Courion Perspective

Reining In SharePoint®

SharePoint is an extremely popular tool that has been widely deployed by many organizations. SharePoint is designed so that it can be implemented without extensive IT involvement. This has given rise to concerns that poorly configured or managed SharePoint sites may risk exposing sensitive information to unauthorized access. This white paper outlines some best practices that have evolved to help protect SharePoint sites. It also describes the capabilities of Courion's identity-aware solutions that enable IT administrators and security managers to locate, analyze and remediate SharePoint sites with users who hold access rights that are inconsistent with best practices, corporate policy, or regulatory requirements.

www.courion.com

Table of Contents

The SharePoint Dilemma

Over the past few years, Microsoft SharePoint has rapidly grown to become one of the most popular products from Microsoft.

- According to the Wall Street Journal[1], by 2007, "Microsoft has sold 85 million licenses to the enhanced version of SharePoint across 17,000 companies."
- At an industry conference in Sept, 2008 a Microsoft spokesman verified that SharePoint had reached the $1 billion threshold.
- Industry analyst firm Gartner reports[2] that approximately 50% of the mid-size businesses they survey are running some variant of SharePoint, primarily to meet their portal, content and collaboration needs.

Customers report that SharePoint is so easy to install and deploy that it doesn't require significant IT expertise or involvement. Many CIOs find that since they're already standardized on Microsoft products, it's highly likely that SharePoint is already in their environment, which makes turning to SharePoint an easy decision when their end users need a collaboration package.

That's the good news.

The bad news is that the ease, convenience and ubiquity of SharePoint come at a price. For many organizations, especially larger ones, the ability for virtually anyone to deploy a SharePoint site internally without support from IT raises significant governance and security concerns.

Governance Model

Many enterprises aspire to establish a comprehensive security and governance model that defines who can access various categories of data and the permission levels internal and external users have to that data.[3]

For example, most companies would not allow the human resources department to access financial data or an accounting clerk in a hospital to view the private healthcare data of a patient.

For some organizations, it's simply good business practice to control access to potentially sensitive information, both in terms of brand protection as well as avoiding costs resulting from a breach. For example, in a study published by the Ponemon Institute[4] , 20% of respondents to a consumer survey reported they had terminated their relationship with a company as a result of a breach, while another 40% indicated they were considering terminating their relationship. The same study indicated the average cost of a data breach was $4.8 million per incident or $182 per record. These cost estimates don't include the ongoing, and potentially long-lasting, cost of damage to the brand and corporate reputation.

---

[1] "Microsoft Embeds Sleeper in Business Software", Wall Street Journal, April 24, 2007, pg. B1

[2] "Q&A: Midsize Business Plans for SharePoint", Gartner, Inc., March 4, 2008.

[3] SharePoint defines groups, such as Visitors, Members and Owners, which have permissions like Read, Contribute, Approve.

[4] "2006 Annual Study: Cost of a Data Breach: Understanding Financial Impact, Customer Turnover, and Preventative Solutions", Ponemon Institute, October, 2006.

Other business drivers include governmental (Sarbanes-Oxley, FISMA, HIPAA) regulations or industry (PCI DSS) requirements, which have stringent mandates governing data protection and compliance reporting.

Because SharePoint doesn't come with a pre-defined governance model, IT administrators and security and compliance personnel are increasingly concerned about the proliferation of SharePoint sites in their environment. They are also unclear about ceates and manages the sites, as well as who can post or retrieve data stored on them.

SharePoint Identity Management

Without a well-defined process and careful site owner training, it is all too easy to create a morass of access levels at a SharePoint site, making it more and more difficult over time to determine who has access to what.

As a result, it's important to have a comprehensive identity and access management policy that can address the fact that entities explicitly created within SharePoint may not be consistent with enterprise-wide security policies.

Authentication and Authorization

Authentication is the process of validating the user's (or application's) identity. This is typically done by the user submitting credentials (i.e., username and password), which are validated before enabling access to the site.

By default, SharePoint uses Windows user accounts and Active Directory (AD) groups to manage access. However, a site owner can also explicitly add SharePoint users and groups directly to a site and assign permission levels to these users and groups. One best practice that Courion recommends is to use AD groups to manage SharePoint access and not to allow the creation of explicit SharePoint accounts.

