10 Best Practices for Microsoft® SharePoint® Security

SHAREPOINT IS A VALUABLE COLLABORATION TOOL. BUT YOUR ORGANIZATION COULD BE VULNERABLE IF YOU DON’T TAKE THE RIGHT STEPS.
10 Best Practices for Microsoft® SharePoint® Security

SHAREPOINT IS A VALUABLE COLLABORATION TOOL.
BUT YOUR ORGANIZATION COULD BE VULNERABLE IF YOU DON’T TAKE THE RIGHT STEPS

Microsoft® SharePoint® is one of the most popular collaboration and content management applications in the world. Users love its rich interface, robust functionality, and ease of use. But this last attribute is both the primary reason for SharePoint’s global success and its greatest weakness.

Precisely because SharePoint can be easily used to align internal and external teams on strategic projects, or coordinate company-wide initiatives, organizations need to be especially careful about security. It doesn’t take a computer scientist to deploy SharePoint—even an inexperienced administrator can get the application up and running in mere hours—but it does take some know-how to do so properly. As it happens, however, many organizations eager to get started fail to consider some security basics—such as user-access privileges, data encryption in motion, or other actions that secure sensitive information.

There’s no silver bullet for securing SharePoint because each deployment is unique. However, there are 10 best practices that everyone should follow when using this collaboration tool.

No. 1: Grant and manage access rights carefully

The most common vulnerability in SharePoint security arises due to a failure to assign and manage access rights—or to do so correctly. In large SharePoint deployments that span company silos or campuses, there could be thousands of documents and hundreds of users—users who might have such broad rights that they can access information they shouldn’t. For example, an employee in engineering having access to personnel information in human resources, or an external contractor gaining access to marketing documents that should remain confidential. Using proper user groups and assigning privileges carefully therefore becomes an absolute necessity when deploying and maintaining SharePoint.

To do this well takes a little planning and a lot of strict governance. In general, it’s best to err on the side of giving fewer rights and putting all users on a need-to-know basis when it comes to granting privileges. Plus, someone has to take ongoing responsibility: In addition to creating identities and assigning rights, you must keep identities and associated privileges current, conduct regular rights audits, and—most importantly—de-provision the rights when users no longer need access.

If this sounds like a lot of work, that’s because it is. But it’s such a common issue that a small cottage industry has sprung up to help. Established players such as IBM, Computer Associates, and Oracle all offer access-rights management solutions. Smaller companies with innovative solutions in this sector include Epok, Quest Software, Idera, and Axceler, among others.

The best scenario: Find a solution that aggregates permissions across your entire SharePoint deployment and automates the review process to keep rights aligned with your organization’s needs.

No. 2: Deploy SSL certificates

When you first load (or download) and install SharePoint, its SQL database is unencrypted. This leaves any subsequently populated information exposed in plain sight for anyone to find and exploit—a critical concern if the information is proprietary, sensitive, or regulated. The solution is simple: Deploy an SSL certificate on your SharePoint site to help ensure that access is secure, as well as all the data moving from the SharePoint server to browsers.

An SSL certificate is a small string of code that provides security for online communications. When a Web browser contacts your secured website or application server, an SSL certificate establishes an encrypted connection. It’s like sealing a letter in an envelope before sending it through the mail. SSL certificates also inspire trust because each one contains identification information about the server on which it’s installed. When you request one, a certification authority (such as Thawte) verifies your organization’s information and issues a unique certificate to you incorporating that information. This is known as the authentication process. When an SSL certificate is used to begin encrypting data in motion, it also provides the validated identity of the site or server.
There are three types of SSL certificates you can use to secure your SharePoint deployment: self-signed certificates that you create yourself; Windows® public key infrastructure (PKI) certificates; and certificates from trusted, independent certification authorities (CAs).

It’s important to note that by “self-signing” SSL certificates, companies are saying in effect that they are who they are. However, to standard Web browsers such as Internet Explorer and Firefox, this “guarantee” is worthless because, in effect, anyone can use such a certificate to claim to be anyone else. As a result, all users who access a site “protected” with a self-signed SSL certificate will usually be greeted by a frightening error notification that the signing entity is unknown and therefore the site cannot be trusted. Not surprisingly, this can send the wrong message to potential customers, partners, and other stakeholders. For this reason, few organizations will self-sign their external-facing websites—and they are likewise hesitant about self-signing their internally facing sites. For more information, see a guide to self-signed certificates.

Retaining user trust is clearly important. For this reason and others, Microsoft recommends using an SSL certification from a trusted, independent third-party CA before putting SharePoint into production.

SSL certificates purchased from commercial CAs encrypt communications and provide essential identity authentication. Bottom line: If your site or SharePoint don’t use an SSL certificate, your organization is vulnerable.

No. 3: Be consistent in user authentication

SharePoint requires users to provide some sort of authenticated access identity. If users connect to SharePoint sites using two different authentication providers or methods, Microsoft SharePoint Server creates two separate profiles and accounts. You should therefore ensure that users use the same account and credentials to log on to sites whether they are inside or outside the network. If you use Windows authentication, you have two options that help ensure that users can log on with the same account both internally and externally:

- Use SSL to implement only one URL that can be used both internally and externally so employees use the same zone that is configured for SSL no matter where they’re located. Again, Microsoft recommends using an SSL certification from a trusted, independent third-party CA.

