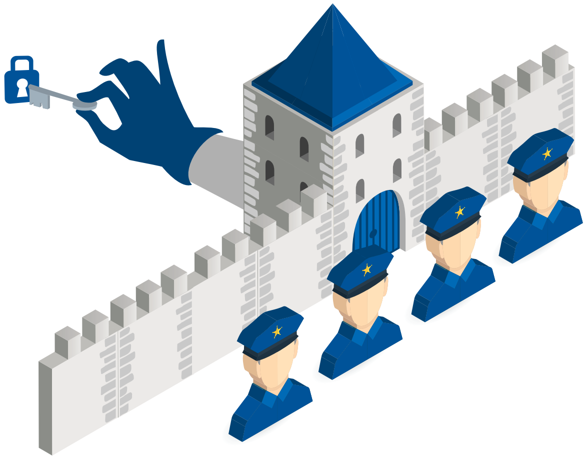
Metalogix

AUTOMATING CONTROL:

PROTECTING SENSITIVE BUSINESS CONTENT IN SHAREPOINT FROM INSIDER THREATS

TABLE OF CONTENTS

THE CHALLENGES OF CONTENT SECURITY



The NSA security breach by Edward Snowden (much of it leaked from a SharePoint server) and a number of other high profile system breaches in the past year have been a wake-up call for businesses to review their security strategies. These attacks proved successful because privileged credentials were compromised and exploited. And the stakes are getting higher – perpetrators are no longer lone hackers, but organized groups, some allegedly sponsored by nation states.

Employees are often the weakest link when it comes to data and network vulnerability. Sending information to the wrong people or inadvertently attaching files to mass emails. Access privileges are particularly vulnerable. By gaining access to user names and passwords (alarmingly, in the case of administrator credentials, many of which are shared or infrequently changed), hackers are able to access multiple systems across the organization. In addition, data is commonly stored in the wrong place, on a less secure system, or incorrectly classified and tagged on a supposedly secure system.

Cloud-based applications are particularly vulnerable because administration and maintenance is often devolved from central IT. The cloud also brings with it a greater reliance on third-party vendors for support and maintenance – such access also needs to be monitored. Physical devices are also at susceptible – unencrypted thumb drives can be lost, paper records may be improperly disposed of, and laptops can be easily stolen.

As users demand increased access to content within enterprise systems – from the office, from home, and on the move – IT must continue to deliver services quickly and in a cost-effective manner, while keeping data secure. This requires an approach that balances productivity, cost, and the value of information. Let's take a look at how SharePoint environments are particularly vulnerable, the limitations of SharePoint out-of-the-box data protection tools, and a better way to solve the SharePoint threat issue.

THE SHAREPOINT APPROACH

The SharePoint approach to protecting critical business data works in three ways:

1. **USER AUTHORIZATION**
2. **PERMISSIONS ON CONTENT**
3. **USER MANAGEMENT**

1 USER AUTHORIZATION

This determines a user's access to a given SharePoint system. The vast majority of SharePoint solutions use Microsoft Active Directory to maintain a list of authorized users. This is a central database that controls user access to core systems like Windows, business enterprise tools like SharePoint, and other HR or Finance tools like SAP or Salesforce.

Active Directory authorization can also be extended to the cloud for use on SharePoint Online or Office 365. These cloud-based platforms also offer a new "Share" feature with gives users outside of Active Directory authorization using a Microsoft approved account of their own.

In exposing content to external users, administrators are forced to keep a watchful eye over content permissions – SharePoint's second layer of data protection.

2 PERMISSIONS ON CONTENT

Once authorized to access SharePoint, a user must be given permission to carry out specific tasks. Using the SharePoint permissions or security model, access can be granted across any scope of a SharePoint farm: web applications, site collections, sites, lists, folders, and items.

Default permission levels are predefined sets of permissions that can be assigned to individual users, groups of users, or security groups, based on the functional requirements of the users and security considerations. SharePoint 2013 permission levels are defined at the site collection level and are inherited from the parent object by default. If needed, inheritance can be broken in order to apply unique permissions to an object.

Default Permission Levels Available for Team Sites in SharePoint 2013:

- **VIEW ONLY**:
  Users are permitted to view application pages only.
- **LIMITED ACCESS**:
  This permission level cannot be applied; instead it is automatically given to a parent object when users are given granular access to SharePoint objects within the parent. This allows users to access a specific list, document library, folder, list item, or document, without granting access to the entire site.
- **READ**:
  Users may view pages and list items and download documents.

