5 STEP PLAN TO SECURING SHAREPOINT

Permissions, Reporting and Audits

Metalogix
# TABLE OF CONTENTS

1. SharePoint Security and Permissions
2. The Limits of ‘Out of the Box’ SharePoint
3. Five Security Problems Facing Every SharePoint Administrator
4. Product Summary
SHAREPOINT SECURITY AND PERMISSIONS

Maintaining a secure, yet collaborative enterprise SharePoint system is crucial to any business. Yet, while maintaining a healthy environment for users takes dedicated resources and thoughtful planning, it doesn’t need to consume every hour of administration work. Instead, there are a number of priority areas to focus on — technical, functional, and strategic — and responsibilities typically sit with one or more SharePoint Administrators.

Quite rightly every organization places huge importance on how their SharePoint data is stored and secured. No matter the configuration, there is always a degree of risk that needs to be properly managed. Areas such as data loss, theft, compliance, and regulatory issues constantly occupy the minds of all good SharePoint Administrators.

HERE AT METALOGIX, WE SUGGEST THREE CORE PRINCIPLES THAT CAN HELP TO MITIGATE MANY OF THESE RISKS:

> Define a security plan and permissions model well in advance of implementation.

> Permissions should always be applied using the ‘least privilege’ principle. This means that users only have the minimum amount of permissions required to complete their job.

> Monitor systems as they grow and develop. Using a general policy of ‘Monitor and Revoke’ can help. Administrators should regularly review permissions and when required remove those that do not meet organizational policies.

In addition to these core principles there are also a number of very practical and actionable steps that every Administrator can use to better secure their SharePoint system. We will look at five such steps, and demonstrate how easy it is to improve the security of any SharePoint system.
THE LIMITS OF ‘OUT OF THE BOX’ SHAREPOINT

Every version of SharePoint, including the latest 2013 release, features a rules-based security model that controls everything within a SharePoint farm right down to individual files. This flexibility also applies to users, who can be assigned a mix of permission levels, granting them access to disparate SharePoint functions as well as content. This combination, being able to leverage users, content, and permission levels in different ways, allows for a large number of security permutations.

Yet this granular approach creates a number of issues. For example, each new user must have their permissions configured after account creation, it is difficult to automate this without considerable technical effort.

SharePoint lacks a centralized way of defining or managing the application of permissions across an entire SharePoint farm. Instead, there are three main out-of-the-box permission management tools, however, these are less than intuitive and must be used in conjunction or in very specific ways, to achieve the desired result.

Now, here’s the crux, generally only a SharePoint Administrator will have access to each tool, and the knowledge of how to use them properly, which more often than not results in a bottleneck to any business workflow.
EACH OF THE PERMISSION TOOLS IS
ACCESSSED IN A DIFFERENT MANNER:

1. The Settings Page
2. Central Administration
3. Powershell
For the most part, SharePoint security is managed through the ‘Settings’ pages within a specific Web Application. Each SharePoint Site has its own Settings page where users or groups can be managed. Libraries, Lists, Documents and other SharePoint objects also have their own Settings pages. The downside here is access to these pages also grants access to a multitude of other configurations options, some which cannot be reversed once enacted.

THE SETTINGS PAGE
CENTRAL ADMINISTRATION

The Central Administration console, a separate tool accessed via the browser, provides the ability to control a higher level of configuration options than those found in Settings pages. These include enormously powerful settings like making a SharePoint Site accessible anonymously via the web. But Central Administration also includes a number of really useful analytical and user reporting tools, highlighting how users interact with content and when, that cannot be accessed by any other means.
PowerShell, a text-driven command line language, is a very technical tool with which SharePoint can be configured. It provides all of the advantages of a scripting tool, such as bulk administration and repeatable processes, but with an extremely steep learning curve. However, getting to grips with “cmdlets” (one of the building blocks of PowerShell) and the lack of a graphical user interface will put off all but the most technical of users.
FIVE SECURITY PROBLEMS FACING EVERY SHAREPOINT ADMINISTRATOR

Here at Metalogix we spend a lot of time listening to our clients, and we hear time and time again that security and integrity of SharePoint data are huge areas of focus for every SharePoint Administrator. Our answer, ControlPoint from Metalogix, extends the basic SharePoint platform, adding powerful functionality to aide Administrators and empower end users. Below, we will look at five typical SharePoint security problems, and demonstrate very simple and practical ways ControlPoint can help to address them.
CONDUCTING A PERMISSIONS REVIEW

These reports typically need to address issues affecting both Administrators ("Which users can access data that they should not be able to?") and end users ("Why can’t I see document x when the person next to me can?") Without this information, it is very difficult to understand how permissions are currently defined within a SharePoint environment. The difficulty comes from the way that SharePoint’s granular SharePoint security model is applied to content. So when user A wants to see what user B is permitted to access, administrators need to look at the user accounts, SharePoint groups and Active Directory groups. The “out-of-the-box” option is to manually inspect each site, list, document or user – a hugely time consuming and error-prone task.

