recipient to work in the applications they are used to.

For any file that an enterprise user would like to share, the user sets one or more permission sets to a file using the FinalCode client. Upon the user activating the file security policy, the FinalCode client encrypts the source file and sets file permissions (e.g. duration, open, edit, save, print, screenshot) for each authorized recipient. These permissions can be set manually by the file owner or automatically based on a pre-defined enterprise template policy. This security control not only can be invoked by the user, but can be automatically applied as files are placed into local or network folders, or triggered by an external application. While the resulting file is encrypted and can only be opened by a FinalCode Client application, only the file security meta data, not the original file, are send to the FinalCode server for secure storage, management and logging.



Once FinalCode has secured the file locally, the file owner can readily share it directly with the intended recipient(s), via any communication channel the user would like, including: enterprise content managers, cloud storage and collaboration apps. The FinalCode server can email new file owners and recipients as a means of self-service on-boarding.

When another user receives the file and tries to open it, FinalCode (installed on the recipient's device) checks the FinalCode server to verify permissions and securely send the respective file encryption key and permissions. The FinalCode client then locally decrypts the file and enforces usage at the application and operating system level. File access attempts and activity is logged and available to the file owner and the enterprise.



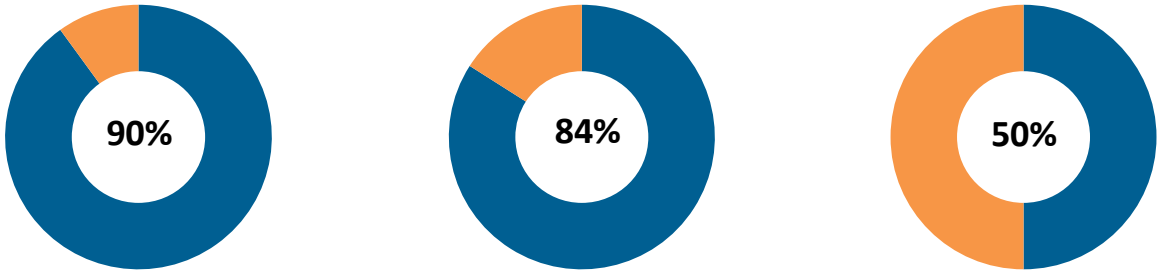
If an unauthorized recipient tries to open the file, FinalCode will deny decryption and log the illicit attempt details. The user can also dynamically modify recipients and permissions and can do so directly or by request from an authorized recipient. Finally, upon unauthorized access or usage attempt or if the file owner decides to remotely delete shared secured file, FinalCode will block any further access attempts and send a File Delete command to the recipient's device.

FinalCode revolutionizes the way businesses can persistently protect sensitive files wherever they go within and outside an organization. It's easy, fast, requires less overheard and is more cost effective when compared to more conventional eDRM and file-based encryption solutions. FinalCode also simplifies user provisioning and managing multiple users and their devices – especially for users outside an organization.

File Collaboration Security Risk Context

Enterprise Management Associates (EMA) recently released the 2015 State of File Collaboration Security report. The survey and analysis of more than 150 respondents from mid-tier and large enterprises was completed by EMA in September 2015. Some of the key findings include:

- All organizations, across IT, security and line of business roles, are concerned about file data leakage risks, and 75% expressed very high to high concern. However, 84% had moderate to no confidence in their security controls and auditing capacity to secure confidential files
- More than 80% experienced file data leakage incidents in their organization, and half expressed frequent incidents
- While the majority of IT organizations have enhanced technical controls and auditing, only 16% felt highly confident in their file security investments – indicating an underlying insecurity in monitoring and enforcement capability. Consequently, file encryption and usage control software was cited as the top upcoming control investment
- More than 90 % stated the lack of protection of files leaving cloud-based platforms or device containers as the highest risk to adopting cloud-based file storage and collaboration service



Fear leakage of files leaving cloud-based collaboration and device containers

Have no to moderate confidence in their file security controls

Experience multiple file data leakage incidents

Source: Enterprise Management Associates, 2015

- The three most likely causes of data leakage cited: Inappropriate file sharing with 1) others inside the organization, 2) those outside the organization, and 3) through malware and hackers

Author: Bojan Simic, Founder and Chief Analyst, Digital Enterprise Journal

Digital Enterprise Journal (DEJ) is a media and research firm focused on digital transformation and the business value of technology deployments. Some of the key areas of DEJ's coverage include: key market dynamics of digital economy, strategies of digital businesses, evaluations of technology solutions, key performance metrics used by digital businesses and digital maturity assessments. More information on dej.io