EFSS with Secrata:

Secure Ad Hoc File Sharing for Financial Institutions

Use Case #1 challenge

Financial institutions face security threats daily, and for today’s banks and their clients, information most often is money. Today’s bank robber wears multiple masks: Identity thief, hacker, and online, check, mail, and card fraudster. Bank security must prevent these attacks 24/7/365, not just during banking hours. And for banks, information is money.

Walk-in loan applicants often need to open a new bank account, provide financial information from other personal sources and other banks or branches, and immediately access and transfer loan funds to cover their immediate financial needs. To securely meet this customer’s needs, a bank’s commercial loan officers, loan documentation specialists, financial analysts, and customer services representatives must be able to securely access and share sensitive data and files with each other—and with the new loan customer. Patching together phone conversations, email attachments, electronic facsimiles, FTP documents, and so-called “secure” file sharing services presents massive security threats to both the bank and the new loan customer.

EFSS with Secrata

Enterprise File Sync and Share (EFSS) with Secrata provides today’s financial institutions and their customers the security they need to securely share files and sensitive data between branches, headquarters, and bank clients without disrupting or delaying bank services.

Using EFSS, the branch loan officer, loan documentation specialist, and customer service representatives can securely access and share all loan-related documents immediately and without threats to data security, whether those documents are produced, accessed, and stored locally, at another branch, or in a cloud service. Built on the Secrata platform, EFSS's unique data storage and security methods allow the bank's and the customer's data and files to be accessible only to authorized and authenticated users. So, when the customer provides identity and financial information, the branch loan officer can convert files to electronic form and immediately allow access to a specific loan documentation specialist for immediate review—without the security threats inherent to email or FTP. Using EFSS workspaces, branch and headquarters bank officials and loan consumers can access the same information securely and immediately, facilitating fast, responsive service without threatening the bank’s or the customer’s data security.

All data being shared during the loan application and approval process are first shredded into chunks, and each chunk is encrypted and protected with an individual key so that unauthorized users cannot access this sensitive data. Additionally, all file sharing required by the process is fully auditable and reportable to both the bank and the customer, further increasing its security and reliability. The loan customer and the bank’s security center and information security team can track the process in real-time and the loan customer’s information is protected throughout the approval process.

The bank’s security—and its reputation for high-quality customer service—is ensured.

Cloudview with Secrata:

Secure Mobile Data Access and Sharing for Financial Institutions

Use Case #2 challenge

Regional banks face tough competition from national and international financial institutions. Bank officials from these smaller banks rely on fast and personal service to win new accounts and retain existing customers—but today's bankers must ensure both data and financial security as well as quality customer service.

Generating commercial clients for the bank means visiting customer business offices and shops to attract new accounts. Currently, that means the customer must gather information and documentation, visit a bank branch, complete paperwork, and wait while the bank processes the new account—and banking hours are also business hours, so the customer may lose valuable time and money in the process. New small business and commercial customers should be sold and secured on-site—any site—during that first meeting.

Cloudview with Secrata

Using Cloudview with Secrata, new account representatives can safely and quickly access the information they need to open accounts and secure new business, on-site at the customer's business or on-the-fly. After hearing about the bank's services, the prospective small business customer wants to immediately open an account. Using Cloudview, the bank representative has access to all bank information immediately, regardless of where he is—on-site with the customer, at the airport, or even in a restaurant—or where that information is stored—whether on the bank's network fileshares, an Internet portal, or the banker's desktop machine.

Using a tablet—or even a smart phone—the banker can pull up and complete new account forms, pull client information gathered prior to the meeting, access collateral banking information, and manage and share sensitive information from the client immediately and securely through a single interface. The security of both the bank's and the client's data are ensured through Secrata's data shredding and encryption layers, which means that data are only accessible to authorized, authenticated users and no data or files are ever transmitted or stored in an intelligible format. The banker can gain approvals from loan officers or branch managers by inviting them to fully secure workspaces where signed forms can be updated and approved, and new account information can be immediately received by the new customer.

Because they can securely access and manage bank and customer data from any device, anywhere, bankers who use Cloudview save new business clients time and money as they open new accounts.

Email Gateway with Secrata:

Secure, Traceable Electronic Information Transfer for Private Banking

Use Case #3 **challenge**

Financial institutions that provide tailored financial solutions to high net-worth clients must ensure the security of both the bank's and the client's information without disrupting the client's work habits.

Services like private banking, asset management, and investment advising require frequent, file-intensive communication between the bank and the client. Attaching these sensitive files to emails is convenient, but hardly secure, and email transactions are neither auditable nor track-able by the sender. Email itself is vulnerable to many different security threats, and bankers providing wealth management services face the challenge of securing client communications without interrupting their clients' workflow. As well, banks must be able to provide their clients with immediate reports detailing when and with whom specific data and files have been shared.

Email gateway with **Secrata**

Email Gateway with Secrata meets the secure file management and sharing needs of both banker and client without requiring clients to learn a new interface or interrupting their workflow. Secrata also gives shared files a single, secure storage location. The file is no longer replicated through multiple email servers; all access to the file is managed securely through the Secrata servers allowing full auditing and access controls to be applied. Additionally, because of the integration with AD and the robust RBAC system in Secrata, permissions to access and/or modify the file can be controlled on both a per group and per user basis.

Private bankers can communicate with their wealth management clients via email, attaching sensitive documents like spreadsheets, investment reports, and asset management plans without worrying that unauthorized users can access the attachments or hackers can intercept the file in transit. Clients can send personal and financial data to the bank in email attachments with the same confidence in their security. When a file is attached to an email message in a standard email client (MS Outlook, for example), Email Gateway immediately secures the file by shredding it into chunks, encrypting each chunk, and creating a unique decryption key for each chunk. The file is then transmitted separately from the decryption keys and is not reassembled until the authorized recipient has been authenticated by Secrata.

All email attachments secured using Email Gateway are fully auditable, which means that the file's identifying information (file type, file name, file size, sender, recipient[s], etc.), as well as information about the transfer itself (transfer time, completion), is tracked and can be reported immediately to the bank and the client. The receipt and access of the file can also be tracked and reported, as can any issues that occur during email transmission. Reports created by Email Gateway can be uploaded into different data visualization applications and reviewed by either bank or client. Email Gateway's full audit trail augments security for both client and bank IT and InfoSec professionals. Because it works behind the scenes of the user's email interface, there are no additional steps or lost time for either banker or client.

Top Five Tech Spending Increases in 2015

46%	42%	38%	36%	35%
Security Technologies	Cloud Computing	Business Analytics	Storage	Wireless Mobile
	52% over 1000	46% over 1000	46% over 1000	
	35% under 1000	26% under 1000	29% under 1000	

The percent of those decreasing spending in each tech area is insignificant for 2015, with the exception of **hardware, where 24% said they expect to decrease spending**.

Source: Computerworld 2015 forcast study