Solving the Challenge of Need-to-Know Security (at Scale)

iManage

These Are Risky Times for Firms

Security used to be a relatively straightforward matter for professional service firms. Implementing antivirus software, firewalls, and other perimeter defences allowed firms to sleep soundly at night, secure in the knowledge that their client data was safely protected from most danger.

Unfortunately, those days are long gone. Increasingly, professional service firms are under cyberattack by outside actors, who use sophisticated social engineering techniques like phishing to gain access to valid user credentials that allow them to entirely bypass a company's perimeter defenses. With legitimate credentials in hand, these hackers can gain access to the sensitive data residing on a company's servers.

At the same time that attacks are coming from outside the firm, malicious users who are already within the firm can cause serious damage, as the Snowden leaks and numerous other incidents involving insider threats have readily demonstrated.

The danger of these threats is amplified by the fact that professional service firms have historically operated with open security so that their professionals can take advantage of previous work material. (According to one survey result in the ILTA 2016 technology survey, 93% of law firms are still running an optimistic security model).

This combination of factors conspires to make people the weakest link in a firm's security model. As a result, firms need to operate with the expectation that a breach is inevitable and look to minimize the impact.

Further driving the sense of urgency around this issue, clients are becoming more demanding about how professional service firms handle their confidential materials — and in many cases, they are calling in their right to audit.

Meanwhile, European regulations such as the General Data Protection Regulation (GDPR) — which takes effect in May 2018 — place explicit reporting requirements on companies in the event of a breach, with penalties as high as 4% of revenue for failure to comply.

The bottom line? How firms approach security is no academic matter. The cost is real in terms of reputational risk and operating risk.

Solutions… in Search of Scalability

Data segmentation and need-to-know security are key parts of the solution to the security challenges that firms face.

- **Data segmentation** ensures that a malicious insider or an attacker using stolen credentials and masquerading as an employee is limited in what he or she can access, minimizing the damage from a breach.
- **Need-to-know security,** in contrast to the open security model traditionally employed at professional service firms, ensures that access to a certain set of data is only given to those that need it, and no one else.

Unfortunately, existing products for security policy management do not present a scalable solution. Many offerings in the space started out as products that delivered ethical walls, keeping conflicted users away from relevant content. Vendors have tried to re-position these solutions as delivering need-to-know security access, but they are struggling to deliver this at scale.

There are several serious drawbacks around existing products:

- **Folder Settings.** Current products typically operate by cascading appropriate security settings when a wall is created, touching every folder and document in the workspace being protected. This cascade has the potential to open up private folders and give access to sensitive content to individuals who were not allowed based on the original security settings.
- **Performance Load.** The cascade also triggers re-filing and full content re-indexing when a wall is created,

resulting in a very noticeable load being placed on the document management system database and server. It also creates a large indexing queue, which prevents new documents from being indexed and delays their inclusion in search results. Users are impacted by a slow running system and inability to search and find recently added documents.

- **User Access.** After a wall has been applied, there is the risk that a suitably privileged user can update the cascaded security settings and accidentally grant access to a user that is not allowed by the wall — opening up access to sensitive content. Some solutions guard against this by running a scheduled check of all security changes at specific time intervals. Even if it runs every 10 minutes, though, there's still a window of time when restricted content could have been made available to people who are not meant to see it. Because of these weaknesses, firms cannot give their clients a *definitive* list of who has had access to their materials.

The strain placed on document management systems by existing security products is only set to get worse over the next 12-18 months, as more and more clients insist that their information be secured appropriately — and the demand for need-to-know policies continues to grow.

The iManage Approach

iManage Security Policy Manager takes a more scalable approach to security. Tightly integrated with iManage Work and iManage Records Manager, Security Policy Manager is a single vendor solution that allows firms to manage their global security policies, including ethical walls and barriers, at the scale needed to meet today's increasing client demands.

There are several key benefits to the iManage approach:

- **Tight integration means that security policy is assessed as part of the iManage Work and Records Manager access algorithms.** As a result, there is no costly cascade of security, no re-filing of content and no content re-indexing. This means no performance impact to iManage Work end users or delays in new documents appearing in search results, even for the largest of workspaces.

Traditional Vendor Cascade vs Integrated iManage Approach

Traditional vendor approach:

>*Step 1:* Access control is built.

>*Step 2:* Walls are identified and constructed.

>Step 3: Walls are cascaded down.

>Step 4: Cascade triggers a refiling of content.

>Step 5: Cascade triggers a re-indexing of content.

The iManage approach:

>*Step 1:* The product evaluates both policy and access control as part of the access determination.

- **Tight integration means that iManage Work and Records Manager product security cannot violate need-to-know restrictions from security policies. Only users and groups allowed by policy can be selected.** Because iManage clients are aware of security policy definitions, Work users are prevented from granting access to anybody who's not permitted by policy — it's simply not possible to violate a policy.

  iManage Work and iManage Records Manager access algorithms have been extended out to not just look at the access control, but also to look at the security policy defined by Security Policy Manager. Users are only granted access if they meet both criteria. This foolproof security can only be achieved if you are a single vendor delivering a combined content management and security solution.

The "Room" Analogy

One helpful way to think about the interplay of different security layers within the iManage environment is to think of a workspace as a room…

- Access to the room is controlled by **Security Policy Manager** and the policies it creates. If you're defined on the policy, you're allowed access to the room.
- Once you're inside the room, what you can do with regards to all of the folders and documents inside that room —for example, if you have full access vs read only access, and so on — is driven by **Work** security.

- **Tight integration means that the presence of security policies is clearly indicated to iManage Work and Records Manager users.** iManage displays clear visual cues against matters that have been designated as need-to-know, allowing users to drill in and see who has access and who doesn't. Users within iManage Work or iManage Records Manager can see immediately if they're working on a restricted matter, and learn who they can safely talk to within the office, versus which people have a conflict with the client or the matter.
- **Security Policy Manager makes it easy to segment data in multiple ways.** Managing security policies at scale can't happen if your options for how you segment your data are artificially limited. To better fit individual needs and scenarios, Security Policy Manager allows data segmentation policies to be applied to a matter team, to a team defined at client level, to a practice group, or to a team identified by any combination of metadata values, such as matter type.
- **Security Policy Manager protects content in iManage repositories but also non-iManage systems –** such as network file shares, SharePoint sites, time and billing systems, Box folders, and so on. An agent framework is available to allow partners and customers to extend the reach of Security Policy Manager into additional less common systems or other specialist repository types, like home-grown offerings.

When it comes to security policy management, iManage is the only company that can offer a single vendor approach — and all of the associated benefits of an integrated solution — to customers looking to improve the security of their data across all of their repositories.

Summary

Professional organizations today are facing increasing pressure — driven by client demand and new government regulations — to implement need-to-know security policies. The additional burden of calculating and managing these policies can be overwhelming, both to security administrators and the systems themselves.

iManage Security Policy Manager represents a scalable way forward. iManage has taken a fundamentally different approach to evaluating and calculating these walls, which enables organizations to apply security policies without the limitations and additional overhead of traditional approaches.

In this manner, Security Policy Manager makes the management of client-driven need-to-know and ethical walls-based security much less of a burden to both the people and systems inside professional service firms — offering a better way for any firm to manage the increasing volume and complexity of security policies.

To learn more about iManage Security Policy Manager, download the data sheet or Contact Us to arrange a demonstration.

ABOUT IMANAGE