(DEFAULT PERMISSIONS LEVELS CONTINUED)

- **CONTRIBUTE:**
  Users can manage personal views and edit items and user information. They can also delete versions in existing lists and add, remove and update personal Web Parts.

- **EDIT:**
  Users can manage lists.

- **DESIGN:**
  Users can view, update, delete, approve, and customize items or pages in the website.

- **FULL CONTROL:**
  Users have full control of the website.

Each of these permission levels are made up of a set of specific permissions that enable users to perform a collection of related tasks, including:

- View items only
- View, add, update and delete items
- Add, edit, and delete lists
- Create sites and pages
- Browse user information
- Manage permissions

A site collection administrator can define custom permission levels, made up of one or more specific permissions like those above. These new levels can be applied to a user and applied to a SharePoint securable object.

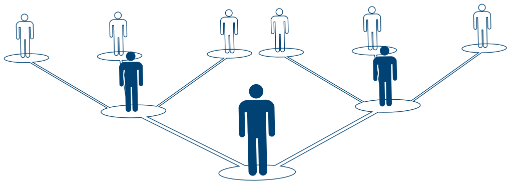
3 USER MANAGEMENT

SharePoint's third layer of data protection allows administrators to manage users directly or via groups. Managing users directly means exactly that – an administrator may grant specific users permission to access specific SharePoint objects (like a site or list). While this is easy to achieve in SharePoint, it can prove difficult to manage and maintain for large numbers of users. Managing users via groups, however, involves applying permissions to the group, not individual users. Users can easily be added or removed to the group, taking on or losing the relevant permissions.

Microsoft Suggests the Following SharePoint Groups:

- A group for site visitors with read permission
- A group for the site members, with contribute permissions
- A group for the site owners who will get full control permissions

If permissions require modification, they are made to the specific group and applied to all users in that group.



HOW SHAREPOINT FAILS TO PROTECT SENSITIVE BUSINESS CONTENT

As data breaches due to insider threats become more commonplace and more devastating in their consequences, security controls that aim to keep system administrators honest or from mistakenly putting the organization at risk has become increasingly important. SharePoint out-of-the-box tools, however, are limited in three key areas:

- **SITE PROVISIONING**
- **PERMISSIONS MODEL**
- **CENTRALIZED SECURITY AND GOVERNANCE CONTROL**
- **LOCATION VERSUS CONTENT SECURITY AND CONTROLS**

1 SITE PROVISIONING LACKS CONTROL FEATURES

As we have seen in the previous section, users, or groups of users, can be assigned relevant permissions to create sites and pages, however SharePoint offers little in the way of control over the site creation process. For example:

- Additional workflow processes cannot be invoked out-of-the-box to approve or deny new site requests. The situation is compounded by the fact that site owners can create an almost unlimited hierarchy of sub-sites at will.

- There is limited support for defining the nature of created sites. While it is possible to facilitate the creation of sites from a predefined list of templates, this process lacks nuanced control. Similarly site metadata, content types, and default permissions are difficult to govern and control within the default user model.

As a result of these limitations, many SharePoint systems quickly suffer from ”site and content sprawl” where an ever increasing number of sites (and lists) are created without proper control – potentially impacting the security of the content within them. Not only are the sites created without adhering to corporate governance rules, but they are often underutilized and left to do nothing but use up system resources.

2 THE STANDARD PERMISSIONS MODEL – INHERENTLY UNSCALABLE

As we have seen, permissions in SharePoint are object-based – meaning that permissions are assigned to a user or group and apply to objects such as a sites, lists, items or documents. SharePoint does not support an easy out-of-the-box method for checking the permissions of multiple objects (for example, a set of ten sites) in one go. Instead, each one must be individually inspected.

In many ways SharePoint's native security model is optimized for team or collaboration sites. It does not adapt well to enterprise deployments where many users have broad access to multiple parts of the farm. The model is based entirely on static permissions, which then must be applied to individual users or groups of users. SharePoint groups help, but often Active Directory groups are also needed to achieve the desired results – a sub-optimal solution since these groups can't be maintained in SharePoint itself. Moreover, the SharePoint interface provides zero visibility into the membership of each Active Directory group.