How do I review and report on the current state of user and content permissions across SharePoint?"
PERMISSIONS: REVIEW AND REPORT

THE SOLUTION

PERMISSIONS ANALYSIS
ControlPoint’s “Permissions Analysis” feature allows Administrators to create reports detailing the permissions of a SharePoint farm from the highest entity to the lowest. This includes Web Applications, Site Collections, Sites, Libraries, Lists and Folders - right down to a specific document or item. Reports can clearly detail what content access a particular user has across farms, and how that access is granted. There is no need to resort to laborious manual checks or clicking through numerous SharePoint screens.

PERMISSIONS CHAIN
ControlPoint allows the “permissions chain” of any SharePoint object to be inspected. This describes how a given user is granted permission to the object in question. Are they getting it directly through permissions applied to the object? Are they getting it through a SharePoint group? Is it being inherited from the parent object? This works even if the user is part of an Active Directory Security Group. This means an Administrator can quickly understand any potential problems, without having check a number of different screens and reports.
TAKING CONTROL OF PERMISSIONS

Just as SharePoint provides limited tools for proper security reporting, it also lacks the ability to apply and manage security and permissions in an effective manner. This leaves no option but to access each individual SharePoint user, group, or object to make changes. With SharePoint farms that can grow to thousands of Sites and users, with possibly hundreds of thousands of documents and items, this quickly becomes an impossible task. Not only is the process a very manual operation, but it is difficult to achieve consistency or a balanced approach.

ControlPoint offers an alternative approach:

“I know where the problems are, but how do I take control and fix permissions across my SharePoint system?”
PERMISSIONS: TAKE CONTROL

THE SOLUTION

A CENTRAL CONSOLE
ControlPoint facilitates permissions management for all types of SharePoint authentication objects, such as user accounts, SharePoint Groups, Active Directory groups and even alternate authentication providers (such as forms-based authentication). Policies can also be defined for these objects - ensuring that permission settings are retained when new entities are created.

The central console also facilitates elegant permissions management across farms regardless of the Library, Site, Site Collection or Web Application. This includes setting of permissions to objects at any level. Using the console is orders of magnitude quicker than navigating to objects individually.

CLEAN UP OF DIRECT PERMISSIONS
ControlPoint also provides a feature to clean up direct permissions (where a user has specific access to a SharePoint object). If the application of direct permissions does not conform to best practice or governance policies, ControlPoint can be used to scan and match individual user permissions with corresponding SharePoint groups. Once direct permissions are matched with groups, ControlPoint automates the implementation of changes, assigning the appropriate users to the correct SharePoint groups and removing redundant permissions.

REMOVING USERS
When users leave an organization their Active Directory account is normally deleted or set to inactive. ‘Out of the Box’ SharePoint provides no functionality for removing the user’s account or their associated permissions. ControlPoint enables easy searching of these users, and allows them to be removed from all Site Collections, along with all permissions throughout the whole farm, their alerts, as well as deletion of their My Site. This means orphaned accounts are properly dealt with, and historic content can be removed or archived as required.
#3 CONDUCTING THOROUGH ONGOING AUDITS

Auditing your SharePoint is a long-term commitment and requires a plan. Begin by running regular reviews of the system, its content, and permissions. Remember, the permissions on a SharePoint system rarely stay the same - users come and go, new sites are created and content changes on a regular basis.

This process can generate a number of challenges, requiring answers to questions such as: “Who is using which content?” and “How often are specific sites and items being accessed?” ControlPoint can provide those answers with more ease.
AUDITS: CONTINUOUS AND THOROUGH

THE SOLUTION

AUDIT AND CHANGE LOG ANALYSIS
ControlPoint empowers Administrators to easily create bespoke reports. These reports can be run as needed, or scheduled to run automatically at set times. If a system uses secure workspaces for specific clients, monthly reports could be scheduled on those workspaces to ensure that they meet governance or compliance constraints. Reports could also be produced to show what changes are being made to permissions throughout a system. This can help Administrators proactively manage any changes.

