resilient
network systems

SECURE DISSEMINATION OF SENSITIVE DATA AND FILES

March 2016

info@resilient-networks.com
415.291.9600

THE CHALLENGE

Throughout government agencies and in many commercial enterprises, sensitive information contained in files is routinely shared with other organizations, including suppliers, distributors, partners, and customers or citizens. While such burgeoning file sharing has led to greater collaboration, once sensitive data is released to external parties, it becomes impossible to control the further dissemination of such data. Liability risks are amplified due to Shadow IT and employee / contractor turnover, mobile devices, unsanctioned applications, personal e-mail, cloud storage and unsanctioned file sharing services that are outside an IT organization's oversight. In the face of these challenges, organizations are seeking ways to protect intellectual property and personally identifiable information (PII), to avoid adverse regulatory, financial and legal liabilities, and to safeguard their reputations while enabling the information sharing necessary for continued business success.

According to the 2015 State of Secure File Collaboration Report, the current state of file sharing is alarming: 83% of organizations experience file leakage incidents, 65% of files have been inappropriately shared, 52% of files have been emailed to the wrong recipient, and 52% of files have been stolen by a trusted insider. Whether these actions are simply user error or malicious, they should be monitored and prevented to protect the business.

Organizations must let files get shared freely, but only with dynamic access and usage control policies that are determined by the original data owner, even on devices beyond the enterprise's IT control. The policies protecting the data must change if necessary, and such changes must be updated to protect copies of those documents, no matter where such files reside at the time. Further, the policies should address the authentication of the individual to the level required by the data owner, the authorization of the individual to see the data based on attributes or roles, and account for other context during the file entitlement decision.

SOLUTION OVERVIEW

To address these sensitive file dissemination challenges, Resilient Network Systems' network-based policy engine has been coupled with FinalCode's file-centric security digital rights management product to provide persistent access control and user rights on all types of data sets and document types.

Without a network-based approach, such access control requires application specific changes that are static and often lack scalability for the enterprise and its partners. Therefore, it would be difficult to implement a comprehensive, enterprise-wide policy that applies to all sensitive information, given the discrepancies between disparate systems.

FinalCode provides the mechanism to protect, limit and revoke access to the data at all times, even when it has been downloaded from the originating system. Resilient's technology connects to any number of authoritative sources to resolve simple or sophisticated policy workflows. The combination of these services addresses both the validation of the user and the file-level rights management required for today's information sharing needs.

SOLUTION DETAIL FOR EXTERNAL SHARING

In order to have proper protection of sensitive data sets and files, first step is to establish receiving party's identity by interacting with authoritative sources (both internal and external). Typically this is a check of a corporate directory to validate their employment status plus an authentication step or two. Resilient is pre-integrated with industry-leading providers of identity proofing, out-of-band phone or SMS authentication and knowledge-based authentication. If higher assurance levels are required, a request for a voice sample, facial/iris scan, or fingerprint to compare it to a known biometric can be added to the workflow. The use of network-based attestation services (i.e. "Click here to attest that you are the authorized recipient of this document") can also be a deterrent and audit trail. For mobile devices, geo-fencing, beacons and device signatures can be included. Finally, if the login is from within an organization's facility, the network can check against physical access security systems to confirm the user is resident at the facility during the time of the access request.

Once the identity of the user has been established, it now becomes important to understand whether the user ***should*** have access to the sensitive file based on their attributes and the context of the data or environment. The owners of a data set can establish policies for file access and usage based on the role or attributes of a user and the situation in which the information is being requested. Such policies will be invoked anytime a user attempts to open the file, irrespective of their organizational affiliation – the ability to maintain persistent control of sensitive files within and especially outside an organization is paramount. This is also true even when files are downloaded from the system to be used in native applications (such as Microsoft Office or Adobe Acrobat Reader) or stored locally on devices. Based on the applied permission template, the solution can restrict the users' ability to view, edit, copy, print, save or forward content. Access to protected documents can be dynamically expired even if it resides on a USB drive or moves to a third party device.