SOME LIMITATIONS OF THE STANDARD SHAREPOINT SECURITY MODEL:

- Manually mapping users or groups to permissions becomes very time-consuming and expensive as the number of sites grows.

- There is often an explosion in the number of permissions when deploying SharePoint enterprise-wide. This is due to the granular levels at which permissions can be set (site collection, site, list, and item) and the number of users.

- It is difficult to enforce enterprise-level policies on distributed SharePoint sites, particularly those created and managed by individual end users. For example, it can prove challenging to prevent external users from accessing resources marked “company confidential” in a consistent and tracked way.

- Specifying and enforcing permissions at a granular level is difficult and time-consuming to administer and maintain. For example, it is hard to enforce permissions on individual documents rather than the full document library.

- Preventing changes to previously agreed security policies is not possible. Initial implementation of the required level of control is one thing, but ensuring it endures over time is quite another.

3 A LACK OF CENTRAL CONTROL

As we have touched on, users can be assigned a mix of permission levels, granting them access to SharePoint functions as well as content – but the resulting security impacts can prove challenging. For example, when a new user joins or an existing user changes roles within an organization their respective permissions must be manually configured or changed. This additional level of granularity increases the complexity of the task. Similarly, SharePoint does not provide a centralized option for approving new site requests or ensuring that these sites adhere to correct policies and governance rules. Instead, SharePoint features three out-of-the-box permission management tools. These lack intuitiveness and must be used in conjunction or in very specific ways to achieve the desired results.

SharePoint Out-of-the-Box Permission Management Tools

SETTINGS PAGE:
For the most part, SharePoint security is managed through the Settings pages within a specific site collection. Each SharePoint site has its own Settings page where users and groups can be managed. Libraries and lists have their own Settings pages. Unfortunately, access to these pages also grants access to a multitude of other configuration options, some which cannot be reversed once enabled.

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 the Settings pages. These include enormously powerful settings such as making a SharePoint site accessible anonymously via the web. Central Administration also includes a number of useful analytical reports as well as overall administrator reports on health, search, and timer jobs. These tools highlight how and when users interact with SharePoint and also allow administrators to enable settings for collecting more granular information at the content level.

POWERSHELL:
PowerShell, a text-driven command line language, is a highly technical tool which can be used to configure and report on SharePoint. It provides all of the advantages of a scripting tool, such as bulk administration and repeatable processes. The learning curve is extremely steep, however. All but the most technical of users may have difficulty getting to grips with “cmdlets” (one of the building blocks of PowerShell) and the lack of a graphical user interface.

LOCATION VERSUS CONTENT SECURITY AND CONTROLS

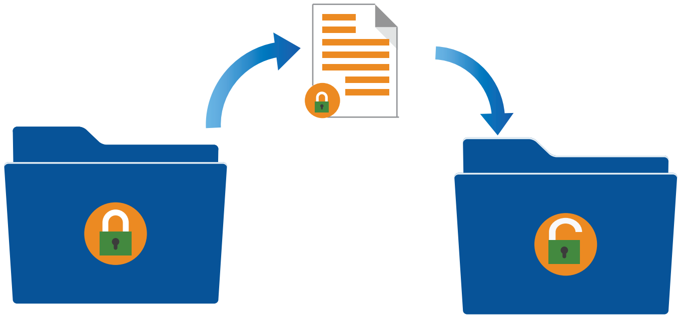
Even if the previous issues with permissions management and site provisioning were resolved they would only mask another problem with how we typically protect sensitive files. The majority of our efforts usually focus on securing access to a location rather than the content itself. But what if a document is moved, either deliberately or inadvertently to a less secure location?

There are technologies that exist that can secure the content itself - regardless of location. Microsoft themselves are investing in this technology area particularly within Office 365. They have recently made improvements to their Rights Management capabilities and introduced Data Loss Prevention (DLP) capabilities within SharePoint Online.

These technologies apply access and usage rights that travel with the document or detect the nature of content within a document, for example if it contains Personally Identifiable Information (PII) such as dates of birth or Social Security Numbers. In future Microsoft will allow policies to be automatically applied to documents. If PII is detected it will be possible to warn a user that information of this type has been added to a SharePoint Online site.

While the Microsoft approach provides some benefit within Office 365 the options for on-premises SharePoint, particularly in the area of Data Loss Prevention, have been very limited up to this point.

However, this is an area that many need to urgently address. The data breaches that have regularly hit the headlines recently and the subsequent damage caused to organizations impacted by those breaches either through loss of revenue, job losses or heavy regulatory fines has dramatically raised the profile of this issue.