CONTENT ANALYSIS
ControlPoint enables Administrators to ensure environments are kept clean, by finding unused content, duplicate content, personal content, old content or groups that may be storing too much content in SharePoint. With this analysis, objects can be located, reviewed, and assessed for removal or archived.

SHAREPOINT ALERTS MANAGEMENT
ControlPoint enables Administrators to set, manage and delete Alerts across a SharePoint implementation. No longer do they need to wade through multiple screens, inspecting individual objects.
#4 ENFORCING BEST PRACTICE

Gaining a regular understanding of SharePoint usage, both content and permissions settings is one thing. Ensuring that users adhere to best practice, security policies, and governance advice in the long term is a different challenge. Without the ability to both monitor and control, Administrators run the risk of security and permissions becoming even more fragmented and even more of a problem. Devolving power to users is only desirable if rules can be enforced to govern what they can and can’t do.

“How do I enforce best practice across my SharePoint system in the long term?”
ENFORCEMENT: MONITOR AND REVOKE

THE SOLUTION

MONITOR CHANGES
With ControlPoint, Administrators can proactively monitor SharePoint farms, and be alerted to predefined changes within the environment. E.g. an Alert can be sent when sites are created or deleted, when inheritance between SharePoint objects has been broken, or when new Security Groups are created.

At a more granular level, Administrators are able to track access and actions by users, the content they've accessed, and the history of a specific document within a SharePoint environment.

REVOKE ACCESS
If a problem is found, ControlPoint provides the tools to fix it. Analysis and search results are tightly integrated with actions, which means that it is easy to act upon a problem once uncovered. For example, if an Alert is triggered to say that the permissions of a particular Site have been changed, it is very simple for an Administrator to locate the Site and reverse the changes. If the change is serious enough then the originating user’s permissions can be easily revoked.
#5 EMPOWERING END USERS

One of the best ways of increasing SharePoint adoption, reducing administrative overhead, and helping to drive best practice, is to empower end users. SharePoint Administrators are generally overloaded, due to the wide range of roles and responsibilities they assume, and as a result users find it frustrating when they have to wait for IT support to configure a new Site or set up a new user.

Obviously, you don’t want to give your users the rights to do whatever they want, and, let’s face it, while the standard settings pages contain a mix of powerful options, these aren’t very user friendly and users could potentially make a given situation worse. Administrators need to be made aware when things change. ControlPoint can help you empower your users without losing central control:

“I can’t do everything myself, how do I empower the right users in the appropriate manner?”
CONFIGURATION: EMPOWERING END USERS

THE SOLUTION

AUDITS AND ALERTS
ControlPoint gives Administrators the peace of mind that, as they empower users, their environment remains under their control. The permissions reporting and alert functionality of ControlPoint delivers confidence that although users (and even other Administrators) are able to make the changes they want, they are still working within the governance and best practice controls set down for the overall SharePoint deployment.

PERMISSIONS MANAGEMENT
ControlPoint supports the Administrator and empowers the end user, by providing a Permissions Management Interface that is extremely easy to use. The interface is launched from a specific Site within SharePoint, and has a self-contained “wizard-like” interface that guides less technical users through the complexities of changing permissions. This means users can make the necessary changes quickly and efficiently.

A PERCEPTION OF FREEDOM
The first two points, when combined, are extremely important because they drive adoption by creating a “perception of freedom” for the end user. From their perspective they can quickly and simply achieve the results they need, without having to resort to an IT helpdesk or additional support. The SharePoint Administrator sees a reduction in workload, but has confidence that although users feel free, they can only use the system in compliance with your governance rules.
ControlPoint from Metalogix significantly enhances SharePoint’s effectiveness by providing a number of powerful features and tools that solve everyday security and permission problems. ControlPoint supports Administrators with detailed permissions reports, tools to address direct permissions, and the ability to analyze and clean up content. ControlPoint also empowers end users by allowing them to configure the permissions and security settings of their own content. Administrators are able to monitor any changes, allowing them to quickly react if required.

Securing SharePoint isn’t easy. But ControlPoint finally gives Administrators the tools they need to address, assess, analyze and solve multiple issues and problems, in ways that will ultimately benefit them and the SharePoint systems they are responsible for.