Once the user has been authenticated, he or she is granted a specific set of access rights or entitlements (i.e., SharePoint permission levels) based on either their individual account or by virtue of membership in one or more groups.

Permission Levels & Security Best Practices

SharePoint enables a range of permission levels that determine how users can interact with the various resources on the site. They include:

- **Full Control**: typically associated with an administrator or site owner.
- **Design:** in addition to the ability to read, add, remove, or update content, the user can also modify the site's workflow and look-and-feel.
- **Contribute:** enables the user to read, modify, add or remove content from the site.

- **Read:** the user can only view content and has no ability to make changes to the site.

SharePoint also enables more granular access rights to objects, such as files or pages, which are beyond the scope of this paper.

In order to protect content on a SharePoint site from inappropriate access, Courion recommends organizations adopt the following principles:

- **Configure access based on data sensitivity** Only users who have a valid business reason should be allowed access to a site containing sensitive data. The more sensitive the data on the site is, the greater scrutiny should be employed in determining who has access to the site.

  For example, a company softball site typically doesn't contain any sensitive or proprietary information, therefore anyone within the company can be allowed access without concern. On the other hand, a site that contains sensitive information (such as social security or credit card numbers, protected health information, corporate financial data, proprietary trade secrets or business processes, etc.) should be restricted to only individuals who require that data to perform their work.

- **Grant lowest permission levels needed.** Users who need access to content should be granted minimal and sufficient permission levels consistent with their work requirements. Few users need Full Control or Design permissions. Sites with sensitive data should only be accessible by known, authenticated and authorized individuals, and those users should be provided with the minimum level of permissions necessary to perform their function.

- **Restrict anonymous or wide-ranging group access.** Anonymous access is rarely required, except in situations where anonymity may be necessary given the site's purpose (i.e., an online complaint site). Similarly, it's generally not a good policy to grant access to SharePoint sites to large groups, such as Everyone or Guest.

- **Use default permission level definitions.** SharePoint comes with pre-defined permissions. However, system administrators have the ability to modify the default permissions. For example, the administrator can redefine the Design level to have the same permissions as Full Control or Read Only. This can lead to significant complications for a security policy based on an understanding of the default permission definitions.

- **Establish an Access Request Policy.** Using the above principles as guidelines, companies should define and enforce an access request policy that implements a workflow to determine who has access to which sites and what permissions are appropriate for the individual.

  Except in circumstances where self-service is reasonable (i.e., registering for the company softball site), users who desire access to a site should be required to submit a request to the appropriate authority (i.e., site owner, the person's manager, the department head, CISO's office, etc.) which, upon approval, provisions the user to the SharePoint site using an automated, auditable process. The provisioning process, which should be monitored on an ongoing basis, can use

highly granular AD groups to define which individuals have access to particular sites, especially sites containing sensitive data.

Compliance Manager for SharePoint

Courion—leaders in enterprise access assurance solutions—markets **Compliance Manager for SharePoint**, which provide administrators and managers with the tools they need to effectively analyze and manage access to SharePoint sites.

SharePoint Discovery

After Compliance Manager for SharePoint is installed, it scans a Microsoft Office SharePoint Server (MOSS) or Windows SharePoint Services (WSS) system to identify all the SharePoint sites configured on it, the users of the sites and their permission levels. This scan can be repeated on a regular basis to to monitor new SharePoint sites, new users on the sites and new or changed permissions. During the scan, the software also scans Microsoft Active Directory (AD) to identify users who have access rights by virtue of their AD profile or membership in one or more AD groups.

SharePoint Site Policy Review

Once the server scan has completed, the system administrator uses the Compliance Manager for SharePoint portal to view a variety of graphs highlighting potential policy violations from the discovered SharePoint sites.