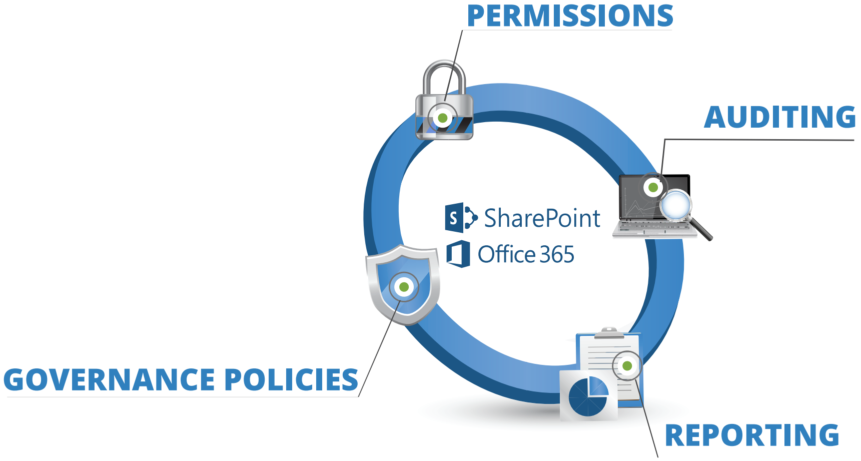


ADDRESSING SECURITY WITH METALOGIX CONTROLPOINT

As we have seen, SharePoint offers an ad hoc means to managing platform-wide security issues, with a number of out-of-the-box tools that are either limited in scope or technical in nature. But users aren't going to stop using SharePoint just because its security system is challenged to keep up with cyber criminals and rogue insiders. However, by adding the right level of security, compliance and administration tools, organizations can achieve a winning combination.

Engineered by experts, Metalogix ControlPoint offers the means to automate control of critical business data, with its rich feature set and intuitive user interface. On-premises, Office 365 or hybrid SharePoint deployment? Single or multiple farms? ControlPoint is ideal for managing and administering them all from one place. ControlPoint is MSO-CAF certified and pre-appoved by Microsoft for Office 365 Dedicated environment.

If you're using SharePoint and are concerned about security threats, consider the benefits of ControlPoint



1 TAKING BACK CONTROL

While the basic process of creating sites in SharePoint is simple. Controlling site creation in an organized way, ensuring sites are created in line with governance policies, and ensuring the necessary permission and content settings is much less straightforward. Indeed properly controlled site provisioning is not supported by native SharePoint.

As a result, SharePoint systems often become sprawling and complex, with layer upon layer of sites and sub-sites. Central administrators struggle to keep on top of newly created content, if they are aware of it at all, and as a result lose control of security and governance.

"You install it one day and the next day you end up with thousands of sites." This is a common criticism of SharePoint that we hear from IT departments all the time. End users, with relatively limited permissions can create endless sub-sites many of which are quickly left abandoned in an unknown state. Each of these sites brings potential security risks. What content do they include? Is this content still needed? Who has access? Who owns the site, and do they even still work in the same team or company?

Using Metalogix ControlPoint, site collections and sub-sites can be automatically provisioned. A provisioning profile can be set up to ensure all sites and site collections are set up with the correct templates, properties, and (optionally) governance policies. Site requests are then sent through an approval process workflow, which includes automatic emails when sites are approved, rejected, or edited.

Site provisioning helps to ensure newly created sites conform to the organization's standards and policies for structure, content, and metadata from the moment it's created. For example, a governance policy created by ControlPoint can contain rules that specify which site and site collection features are activated and others deactivated, if versioning is enabled on every list created in the site or if auditing is enabled and audit reports are sent to business administrators on a daily basis. Used in conjunction with out-of-the-box site definitions and site templates, users can create sites that conform to a specific structure and particular SharePoint features are enabled and never changed by rogue administrators.

Site provisioning tools in ControlPoint help maintain SharePoint's intuitive site creation interface for end users, allowing them to request new sites and site collections directly from a SharePoint site. But it adds the control that enterprises need as systems grow and develop over longer periods of time.

2 CONFIDENTLY MANAGE PERMISSIONS

The most difficult part of managing SharePoint permissions is ensuring permission policy compliance, and preventing security breaches and unauthorized access to sensitive content occurring over time. This issue is even more relevant with the new externally accessible 'Share' feature of the latest versions of SharePoint.