Ideally, sensitive files should not remain accessible on a recipient device should there be unauthorized attempts to access the files, or if the need to share expires. This solution includes the capability to delete and erase files after they are shared. Likewise, recipients may require additional and new sensitive file usage capabilities depending on different conditions. In such case, the data owner should have an efficient way to dynamically modify access and usage policy based on recipient request or policy change.

SECURITY EVOLVES WITH THREAT LEVEL AND USER RISK

In an emergency situation, policies automatically adjust to allow or restrict data access, or to require additional validations. Data security officers can also set policies based on threat levels issued by their Security Operations Center (SOC). These dynamic changes can be achieved without requiring changes to the specific data sets or documents being protected.

Likewise, since a user's trustworthiness can change over time, policies enforced by the network

can be written to include input from insider threat systems and anomaly detection systems. If an insider threat system is not available, policies related to the volume of access request (i.e. over 100 in a day) can trigger phone authorization to a supervisor. The solution can also be set to automatically revoke access until alert are resolved.

FINALCODE SCALES, WITHOUT MOVING YOUR FILES

This solution is compatible with local storage, cloud storage and existing infrastructure investments. Scalability is achieved by separating the DRM function from file sync containers. This approach ensures that files are protected wherever they go, not just inside secure containers. FinalCode performs file encryption locally and then sends the security meta data (key and entitlement controls) to its central file security management system, whereby the sensitive data remains with the data owner / organization. Employing standards-based key management functions, a unique key is applied to each file. This file security management capability enables users to easily extend file access and usage controls to a wide variety of file types including Microsoft Office, Adobe Acrobat, and video, audio, and Computer Aided Design (CAD).

For manageability, DRM polices are maintained outside the secured file so that control is maintained on such files where they are stored. This prevents a loss of visibility and control when files are being downloaded from a cloud-based application or device container. In addition, file DRM policy can be a centrally managed policy and applied to shared network folders. By dynamically applying control to files being placed in monitored folders, such automation assured policy application while eliminating any workflow change requirements of end-users - allowing them to continue working with familiar applications and storing files in existing network shares. File lifecycle auditing capability allows organizations to have control over their data regardless of how and where the files are shared. It also allows the organization to see where the data is being consumed. More importantly, failed attempts at opening files can serve as a threat detection mechanism for both insider threat and outside adversaries trying to gain access to critical data. Lastly, it allows for data privacy breach notification safe harbors since the organization can prove that shared sensitive files were encrypted and both access and usage were under control.

Finally, from a secure mobility perspective, it is also critical for the solution to have integrated productivity tools to equip users to work with content on mobile devices. Users need to be able to view, create, edit, and annotate documents in order to be productive. Without such tools, users will turn to unauthorized third party applications and seek ways to bypass the security controls mandated by the organization. That is why a truly effective, comprehensive security solution must implement and enforce policies as well as empower users to get work done. The architectural approach taken by both companies and both products is optimal for scalability, manageability, auditing and control.

ABOUT RESILIENT

Resilient Network Systems makes adaptive access management software for identities you

don't (or can't) manage. Our network-based, distributed architecture is highly flexible and scalable, allowing customers in government and enterprises to safeguard their data and applications, while enabling more collaboration and information sharing with their entire ecosystem. We make it simple to leverage existing identity and security products, or add external identity sources and services, with easy-to-implement, predefined and custom policies. Resilient Network Systems is a privately held, venture-backed company based in San Francisco.

ABOUT FINALCODE

FinalCode delivers a file security platform that allows any business to persistently protect sensitive files wherever they go inside and outside of their organization. Available as a SaaS or virtual appliance offering, FinalCode makes securing file collaboration easy, flexible and cost-effective and in a way that works with popular applications, platforms and devices while preserving user experience and workflow. The solution applies strong encryption and granular usage control on demand or by corporate policy with the ability to remotely delete files on unauthorized access and usage attempts. As a result, companies can confidently share files and reduce data leakage risks. Headquartered in San Jose, California, FinalCode offers its solutions through its global network of authorized partners. For more information, visit www.finalcode.com.