The Compliance Manager for SharePoint portal helps the SharePoint administrator understand how many sites are on the SharePoint server, the history of site proliferation on that server, and which sites represent security risks. Along with summary statistics, such as total number of sites, number of sites in and out of compliance with policy, the portal also provides the following graphs:

Site Creation History

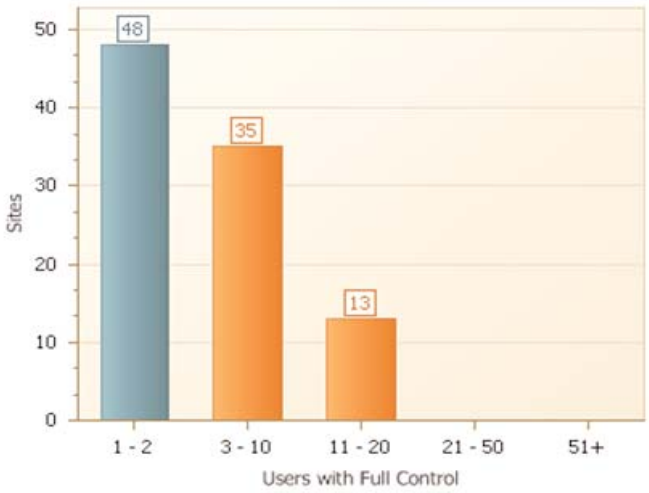
This graph shows the historical growth of SharePoint sites discovered by the scan. By default, the report covers the period of time since the first SharePoint site was deployed to the present, but the viewer can also examine site growth during a specific period of time.

Site Compliance by Policy

Displays the number of policy and best practices violations and highlights the percentage of sites that are out of compliance.

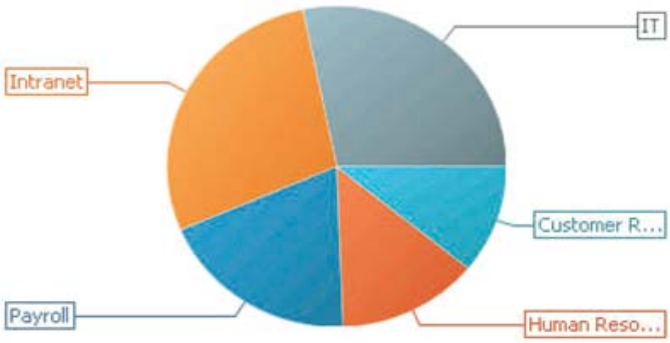
Full Control Permission Level

Shows how many sites have more than one user with the Full Control (administrative) permission level. Sites with many users holding administrative privileges may represent a higher level of risk.



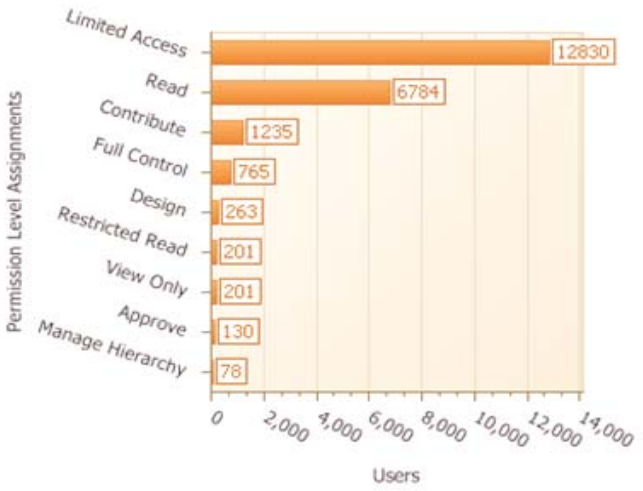
Sites Accessible By Most Users

Shows the sites with the largest number of users. The number of displayed sites can be customized.



Permission Levels

Shows the sum of all accounts for all sites, grouped by permission levels. For example, in this view there are 765 accounts with the Full Control permission across all sites.