As SharePoint systems grow, the complexity of permissions tends to increase exponentially. SharePoint groups are used sporadically, direct permissions create a confusing picture, and users move around departments or leave altogether. SharePoint offers no holistic view of these issues. ControlPoint does exactly that.

ControlPoint includes a variety of options that facilitate the management of SharePoint users, groups, and permissions. These actions are accessible from various levels in the hierarchy like a single site, a site collection, multiple site collections, or even the entire farm.

- Deleting user permissions for users and groups across the entire farm
- Duplicating user permissions
- Automatically cleaning up user permissions
- Adding users to multiple groups across multiple site collections
- Syncing SharePoint group membership and permissions across the entire farm
- Backing up and restoring site permissions
- Duplicating security from one site to another

Metalogix ControlPoint can also help drive long term permission policy compliance. A single ControlPoint console is used to audit, clean up, and manage permissions and users across all sites, site collections, and farms. It allows all aspects of permissions to be analyzed and managed, no matter if they are directly assigned, inherited, or specifically granted via Active Directory or SharePoint Groups.

ControlPoint's policy enforcement function also automatically controls access privileges, versioning use, file upload limits, site quotas, and site template use. Control can even be delegated to site administrators or power users.

ControlPoint now includes enhancements to its Policies feature, with new rules to prevent permission changes in SharePoint 2013 farms. Not only can the following actions be prevented, but notifications can be sent out if users attempt to do any of the following:

- Add or delete a permission
- Add, delete, or update a Permissions Level
- Add, delete, or update a SharePoint group
- Add or delete SharePoint group members
- Break or restore permissions inheritance

3 TAKING THE PAIN OUT OF AUDITING USERS

When rolling out a SharePoint environment, planning an upgrade, or performing a maintenance check it is important to understand who has access to sensitive content. SharePoint's standard features don't provide information on who has access to what part of SharePoint structure or data.

The auditing features of ControlPoint ensure a quick response to any request of this nature. ControlPoint provides information on who has accessed sensitive content during a particular time period. ControlPoint's powerful auditing features take the pain out of complex and time-consuming compliance, auditing, and reporting tasks.

ControlPoint provides reports on everything from configuration changes to documents accessed or deleted. Each report contains granular details such as the date and time of the event, and the user responsible. It also provides the scope - whether it is a site collection, a site, a list, or a document (including a URL for each).

This information is key for organizations who need determine if users, either existing or those that no longer have access, are in compliance with governance plans and formal policies. Metalogix ControlPoint can be used to check this data on an ad-hoc basis, or as part of a specific audit or security project. ControlPoint can also archive audit data for long term compliance.

4 IDENTIFYING AND SECURING PERSONALLY IDENTIFIABLE INFORMATION (PII)

High profile data leaks of sensitive content such as PII highlight the need to provide adequate protection for this type of information in systems such as SharePoint. Relying solely on location based security, e.g. only allowing PII to exist in certain sites or document libraries, is not sufficient as content can easily be copied or moved to different locations or new content containing PII is uploaded in the wrong place.

ControlPoint and the new Metalogix Sensitive Content Manager provide a new layer of security for PII by identifying where content of this type exists and provides SharePoint Administrators with the tools they need to take action to secure this content.

Entire farms or discrete locations within SharePoint can be scanned for PII and content is classified based on the severity level of the information contained. Upon detection content can be automatically quarantined, deleted or flagged for further action.

ControlPoint provides SharePoint Administrators with the tools they need to take a number of actions when PII is detected. Permissions reports can be run against the Sensitive Content Manager scan to check who has access to the content containing PII and corrective permissions management steps can be taken if a security risk is identified. ControlPoint also enables an administrator to run a report on who has recently accessed sensitive content.

Real-time PII Content Shield

Sensitive Content Manager can also be deployed to automatically provide almost instantaneous detection of PII within newly added SharePoint content.

Upon detection of content containing PII, the upload can be blocked or quarantined until approved by designated content reviewers.

Metalogix is redefining Data Loss Prevention for sensitive content such as PII in SharePoint both on-premises and in the cloud. Powered by advanced machine learning technologies, Metalogix Sensitive Content Manager surpasses existing data protection strategies and provides a far higher degree of accuracy for context aware identification, filtering and classification of content. Additionally the machine learning nature of the solution means that it is ready to go out-of-the-box and lengthy and expensive consultative configuration exercises such as rule definition typically required by other DLP solutions are not required.