- Use forms-based authentication on your firewall or gateway product to collect Windows credentials that are forwarded to SharePoint. If you are using classic-mode authentication in which forms-based authentication for SharePoint isn’t allowed, this approach will work.

No. 4: Properly configure service accounts

At multiple times during the process of deploying and configuring SharePoint, you are requested to create a service account. A very common error is for an administrator to create a single service account and utilize it throughout the SharePoint installation and configuration process. This works in the sense that the SharePoint server will be successfully configured for operation. However, from a security perspective, this can make your SharePoint deployment extremely vulnerable.

Whenever you create a service account with SharePoint, the account is given access rights to perform any tasks. Although SharePoint is intelligent enough to give the account just sufficient permissions to function properly, the account accumulates additional rights every time you use it. If you use the same service account throughout the deployment and configuration process, you end up with accrued permissions that are quite broad in nature. Someone could theoretically exploit these rights to gain access to (i.e., unwarranted control of) the SharePoint server. Although experts differ on how best to structure service accounts, they generally agree that you should use a minimum of five accounts in a basic SharePoint deployment. You should also create a special account that you use only to install SharePoint and Microsoft SQL Server.

No. 5: Minimize your server’s attack surface

A basic IT security strategy is to make a server’s “attack surface” as small as possible. A server with both SharePoint and SQL deployed will have a fairly large attack surface. The obvious (and easy) solution: Run the two programs on separate machines. If your organization can’t afford to dedicate a server each to SQL and SharePoint, you can use virtualization to create two virtual machines (VMs) on the same physical server, keeping SharePoint and SQL separate, thus reducing the potential attack surface.

No. 6: Scan for viruses

It sounds simplistic, but many organizations don’t take the basic step of scanning files that are being uploaded to the SharePoint content libraries. This gives malware an open door into your organization.
No. 7: Train users thoroughly in security risks

Your users represent one of your key vulnerabilities because many people don’t fully grasp the security implications involved in using SharePoint. It’s not uncommon, for example, for users to download documents from SharePoint into Dropbox or other cloud-based file-sharing solution to work on at home. Having potentially sensitive data moving from a secured to an unsecured environment can put organizations at risk.

Security vendor Cryptzone performed a survey of 100 SharePoint users in November 2011 and found some striking results. Although 92 percent agreed that removing information from SharePoint made it less secure, 30 percent said they were willing to risk it “if it helps me get the job done.” Demonstrating even further that there was a misalignment between security and productivity in users’ minds, a significant proportion of those surveyed—34 percent—confessed that they had never thought about security when using SharePoint in this way.

The survey also uncovered that 45 percent of users routinely copied confidential data from SharePoint to their hard drives or a USB drive or emailed it to someone else. In most instances (55 percent), the intent was to share information with someone who did not have access rights to SharePoint.

These survey results only underscore how important it is for organizations to put clear security policies in place regarding how SharePoint information can and can’t be shared—and then ensure that those policies are followed.

No. 8: Automate compliance reporting

SharePoint doesn’t have a friendly, easy-to-use interface for reporting on activity monitoring. Because of this, organizations must first translate SharePoint’s native representation of log data into readable form before they can turn it into information they can use. However, by using third-party technology that integrates permissions and activity details, organizations can automate compliance reporting. This allows them to generate compliance reports in a timelier manner; drill down, filter, and organize log data; and supplement native data with other useful information, such as type of data, department, and data owner.

No. 9: Respond to suspicious activity in real time

The native activity auditing capability of SharePoint doesn’t give organizations the ability to automatically analyze access activity and promptly respond to suspicious behavior by alerting an administrator or blocking access. By using a policy framework to build rules that span SharePoint’s database, file, and Web components, organizations can identify suspicious activity and bolster native access controls. This allows them to monitor, control, and respond to it in real time.

No. 10: Plan, plan, plan ahead

Ultimately, the key to effective deployment lies in preparation and planning. Although SharePoint may appear easy to use, as it begins to gain momentum within your organization, you may find that managing it can become a surprisingly complex affair, and you may end up in constant catch-up mode. First decide what you want to use SharePoint for. Collaboration? Content management? Business intelligence? Then brainstorm different security scenarios, allocate sufficient resources to meet the anticipated vulnerabilities, and revisit your plan six months later to ensure you are in fact tracking to projections.

The time to secure SharePoint is now

Because SharePoint is so versatile and easy to deploy, usage can spread quickly throughout your organization—for strategic as well as tactical projects. Little or no expertise is required to set up a SharePoint deployment, which is the reason that you have to be particularly vigilant about security. The best way to do this is to follow some or all of these best practices, starting at the top of the list.

There’s no one solution for securing SharePoint because each deployment is unique. But these 10 best practices should be followed by everyone when deploying this collaboration tool.