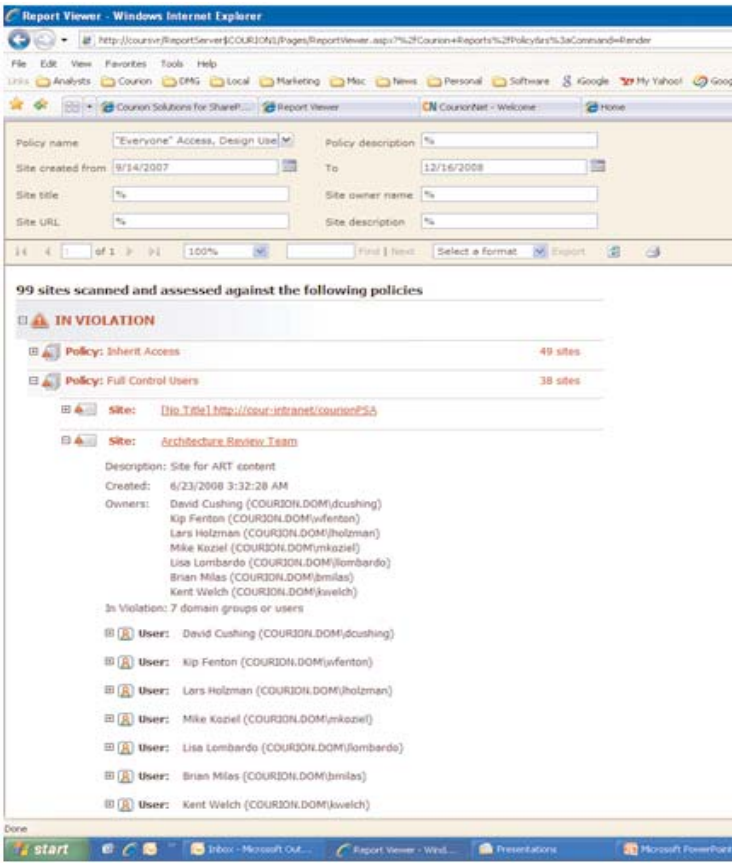


Sites that violate either pre-configured or customized best practices are highlighted, making it easy for system administrators to focus their attention on the sites that represent the greatest risk to the organization.

Policy Review Reports

These graphs are linked to drill-down reports, which enable the administrator to perform a deeper evaluation of the specific policy violations associated with the site or user profiles.

For example, the system administrator can double-click the Site Compliance by Policy graphic, and view the Policy Review report. This interative report lists specific SharePoint policies, and enables the viewer to drill-down on specific policies to determine the sites, along with the users or groups holding with permission levels that led to the policy violation.



Benefits

By implementing Compliance Manager for SharePoint, IT administrators, security and compliance personnel can:

- Know what SharePoint sites are deployed.
- Highlight sites that may be out of compliance with corporate security policies or industry best practices.
- Understand which users have access to the sites and what permissions levels they hold on the site.
- Monitor the ongoing growth of the SharePoint server to identify new sites, users or groups.
- Provide ongoing assurance to management and auditors that users have appropriate permission levels for access to internal SharePoint sites.

Remediation Options

The data provided by Compliance Manager for SharePoint gives the security personnel the information they require to make decisions on how best toreduce the risks associated with accounts or groups with inappropriate permission levels.

Using the data provided by Compliance Manager for SharePoint, they can determine which steps are appropriate to remediate the risks. Depending on the business needs of the organization, they may include:

- Generate a trouble ticket on the IT help desk system (such as Remedy), invoking their internal change management processes.
- Send a notification by email to the most appropriate authority (the person's manager, the CISO's office, the HR department, etc.) asking that further steps be taken.
- Modify permissions to a more appropriate level (e.g., demote Full Control permission level to Read-only) for either the individual or the group.
- Remove individuals or groups who have been granted explicit access rights to the site or modify their profiles in AD.

More Information

Courion is a leading provider of access management and compliance solutions to more than 400 companies around the globe, ranging from mid-size to multi-national organizations. Courion customers include Boeing, Dell, CapitalOne, Office Depot, Nationwide, various agencies of the US Government, T-Mobile, Verizon and many others.

To learn more about how Courion's access and compliance solutions can help your company increase productivity and reduce risk, visit Courion's website at www.courion.com, send email to info@courion.com, or call 1-866-COURION (international: +1-508-879-8400).

Worldwide Headquarters
Courion Corporation
1881 Worcester Road
Framingham, MA 01701 USA
phone + 1 508 879-8400
fax + 1 508 879-8500
www.courion.com