SUMMARY

Protecting sensitive business content in SharePoint is no easy task. Not only does the standard authorization and permissions model allow a level of granularity that is difficult to manage in the long term, but native SharePoint offers little in the way of platform-wide user auditing. At the same time it is all too easy for end users, with the right permissions, to create sites and sub-sites with little in the way of provisioning control. The end result is all too often a sprawling hierarchy that doesn't comply with any form of governance.

Metalogix ControlPoint addresses these issues with a number of features:

- The Site Provisioning functionality in ControlPoint is an easy way to automate the management of end user requests for new sites and sites collections.

- ControlPoint supports advanced management of user permissions. Quickly modify permissions across an entire farm, or from site-to-site. Permissions can be duplicated quickly between users, or automatically cleaned up. ControlPoint also supports the backing up and restoring to site permissions, for pain free migration tasks.

- ControlPoint can be used to prevent users from carrying out specific actions, like deleting documents or creating sub-sites. Notifications can inform administrators of any attempts at prohibited actions. ControlPoint supports additional policies over SharePoint 2013 farms, including the ability to prevent changes to permissions like updating specific levels or groups.

- A number of auditing and governance features provide a wealth of information that native SharePoint cannot match. This includes reports on configuration changes and document and content access. Reports include times and dates of relevant events, along with responsible users and the scope of SharePoint objects involved.

- ControlPoint and Sensitive Content Manager provide a highly accurate and flexible out of the box solution for detecting PII inside SharePoint that can also be customized to meet specific client needs. The combined solution provides the ability to identify, track, and secure documents using advanced neural network powered machine learning, which enables a more robust level of contextual content awareness inside increasingly complex enterprise environments.

ABOUT METALOGIX

Metalogix is the premier provider of management software to move, manage and secure content for Office 365, SharePoint, OneDrive for Business, Exchange, Box, Dropbox, Amazon, Google and other enterprise content management (ECM) systems. Over 20,000 client rely on Metalogix and the industry's highest rated LIVE 24x7 support to enhance the use, performance and security of content collaboration in the cloud, on-premises and in hybrid environments.

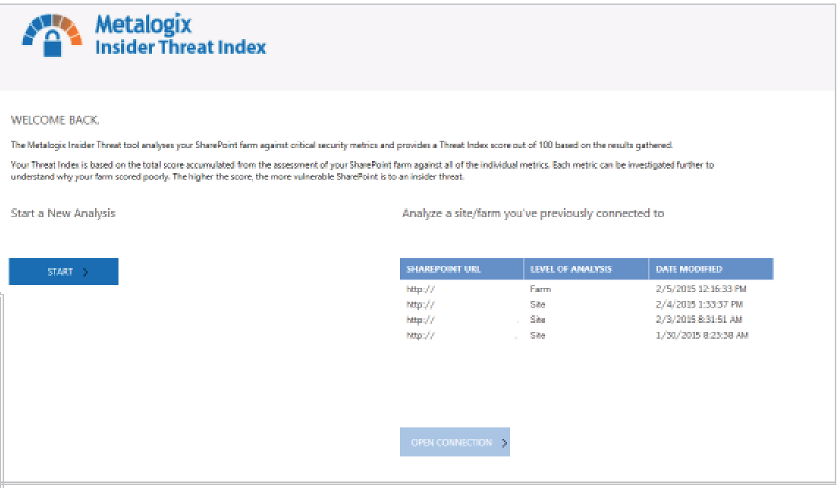
Metalogix is a Microsoft Gold Partner in Cloud, Collaboration and Content, and Application Development, an EMC Select Partner, and a GSA provider. Our Client Service division of certified specialists is a two-time recipient of the prestigious NorthFace ScoreBoard Award for World Class Excellence in Customer Service.

Metalogix
Security Threat Index

SECURE YOUR SHAREPOINT CONTENT

Analyze the Risk of Data Leaks from Insider Threats

Use Metalogix's Insider Threat Index to assess SharePoint security against nine key best practice metrics and get unprecedented visibility into the exposure risk of your sensitive business content.



Metalogix
Insider Threat Index

WELCOME BACK.

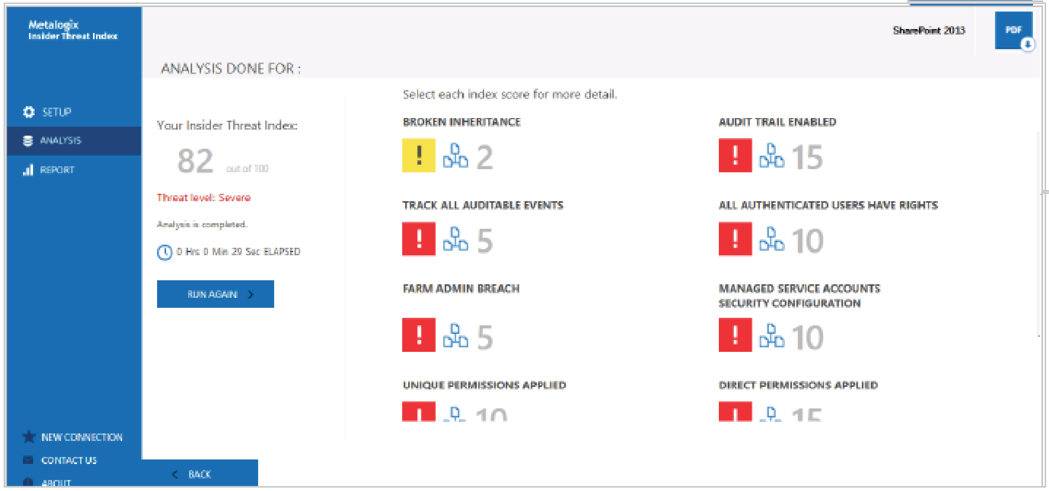
The Metalogix Insider Threat tool analyses your SharePoint farm against critical security metrics and provides a Threat Index score out of 100 based on the results gathered.

Your Threat Index is based on the total score accumulated from the assessment of your SharePoint farm against all of the individual metrics. Each metric can be investigated further to understand why your farm scored poorly. The higher the score, the more vulnerable SharePoint is to an insider threat.

Start a New Analysis

Analyze a site/farm you've previously connected to

SHAREPOINT URL	LEVEL OF ANALYSIS	DATE MODIFIED
http://	Farm	2/5/2015 12:16:33 PM
http://	Site	2/4/2015 1:33:37 PM
http://	Site	2/3/2015 8:31:51 AM
http://	Site	1/30/2015 8:23:38 AM



Metalogix
Insider Threat Index

ANALYSIS DONE FOR :

Your Insider Threat Index:
82 out of 100
Threat level: Severe
Analysis is completed.
0 Hrs 0 Min 29 Sec ELAPSED

Select each index score for more detail.

BROKEN INHERITANCE
! 2

AUDIT TRAIL ENABLED
! 15

TRACK ALL AUDITABLE EVENTS
! 5

ALL AUTHENTICATED USERS HAVE RIGHTS
! 10

FARM ADMIN BREACH
! 5

MANAGED SERVICE ACCOUNTS SECURITY CONFIGURATION
! 10

UNIQUE PERMISSIONS APPLIED
! 10

DIRECT PERMISSIONS APPLIED
! 15

DOWNLOAD INSIDER THREAT INDEX:

www.Metalogix.com//InsiderThreat

MOST TRUSTED SUITE OF PRODUCTS

Diagnostic Manager

SharePoint Monitoring

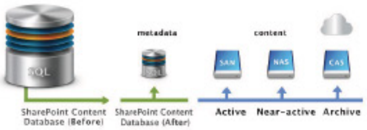
Content Matrix

SharePoint Migration
& Management

Replicator

Multi-farm Sync & Replication

StoragePoint


SQL
metadata
content
SAN
NAS
CAS
SharePoint Content Database (Before)
SharePoint Content Database (After)
Active
Near-active
Archive

Storage Optimization
& Performance

SharePoint Backup

SharePoint Backup & Restore

Archive Manager

ARCHIVE MANAGER
EDISCOVERY & COMPLIANCE
USER TRANSPARENCY
GROWTH MANAGEMENT
TIERED STORAGE
CLOUD+HYBRID

Email, File & SharePoint
Archiving

ControlPoint

PERMISSIONS
AUDITING
SharePoint
Office 365
GOVERNANCE POLICIES
REPORTING

Security, Compliance &
Administration

Watch a Live Daily Demo
www.Metalogix.com

Metalogix